תורת האינפורמציה 2/ נושאים מתקדמים בתורת האינפורמציה

סיכומי הרצאות

ע"פ הרצאותיו של פרופ' רמי זמיר

2004, 2006, 2008, 2010

תוכן עניינים

2004 7

הרצאה - 1 8

נושאים מתקדמים בתורת האינפורמציה - מבוא 8

תזכורת לקיבול ערוץ גאוסי רציף בזמן 8

זרימת אינפורמציה לעומת זרימת "חומר": 10

דוגמאות לפתרונות לרשתות גאוסיות 10

הרצאה - 2 13

בעיית הממסר הגאוסי (Degraded Relay Channel) 13

סכימת השידור והקליטה 14

ממסור ברשת נתונים :בעיית ה MultiCast 16

בעיית Slepian-Wolf (קידוד נפרד של מקורות קורלטיביים) 17

הרצאה - 3 21

The Asymptotic Equipartition Property (AEP) 21

חוק המספרים הגדולים LLN 21

קבוצות (הסדרות) אופייניות 22

AEP (Asymptotic Equipartiotion Property) 24

קבוצות (הסדרות) אופייניות במשותף 25

JAEP (Jointly Asymptotic Equipartiotion Property) 25

Conditional AEP 26

"מפענח אופייניות משותפת" – השלכה של כל הקשרים שראינו 28

הרצאה - 4 29

Multiple Access Channel (MAC) 29

משפט הקיבול של ערוץ ה-MAC 29

השגת נקודות שפה – (Rate splitting approach) ב – MAC גאוסי עם קידוד (1996 Urbanke-Rimoldi): 33

הוכחת המשפט הישר: 33

הוכחת המשפט ההפוך: 34

הרצאות 5-6 36

קידוד מקורות קורלטיביים או קידוד מקור מבוזר 36

הגדרת הבעיה: 36

משפט הקידוד (Slepian-Wolf, 1973): 36

הרחבות לבעית Slepian Wolf: 41

הרצאה – 7 43

בעיית Slepian-Wolf עם עיוות 43

בעיית Slepian-Wolf עם עיוות במקרה הכללי 43

משפט קצב-עיוות 44

בעיית קידוד מקור ללא עיוות עם מסייע (WAK - Wyner, Ahlswede, Körner, 1975) 46

פונקצית קצב-עיוות עם מידע-צד במפענח (Wyner-Ziv, 1976) 49

הרצאה 8-9 52

The Broadcast Channel 52

The Broadcast Channel an Overview 52

Operative Capacity Region 54

The Degraded BCC 56

Converse for the Gaussian Degraded BCC 64

Entropy Power Inequality (EPI) 68

Mrs Gerber's Lemma (Wyner-Ziv 1973) 71

הרצאה – 10 73

Joint Source / Channel coding over the Gaussian BCC Channel 73

The degraded Broadcast Channel – analog transmission vs. digital transmission .. 73

הרצאה – 11 ... 79
אקספוננטי שגיאה לפי שיטת הטיפוסים (Method of types) ... 79
מוטיבציה ... 79
שיטת הטיפוסים – The Method of Types ... 81
שיטת ניתוח חליפית (Csiszár & Körner) ... 83
פענוח Maximum Mutual Information (MMI) ... 85
הרצאות 12-13 ... 87
משפט Gelfand & Pinsker או Writing on Dirty Paper Theorem ... 87
ערוצים תלויי מצב ... 87
אינפורמציית צד וקיבולת של ערוצים בעלי אינפורמציית צד ... 87
הוכחת השגת הקצב של Gelfand & Pinsker ... 94
מימוש אלגברי של קידוד לערוצים עם אינפורמציית צד הידועה למשדר בלבד ... 96
2006 ... 100
הרצאה - 1 ... 101
משוונים, חיזוי וכלל השרשרת לאינפורמציה הדדית בעולם הגאוסי ... 101
ערוץ רעש גאוסי עם הפרעה בין סימנית (ISI) ... 101
מציאת קיבול הערוץ – לפי כלל מזיגת מים ... 102
שימוש במשוון עם משוב החלטה לשידור וגילוי בערוץ ISI גאוסי ... 103
משפט (Cioffi, Dudevoir, Eyuboglu, Forney) : ... 105
דחיסה עם עיוות ריבועי של מקור גאוסי צבעוני ... 108
מציאת פונקצית קצב עיוות – לפי כלל מזיגת מים ... 108
מקרים פרטיים ותכונות : ... 109
שימוש בחיזוי לדחיסת מקור AR גאוסי צבעוני ... 110
הרצאה – 2 ... 113
קידוד ערוץ גאוסי עם אינפורמציית צד - Writing on Dirty Paper (Costa) ... 113
הרצאה 3-4 ... 120
סריגים ושימושם במערכות תקשורת ... 120
"כתיבה על נייר מלוכלך" ... 120
תורת אינפורמציה למערכות מרובות משתמשים ... 120
קידוד ערוץ ... 120
ייצוג בעיות תקשורת כבעיות "כתיבה על נייר מלוכלך" ... 121
סריגים ... 122
משפט (שקילות רעש גאוסי לבן לפילוג אחיד על פני כדור) ... 122
סריג – הגדרה: ... 123
חלוקה סריגית של המרחב: ... 124
גורמי טיב לקידוד ... 126
משפט (סריגי קוונטיזציה טובים אסימפטוטית): ... 126
משפט (סריגים טובים לערוץ AWGN): ... 127
סריגים מקוננים ... 127
סריגים מקוננים טובים אסימפטוטית ... 128
הרצאה - 5 ... 129
בעיית קידוד מקור עם אינפורמציית-צד למקרה הגאוסי (Gaussian Wyner-Ziv) ... 129
הגדרת הבעיה: ... 129
משפט (Wyner-Ziv (1976, 1978: ... 130
פתרון ע"י שריגים מקוננים: ... 130
הסבר אינטואיטיבי וגרפי לגבי בחירת השריגים: ... 133
דואליות: ... 134
הרצאה - 6 ... 135
בעית גלפנד-פינסקר (Gel'fand-Pinsker) ... 135
קידוד עם אינפורמצית צד (לא סיבתית) במשדר ... 135
הגדרת הבעיה ... 135
רקע היסטורי ... 135
קיבולים נוספים - הגדרות ... 136
משפט GP (1980) ... 136

הערות על משפט GP 136
דוגמאות למקרים פרטיים של בעית GP...137
ערוץ עם הפרעה אדיטיבית ידועה במשדר (Writing on Dirty Paper או בעית Costa [3])
....137
משפחה של בעיות "סימני מים" (digital watermarking) 137
ערוץ עם דעיכות (fading channel)..138
ערוץ עם רעש אימפולסיבי...138
ערוץ קוסטה/שאנון בינארי 138
"זיכרון עם תאים דפוקים" 138
ערוץ Blackwell (ערוץ Broadcast דטרמיניסטי) 138
הוכחת המשפט הישר בעזרת Random Coding and Random Binning................139
שלב Offline 139
שלב הקידוד...139
שלב הפענוח..139
תהיות לגבי המנגנון ומקור לשגיאות: 139
טענת עזר: "אכספוננט סף ההצלחה" ([4]) 140
הוכחה: 140
הסתכלות גיאומטרית...141
דוגמא לבעיית GP: קידוד לזיכרון עם תאים תקולים (defective cells) 141
דוגמא לקוד עבור זיכרון עם תאים תקולים: 142
הדואליות לבעיית Wyner-Ziv...142
ביבליוגרפיה 143
הרצאה - 7 144
ערוצי MAC ו BC וקטוריים - ערוצי MIMO..144
הרצאה - 8 152
Successive Refinement and Multiple Descriptions 152
קידוד מקור עם עיוות בשלבים (SR - Successive Refinement)............................152
קידוד מקור בריבוי תיאורים (Multiple Descriptions) 153
2008...155
הרצאה מס' 1 156
אופייניות וטיפוסיות, חריגות גדולות ובעיית "מעבר סף" 156
מבוא..156
חוק השוויון לאחרית הימים (AEP) Asymptotic Equi-Partition Property 156
טיפוסים - Types..157
אקספוננט סף הצלחה..161
תורת החריגות הגדולות - Large Deviations..162
משפט סאנוב 162
משפט הגבול המותנה - Conditional Limit Theorem 167
נספח: התכנסות סדרות...167
הרצאה מס' 2 169
שימוש בסאנוב לבחינת השערות, אקספוננט השגיאה לפענוח בערוץ רועש, ואי שיוויונים אינפורמציוניים 169
שימוש בסאנוב לבחינת השערות - Hypothesis Testing via Sanov.......................169
הלמה של ניימן ופירסון - Neyman Pearson Lemma 170
אקספוננט השגיאה לפענוח בערוץ רועש - Error Exponent..................................173
מקסימום אנטרופיה - Maximal Entropy 177
אי שוויון הספק האנטרופיה - Entropy Power Inequality (EPI)..........................178
אינפורמציית פישר וחסם קרמר ראו - חזרה 179
הרצאה מס' 3 181
קוונטיזציה, סריגים ותורת האינפורמציה 181
המגבלה של פילוג אחיד...181
"רעש" אחיד לעומת גאוסי בבעיית Rate-distortion 181

קוונטיזציה.......... 183
סריגים - קודים ליניאריים טובים במרחב האוקלידי 188
הרצאה מס' 4 192
קידוד מקור עם עיוות לבעיות רשת 192
מבוא.......... 192
דחיסה מבוזרת של מקורות עם עיוות 192
דחיסה בתנאי אי-ודאות 196
Successive Refinement.......... 196
דחיסת מקור עם ריבוי תיאורים (Multiple Description).......... 198
הרצאה מס' 5 202
ערוץ ההפצה.......... 202
Marton bounds for the broadcast channel.......... 202
2010.......... 208
הרצאה מס' 1.......... 209
מבוא 209
ערוץ מרובה משתנים – Multi user channel.......... 209
RELAY.......... 210
Multi-User sources 211
סוגי מיון הבעיות: 212
מה יש בבעיות רשת שאין ב p2p 212
בעיית ה MAC עבור M=2:.......... 213
בעיית Gaussian B.C.C.......... 214
הרצאה מס' 2.......... 215
טיפוסים, אופייניות, "חריגות גדולות" ואקספוננט שגיאב.......... 215
חוק המספרים הגדולים (L.L.N.).......... 215
אופייניות.......... 215
A.E.P. – 'חוק השוויון באחרית הימים' 216
טיפוסים 217
חריגות גדולות (large deviations).......... 220
סאנוב ביחס למעבר סף (threshold crossing) וקישור לחסם צ'רנוף 221
קישור סאנוב לחסמים קלאסיים 223
הרצאה מס' 3.......... 225
"חריגות גדולות" ומשפט סאנוב - המשך.......... 225
Large Deviation Theory ומשפט סאנוב – המשך מההרצאה הקודמת.......... 225
אקספוננט שגיאה במונחי דיברגנס 227
הרצאה מס' 4 234
ערוץ מרובה משדרים (Multiple Access Channel - MAC).......... 234
מודל.......... 234
הרצאה מס' 5.......... 244
קידוד מבוזר של מקורות קורלטיביים – בעיית Slepain-Wolf 244
תאור הבעיה.......... 244
מקרה פרטי – קידוד מקור עם אינפורמצית צד (לא מקודדת).......... 244
תרחיש הייחוס: קידוד משותף של זוג מקורות 244
משפט Slepian-Wolf 245
הרצאה מס' 6.......... 252
סריגים.......... 252
Minkowski – Hanwha Theorem (סוף המאה ה-19) 260
רוג'רס (60's).......... 260
הרצאה מס' 7 261
שימוש בסריגים לקידוד – קודי Voronoi.......... 261
סריגים מקוננים.......... 261
Dithered Voronoi Codebook.......... 262

השגת קיבול ערוץ AWGN ע"י קוד וורונוי 262
השגת הקיבול בSNR כללי 265
התאמת הסכמה לSNR כללי 266
ערוץ עם אינפורמצית צד – המקרה הגאוסי 267
הרצאה מס' 8 270
קידוד מקור עם אינפורמציית צד 270
בעיית Wyner-Ziv – קידוד מקור עם עיוות עם אינפורמציית צד במפענח 273
הרצאה מס' 9 278
ערוצים תלויי מצב עם אינפורמציית צד 278
אינפורמציית צד בשני הצדדים לעומת במקלט בלבד 282
האם זיכרון במצב משפיע על קיבול $C_{SI@Rx}$ או $C_{SI@Both}$? 282
קיבול $C_{SI@Rx}$ עבור מצבים עם זיכרון (ערוץ חסר זיכרון באופן מותנה) 282
משפט קידוד לערוץ עם מצב ידוע לא סיבתית במשדר 285
הרצאה מס' 10 290
ערוץ הפצה (Broadcast Channel) 290
ערוץ הפצה מידרדר (DEGRADED BROAD-CAST CHANNEL) 293
הרצאה מס' 11 298
ערוצים מרובי כניסות ומוצאים (MIMO) 298
ערוצים וקטוריים גאוסיים P2P 298
MAC משדרים מבוזרים 298
B.C.C. משדר משותף מקלטים מבוזרים 299
MIMO MAC 305
MIMO BC Channel 305
הרצאה מס'12 306
קידוד מקור מבוזר עם עיוות 306
בעיית ה-CEO 307
בעיית העוזר 308
Wyner, Ahlswede – Korner (WAK) 308
בעיית העוזר הכפול 309
Korner-Marton (1979) 309
הרצאה מס' 13 311
ערוץ הפרעה 311

2004

מרצה: פרופ׳ רם זמיר
מתרגל: טל פילוסוף

הרצאה - 1

נושאים מתקדמים בתורת האינפורמציה - מבוא

סוכם ע״י אורי לנדאו

תזכורת לקיבול ערוץ גאוסי רציף בזמן

מודל הערוץ (ערוץ ממשי): $y(t)=x(t)*h(t)+z(t); S_z(f); H(f); |f|<\infty$.

מגבלת הספק $\lim_{T\to\infty} E\left\{\frac{1}{2\cdot T}\int_{-T}^{T} x(t)^2\cdot dt\right\}\le P$. z(t) רעש גאוסי סטציונרי עם תוחלת אפס.

$H(f)$ חסומת סרט W[Hz] ($H(f)=0$ $|f|>W$) כלומר LPF.

במקלט הדרגה הראשונה היא מסנן LPF אידיאלי ברוחב סרט W (ברור למה).
אח״כ מתבצעת דגימה בקצב 2W (לפי משפט הדגימה, הפעולה הנ״ל הפיכה ולכן משמרת אינפורמציה!).
קיבלנו ערוץ בדיד (בזמן) שקול $y_n=x_n*h_n+z_n$,

$S_z\left(e^{j\cdot 2\cdot\pi\cdot f}\right)=2\cdot W\cdot S_z(2\cdot W\cdot f)$, $f\in\left(-\frac{1}{2},\frac{1}{2}\right)$, $h_n=\frac{1}{2\cdot W}\cdot h\left(\frac{n}{2\cdot W}\right)$,

$H\left(e^{j\cdot 2\cdot\pi\cdot f}\right)=H(2\cdot W\cdot f)$, $f\in\left(-\frac{1}{2},\frac{1}{2}\right)$.

מגבלת הספק זהה $\lim_{N\to\infty} E\left\{\frac{1}{2\cdot N+1}\sum_{n=-N}^{N} x_n^2\right\}\le P$.

קיבול הערוץ הרציף וקיבול הערוץ הבדיד השקול מקיימים את הקשר:

$$C_{continuous}\left(W,P,H(f),S_z(f)\right)\left[\frac{bits}{\sec}\right]=C_{discrete}\left(P,H\left(e^{j\cdot 2\cdot\pi\cdot f}\right),S_z\left(e^{j\cdot 2\cdot\pi\cdot f}\right)\right)\left[\frac{bits}{channeluse}\right]\cdot 2\cdot W[Hz]$$

קיבול הערוץ הבדיד נתון כידוע ע״י הנוסחא הפרמטרית של כלל ״מזיגת המים״:

$$C_{discrete}=\frac{1}{2}\cdot\int_{-\frac{1}{2}}^{\frac{1}{2}}\log_2\left(1+\frac{\left(water_level-\frac{S_z\left(e^{j\cdot 2\cdot\pi\cdot f}\right)}{\left|H\left(e^{j\cdot 2\cdot\pi\cdot f}\right)\right|^2}\right)^+}{\frac{S_z\left(e^{j\cdot 2\cdot\pi\cdot f}\right)}{\left|H\left(e^{j\cdot 2\cdot\pi\cdot f}\right)\right|^2}}\right)\cdot df\left[\frac{bits}{channeluse}\right]$$

כאשר ההספק הוא:

$$P=\int_{-\frac{1}{2}}^{\frac{1}{2}}\left(water_level-\frac{S_z\left(e^{j\cdot 2\cdot\pi\cdot f}\right)}{\left|H\left(e^{j\cdot 2\cdot\pi\cdot f}\right)\right|^2}\right)^+\cdot df$$

קיבול הערוץ הרציף הוא לכן:

$$C_{continuous} = \frac{1}{2} \cdot \int_{-W}^{W} \log_2 \left(1 + \frac{\left(water_level' - \frac{S_z(f)}{|H(f)|^2} \right)^+}{\frac{S_z(f)}{|H(f)|^2}} \right) \cdot df \left[\frac{bits}{\sec} \right]$$

$$P = \int_{-W}^{W} \left(water_level' - \frac{S_z(f)}{|H(f)|^2} \right)^+ \cdot df$$

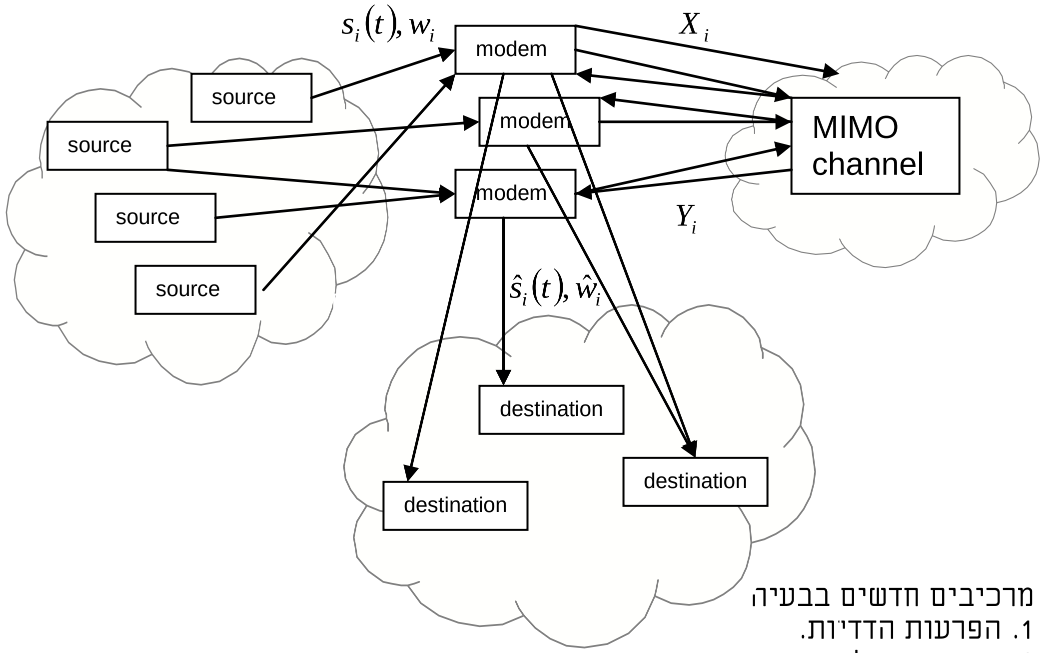
עבור ערוץ רציף "אידיאלי" (כלומר flat בתחום התדרים הרלוונטי) עם AWGN (רעש גאוסי חיבורי לבן) $S_z(f) = \frac{N_0}{2}$ נקבל ערוץ בדיד בזמן שקול $y_n = x_n + z_n$ כאשר $z_n \sim N(0, W \cdot N_0)$ $i.i.d.$.

הקיבול המתקבל הוא

$$C_{discrete} = \frac{1}{2} \cdot \log_2 \left(1 + \frac{P}{N_0 \cdot W} \right) \left[\frac{bits}{channeluse} \right]$$

$$C_{continuous} = W \cdot \log_2 \left(1 + \frac{P}{N_0 \cdot W} \right) \left[\frac{bits}{\sec} \right]$$

<u>רשתות אינפורמציה</u>



מרכיבים חדשים בבעיה

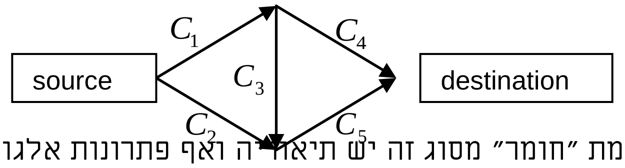
1. הפרעות הדדיות.
2. שיתוף פעולה.
3. משוב.

"הפתעות":

1. לא מתקיים עיקרון ההפרדה בין קידוד מקור לערוץ.
2. לא תמיד קיים פתרון single letter.

זרימת אינפורמציה לעומת זרימת "חומר":

בעיות רשת רבות ניתנות לתיאור ע"י גרף כיווני שצמתיו הם מקורות, ממסרים ויעדים המחוברים ביניהם ע"י קשתות. כל קשת מסמלת ערוץ שקיים בין שני קצותיה. לקשת מוצמד מספר שהינו קיבול הערוץ המתאים. דוגמא:



לבעיית זרימת "חומר" מסוג זה יש תיאוריה ואף פתרונות אלגוריתמיים יעילים. למשל אלגוריתם "Ford-Fulkerson". כל האלגוריתמים הנ"ל מבוססים על " min cut max flow theorem". במילים פשוטות: מקסימום הזרימה הניתנת להשגה ברשת נקבעת לפי "צוואר הבקבוק" הצר ביותר. בדוגמא לעיל, למשל, ישנם ארבע חתכים אפשריים המפרידים בין המקור ליעד. מקסימום קיבול הזרימה מהמקור ליעד הוא אם כן: $\min\{C_1+C_2, C_3+C_2+C_4, C_4+C_5, C_1+C_5-0\}$.

התורה של זרימת אינפורמציה מכילה מרכיבים נוספים כמו קורלציה בין מקורות, הפרעה או תלות בין ערוצים, שיתוף פעולה ועוד. אין כיום תורה כללית עם פתרונות פשוטים לבעיה. בפרט, חסם ה min cut max flow (שהינו מושג בבעיות זרימת "חומר") משמש בתנאים מסוימים חסם **תחתון** לזרימת אינפורמציה!

דוגמאות לפתרונות לרשתות גאוסיות

הגדרות כלליות

אילוץ הספק (לערכים רציפים): לכל מקודד (מתוך M מקודדים), לכל מילת קוד (באורך n):

$$\frac{1}{n}\cdot\left\|\underline{X}_i(w_i)\right\|^2 \le P_i \quad w_i \in \{1,\ldots,2^{n\cdot R_i}\} \quad i=1..M .$$

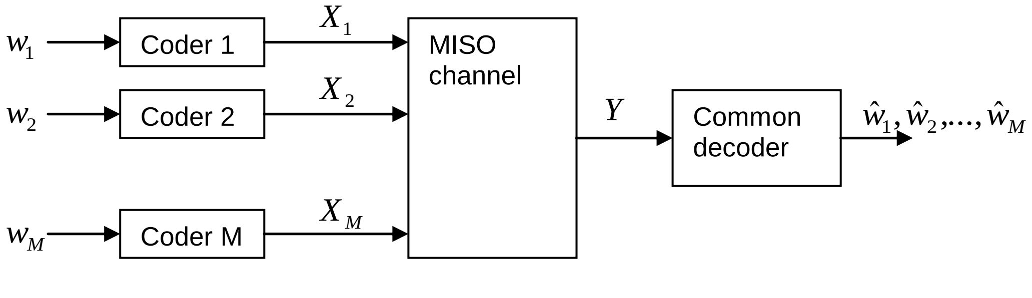
מכיוון שהפתרונות בהוכחות הם הגרלת ספרי קוד, אילוץ ההספק מתקיים בממוצע ולא עבור כל מילה. אבל, תמיד ניתן לנפות מילים שאינן מקיימות את אילוץ ההספק ולהגריל אחרות במקומן!

לכן הדרישה מפילוג הכניסה תהיה $E\{X_i^2\} \le P_i$.

הגדרה: $convex_hull(A) = \{x : x = \lambda\cdot a + (1-\lambda)\cdot b; a,b\in A; 0\le\lambda\le 1\}$.

סימון: $C(x) = \frac{1}{2}\cdot\log_2(1+x)$.

ערוץ מרובה משדרים MAC – multiple access channel



המקרה הגאוסי: $Z \sim N\left(0,\sigma^2\right) \quad ; \quad Y = Z + \sum_{i=1}^{M} X_i$.

<u>פיתרון</u>

<u>M=1</u> :
כללי:

$$C = \{R : R \le I(X;Y)\}$$
for some pdf $f_X(x)$ *satisfying power* (or other) constraint

גאוסי:

$$C = \left\{R : R \le C\left(\frac{P}{\sigma^2}\right)\right\}$$

<u>M=2</u> :
כללי:

$$C = closure\ convex_hull\left\{\bigcup_{f_{X_1}, f_{X_2}} C\left(f_{X_1}, f_{X_2}\right)\right\}$$

$$where\ C\left(f_{X_1}, f_{X_2}\right) = \left\{\begin{array}{l}(R_1, R_2) : R_1 + R_2 \le I(X_1, X_2; Y), \\ R_1 \le I(X_1; Y \mid X_2), \\ R_2 \le I(X_2; Y \mid X_1)\end{array}\right\}$$

$f_{X_1,X_2}(x_1,x_2) = f_{X_1}(x_1) \cdot f_{X_2}(x_2)$ *satisfying power* (or other) constraint

גאוסי:

$$C = \left\{(R_1, R_2) : R_1 + R_2 \le C\left(\frac{P_1 + P_2}{\sigma^2}\right), R_1 \le C\left(\frac{P_1}{\sigma^2}\right), R_2 \le C\left(\frac{P_2}{\sigma^2}\right)\right\}$$

ניתן הסבר אינטואיטיבי לנקודה המושגת $C \in \left(C\left(\frac{P_1}{\sigma^2 + P_2}\right), C\left(\frac{P_2}{\sigma^2}\right)\right) = (R_1, R_2)$:

מפענחים את w_1. זה מתבצע בתנאי $SNR = \frac{P_1}{\sigma^2 + P_2}$ מכיוון ש X_2 הוא בעצם רעש כי אינו ידוע. עתה מחסירים מ Y את X_1 (שכבר ידוע) ולכן נותר לפענח את w_2 בתנאי $SNR = \frac{P_2}{\sigma^2}$.

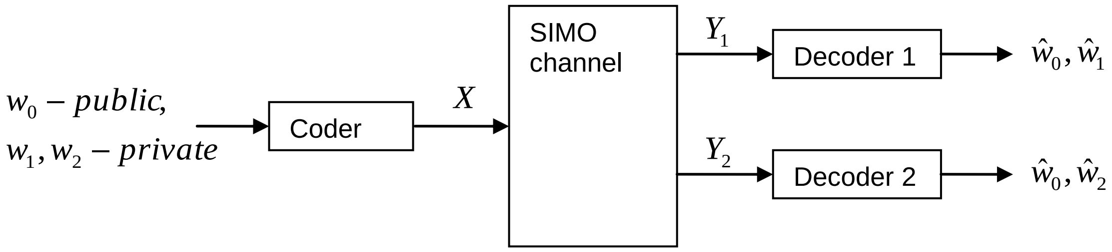
לשם השוואה, קידוד משותף:
כללי:

$$C = \{R : R \le I(X_1, X_2; Y)\}$$
for some pdf $f_{X_1,X_2}(x_1,x_2)$ *satisfying power* (or other) constraint

גאוסי:

$$C = \left\{R : R \le C\left(\frac{\left(\sqrt{P_1} + \sqrt{P_2}\right)^2}{\sigma^2}\right)\right\}$$

ערוץ מרובה משתמשים: **Broadcast channel**



נעסוק במקרה פרטי: degraded broadcast channel, כלומר הערוץ של מקלט 2 "גרוע" יותר משל מקלט 1. ההגדרה של "גרוע": $X \to Y_1 \to Y_2$ שלשה מרקובית.

המקרה הגאוסי: $Y_2 = Y_1 + Z_2; Y_1 = X + Z_1; Z_1 \sim N(0,\sigma_1^2), Z_2 \sim N(0,\sigma_2^2)$.

<u>פיתרון עבור המקרה בו אין הודעה public</u>

כללי:

$$C = closure\,convex_hull\{(R_1,R_2): R_1 \le I(X;Y_1 \mid U), R_2 \le I(U;Y_2)\}$$

$$for\ some\ pdf\ U \to X \to Y_1 \to Y_2\ \ satisfying\ power\ \text{(or other) constraint.}$$

$$if\ discrete\ R.V's,\ one\ more\ restriction: |\chi_U| \le \min\{|\chi_X|, |\chi_{Y_1}|, |\chi_{Y_2}|\}$$

גאוסי (כאן w_2 היא הודעה public דה פקטו):

$$C = closure\,convex_hull\left\{(R_1,R_2): R_1 \le C\left(\frac{(1-\alpha)\cdot P}{\sigma_1^2}\right), R_2 \le C\left(\frac{\alpha \cdot P}{(1-\alpha)\cdot P + \sigma_1^2 + \sigma_2^2}\right), 0 \le \alpha \le 1\right\}$$

ניתן הסבר אינטואיטיבי לנקודה

$$(R_1,R_2) = \left(C\left(\frac{(1-\alpha)\cdot P}{\sigma_1^2}\right), C\left(\frac{\alpha\cdot P}{(1-\alpha)\cdot P + \sigma_1^2 + \sigma_2^2}\right)\right) \in C:$$

ההספק שמוקצה ל w_2 הוא $\alpha \cdot P$ ואילו ל w_1 מוקצה $(1-\alpha)\cdot P$. X הוא סכום שתי מילות הקוד. מכיוון ש w_2 בת"ס ב w_1, ההספק הכולל הוא אכן P. מקלט 2 מפענח את w_2 בתנאי $SNR = \frac{\alpha \cdot P}{(1-\alpha)\cdot P + \sigma_1^2 + \sigma_2^2}$. למקלט 1 יש בהגדרה תנאים טובים יותר לכן יוכל לפענח את w_2 ולחסר את מילת הקוד המתאימה מ Y_1. עתה, בתנאי $SNR = \frac{(1-\alpha)\cdot P}{\sigma_1^2}$ הוא מפענח את w_1.

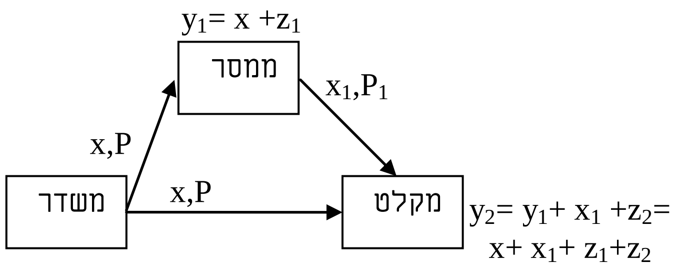
<u>הרצאה - 2</u>

<u>בעיית הממסר הגאוסי (Degraded Relay Channel)</u>

סוכם ע"י: ניב בומש

<u>נתוני הבעיה:</u>
נתון משדר המשדר למקלט. לרשות המקלט עומד ממסר, שעוזר לו להעביר את ההודעה למקלט.

המשדר משדר את האות x בהספק P, ואילו הממסר משדר את האות x_1 בהספק P_1.
האות הנקלט בממסר טבול ברעש גאוסי z_1 בעל שונות N_1 ואילו המקלט קולט את מה ששידר המשדר כאשר בנוסף אליו מצטרף מה ששידר המקלט וגם הנ"ל טבול ברעש נוסף – z_2 בעל שונות N_2.



המשדר משדר את x.
הממסר קולט את האות: $y_1 = x + z_1,\ z_1 \sim N(0, N_1)$ ומשדר את x_1.
המקלט קולט את האות: $y = y_1 + x_1 + z_2 = x + x_1 + z_1 + z_2,\ z_2 \sim N(0, N_2)$.
נשים לב, שהרעש בערוץ "משדר – מקלט" ($z_1 + z_2$) גדול מהרעש במסלול "משדר – ממסר" (z_1).

הערה: בעיית הממסר הקלאסית (שבה אין למשדר ערוץ ישיר אל המקלט), ניתנת לקירוב ע"י המודל הנ"ל כאשר $N_1, P << P_1, N_2$ ובנוסף תנאי ה SNR בכל אחד מהערוצים ("משדר – מקלט" ו-"משדר – ממסר") עדיין מאפשרים שידור.
המודל הפיסיקלי, שבו הממסר הוא ממסר אנלוגי פשוט, המשדר את מה שהוא קולט בהגבר מסוים (ובכך משדר גם את הרעש...) מהווה הסבר למודל דלעיל, שבו המקלט קולט גם את הרעש "שלו" וגם את הרעש "של הממסר". צידוק נוסף אפשרי לחיבור הרעש z_1 במקלט, הוא לגרום לכך שבמקלט תמיד תהיה שונות רעש גבוהה יותר מאשר בממסר (יכולנו לגרום לכך ע"י הצגת מודל בו יש בשני המקלטים את אותה שונות רעש, אולם האות המשודר מהמשדר, נקלט עם הגבר/ניחות בשניהם, כאשר באזור המקלט הניחות גבוה מאשר באזור הממסר (וכך גם נשמרים תנאי ה- SNR)).

השאלה: מהו קצב השידור המקסימלי הניתן להעברה?
התשובה:הקיבול C, קצב ההודעות המקסימלי לביט עבור כל שימוש ערוץ נתון ע"י הנוסחא הבאה:

$$C=\max_{0<\alpha<1}\left(\min\left\{C\left(\frac{P+P_1+2\sqrt{(1-\alpha)P_1P}}{N_1+N_2}\right),C\left(\frac{\alpha P}{N_1}\right)\right\}\right)$$

$$C(X)\equiv\frac{1}{2}\log(1+X).$$

כאשר $C(X)$ מוגדר כקיבול הערוץ הגאוסי עבור SNR=X.

הביטוי $C\left(\frac{P+P_1+2\sqrt{(1-\alpha)P_1P}}{N_1+N_2}\right)$ נובע מהיכולת לסנכרן בין שני המקלטים.

סכימת השידור והקליטה

האינפורמציה מועברת בשני שלבים:

שלב א:

1. שידור בלוק אינפורמציה בקצב R ובהספק αP. כאשר מתקיים:

$$C\left(\frac{\alpha P}{N_1+N_2}\right)<R<C\left(\frac{\alpha P}{N_1}\right).$$

2.קליטה ע"י הממסר: הנ"ל מפענח במדויק מה שודר,קרי את ההודעה w.

קליטה ע"י המקלט: המקלט לא יודע מה שודר במדויק, ויש לו ריבוי משמעות (ambiguity) בקצב של $\Delta=R-C\left(\frac{\alpha P}{N_1+N_2}\right)$. ז"א, הוא יודע שההודעה ששודרה היא אחת מתוך $2^{n\Delta}$ הודעות אפשריות.

שלב ב:

3.שידור אינפורמציה חדשה מהמשדר לממסר בקצב R ובהספק αP.

4.שידור (בו זמני מהמשדר ומהממסר) בקצב Δ ובהספק המתקבל מחיבור קוהרנטי של אות בהספק P_1 (מהממסר) ובהספק $(1-\alpha)P$ (מהמשדר).

נשים לב: גם הממסר וגם המשדר יודעים שלמקלט ישנן $2^{n\Delta}$ הודעות אפשריות, אולם **אין הם יודעים מיהן אותן ההודעות האפשריות**(אין משוב מהמקלט לממסר ולמשדר). למרות זאת, ניתן להתגבר על הבעיתיות, בעזרת טכניקה הקרויה – binning , טכניקה שנלמד בהמשך הקורס.

הערה: מציאת ההספק של שני משתנים אקראיים עם קורלציה 1 ביניהם נתונה ע"י: $\sigma_t^2=(\sigma_1+\sigma_2)^2$ ובמקרה שלנו: $P_t=\left(\sqrt{P_1}+\sqrt{P(1-\alpha)}\right)^2$

מהו הקצב R?

יש כאן נוכחות של רעש שקול בגודל של αP כתוצאה מהשידור החלקי של מילת הקוד הבאה מהמשדר לממסר.

$$R=C\left(\frac{\alpha P}{N_1+N_2}\right)+\Delta=C\left(\frac{\alpha P}{N_1+N_2}\right)+C\left(\frac{\left(\sqrt{P_1}+\sqrt{(1-\alpha)P}\right)^2}{N_1+N_2+\alpha P}\right)=\ldots=C\left(\frac{P+P_1+2\sqrt{(1-\alpha)PP_1}}{N_1+N_2}\right)$$

כאשר המעבר האחרון נובע מהצבה פשוטה בנוסחא של קיבול הערוץ הגאוסי.

הביטוי $C\left(\frac{\alpha P}{N_1}\right)$ נובע מהערוץ בין המשדר והממסר.

5.קליטה בשלב ב':

המקלט מפענח את האינפורמציה ששודרה מהמשדר ומהממסר בנוגע לפתרון בעיית ריבוי המשמעות בהתייחסו לאות המשודר בהספק αP כאל רעש. לאחר פענוח את האינפורמציה החדשה, **<u>המקלט מחסר את האות ששודר בהספק P_t מהאות הנקלט</u>**, וממשיך לפענח את האינפורמציה הנוספת מהאות הנקלט לאחר ההחסרה. אות שבו יש אינפורמציה בנוכחות רעש של (N_1+N_2) בלבד. למעשה, הגיע המקלט כרגע, למצב בו יש לו ambiguity בקשר לאיזו הודעה שודרה, ambiguity שתיפתר עם השידור הבא.

6. חזור לשלב 3.(שלב ב' חוזר על עצמו).

<u>הערות כלליות:</u>

1.ניתן לראות בבעיית הממסר וריאציה של בעית ה- multi-access channel ו/או וריאציה של בעית ה "Broadcast channel".

הדמיון לערוץ ה MAC נובע מהעובדה שקיימות שתי ישויות המשדרות לאותו מקלט.

ההבדל: בבעית הממסר קיים שיתוף פעולה בין שתי הישויות שלא כמו בבעיית ה MAC.

הדמיון לערוץ ה BC נובע מהעובדה שיש שתי ישוייות שקולטות שידור מיישות אחת, אולם – בערוץ הBC אין שיחה בין שתי הישויות הקולטות.

2.<u>מקרה מעניין:</u>

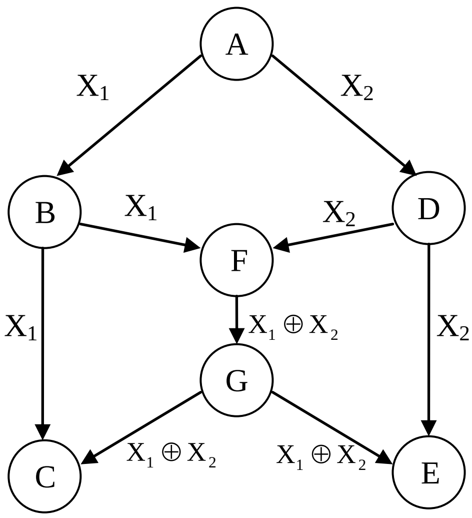
אם $\frac{P}{N_1} \le \frac{P_1}{N_2}$, קרי – ה-SNR בין המקלט לממסר טוב מה SNR בין המשדר לממסר, אזי

נבחר $\alpha = 1$ ונקבל $c = C\left(\frac{P}{N_1}\right)$. (והמשמעות - הקטע בין הממסר למקלט 'שקוף' למשדר).

3. את הבעיה פתרו בשנת 1980 El-Gamal & Cover.

ממסור ברשת נתונים: בעיית ה MultiCast

נתונה רשת הנתונים הבאה הכוללת מקור מידע יחיד (A) ושני יעדים (קודקודים C ו-E).
המקור משדר בקצב של שני ביטים(X_1 X_2) ליחידת זמן.קיבול כל קשת בגרף הוא ביט בודד ליחידת זמן.
שני המקורות צריכים לקלוט את המידע במלואו.

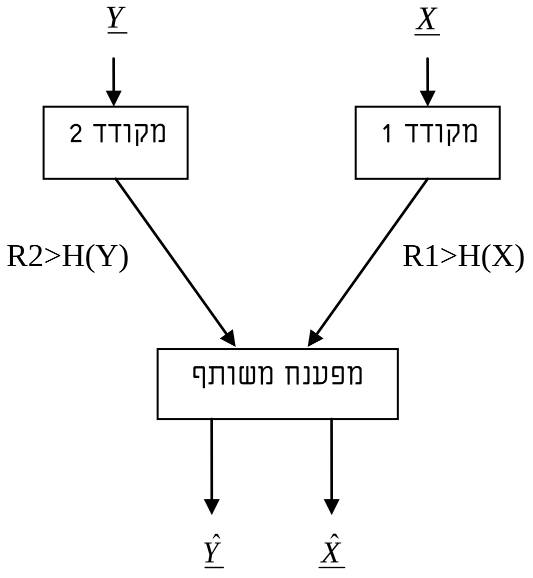


נשים לב שללא "קידוד"/התערבות הקודקוד F במידע עצמו, לא ניתן היה להעביר את מלוא המידע לשני הקודקודים במקביל.
לעומת זאת, כאשר מוסיפים את התערבותו של הקודקוד F, המבצע פעולת XOR על הביטים המגיעים אליו ומעביר את התוצאה הלאה, יכולים הקודקודים C ו- E לפענח את המידע. קודקוד C יקבל את הביט X_1 מקודקוד B ואת הביט $X_1 \oplus X_2$ מקודקוד G. את הביט X_2 הוא יפענח באמצעות פעולת XOR בין שני הביטים הנ"ל:
$X1 \oplus (X1 \oplus X2) = (X1 \oplus X1) \oplus X2 = '0' \oplus X2 = X2$.
קודקוד E מפענח באופן דומה.

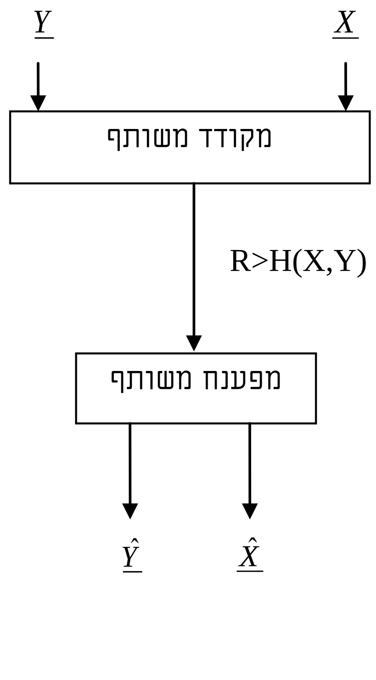
ניתן לראות בקודקודים F ו-G מעין ממסר מקומי, שבלעדיו לא היה המקור מסוגל להעביר את המידע למקלטים. כמו כן אותו ממסר יכול לשרת יותר ממקלט אחד (כולל את עצמו) מבלי שיש 'ניגוד אינטרסים'.

בעיית Slepian-Wolf (קידוד נפרד של מקורות קורלטיביים)

נתונה מערכת של שני מקורות מידע קורלטיביים $X(X_1, X_2,,,, X_n), Y(Y_1, Y_2,,,, Y_n)$. הנ"ל מקודדים כל אחד בנפרד (ללא ידיעת המקור השני) ונדחסים לקצבים של R_1, R_2 בהתאמה.
המפענח הינו מפענח משותף, והוא משחזר את $\hat{X}, \hat{Y}$ בהתאמה.
כעת, לכאורה נראה כי על מנת לדחוס את X ללא פגיעה, על הקצב R_1 להיות גדול מהאנטרופיה של X $\boldsymbol{R_1 \geq H(X)}$. באותו אופן על הקצב R_2 להיות גדול מהאנטרופיה של Y $R_2 \geq H(Y)$.
ז"א ש - $R1 + R2 \geq H(X) + H(Y) \geq H(X,Y)$ כאשר שוויון יתקיים רק עבור מקורות בלתי תלויים סטטיסטית.



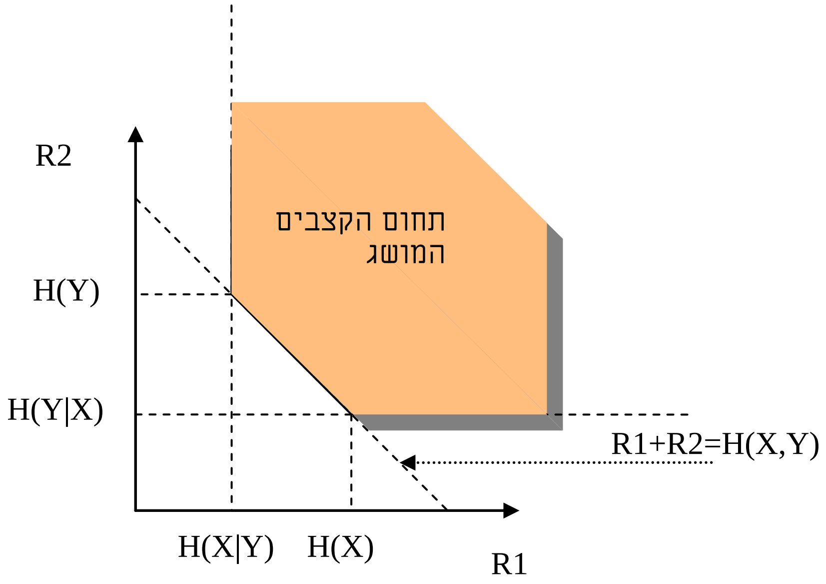
לייחוס, ניתן להסתכל על מערכת בעלת מקודד משותף ומפענח משותף. ברור כעת כי על מנת לדחוס את שני המקורות X ו Y ללא עיוות, הקצב המינימאלי הניתן להשגה הוא $R_1 + R_2 = H(X+Y)$.



נשאלת השאלה, האם ניתן לקודד כל מקור באופן עצמאי (בקצב הקטן מהאנטרופיה של כל מקור בנפרד), ועדיין להשיג את אותו קצב כולל.

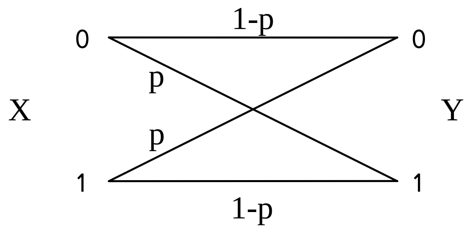
<u>פתרון הבעיה:</u>
תחום הקצבים הניתן להשגה נתון על ידי :

$$R=\{(R_1,R_2): R_1 \ge H(X\mid Y), R_2 \ge H(Y), R_1+R_2 \ge H(X,Y)\}$$



כיצד משיגים את נקודת הפינה של $(R_1,R_2)=(H(X\mid Y),H(Y))$?
Y משדר באופן רגיל ואילו X משדר כאילו הוא יודע את Y.
הנ"ל מבוצע ע"י שימוש בקודים בינאריים.

נניח ש X ו-Y הם משתנים אקראיים מסוג $Bernuolli(\frac{1}{2})$ וקיימת תלות סטטיסטית המתוארת באופן הבא:



בגלל ש- X מתפלג $Bernuolli(\frac{1}{2})$ ניתן לראות שמתקיים הקשר הבא:

$$H(X\mid Y)=H(Y\mid X)=h(p)\equiv -p\log(p)-(1-p)\log(1-p)$$

ניתן אם כן, לתאר את המערכת גם באופן הבא:

$$Y=X\oplus N,\ \ N\sim bernoulli(p),\ \ \text{X \& N are indipenden t}$$

השידור של X יעשה באמצעות מקודד מקור רגיל, שידחס אותו לקצב של $R_1=h(p)$ ביט לדגימה.

כיצד נדחס את X לקצב של h(p)? באמצעות קודי בלוק לינאריים.

<u>קצת על קודי בלוק לינאריים:</u>

קוד בלוק לינארי (n,k) הוא קוד בלוק המקבל k ביטי מקור/אינפורמציה ,מכפיל אותם במטריצה יוצרת $G(n\times k)$ ומוציא כפלט מילת קוד באורך n. היתירות שנוספה למילת המקור מסומנת ב – r.
.(r = n- k)
כחלק מתכונות הקוד, מוגדרת מטריצת בדיקת זוגיות $H(n\times r)$, בעלת התכונה הבאה:
הכפלה של כל מילות הקוד החוקיות במטריצה H נותנת את מילת האפס.
קרי: $C=\left\{\underline{c}\in\{0,1\}^n : \underline{c}_{1\times n}\cdot \underline{\underline{H}}_{n\times r}=\underline{0}_{1\times r}\right\}$.

<u>הגדרות:</u>
1.סינדרום של $\underline{Z}$: תוצאת המכפלה של הוקטור $\underline{Z}$ במטריצת בדיקת הזוגיות $\underline{\underline{H}}$.
$\underline{S}=\underline{Z}\cdot\underline{\underline{H}}$.
(הסינדרום של מילת קוד הוא תמיד $\underline{0}$.)

2."הקוסט של $\underline{S}$": קבוצת הנקודות שהסינדרום שלהם הוא $\underline{S}$.
$\text{coset of }\underline{S}=\left\{\underline{x}\in(0,1)^n : \underline{x}\cdot\underline{\underline{H}}=\underline{S}\right\}$.

הערה: נניח מעתה ש p<0.5 , אולם עבור המקרה ההפוך (p>0.5), ההוכחה ניתנת להשלמה בקלות ע"י הכנסת מהפך בסכימת הפיענוח, ואז הסתברות ההיפוך, p' , p'=1-p קטנה מ 0.5וחזרנו למקרה הראשון.

3. "קוד טוב" לערוץ BSC:
א.הקצב קרוב לקיבול : $\frac{k}{n}\xrightarrow{\text{close to}}1-h(p)$
ב.פענוח הסבירות המירבית הוא אמין, כלומר:
$$MaximumLikelyhood(\underline{y}=\underline{c}+\underline{n})=\underline{c},\ \text{w.h.p.}\,(\text{with high probability})$$

פענוח הסבירות המירבית מבוצע באופן הבא:
המפענח מחפש מהי מילת הקוד הקרובה ביותר (במובן מרחק המינג) למילה שהתקבלה.
$$\hat{\underline{c}}=\text{argmin}\ (\text{over c' the code words})\,of\ \text{d}_\text{H}(\underline{c}\oplus\underline{n},\underline{c}')$$

משקל המינג של מילה W_H מוגדר כמספר הפעמים שמופיעים בה ביטי '1'.
מרחק המינג d_H בין שתי מילים מוגדר כמשקל המינג של המילה שהיא תוצאת הXOR בין שתי המילים.
ולכן נקבל:
$$\hat{\underline{c}}=\text{argmin}\ (\text{over c' the code words})\,of\ \text{d}_\text{H}(\underline{c}\oplus\underline{n},\underline{c}')=$$
$$=\text{argmin}\ (\text{over c' the code words})\,of\ \text{W}_\text{H}(\underline{c}\oplus\underline{n}\oplus\underline{c}')=\underline{c}$$
מכיוון שהקוד לינארי, תוצאת XOR בין כל שתי מילות קוד היא מילת קוד בעצמה, $\underline{c}''=\underline{c}'\oplus\underline{c}$. מכיוון שחוק החילוף פועל בפעולת ה XOR , קרי:
$\underline{c}'\oplus\underline{n}\oplus\underline{c}=\underline{c}'\oplus\underline{c}\oplus\underline{n}=\underline{c}''\oplus\underline{n}$,
שני התנאים הבאים שקולים:
1. $\text{argmin}\ (\text{over c' the code words})\,of\ \text{W}_\text{H}(\underline{c}\oplus\underline{n}\oplus\underline{c}')=\underline{c}$

2. $\operatorname{argmin}\left(\text{over c'' the code words}\right) of\ W_H\left(\underline{n}\oplus\underline{c}''\right)=\underline{0}$

וזה נובע מהצבת $\underline{c}$ בערך של $\underline{c}'$ בביטוי העליון וקבלת הביטוי הבא:

$$\left(\underline{c}\oplus\underline{n}\oplus\underline{c}\right)=\left(\underline{c}\oplus\underline{c}\oplus\underline{n}\right)=\left(\underline{0}\oplus\underline{n}\right)$$

מכיוון ש- $\underline{0}$ היא תמיד מילת קוד חוקית בקוד לינארי, היא צריכה להיות המילה הקרובה ביותר לרעש, שאם לא כן, הנ"ל יצביע על כך שהרעש היה קרוב יותר למילת קוד אחרת (לדוגמא $\underline{c}'''$) מאשר למילת ה - $\underline{0}$, והוא היה גורם למפענח להחליט על המילה $\underline{c}\oplus\underline{c}'''$.

<u>טענה:</u>

אם $\underline{N}\sim bernoulli(p)$, אזי הווקטור עם משקל המינג מינימלי בקוסט של $\underline{S}$ כאשר $\underline{S}=\underline{N}\cdot\underline{\underline{H}}$ הוא בהסתברות גבוהה – $\underline{N}$ עצמו.

<u>הוכחה:</u>

מערכת המפענחת את $\underline{c}$, נותנת גם את $\underline{\hat{n}}$ (כחיסור מהוקטור הנקלט).

$$\underline{\hat{n}}=m.l.(\underline{y})\oplus\underline{y}=_{w.h.p.}\arg\min w_H\left(\cos et(\underline{S})\right)=_{w.h.p}\underline{n}$$

אילולא $\underline{\hat{n}}$ היה הוקטור בעל המשקל המינימלי בקוסט – אלא $\underline{\hat{n}}\oplus\underline{c}'$ לדוגמא, זה היה גורר בהכרח שהרעש היה קרוב יותר למילה שהיא לא מילת ה-0, ואז זה אומר שהמפענח היה שוגה בפענוח.

<u>סכימת הקידוד והפענוח בבעיית Slepian-Wolf המשיגה את קצבי נקודת הפינה:</u>
<u>$(R_1,R_2)=(H(X|Y),H(Y))$</u>

קידוד:

המקודד משתמש בקוד בלוק לינארי טוב כפי שהוגדר דלעיל. הוא לוקח את המילה X, מכפיל אותה במטריצת בדיקת הזוגיות H, ומשדר את הסינדרום המתקבל (תוצאת המכפלה). גודל/אורך הסינדרום הוא r ביטים שהם בקירוב $r=n-k=n(1-k/n)\cong n(1-(1-h(p)))=nh(p)$ ביטים. (מהגדרת קצב הקוד הטוב.)

פענוח:

המפענח, שכבר פענח את הוקטור $\underline{Y}$ ללא שגיאות, מחבר את הבלוק הנקלט עם תוצאת המכפלה של $\underline{Y}$ במטריצת בדיקת הזוגיות H.

מה קיבלנו: $\underline{S}'=S\oplus\left(\underline{Y}\cdot\underline{\underline{H}}\right)=\left(\underline{X}\cdot\underline{\underline{H}}\right)\oplus\left(\underline{Y}\cdot\underline{\underline{H}}\right)=\left(\underline{X}\oplus\underline{Y}\right)\cdot\underline{\underline{H}}=\underline{N}\cdot\underline{\underline{H}}$

לפי הטענה דלעיל, אם נחפש בקוסט של $\underline{S}'$ את המילה בעלת משקל ההמינג המינימלי, נקבל בהסתברות גבוהה את N עצמו. לאחר שהמפענח פענח את N ואת Y, כל שנותר לו לעשות הוא לבצע פעולת XOR בינהם ולקבל את X.

הרצאה - 3

The Asymptotic Equipartition Property (AEP)

סוכם ע"י אייל גורג'י

חוק המספרים הגדולים LLN

נתונה סדרת משתנים אקראיים... $Z_1, Z_2 ...$ מתפלגים i.i.d. מעל א"ב סופי χ .
חוק המספרים הגדולים טוען שהממוצע החשבוני של סדרת המשתנים האקראיים שואף לתוחלת של משתנה אקראי:

$$\frac{1}{n}\sum_{i=1}^{n} Z_i \xrightarrow[n\to\infty]{w.p.\,1} E\{Z\}$$

ההתכנסות לתוחלת היא בהסתברות 1, כלומר התכנסות במובן החזק ביותר.

<u>מסקנה מחוק המספרים הגדולים:</u>
נתונה סדרה של משתנים אקראיים $X_1, X_2,...$ מתפלגים i.i.d. לפי פילוג $p_x(X)$.
נסמן ב-$\underline{x} = X^n = (X_1, X_2,..., X_n)$ וקטור של n מ.א. בעלי פילוג משותף:

$$p(\underline{X}) = p(X^n) = p(X_1, X_2,.., X_n) \underbrace{=}_{i.i.d.} \prod_{i=1}^{n} p(X_i)$$

וכמובן מתקיים:

$$\log p(\underline{X}) = \sum_{i=1}^{n} \log p(X_i)$$

לפי LLN מתקיים:

$$-\frac{1}{n}\log p(\underline{x}) = -\frac{1}{n}\sum_{i=1}^{n}\log p(x_i) \xrightarrow[n\to\infty]{w.p.\,1} -E\{\log p(X)\} = H(X) \equiv H(p)$$

עבור $a \in \chi$, נסמן ב-$N(a/\underline{x})$ את מספר ההופעות של a בווקטור $\underline{x}$,
כמו כן נסמן ב- $1_{\{x_i=a\}} = \begin{cases} 1 & x_i = a \\ 0 & x_i \neq a \end{cases}$ פונקצית אינדיקאטור. שוב, לפי LLN מתקיים:

$$\frac{1}{n}N(a/\underline{x}) = \frac{1}{n}\sum_{i=1}^{n} 1_{\{x_i=a\}} \xrightarrow[n\to\infty]{w.p.\,1} E\{1_{\{x_i=a\}}\} = p_x(a)$$

כלומר, מספר הפעמים ש-a יופיע בווקטור באורך n של המשתנה x הוא $n \cdot p_x(a)$
בהסתברות 1, עבור $n \to \infty$. המשמעות היא שהפילוג האמפירי של x מתכנס (שוב, בהסתברות 1) לפילוג הסטטיסטי של x עבור $n \to \infty$.

קבוצות (הסדרות) אופייניות

נתונה סדרה של משתנים אקראיים $X_1, X_2, \ldots$ מתפלגים i.i.d. לפי פילוג $p_x(X)$ מעל א-ב סופי χ .

נסמן ב-$\underline{x} = x^n = (X_1, X_2, \ldots, X_n)$ וקטור של n מ.א. ונגדיר את הקבוצה האופיינית באופן הבא:

<u>הגדרה חלשה:</u>

$$A_\varepsilon^{(n)}(X) \equiv A_\varepsilon^{(n)} = \left\{ x^n : -\frac{1}{n}\log p(x^n) = H(X) \pm \varepsilon \right\}$$

קבוצת הסדרות האופייניות זוהי פונקציה של הפילוג, מוגדרת עבור ε, n מסוימים.
המשמעות היא שבקבוצה האופיינית נמצאות כל הסדרות האפשריות באורך n , שעבורן הביטוי $-\frac{1}{n}\log p(x^n)$ שווה ל-$H(X)$ עד כדי ε .

<u>הגדרה חזקה:</u>

$$A_\varepsilon^{*(n)}(X) \equiv A_\varepsilon^{*(n)} = \left\{ x^n : \frac{1}{n}N(a/x^n) = \begin{cases} p(a) \pm \varepsilon' & p(a) > 0 \\ 0 & p(a) = 0 \end{cases} \right\} \quad , \forall a \in \chi$$

שוב, גם הגדרה זו (כמובן) היא פונקציה של הפילוג, מוגדרת עבור ε, n מסוימים. המשמעות היא שבקבוצה האופיינית נמצאות כל הסדרות האפשריות באורך n שמקיימות "פיזור אמפירי" לפי "הפיזור ההסתברותי", כלומר שכל איבר מהא-ב של הפילוג מופיע $p(a)$ פעמים עד כדי ε', כאשר מס' ההופעות מנורמל לאורך הסדרה.

איך נקשר בין שתי ההגדרות?
ניתן להשתמש בשתי קשרים בין ε' של ההגדרה החזקה לבין ε של ההגדרה החלשה:

$$1. \varepsilon' = \varepsilon / |\mathrm{X}|$$

$$2. \varepsilon' = \frac{\varepsilon \cdot p(a)}{\log|\mathrm{X}|}$$

כאשר אם נשתמש בקשר השני נקבל יחס סדר (המשתמע מהשמות) בין שתי ההגדרות, כלומר נקבל שכל סדרה אופיינית במובן החזק היא גם אופיינית במובן החלש. נוכיח זאת:

$$p(x^n) = \prod_{i=1}^{n} p(X_i) = \prod_{a\in\chi} p(a)^{N(a/x^n)}$$

תוך שימוש בהגדרה של אופייניות חזקה ניתן לקבל את אי השוויון הבא (נזכור ש-$p(a) \le 1$):

$$\prod_{a\in\chi} p(a)^{n(p(a)+\varepsilon')} \le \prod_{a\in\chi} p(a)^{N(a/x^n)} \le \prod_{a\in\chi} p(a)^{n(p(a)-\varepsilon')}$$

$$\prod_{a\in\chi} p(a)^{n(p(a)+\varepsilon')} \le p(x^n) \le \prod_{a\in\chi} p(a)^{n(p(a)-\varepsilon')}$$

ולכן כל סדרה אופיינית חזקה מקיימת את אי שוויון הבא:

$$-\frac{1}{n}\log p(x^n) \ge -\frac{1}{n}\log \prod_{a\in\chi} p(a)^{n(p(a)-\varepsilon')} = -\frac{1}{n}\cdot n\sum_{a\in\chi}\left(p(a)-\varepsilon'\right)\log p(a)$$

$$= -\sum_{a\in\chi} p(a)\left(1-\frac{\varepsilon}{\log|\chi|}\right)\log p(a) = \left(1-\frac{\varepsilon}{\log|\chi|}\right)\cdot\left(-\sum_{a\in\chi} p(a)\log p(a)\right) =$$

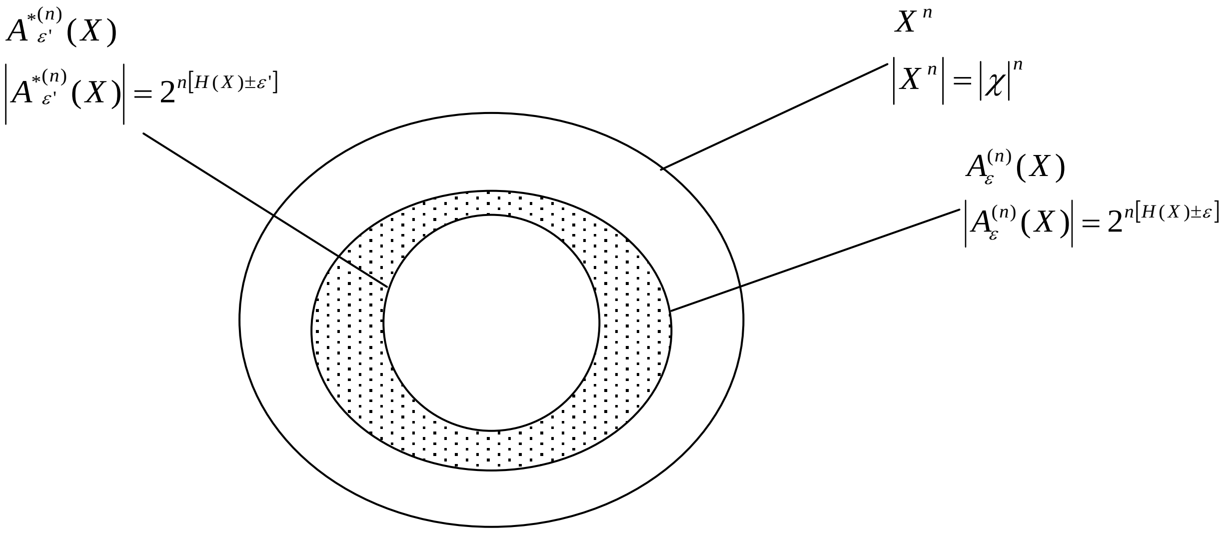
$$= \left(1-\frac{\varepsilon}{\log|\chi|}\right)\cdot H(X) = H(X) - \varepsilon\frac{H(X)}{\log|\chi|} \ge H(X)-\varepsilon$$

כאשר מעבר הראשון הוא היפוך של אי השוויון שראינו קודם (הכפלה במינוס), במעבר השלישי השתמשנו בהגדרה 2. של ε' והמעבר האחרון מכיוון ש- $\frac{H(X)}{\log|\chi|} \le 1$.

באותו אופן בדיוק ניתן להראות את אי השוויון:

$$-\frac{1}{n}\log p(x^n) \le H(X)+\varepsilon$$

והוכחנו שכל סדרה אופיינית חזקה היא גם אופיינית חלשה.
ההיפך הוא כמובן לא נכון, נראה זאת אינטואיטיבית: סדרה אופיינית חלשה צריכה לקיים שהאינפורמציה העצמית (הגודל $-\frac{1}{n}\log p(x^n)$) מתכנסת לאנטרופיה ההסתברותית, ודבר כזה יכול להתקיים עבור שתי סדרות אשר הפילוגים האמפיריים שלהן (למשל q, p) שונים, אם האינפורמציה העצמית של q קרובה ל- $H(p)$, כלומר, מתקיים
$-\frac{1}{n}\log p(x^n) \xrightarrow[n\to\infty]{LLN} E_q\left\{-\frac{1}{n}\log p(x^n)\right\} = H(p)$ עד כדי ε. לעומת זאת סדרה אופיינית חזקה צריכה לקיים שהפילוג האמפירי מתכנס לפילוג ההסתברותי, ודבר כזה כמובן לא יכול להתקיים עבור שתי סדרות המקיימות פילוגים אמפיריים שונים.
זוהי הסיבה שבמקרה הבינארי אופייניות חזקה ואופייניות חלשה זה אותו הדבר, מכיוון שבמקרה זה האנטרופיה ההסתברותית שווה רק עבור שני פילוגים שהם בעצם אותו פילוג (עד כדי ייצוג בא-ב).
לשתי הקבוצות (אופיינית חזקה וחלשה) יש אותו גודל אכספוננציאלי $\left(\sim 2^{nH(X)}\right)$.



נשים לב שגודל האזור המקווקו (אופיינית חלשה ולא חזקה) הולך לאפס כאשר n הולך לאינסוף.

AEP (Asymptotic Equipartiotion Property)

כל הטענות שבתכונת ה-AEP מתייחסות להגדרה החלשה של הקבוצות (סדרות) אופייניות, אבל אותן תכונות מתקיימות גם ביחס להגדרה החזקה.

א. לכל הסדרות $\underline{x}$ בקבוצה האופיינית יש בערך את אותה ההסתברות: $2^{-n[H(X)\pm\varepsilon]}$.

<u>הוכחה</u>: נובע ישירות מההגדרה (החלשה).

ב. עבור n מספיק גדול, ההסתברות ש-$\underline{x}$ אקראי יהיה שייך לקבוצה האופיינית היא 1 עד כדי ε, כלומר $\Pr\left\{A_\varepsilon^{(n)}\right\} > 1-\varepsilon$.

<u>הוכחה</u>: מחוק המספרים הגדולים ראינו כי

$$-\frac{1}{n}\log p(\underline{x}) \underbrace{\xrightarrow[n\to\infty]{w.p.\,1}}_{LLN} H(X)$$

כלומר, $\forall\delta>0,\ \exists n_0,\ such\,that\,\forall n>n_0$:

$$\Pr\left\{\left|-\frac{1}{n}\log p(\underline{x}) - H(X)\right| < \varepsilon\right\} > 1-\delta$$

נקבע $\delta=\varepsilon$ ונקבל את ההוכחה.

ג. גודל הקבוצה הוא אכספוננציאלי באנטרופיה:

$$\left|A_\varepsilon^{(n)}\right| = 2^{n[H(X)\pm\varepsilon]} \quad for\,n\,sufficiently\,large$$

<u>הוכחה</u>: חסם עליון לגודל הקבוצה (נכון לכל n), נתון על ידי הביטוי $\left|A_\varepsilon^{(n)}\right| \le 2^{n[H(X)+\varepsilon]}$:

$$1=\sum_{x\in X^n} p(x) \underbrace{\ge}_{\substack{decrease\\ the\,numbers\\ of\,elements\\ in\,sum}} \sum_{x\in A_\varepsilon^{(n)}} p(x) \underbrace{\ge}_{\substack{from\,the\\ definition\\ of\,AEP}}$$

$$\ge \sum_{x\in A_\varepsilon^{(n)}} 2^{-n[H(X)+\varepsilon]} = 2^{-n[H(X)+\varepsilon]}\cdot\left|A_\varepsilon^{(n)}\right|$$

חסם תחתון לגודל הקבוצה (נכון ל-n מספיק גדול) נתון על ידי הביטוי $\left|A_\varepsilon^{(n)}\right| \ge (1-\varepsilon)\cdot 2^{n[H(x)-\varepsilon]}$:

$$1-\varepsilon \underbrace{<}_{\substack{from\\ prop.\,b.}} \Pr\left\{A_\varepsilon^{(n)}\right\} \underbrace{\le}_{\substack{from\,the\\ definition\\ of\,AEP}}$$

$$\le \sum_{x\in A_\varepsilon^{(n)}} 2^{-n[H(X)-\varepsilon]} = 2^{-n[H(X)-\varepsilon]}\cdot\left|A_\varepsilon^{(n)}\right|$$

נשים לב שהגודל היחסי של הקבוצה האופיינית בתוך קבוצת כל הסדרות קטן עם n (והופך לזניח עבור $n\to\infty$), ואילו ההסתברות לקבל סדרה מתוך הקבוצה האופיינית שואפת ל-1.

קבוצות (הסדרות) אופייניות במשותף

נתונה סדרה של זוגות של משתנים אקראיים $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix},\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},...$ מתפלגים i.i.d. לפי פילוג משותף $p_{x.y}(x,y)$ $\left(p_{x,y}\left(x^n,y^n\right)=\prod_{i=1}^{n} p_{x,y}\left(x_i,y_i\right) \right)$, המגדיר גם את הפילוגים השוליים $p_x(x), p_y(y)$.

נסמן ב- $\left(x^n,y^n\right)=\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix},\begin{pmatrix} x_2 \\ y_2 \end{pmatrix},...,\begin{pmatrix} x_n \\ y_n \end{pmatrix}\right)$ וקטור של n זוגות של מ.א. ונגדיר את הקבוצה האופיינית באופן הבא:

<u>הגדרה חלשה:</u>

$$A_\varepsilon^{(n)}\left(X,Y\right)=\left\{\left(x^n,y^n\right): \begin{array}{l} -\frac{1}{n}\log\ p(x^n)=H\left(X\right)\pm\varepsilon \\ -\frac{1}{n}\log\ p(y^n)=H\left(Y\right)\pm\varepsilon \\ -\frac{1}{n}\log\ p(x^n,y^n)=H\left(X,Y\right)\pm\varepsilon \end{array}\right\}$$

<u>הגדרה חזקה:</u>

נסמן ב-$N\left(a,b/x^n,y^n\right)$ את מספר ההופעות של הזוג (a,b) בווקטור $\left(x^n,y^n\right)$.

$$,\forall a,b\in \mathrm{X}\times\mathrm{Y} \qquad A_\varepsilon^{*(n)}\left(X,Y\right)=\left\{\left(x^n,y^n\right): \frac{1}{n}N\left(\left(a,b\right)/\left(x^n,y^n\right)\right)=\begin{cases} p(a,b)\pm\varepsilon' & p(a,b)>0 \\ 0 & p(a,b)=0 \end{cases}\right\}$$

JAEP (Jointly Asymptotic Equipartiotion Property)

כל הטענות שבתכונת ה-AEP מתייחסות להגדרה החלשה של הקבוצות (סדרות) אופייניות במשותף, אבל אותן תכונות מתקיימות גם ביחס להגדרה החזקה.

א. לכל הסדרות $\left(x^n,y^n\right)$ בקבוצה האופיינית יש בערך את אותה ההסתברות: $2^{-n[H(X,Y)\pm\varepsilon]}$.

ב. עבור n מספיק גדול, ההסתברות ש-$\left(x^n,y^n\right)$ אקראי יהיה שייך לקבוצה האופיינית היא 1 עד כדי ε, כלומר $\Pr\left\{A_\varepsilon^{(n)}\right\}>1-\varepsilon$.

ג. גודל הקבוצה הוא אכספוננציאלי באנטרופיה:

$$\left|A_\varepsilon^{(n)}\right|=2^{n[H(X,Y)\pm\varepsilon]}\quad for\, n\, sufficiently\, large$$

ד. עבור זוגות המ.א. $\left(\tilde{x}^n,\tilde{y}^n\right)$, המתפלגים i.i.d. ובת"ס אחד בשני, לפי הפילוגים השוליים המוגדרים ע"י $p_{x,y}(x,y)$, כלומר $p_{\tilde{x},\tilde{y}}\left(\tilde{x},\tilde{y}\right)=p_{\tilde{x}}\left(\tilde{x}\right)p_{\tilde{y}}\left(\tilde{y}\right)=p_x(x)p_y(y)$, מתקיים:

$$\Pr\left\{\left(\tilde{x}^n,\tilde{y}^n\right)\in A_\varepsilon^{(n)}\right\}=2^{-n[I(X;Y)\pm3\varepsilon]}\quad for\, n\, sufficiently\, large$$

<u>הוכחה</u>: חסם עליון (נכון לכל n) נתון ע"י הביטוי $\Pr\left\{\left(\tilde{x}^n,\tilde{y}^n\right)\in A_\varepsilon^{(n)}\right\}\le 2^{-n[I(X;Y)-3\varepsilon]}$:

$$\Pr\left\{\left(\tilde{x}^n,\tilde{y}^n\right)\in A_\varepsilon^{(n)}\right\}=\sum_{\left(x^n,y^n\right)\in A_\varepsilon^{(n)}} p\left(x^n\right)\cdot p\left(y^n\right)\le$$
$$\le 2^{-n[H(X)-\varepsilon]}\cdot 2^{-n[H(Y)-\varepsilon]}\cdot\left|A_\varepsilon^{(n)}\right|\le$$
$$\le 2^{-n[H(X)-\varepsilon+H(Y)-\varepsilon-H(X,Y)-\varepsilon]}=2^{-n[I(X;Y)-3\varepsilon]}$$

חסם תחתון (נכון ל-n מספיק גדול) נתון ע"י הביטוי
$\Pr\left\{\left(\tilde{x}^n,\tilde{y}^n\right)\in A_\varepsilon^{(n)}\right\}\ge(1-\delta)\cdot 2^{-n[I(X;Y)+3\varepsilon]}$:

$$\Pr\left\{\left(\tilde{x}^n,\tilde{y}^n\right)\in A_\varepsilon^{(n)}\right\}=\sum_{\left(x^n,y^n\right)\in A_\varepsilon^{(n)}} p\left(x^n\right)\cdot p\left(y^n\right)\underbrace{\ge}_{for\,n\,s.l.}$$
$$\ge 2^{-n[H(X)+\varepsilon]}\cdot 2^{-n[H(Y)+\varepsilon]}\cdot(1-\delta)\cdot 2^{n[H(X,Y)-\varepsilon]}=$$
$$=(1-\delta)\cdot 2^{-n[H(X)+\varepsilon+H(Y)+\varepsilon-H(X,Y)+\varepsilon]}=$$
$$=(1-\delta)\cdot 2^{-n[I(X;Y)+3\varepsilon]}$$

Conditional AEP

עבור $\underline{y}'$ אופייני ל-$p_y(y)$ $\left(y'\in A_\varepsilon^{(n)}(Y)\right)$, נגדיר את קבוצת כל ה-$\underline{x}$-ים שהם אופיינים במשותף עם ה-$\underline{y}'$ הנתון:

$$A_\varepsilon^{(n)}\left(X/\underline{y}'\right)=\left\{x^n:\left(\underline{x},\underline{y}'\right)\in A_\varepsilon^{(n)}(X,Y)\right\}$$

מתקיים:

א. לכל ה-$\underline{x}$-ים בקבוצה האופיינית יש בערך את אותה ההסתברות: $2^{-n[H(X/Y)\pm 2\varepsilon]}$.

<u>הוכחה</u>:

$$p(\underline{x}/\underline{y}')=\frac{p(\underline{x},\underline{y}')}{p(\underline{y}')}=\frac{2^{-n[H(X,Y)\pm\varepsilon]}}{2^{-n[H(Y)\pm\varepsilon]}}=2^{-n[H(X/Y)\pm 2\varepsilon]}\quad\forall\underline{x}\in A_\varepsilon^{(n)}\left(X/\underline{y}'\right)$$

ב. לכל $\underline{y}'$ אופייני חזק, ולכן "כמעט" לכל $\underline{y}'$ אופייני חלש גודל הקבוצה אכספוננציאלי באנטרופיה המותנית, $\left|A_\varepsilon^{(n)}\left(X/\underline{y}'\right)\right|\underbrace{=}_{\substack{almost\,for\\ every\,\underline{y}'}}2^{n[H(X/Y)\pm 2\varepsilon]}$:

<u>הוכחה</u>: חסם עליון (נכון לכל n ולכל $\underline{y}'$) נתון ע"י הביטוי
$\left|A_\varepsilon^{(n)}\left(X,\underline{y}'\right)\right|\le 2^{n[H(X/Y)+2\varepsilon]}$:

$$1=\sum_{\underline{x}\in\left(\underline{x},\underline{y}'\right)}p_{x/y}(\underline{x}/\underline{y}')\underbrace{\ge}_{\substack{decrease\\ the\,numbers\\ of\,elements\\ in\,sum}}\sum_{\underline{x}\in A_\varepsilon^{(n)}\left(X/\underline{y}'\right)}p_{x/y}(\underline{x}/\underline{y}')\underbrace{\ge}_{\substack{from\\ property\\ a.}}$$
$$\ge\sum_{\underline{x}\in A_\varepsilon^{(n)}\left(X/\underline{y}'\right)}2^{-n[H(X/Y)+2\varepsilon]}=2^{-n[H(X/Y)+2\varepsilon]}\cdot\left|A_\varepsilon^{(n)}\left(X/\underline{y}'\right)\right|$$

חסם תחתון (נכון לכל $\underline{y}'$ ועבור n מספיק גדול) נתון ע"י הביטוי
$\sum_{\underline{y}'\in A_\varepsilon^{(n)}(Y)}p(\underline{y}')\left|A_\varepsilon^{(n)}\left(X/\underline{y}'\right)\right|\ge(1-\varepsilon)\cdot 2^{n[H(X/Y)-2\varepsilon]}$:

$$1-\varepsilon \underbrace{\le}_{\substack{proved\\ in\ JAEP}} \Pr\left\{A_\varepsilon^{(n)}(X,Y)\right\} = \sum_{(\underline{x},\underline{y}')\in A_\varepsilon^{(n)}(X,Y)} p(\underline{x},\underline{y}') =$$

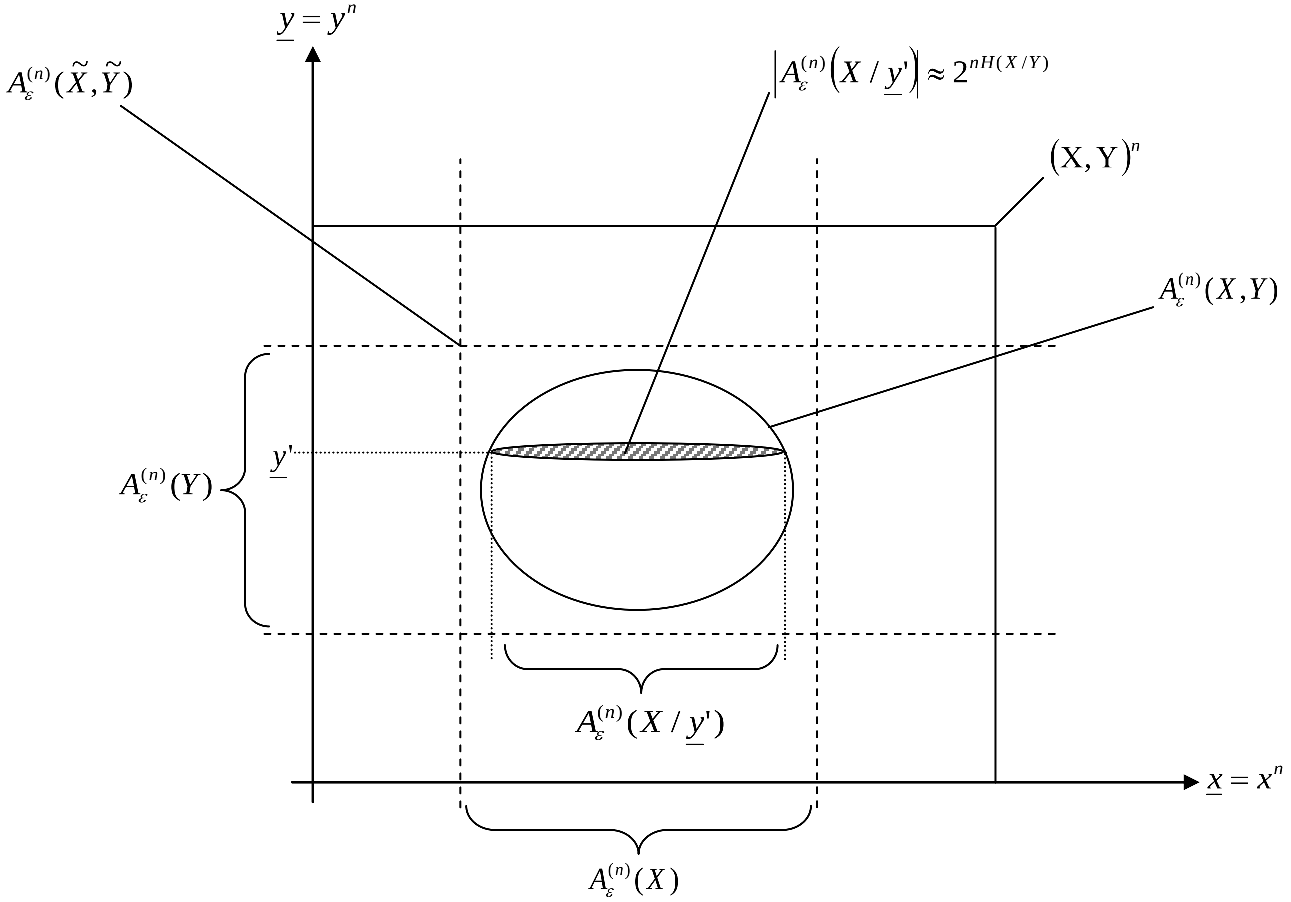
$$= \sum_{\underline{y}'\in A_\varepsilon^{(n)}(Y)} p(\underline{y}') \sum_{\underline{x}\in A_\varepsilon^{(n)}(X/\underline{y}')} p(\underline{x}/\underline{y}') \underbrace{\le}_{\substack{from\\ property\\ a.}}$$

$$\le \sum_{\underline{y}'\in A_\varepsilon^{(n)}(Y)} p(\underline{y}') \sum_{\underline{x}\in A_\varepsilon^{(n)}(X/\underline{y}')} 2^{-n[H(X/Y)-2\varepsilon]} =$$

$$= 2^{-n[H(X/Y)-2\varepsilon]} \cdot \sum_{\underline{y}'\in A_\varepsilon^{(n)}(Y)} p(\underline{y}') \cdot \left|A_\varepsilon^{(n)}(X/\underline{y}')\right|$$

אפשר להגיד שלכל $\underline{y}'$ אופייני חזק מתקיים החסם התחתון $\left|A_\varepsilon^{(n)}(X,\underline{y}')\right| \ge 2^{n[H(X/Y)-2\varepsilon]}$.

ניתן לתאר את כל היחסים בין הקבוצות האופייניות המשותפות שהגדרנו בדיאגרמה הבאה:



"מפענח אופייניות משותפת" – השלכה של כל הקשרים שראינו

א. נגריל $\underline{x}$ לפי פילוג $p_x(x)=\sum_y p_{x,y}(x,y)$. עבור $\underline{y}'$ אופייני (המוגרל באופן בלתי תלוי ב-$\underline{x}$ לפי פילוג $p_y(y)=\sum_x p_{x,y}(x,y)$), הסיכוי של $\underline{x}$ להיות אופייני במשותף עם $\underline{y}'$ הוא בערך $2^{-nI(X;Y)}$.

<u>הוכחה</u>:

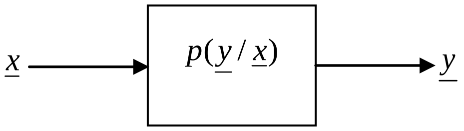
$$p\left(\left(\underline{x},\underline{y}'\right)\in A_\varepsilon^{(n)}\left(X/\underline{y}'\right)\right)\underbrace{\cong}_{\substack{x\,is\,approx\\ uniformly\\ distributed}}\frac{\left|A_\varepsilon^{(n)}\left(X,\underline{y}'\right)\right|}{\left|A_\varepsilon^{(n)}\left(X\right)\right|}\le\frac{2^{n[H(X/Y)+2\varepsilon]}}{2^{n[H(X)-\varepsilon]}}=2^{-n[I(X;Y)-3\varepsilon]}\qquad\forall\underline{y}'$$

$$p\left(\left(\underline{x},\underline{y}'\right)\in A_\varepsilon^{(n)}\left(X/\underline{y}'\right)\right)\underbrace{\cong}_{\substack{x\,is\,approx\\ uniformly\\ distributed}}\frac{\left|A_\varepsilon^{(n)}\left(X,\underline{y}'\right)\right|}{\left|A_\varepsilon^{(n)}\left(X\right)\right|}\ge\frac{2^{n[H(X/Y)-2\varepsilon]}}{2^{n[H(X)+\varepsilon]}}=2^{-n[I(X;Y)+3\varepsilon]}\qquad almost\,\forall\underline{y}'$$

$$\Rightarrow p\left(\left(\underline{x},\underline{y}'\right)\in A_\varepsilon^{(n)}\left(X/\underline{y}'\right)\right)\approx 2^{-nI(X;Y)}$$

ב. עבור הסכימה הבאה:

ערוץ חסר זיכרון



נניח קוד אקראי לפי פילוג $p(x)$, כלומר מגרילים $M=2^{nR}$ מילות קוד:
$\left(X(1),X(2),...,X(M)\right)$, כך שכל רכיב הוא i.i.d. לפי $p(x)$. משדרים את $X(1)$,
קולטים את $\underline{y}$ ושואלים מהו הסיכוי ש-"מפענח סבירות מירבית" ישגה?

נגדיר את מאורע הטעות של מפענח כזה: המפענח בודק כמה $\underline{x}$-ים אופייניים יש עם ה-$\underline{y}$ הנקלט. המפענח מחליט רק כאשר יש בדיוק $\underline{x}$ אחד כזה, ואותו $\underline{x}$ הוא המילה המפוענחת, ולכן המפענח צודק רק אם אותו $\underline{x}$ שודר.

נגדיר מאורע E_i , שאומר כי המילה $\underline{x}(i)$ אופיינית במשותף עם $\underline{y}$:

$$E_i:\left(\left(\underline{x}(i),\underline{y}\right)\in A_\varepsilon^{(n)}\left(\underline{x},\underline{y}\right)\right)$$

ניתן לבטא את הסתברות השגיאה באופן הבא:

$$P_e=\Pr\left\{E_1^C\bigcup\left(\bigcup_{i=2}^{M}E_i\right)\right\}\underbrace{\le}_{\substack{union\\ bound}}\underbrace{\Pr\left\{E_1^C\right\}}_{\substack{=\varepsilon,\,according\\ to\,JAEP}}+\left(M-1\right)\underbrace{\Pr\left\{E_i\right\}}_{\substack{doesn't\,depend\\ on\,i\,due\,to\\ random\,coding}}\le$$

$$\le\varepsilon+2^{nR}\cdot 2^{-n[I(x;y)-3\varepsilon]}=\varepsilon+2^{-n[I(x;y)-R-3\varepsilon]}\xrightarrow[n\to\infty]{if\,R<I(x;y)}0$$

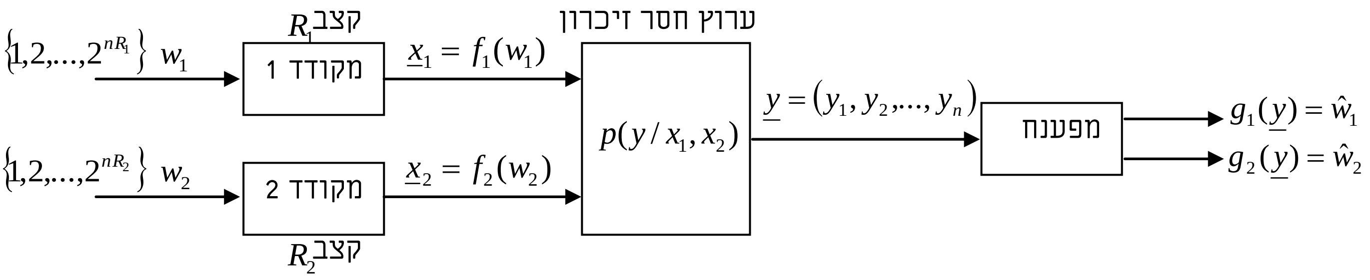
הרצאה - 4

Multiple Access Channel (MAC)

סוכם ע"י חן בנקירד

משפט הקיבול של ערוץ ה-MAC

מניחים א-ב דיסקרטי בסכימה הבאה:



<u>הסתברות השגיאה:</u> $P_e^{(n)} = \Pr\{\hat{w}_1 \neq w_1 \;\; or \;\; \hat{w}_2 \neq w_2\}$

באופן כללי המערכת מוגדרת ע"י 4 פונקציות: f_1, f_2, g_1, g_2 .

נאמר שזוג קצבי קידוד (R_1, R_2) הוא בר השגה את קיימת סדרת מערכות עם קצבים $(f_1^{(n)}, f_2^{(n)}, g_1^{(n)}, g_2^{(n)})_{n=1,2,\ldots}$ (R_1, R_2) כך ש: $P_e^{(n)} \xrightarrow[n\to\infty]{} 0$.

<u>תחום הקיבול האופרטיבי:</u>

$$C = closure\{ConvexHull\{(R_1, R_2): achievable\,rates\}\}$$

<u>תחום הקיבול האינפורמציוני:</u>

$$C^* = closure\left\{convex\,hall\{\bigcup_{P(X1),P(X2)} C^*(P(X1), P(X2))\}\right\}$$

כאשר האיחוד הוא על תחומים מהצורה :

$$C^*(P(X1), P(X2)) \overset{\Delta}{=} \left\{ (R1, R2): \begin{array}{c} R1 + R2 \le I(X1, X2; Y) \\ R1 \le I(X1; Y/X2) \\ R2 \le I(X2; Y/X1) \end{array}, \begin{array}{c} where \\ P(x1, x2, y) = P(x1)\cdot P(x2)\cdot P(y/x1, x2) \end{array} \right\}$$

משפט הקיבול

הקיבול האינפורמציוני שווה לקיבול האופרטיבי:

$$C = C^*$$

את המשפט נוכיח בשני חלקים:

<u>החלק הישר:</u> (הוכחה קונסטרוקטיבית) ניתן להשיג כל זוג קצבים (R_1, R_2) המקיימים $(R_1, R_2) \in \underline{C}^*$ ע"י סדרת מערכות ממימד $n = 1,2,\ldots$, כאשר $\underline{C}^*$ הוא התחום C^* ללא השפה.

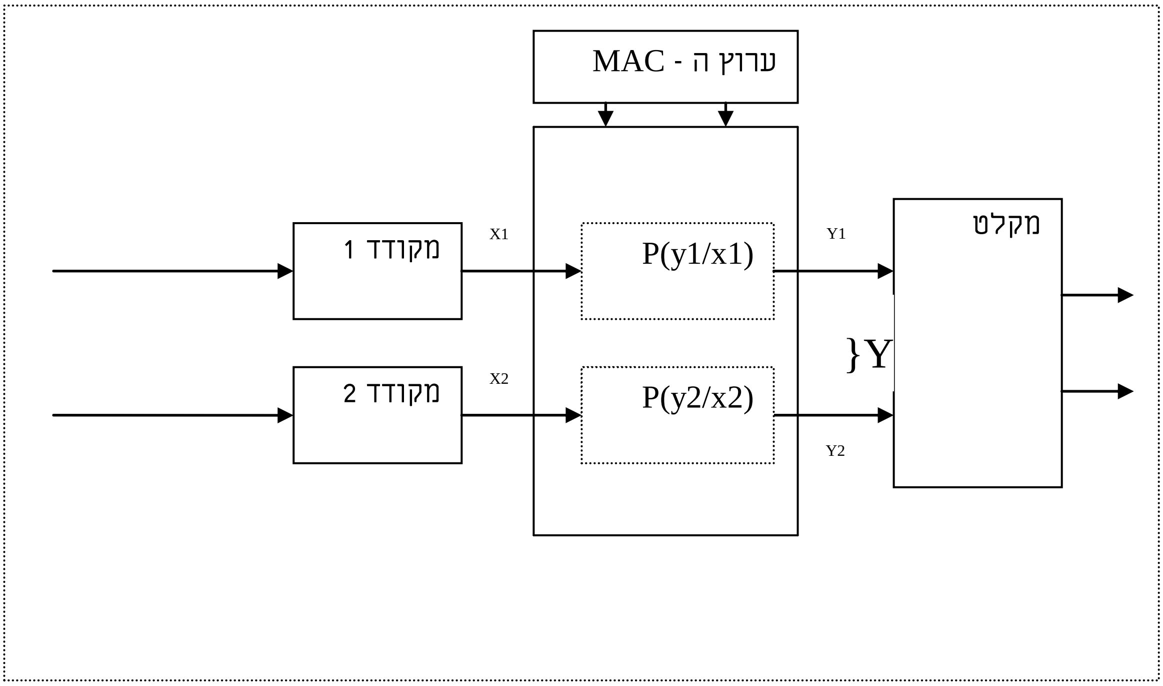
שקול לומר $\underline{C}^* \subset C$.

<u>החלק ההפוך:</u> אם זוג הקצבים (R_1,R_2) ניתן להשגה ע"י סדרת מערכות ממימד $n=1,2,\ldots$ (כלומר $P_e^{(n)} \xrightarrow[n\to\infty]{} 0$) אזי בהכרח $(R_1,R_2)\in C^*$.

שקול לומר $C^* \supset C$.

דוגמאות

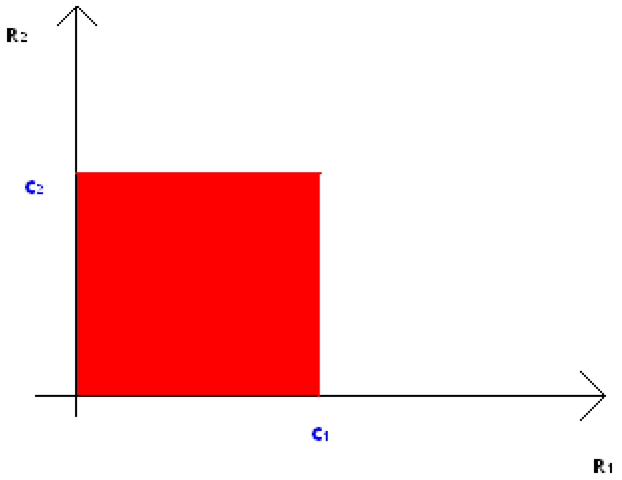
- ערוצים בת"ס במקביל



במקרה הזה $R1 \le I(X1;Y/X2) = I(X1;Y1)$ כאשר Y=(Y1,Y2) ובדומה $R2 \le I(X2;Y2)$

ולכן המגבלה $R1+R2 \le I(X1,X2;Y) = I(X1;Y1)+I(X2;Y2)$ ניתנת תמיד להשגה.

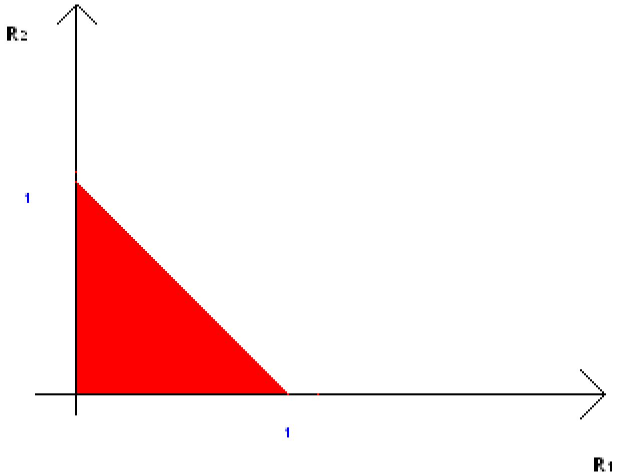
כלומר ה – MAC משיג את מה שהיה משיג המקודד המשותף.



- Binary Multiplier

הפלט נתון ע"י $Y = X1 \& X2$ כאשר $X1,X2\in\{0,1\}$. ניתן גם להסתכל על זה בתור $Y = X1\cdot X2$ כאשר $X1,X2\in\{-1,1\}$.

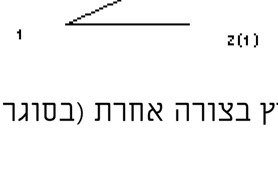
יש לשים לב כי אין כאן רעש נוסף, כלומר $H(Y/X1,X2)=0$.
נשים גם לב לכך שאם ערוץ אחד "יקריב" עצמו למען השני (ישדר 1 כל הזמן), נקבל העברה נקייה של הערוץ השני (כלומר קצב של 1 ביט לסימבול) ואם נשים לב ש – $R1+R2 \le I(X1,X2;Y) \le H(Y) \le 1bit$ אז בעצם קיבלנו נקודות קצה. מכיוון שבנוסחא של המשפט מופיע ConvexHull, נקבל שהקו המחבר בין נקודות הקצה הוא בדיוק גבול הקיבול.



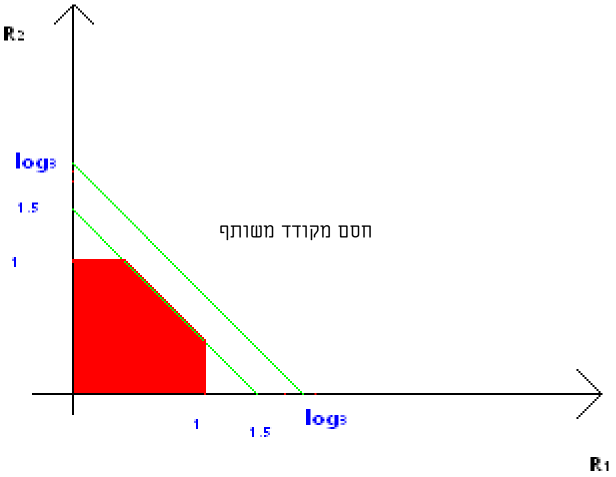
נראה שניתן להשיג את קו השפה R1+R2=1 גם ללא "חלוקת זמן". לשם כך נציב פילוגי מבוא מהצורה Pr(X1=1)=P1, Pr(X2=1)=0.5/P1 ואז H(Y)=1.

- Binary Adder

הפלט נתון ע"י $Y=X1+X2$ כאשר $X1,X2\in\{0,1\}$ והחיבור הוא חיבור רגיל ולכן $Y\in\{0,1,2\}$.
גם ערוץ זה פועל ללא רעש, ומתקיים $H(Y/X1,X2)=0$.
ניתן לראות שמתקיים $I(X1,X2;Y)\le H(Y)\le \log(3)$.
אם ניקח פילוגי כניסה אחידים (ובת"ס), נקבל
$R1+R2 \le I(X1,X2;Y)=H(Y)=H(\frac{1}{4},\frac{1}{2},\frac{1}{4})=1.5bit$.
למעשה, 1.5bit הוא חסם עליון של האנטרופיה של Y – עבור X1, X2 בלתי תלויים ולכן מהווה את חסם ה - MAC. בניגוד לכך, אם מותר ל – X1,X2 להיות תלויים (וכאשר הקידוד משותף), ניתן לקחת Pr(1,1)=Pr(0,1)=Pr(0,0)=1/3 ואז H(Y)=log3.
נקודות הקצה מתקבלות ע"י שידור (0.5, 0.5) דרך ערוץ אחד, ושימוש בערוץ השני בתור ערוץ עם מחיקה. ערוץ המחיקה מושג ע"י כך שמסתכלים על העובדה ש – Y=X1+X2

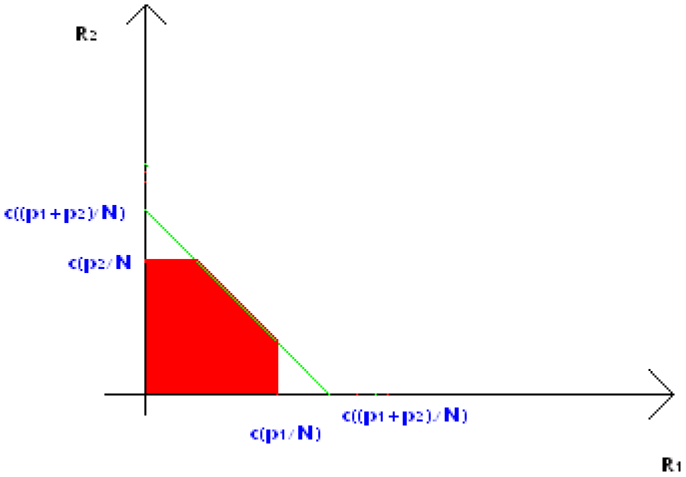


כאשר X2 אינו ידוע ומתפלג (0.5, 0.5) , ואז מתקבל
כאשר כל הסתברויות המעבר הן 0.5, והסתכלות על הערוץ בצורה אחרת (בסוגריים בציור) היא למעשה ערוץ המחיקה.



- **MAC גאוסי**

נזכיר את נוסחת השידור $Y = X1 + X2 + Z$, כאשר על X1, X2 יש מגבלות הספק של P1, P2 בהתאמה, והרעש הוא גאוסי ומקיים $Z \sim N(0, \sigma_z^2)$. המגבלות $R1 \le I(X1;Y/X2)$ ו - $R2 \le I(X2;Y/X1)$ נותנות מגבלות מקסימום $R1 \le c(\frac{P1}{\sigma_z^2})$ ו - $R2 \le c(\frac{P2}{\sigma_z^2})$ הנובעות מהקרבה מלאה של אחד המשדרים עבור המשדר השני. המגבלה $R1 + R2 \le I(X1, X2; Y)$ והעובדה שהמשדרים בלתי תלויים גוררת ש - $R1 + R2 \le c(\frac{P1 + P2}{\sigma_z^2})$. כאשר נקודות הקצה נובעות משידור של אחד הערוצים בקצב המהיר ביותר האפשרי, ובערוץ השני שידור עם רעש שקול הנובע מחיבור בין הערוץ הראשון ל – Z.(באיור הבא $N = \sigma_z^2$)



היתרון של נקודות הפינה במקרה הגאוסי הוא שהפתרון שלהם לא שונה מבחינת סכימת שידור-פענוח מאשר פתרון של מקרה גאוסי נל"נ. כלומר בהנתן מקודד ומפענח (מודם) שיודע לטפל בנל"נ גאוסי, ניתן להשתמש בו על מנת לייצר פתרון ל – MAC הגאוסי. נרצה פתרון דומה עבור נקודות שאינן נקודות קצה. כלומר נרצה פתרון של נקודות הקצה ע"י שימוש בקופסאות שיודעות לשדר ולפענח מעל ערוץ נל"נ גאוסי. הדרך

הכללית להשגת נקודות שפה היא ע"י joint detection , הגרך החלופית היא ע"י חלוקת זמן (time sharing), אך היא מחייבת סוג של סנכרון בין המשדרים, ולכן לא ניתנת להשגה ע"י שימוש במקודדים ומפענחים של נל"נ "רגיל".

השגת נקודות שפה – (Rate splitting approach) ב – MAC גאוסי עם קידוד (Urbanke-Rimoldi 1996):

נחלק את משדר מספר אחד לשני משדרים בת"ס וגאוסיים.

$R1 = R1'+R1''; P1 = P1'+P1''$.

סכמת השידור (לוגית):

1. משדר 1 משדר בקצב 'R1, בהספק 'P1, רעש שקול N.
2. משדר 2 משדר בקצב R2, בהספק P2, רעש שקול N + 'P1.
3. משדר 1 משדר בקצב "R1, בהספק "P1, רעש שקול N + P2 + P1'.

יש לשים לב כי בפועל משדר 1 משדר את סכום תתי הקודים שלו, ולא משדר פעמיים.

סכמת הפענוח :

1. מפענח אינפורמציה בקצב "R1, ומחסר אותה.
2. מפענח אינפורמציה בקצב R2, ומחסר אותה.
3. מפענח אינפורמציה בקצב 'R1.

קצבי השידורים :

$R1' = c(\frac{P1'}{N}); R2 = c(\frac{P2}{N+P1'}); R1'' = c(\frac{P1''}{N+P1'+P2})$ ונשים לב כי

$R1+R2 = R1'+R1''+R2 = c(\frac{P1+P2}{N})$ כלומר סכימת שידור זו משיגה את המקסימום (הנובע מחסם ה – MAC הגאוסי), ואם נסמן $0 \le \lambda \le 1; P1' = \lambda P1$ אז נשים לב כי R2 יקבל את כל הערכים האפשריים המהווים את נקודות האמצע. לכן אם רוצים לשדר מנקודה מסוימת על שפת הקיבול (או קרוב כרצוננו אליה), כלומר רוצים קצבי שידור המקיימים

$$R1 = c(\frac{P1}{N}) \cdot \alpha + c(\frac{P1}{N+P2}) \cdot (1-\alpha); R2 = c(\frac{P2}{N+P1}) \cdot \alpha + c(\frac{P2}{N}) \cdot (1-\alpha)$$

אז מתקבל $R2 = c(\frac{P2}{N+P1}) \cdot \alpha + c(\frac{P2}{N}) \cdot (1-\alpha) = c(\frac{P2}{N+P1'}) = c(\frac{P2}{N+\lambda P1})$

כלומר $\alpha = \dfrac{c(\frac{P2}{N}) - c(\frac{P2}{N+\lambda P1})}{c(\frac{P2}{N}) - c(\frac{P2}{N+P1})}$

הוכחת המשפט הישר:

1. **בניית הקוד-** ספר קוד 1, בעל 2^{nR1} מילות קוד, יוגרל בצורה רנדומית (i.i.d) לפי הפילוג P(X1), כלומר כל רכיב בכל מילת קוד מוגרל בת"ס לפי P(X1). בדומה ספר קוד 2 יוגרל לפי P(X2), ויהיה בעל 2^{nR2} מילות קוד. הן המשדר והן המקלט יודעים את הקודים שהוגרלו.
2. **שידור-** בהינתן $1 \le W1 \le 2^{nR1}, 1 \le W2 \le 2^{nR2}$ משדר 1 משדר את מילת הקוד של W1 ומשדר 2 משדר את מילת הקוד של W2.יש לזכור כי ההודעות ,W1 W2 הן בת"ס, ולכן כל הזוגות אפשריים.

3. **פענוח-** פענוח נעשה לפי אופייניות משותפת עבור הפילוג $P(X1)\cdot P(X2)$. מחפשים אינדקסים i, j שמילות הקוד שמתאימות להם אופייניות במשותף עם פלט הערוץ, כלומר שייכות לקבוצה $A_{\varepsilon}^{(n)}(X1, X2/\underline{y})$. אם יש רק זוג אחד – מכריזים עליו כפלט המפענח. אחרת (יותר מזוג אחד, אף זוג) מכריזים על מאורע שגיאה. נניח בה"כ כי W1=W2=1, ונגדיר מאורעות $E_{i,j}$ שהם המאורע שזוג מילות הקוד של i,j אופייני במשותף עם $\underline{y}$. שגיאה תתרחש כשאר $E^{c}{}_{1,1}$ או כאשר $E_{i,j}$ כאשר i או j שונים מאחד. לכן

$$P_e = \Pr(E_{11}^{c}\bigcup_{i=2}^{2^{nR1}} E_{i1}\bigcup_{j=2}^{2^{nR2}} E_{1j}\bigcup_{i,j=2}^{2^{nR1},2^{nR2}} E_{ij}) \le \Pr(E_{11}^{C}) + 2^{nR1}\Pr(E_{21}) + 2^{nR2}\Pr(E_{12}) + 2^{n(R1+R2)}\Pr(E_{22})$$

כאשר אי השוויון נובע משימוש בחסם האיחוד, ובעובדה שהקודים אקראיים ובת"ס. ההסתברות מחושבת גם ביחס לאקראיות הערוץ וגם ביחס לאקראיות הקוד. ומתקיים עבור n גדול מספיק כי :

- $\Pr(E_{11}^{c}) < \varepsilon$ הסתברות שמוצא ערוץ לא יהיה אופייני במשותף עם המבוא.
- $\Pr(E_{22}) < 2^{-n[I(X1,X2;Y)-3\varepsilon]}$ הסתברות שמבוא רנדומי יהיה אופייני עם המוצא.
- $\Pr(E_{12}) < 2^{-n[I(X2;Y,X1)-3\varepsilon]}$ הסתברות ש-X2 רנדומי יהיה אופייני עם $\underline{x1}, \underline{y}$.
- $\Pr(E_{21}) < 2^{-n[I(X1;Y,X2)-3\varepsilon]}$ הסתברות ש-X1 רנדומי יהיה אופייני עם $\underline{x2}, \underline{y}$.

לכן:

$$\ldots \le \varepsilon + 2^{-n[I(X1;Y/X2)-3\varepsilon]}\cdot 2^{nR1} + 2^{-n[I(X2;Y/X1)-3\varepsilon]}\cdot 2^{nR2} + 2^{-n[I(X1,X2;Y)-3\varepsilon]}\cdot 2^{n(R1+R2)}$$

כעת אם ניקח

$R1 < I(X1; X2, Y) - 3\varepsilon;\ R2 < I(X2; X1, Y) - 3\varepsilon;\ R1 + R2 < I(X1, X2; Y) - 3\varepsilon$ אז

עבור n ששואף לאינסוף נקבל הסתברות שגיאה השואפת לאפס. בנוסף נשים לב כי $I(X1;X2,Y) = I(X1;X2) + I(X1;Y/X2) = I(X1;Y/X2)$ ובדומה $I(X2;X1,Y) = I(X2;X1) + I(X2;Y/X1) = I(X2;Y/X1)$ אז נוכל להתקרב לגבול הקיבול התיאורטי כרצוננו. הפעלת תכונת ה – closure תיתן את התוצאה הדרושה.

- צריך להדגיש כי בהוכחה הראינו כי הסתברות השגיאה הממוצעת (על כל ספרי הקוד ועל כל המילים) קטנה מ - ε , ולא עבור ספר קוד או מילה ספציפית. עובדה זו גוררת קיום של לפחות ספר קוד אחד שעבורו הסתברות השגיאה הממוצעת על כל המילים קטנה מ - ε . בשידור נל"נ רגיל יודעים ניתן להמשיך ולהסיק גם קיום של ספר קוד עם הסתברות שגיאה קטנה מ - ε לכל סימבול כניסה (ע"י זריקת חצי מהמילים ה"רעות" ושימוש באי שוויון מרקוב), ב- MAC זה לא טריויאלי להוכיח זאת, מפני שספר הקוד חייב להיות מכפלה קרטזית של שני ספרי קוד.

<u>הוכחת המשפט ההפוך:</u>

נניח כי קיימת מערכת f1,f2 המשיגה קצבים R1, R2, עם הסתברות שגיאה Pe.
נניח שמדובר בהודעות שוות הסתברות, ונניח שההודעות הם
$W1 \in \{1..2^{nR1}\}; W2 \in \{1..2^{nR2}\}$. את המשתנים האקראיים המשודרים בערוצים 1
ו-2 נסמן ב – X1,X2. את הוקטורים שמשודרים בערוצים אלו נסמן ב - $\underline{x}_1, \underline{x}_2$,
ואת הוקטור המתקבל נסמן ב - $\underline{y}$
תחילה **נראה את משפט Fano** עבור (X1,X2),X1,X2 :

$$n\cdot(R1+R2)=H(W1,W2)=I(W1,W2;\underline{Y})+H(W1,W2/\underline{Y})=I(\underline{X1},\underline{X2};\underline{Y})+H(W1,W2/\underline{Y})$$

$$n\cdot R1=H(W1)=H(W1/W2)=I(W1;\underline{Y}/W2)+H(W1/W2,\underline{Y})=I(\underline{X1};\underline{Y}/\underline{X2})+H(W1/W2,\underline{Y})$$

$$n\cdot R2=H(W2)=H(W2/W1)=I(W2;\underline{Y}/W1)+H(W2/W1,Y)=I(\underline{X2};\underline{Y}/\underline{X1})+H(W2/W1,\underline{Y})$$

כאשר בשוויון האחרון בשלושת הפיתוחים השתמשנו בעובדה ש - $\underline{X1},\underline{X2}$ הם
פונקציות דטרמיניסטיות של W1,W2 ובאי שוויון עיבוד הנתונים. בשני
הפיתוחים האחרונים השתמשנו גם בעובדה ש – W1,W2 הם בת"ס.
כעת נזכר שהסתברות השגיאה היא Pe, ונסמן במאורע E את מאורע השגיאה.
כלומר E=0 גורר פענוח נכון, ו – E=1 גורר מאורע שגיאה. ואז מתקיים כי :

$$H(W1,W2/\underline{Y})\le H(W1,W2,E/\underline{Y})=Pe\cdot H(W1,W2/\underline{Y},E=1)+(1-Pe)\cdot H(W1,W2/\underline{Y},E=0)\le Pe\cdot n\cdot(R1+R2)$$

$$H(W1/W2,\underline{Y})\le H(W1,E/W2,\underline{Y})=Pe\cdot H(W1/W2,\underline{Y},E=1)+(1-Pe)\cdot H(W1/W2,\underline{Y},E=0)\le Pe\cdot n\cdot R1$$

$$H(W2/W1,\underline{Y})\le H(W2,E/W1,\underline{Y})=Pe\cdot H(W2/W1,\underline{Y},E=1)+(1-Pe)\cdot H(W2/W1,\underline{Y},E=0)\le Pe\cdot n\cdot R2$$

כאשר בשלושת הפיתוחים האי שוויון הראשון נובע מכך שתוספת משתנים
מוסיפה אנטרופיה, השוויון שאח"כ הוא פשוט פיתוח לפי E, והאי שוויון האחרון
נובע מכך שכאשר אין טעות, W1,W2 הם פשוט פונקציה דטרמיניסטית של Y.

בנוסף מתקיים כי בגלל שהערוץ חסר זיכרון:

$$I(\underline{X1},\underline{X2};\underline{Y})=H(\underline{Y})-H(\underline{Y}/\underline{X1},\underline{X2})\le n\cdot(H(Y)-H(Y/X1,X2))=n\cdot I(X1,X2;Y)$$

ובדומה

$$I(\underline{X1};\underline{Y}/\underline{X2})\le n\cdot I(X1;Y/X2)$$

$$I(\underline{X2};\underline{Y}/\underline{X1})\le n\cdot I(X2;Y/X1)$$

בסה"כ מתקבלים :

$$(R1+R2)\cdot(1-Pe)\le I(X1,X2;Y)$$

$$R1\cdot(1-Pe)\le I(X1;Y/X2)$$

$$R2\cdot(1-Pe)\le I(X2;Y/X1)$$

כעת נשתמש בעובדה כי ניתן למצוא סידרת מערכות כאלו המקיימת Pe שואף
לאפס. ולכן מתקבל בצורה ישירה המשפט ההפוך. (מש"ל).

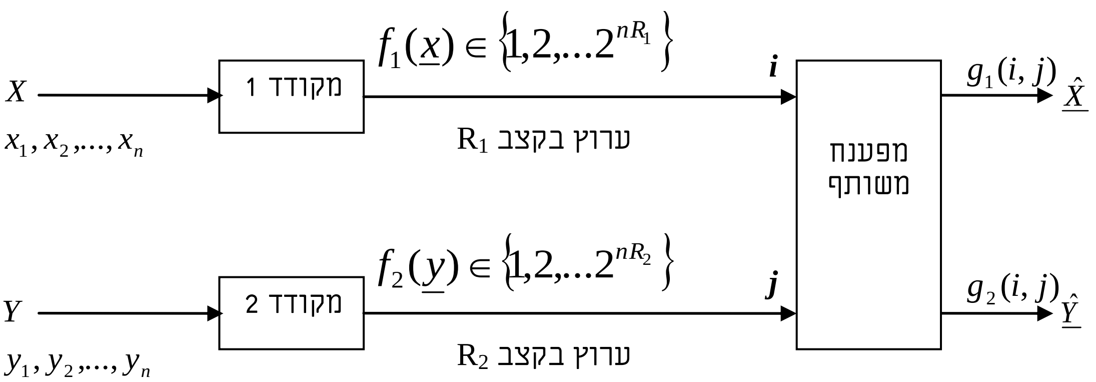
הרצאות 5-6

קידוד מקורות קורלטיביים או קידוד מקור מבוזר

סוכם ע"י איתי ליבוביץ

הגדרת הבעיה:

בבעיה נתון מקור אות כפול וחסר זיכרון בעל פילוג $P_{X,Y}(x,y)$. לכל אחד מהאותות יש מקודד משלו ואין ביניהם שיתוף פעולה . מקודד 1 מקודד את X בקצב R_1 ביטים לדגימת מקור, ומקודד 2 מקודד את Y בקצב R_2 ביטים לדגימת מקור, והקודים מפוענחים במשותף כדי לגלות את X ו- Y. המטרה היא לקודד בקצב כמה שיותר נמוך עם הסתברות שגיאה שואפת לאפס.



הגדרה:

זוג קצבים (R_1,R_2) ייקרא בר השגה אם קיימת סדרת מקודדים f_1,f_2,g_1,g_2 עם מימד n הולך וגדל בקצבים R_1 ו- R_2 כך שהסתברות השגיאה, המוגדרת כ: $\Pr(\varepsilon) = \Pr(\hat{\underline{x}} \neq \underline{x} \cup \hat{\underline{y}} \neq \underline{y})$, שואפת לאפס כאשר n שואף לאינסוף.

הגדרה:

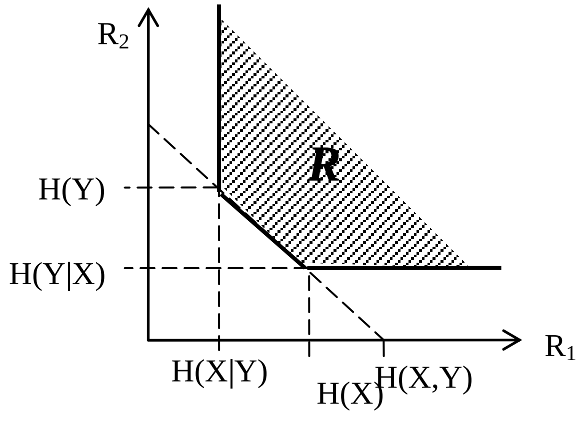
תחום הקצבים האופרטיבי ***R*** הוא הסגור של תחום הזוגות (R1,R2) ברי ההשגה.

הגדרה:

תחום הקצבים האינפורמציוני $\boldsymbol{R^*}$:

$$R^* = \left\{ (R_1,R_2): \begin{array}{r} R_1 + R_2 \geq H(X,Y) \\ R_1 \geq H(X|Y) \\ R_2 \geq H(Y|X) \end{array} \right\}$$

משפט הקידוד (Slepian-Wolf, 1973): **R=R***



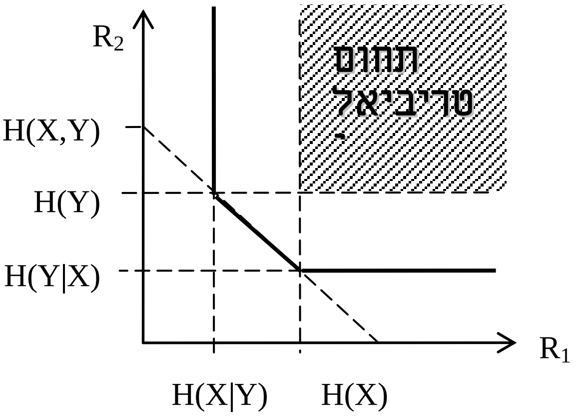
הוכחת המשפט ההפוך:

במקרה זה הוכחת המשפט ההפוך היא ברורה בהסתמך על משפטי הקידוד של מ״א יחיד. נראה זאת באמצעות שני תרחישי ייחוס:

1. מקודד משותף: במקודד משותף הקידוד הוא פונקציה של שני המ ״א X ו- Y יחד: $i=f(\underline{x},\underline{y})$, ובמקרה זה אנו מכירים את התוצאה של קידוד מקור יחיד ללא עיוות שלפיה $R \geq H(X,Y)$
במקרה של מקודד יחיד משותף קיימת מילת קוד אחת המקיימת: $i \in \{1,2,...,2^{nR}\}$. המקודדים המבוזרים הם מקרה פרטי של המקודד המשותף והם משדרים שתי מילות קוד השייכות לקבוצה בת $2^{n(R_1+R_2)}$ איברים של זוגות מילות קוד. מכאן ברור כי סכום הקצבים R_1+R_2 חייב להיות גדול או שווה למה שהיה משיג מקודד משותף, כלומר H(X,Y).

2. מקודד עם אינפורמציית צד: במקרה זה אנו רוצים לקודד את X בקצב R_1 כאשר גם למקודד וגם למפענח יש אינפורמציית צד Y. במקרה זה ההגבלה היא: $R_1 \geq H(X|Y)$, מכיוון שבהינתן Y, המ״א X מתפלג לפי P(X|Y), וגודל הקבוצה האופיינית שלו בהינתן וקטור $\underline{y}$ נקבע לפי האנתרופיה המותנית $H(X|\underline{y})$. ממה שאנו כבר יודעים על קידוד מקור יחיד ברור כי $R_1 \geq H(X|Y)$.
במקרה שלנו מקודד 1 לא יודע את Y בתור אינפורמציית צד ולכן זהו מקרה פרטי של המקרה הנ״ל, ולכן גם בבעיית SW חייב להתקיים $R_1 \geq H(X|Y)$, ובדומה, $R_2 \geq H(Y|X)$.

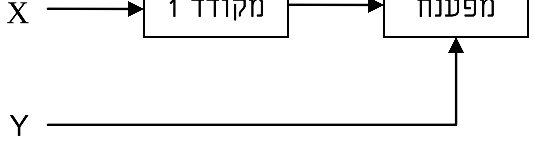
מכאן הוכחנו את המשפט ההפוך: $R \subseteq R^*$



עד עתה ידענו לקודד את X בקצב H(X) ואת Y בקצב H(Y) ולכן תחום הקצבים בו $R_1 \geq H(X)$ ו-$R_2 \geq H(Y)$ הוא תחום טריביאלי.

כיצד נוכל להשיג את שאר התחום $\boldsymbol{R^*}$?

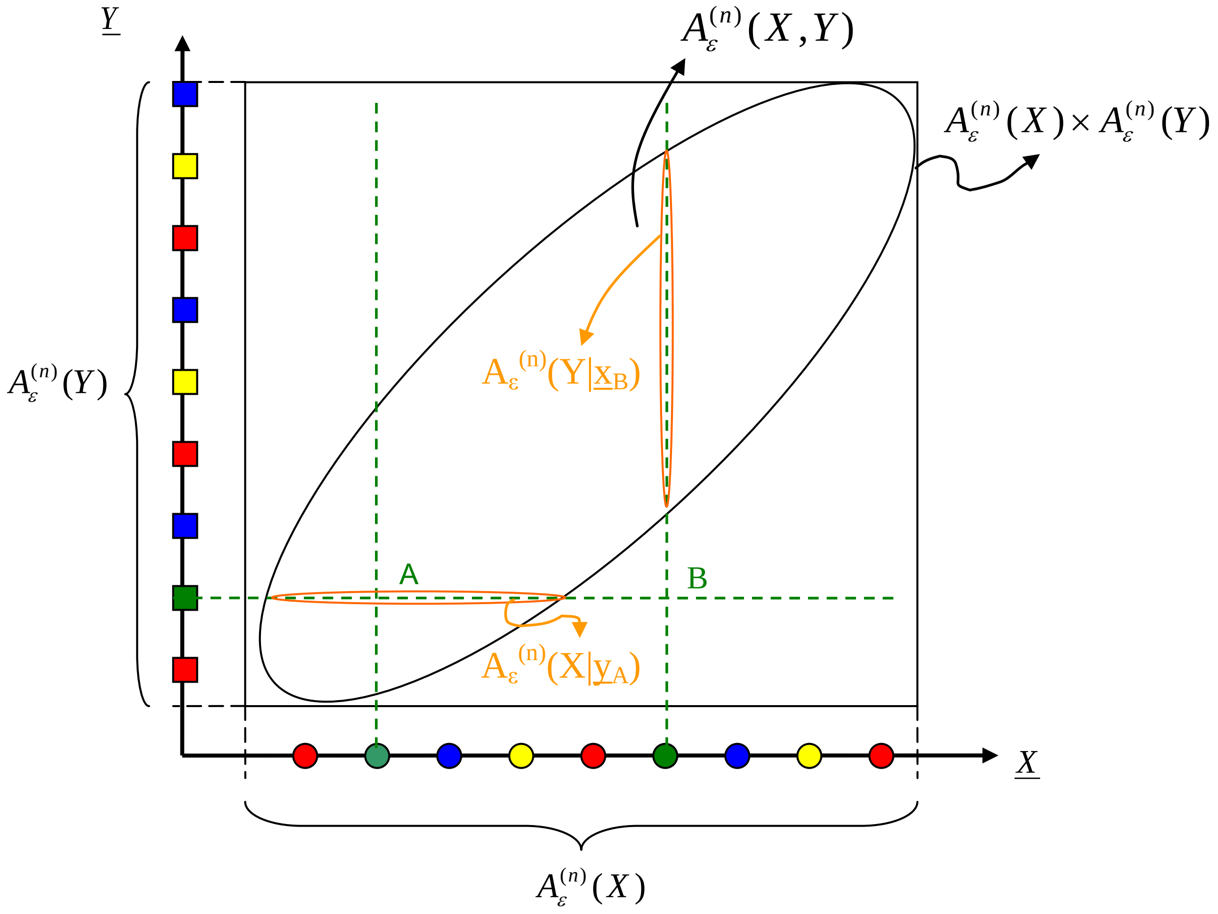
ראינו בעבר כבר רמז לפתרון. אם נסתכל על נקודות הפינה, נראה שבאחת מהן יש קידוד של Y בקצב H(Y) שהוא קצב שבו אנו כבר יודעים לקודד, וקידוד של X בקצב H(X|Y). אם Y היה ידוע גם למקודד 1 היינו יודעים לקודד את X בקצב זה, אך במקרה שלפנינו מקודד 1 לא יודע מהו Y, ואנו עומדים בפני בעיה מהצורה:



בהרצאה השנייה ראינו פתרון של ״אינפורמציית מודולו״ שבה X ו-Y היו מחוברים דרך ערוץ BSC, ובהשתמש בקוד לינארי טוב לערוץ ה- BSC, מקודד 1 שידר את הסינדרום של X לפי מטריצת הבדיקה של הקוד. שידור הסינדרום היה בדיוק בקצב H(X|Y).

כעת אנו מחפשים הרחבה של הפתרון למקר ה הכללי , שבו יש א ״ב ופילוג כלליים של (X,Y), וכן הקידוד נעשה בקצבים (R_1,R_2) שאינם נקודות פינה.

פתרון זה הוא פתרון ה- "binning" המוצג באיור הבא:



כאמור, התחום המעניין אותנו כרגע הוא זה שבו:

$$H(X|Y)<R_1<H(X)$$

$$H(Y|X)<R_2<H(Y)$$

מכאן ברור שהמקודד של X ייתן את אותה מילת קוד למספר סדרות אופייניות של X, וכך גם המקודד של Y ייתן את אותה מילת קוד למספר סדרות אופייניות של Y (כמות מילות הקוד היא 2^{nR} וכמות הסדרות האופייניות היא $2^{nH(X)}$).
זה מה שמודגם באיור . כל אחד מהעיגולים הצבעוניים מייצג מילת קוד של מקודד 1 וכל אחד מהריבועים מייצג מילת קוד של המקודד 2. כל נקודה על ציר $\underline{X}$ מסמנת סדרה של המ״א X, וכנ״ל לגבי Y. ניתן לראות שיש מספר סדרות ב- $A_\varepsilon^{(n)}(X)$ שקיבלו את אותו צבע (מילת קוד). נאמר שהן שייכות לאותו "bin".

מפענח אופייניות משותפת מקבל את מילות הקוד ובודק אם קיים זוג סדרות אופייניות $(\underline{x},\underline{y})\in A_\varepsilon^{(n)}(X,Y)$ שהקידוד שלהן מתאים למילים שהתקבלו . אם קיימת "נקודה" (זוג סדרות) אחת כזו, הוא יפענח אותה בתור הסדרות שקודדו.

אירועי השגיאה יהיו למשל כאשר יש יותר מזוג סדרות אופייני אחד המקודד באותו זוג סימנים, או כשמקודד האות פלט זוג סדרות שאינן אופייניות במשותף והן פוענח ו כזוג אופייני.

באיור שלמעלה מופיעה נקודה A המייצגת זוג סדרות $(\underline{x}_A,\underline{y}_A)$ השייך לתחום $A_\varepsilon^{(n)}(X,Y)$, כלומר זוג של סדרות אופייניות במשותף. לעומתה, נקודה B $(\underline{x}_B,\underline{y}_B)$ שייכת לתחום $A_\varepsilon^{(n)}(X)\times A_\varepsilon^{(n)}(Y)$, אך לא לתחום $A_\varepsilon^{(n)}(X,Y)$, כלומר $\underline{x}_B$ ו- $\underline{y}_B$ הן סדרות אופייניות כל אחת בנפרד אך אינן אופייניות ביחד. בעת קליטת זוג "ירוק" על המפענח להחליט בין נקודה A לבין נקודה B. מכיוון שנקודה B מייצגת זוג סדרות שאינו אופייני במשותף, הסתברותה אפסית, ולכן מפענח אופייניות משותפת יחליט תמיד שהנקודה שקודדה היא הנקודה A, והסיכוי לשגיאה במקרה זה הוא אפסי.
בעת הקידוד נרצה לדרוש שהחלוקה לצבעים תהיה בצורה כזו שסדרות הממופות לאותן מילות קוד יהיו "רחוקות" אחת מהשנייה, כמו במקרה של נקודות A ו- B.
מתברר, שאם נעשה את הקידוד בצורה רנדומלית, נקבל אוטומטית חלוקה "טובה" עם הגדלת המימד.

<u>הוכחת המשפט הישר באמצעות **random binning**</u>

ה"צבעים" שראינו בציור נקראים "בינים" (bins), והחלוקה לקבוצות של סדרות שלהן אותה מילת קוד נקראת binning. אנו נבנה את הקוד בצורה רנדומלית, ונראה שניתן לפענח את המידע בהסתברות שגיאה ששואפת לאפס. מכיוון שאנו נבחר קוד רנדומלי, הסתברות השגיאה שנקבל היא הסתברות שגיאה ממוצעת על פני כל ספרי הקוד, ומכאן נטען שחייב להיות קוד מסוים אחד לפחות שבו הסתברות השגיאה שואפת לאפס עם הגדלת n לאינסוף:

1. <u>בנית ספר הקוד:</u>
נתאים את מילות המקור X למילות הקוד: $i\in\{1,2,...,2^{nR_1}\}$ ואת מילות המקור Y למילות הקוד: $j\in\{1,2,...,2^{nR_2}\}$ באופן אקראי וחסר תלות ולפי פילוג אחיד:
$$\Pr\{f(\underline{x}^n)=i\}=2^{-nR_1}$$
$$\Pr\{f(\underline{y}^n)=j\}=2^{-nR_2}$$
ההגרלה של i ו- j תתבצע באופן בלתי תלוי זו בזו.

2. <u>הקידוד</u> יבוצע לפי ההגדרה $i=f_1(\underline{x}^n),\ j=f_2(\underline{y}^n)$.

3. <u>הפענוח</u> נעשה לפי אופייניות משותפת – joint typicality decoding:
המפענח מחפש את הסדרות המקיימות: $(x^n,y^n)\in(Bin-i,Bin-j)\quad and\quad \in A_\varepsilon^{(n)}(X,Y)$
אם קיים פתרון יחיד, נבחר אותו בתור הפענוח, ואם אין בכלל פתרון או יש יותר מאחד נכריז על שגיאה.

<u>ניתוח של הסתברות השגיאה:</u>
סוגי השגיאה השונים המופיעים כאן מתוארים גם באיור בעמוד הבא:

1. E_0 – המאורע שהזוג (x^n,y^n) אינו אופייני במשותף. מתכונות ה- AEP נובע: $\Pr(E_0)<\varepsilon$.

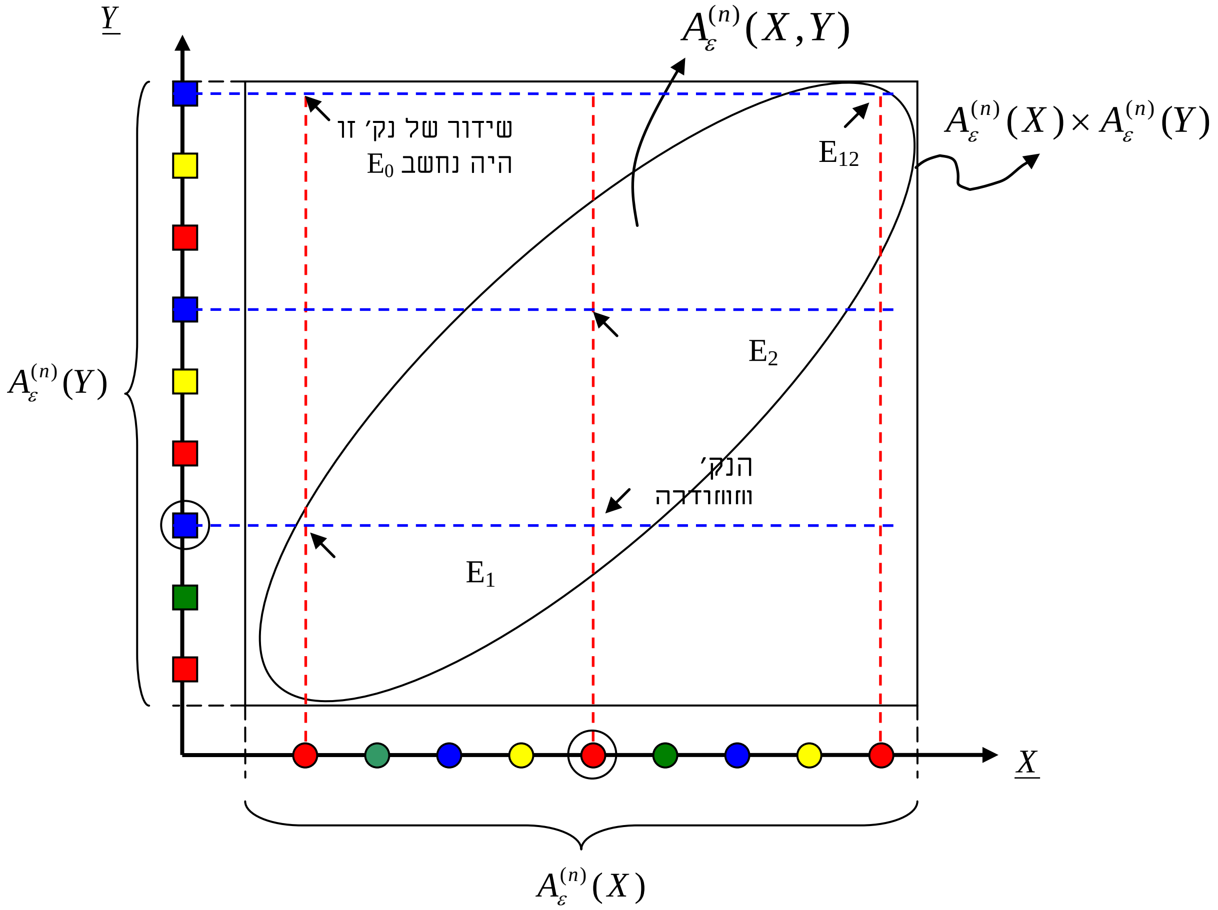
2. E_{12} – המאורע שזוג אחר לחלוטין $(x^{n'},y^{n'})$ ייפול לזוג הבינים ששודר:
מהגדרת הקוד האקראי הסיכוי לקודד את $(x^{n'},y^{n'})$ בבין כפול נתון הוא $2^{-n(R_1+R_2)}$.
מספר הזוגות שהם שונים לחלוטין וגם אופייניים במשותף הוא (עד כדי ε במעריך) $2^{nH(X,Y)}$. לכן לפי חסם האיחוד:

$$\Pr\left\{\bigcup_{(x^n,y^n)\in A_\varepsilon^{(n)}(X,Y)} (f_1(x^n), f_2(y^n))=(i,j)\right\} \le \sum_{(x^n,y^n)\in A_\varepsilon^{(n)}(X,Y)} \Pr\{(f_1(x^n), f_2(y^n))=(i,j)\} =$$

$$= \left|A_\varepsilon^{(n)}(X,Y)\right| \cdot 2^{-n(R_1+R_2)} = 2^{-n[(R_1+R_2)-H(X,Y)-\varepsilon_{12}]}$$

3. E_1 – המאורע שזוג בעל אותו y ו- x אחר $(x^{n'},y^n)$ ייפול לזוג הבינים ששודר:
מהגדרת הקוד האקראי הסיכוי לקודד את $x^{n'}$ בבין נתון הוא 2^{-nR_1}. מספר הזוגות שהם שונים ב-x אך בעלי אותו y וגם אופייניים הוא (עד כדי ε במעריך) $2^{nH(X|Y)}$.
לכן לפי חסם האיחוד ובאותה שיטה כמו בחישוב הקודם:

$$\Pr\{E_1\} \le 2^{-n[R_1-H(X|Y)-\varepsilon_1]}$$



3. E_2 –המאורע הסימטרי ל- E_1 כאשר x זהה לזה שקודד ו- y שונה, שהסתברותו חסומה ע"י:

$$\Pr\{E_2\} \le 2^{-n[R_2-H(Y|X)-\varepsilon_2]}$$

אם נסכם כעת את כל הסתברויות השגיאה השונות נקבל:

$$\Pr(\varepsilon) = \Pr\{E_0 \cup E_1 \cup E_2 \cup E_{12}\} \le \Pr\{E_0\} + \Pr\{E_1\} + \Pr\{E_2\} + \Pr\{E_{12}\} \le$$

$$\le \varepsilon + 2^{-n[R_1-H(X|Y)-\varepsilon_1]} + 2^{-n[R_2-H(Y|X)-\varepsilon_2]} + 2^{-n[(R_1+R_2)-H(X,Y)-\varepsilon_{12}]}$$

כעת ניתן לראות שאם תנאי SW מתקיימים, כאשר n שואף לאינסוף הסתברות השגיאה שואפת לאפס.

הרחבות לבעית Slepian Wolf:

1. Algebraic Binning – כיצד ניתן להשתמש בקודים ליניאריים ליצירת הבינים ? המקרה של מקורות בינאריים סימטריים טופל במאמרים שפורסמו לאחרונה.

2. Zero-error SW – מתי בכלל אפשרי להגיע לשגיאה בהסתברות אפס ממש? מתברר שלא תמיד.

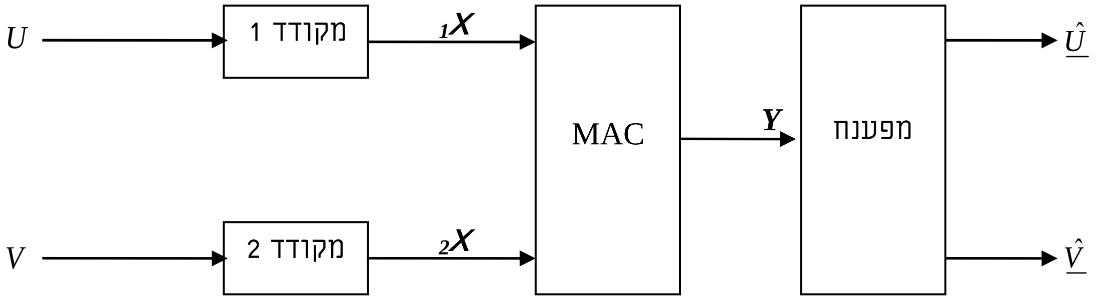
למשל, אם ניקח X ו- Y המחוברים ביניהם בערוץ BSC עם הסתברות חילוף p≠0 , ונקודד בקצב קטן מהטריביאלי , (כלומר לא נשדר את כל הביטים של X^n,Y^n) יש הסתברות גדולה מאפס לשגיאה כי לכל זוג סדרות כלשהו X^n,Y^n יש הסתברות גדולה מאפס לקרות.

נשים לב גם שקידוד באורך משתנה , כמו קידוד Huffman במקרה של מקור בודד , אינו יכול לקחת בחשבון את התלות המשותפת בין X ו- Y עקב הקידוד בנפרד.

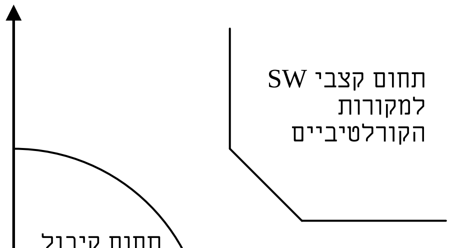
3. עקרון הפרדה לקידוד מקור – ערוץ?

בתקשורת נל "נ אנו מכירים את התוצאה שלפיה קידוד של המידע במקודד מקור אופטימלי ושידור של המידע בקוד אופטימלי לערוץ נותנים יחד את הביצועים האופטימליים האפשריים.

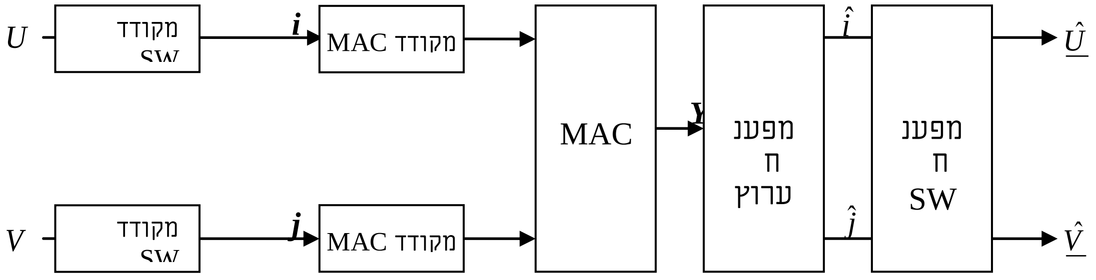
אבל במספר מקורות וערוצים זה לא כך , ונראה דוגמא של חיבור בעיית SW עם ערוץ MAC:



U ו- V הם מקורות קורלטיביים.



אם נתאר בציור את התחומים ברי ההשגה של שתי הבעיות, נוכל לומר שאם יש חיתוך ביניהם, אז ישנה נקודה שבה אפשר לקודד בשני שלבים – קידוד מקור וקידוד ערוץ, כפי שנראה באיור:



נראה דוגמא שבה ניתן לעשות יותר טוב מקידוד בשני שלבים:
ניקח ערוץ MAC מסוג binary adder ומקורות כאלה:

V \ U	**0**	**1**
0	1/3	1/3
1	0	1/3

לערוץ ה- binary adder תחום קיבול המוגבל ע"י $R_1+R_2=1.5bits$, ואילו לפי בעיית SW, ניתן לקודד את U,V רק בקצב: $R_1+R_2\geq H(U,V)=3\cdot 1/3\cdot \log(3)=\log(3)=1.58bits$, כלומר אין חיתוך בין התחומים. מכאן שלא ניתן להעביר את (U,V) על ידי שילוב של קידוד מקור בנפרד וקידוד ערוץ בנפרד.

לעומת זאת, אם במקום לקודד פשוט נשדר את U ו- V בערוץ ה- binary adder, נגלה שאין לנו כל בעיה לפענח אותם ללא שגיאה. אם נקלוט 2 נפענח (1,1), אם נקלוט 0 נפענח (0,0), ואם נקלוט 1 נפענח (0,1) כי לאפשרות השנייה יש הסתברות 0. בצורה זו הפענוח של (U,V) נעשה ללא שגיאה, והצלחנו להעביר מקור כפול בעל אנתרופיה של 1.58bit למרות שהנקודה $R_1+R_2=1.58bit$ היא מחוץ לתחום הקיבול של ה- MAC.
הסיבה לכך שהניסיון להחיל את עקרון ההפרדה לא פועל טוב היא שמערכת הקידוד שלנו לערוץ ה- MAC לא מנצלת את התלות שיש בין הכניסות.

בהמשך הקורס נראה דוגמאות נוספות של בעיות רשת שבהן קידוד נפרד למקורות ולערוצים הוא תת- אופטימלי

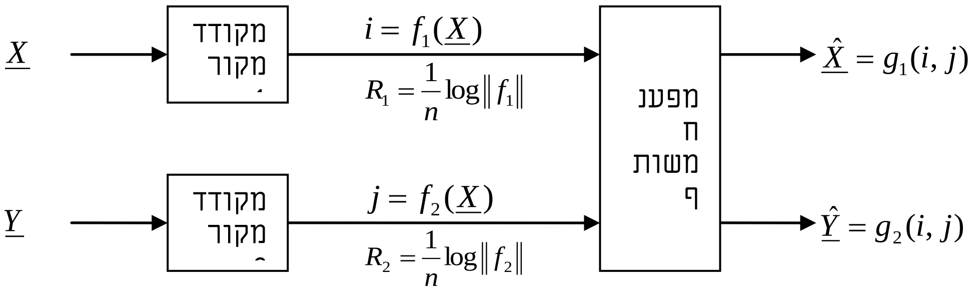
הרצאה – 7

בעיית Slepian-Wolf עם עיוות

סוכם ע"י אמיר אינגבר

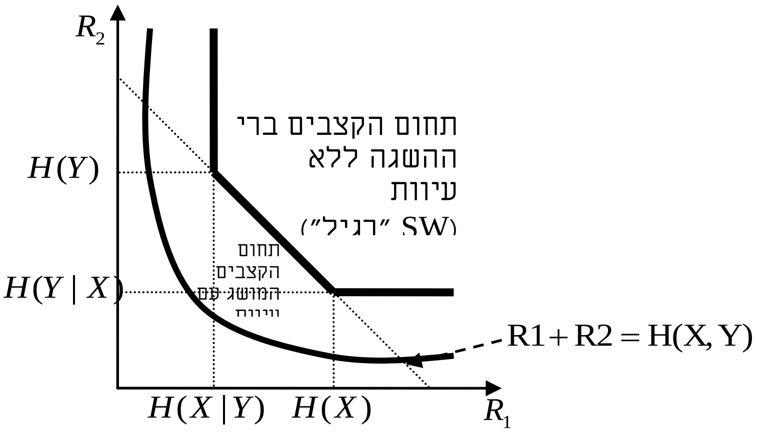
בעיית Slepian-Wolf עם עיוות במקרה הכללי

נתונה מערכת של שני מקורות קורלטיביים: $\underline{X}=(X_1,X_2,,,,X_n),\underline{Y}=(Y_1,Y_2,,,,Y_n)$
המקורות מקודדים באופן נפרד, בקצבים R_1,R_2 [ביטים לדגימת מקור] בהתאמה. המפענח הינו מפענח משותף, והוא משחזר את $\hat{\underline{X}},\hat{\underline{Y}}$ בהתאמה.



ציור 1: מערכת קידוד משותף של מקורות קורלטיביים

בבעיית SW המקורית, נשאלת השאלה "מהו תחום הקצבים ברי ההשגה", כאשר זוג קצבים נקרא "בר השגה" אם קיימת מערכת קידוד-פענוח, עבורה **הסתברות השגיאה** בפענוח קטנה כרצוננו.
במקרה של SW עם עיוות:
מוגדרים שני מדדי עיוות - $d_1(\hat{\underline{X}},\underline{X});d_2(\hat{\underline{Y}},\underline{Y})$ (דוגמאות נפוצות – ריבועי לאותות רציפים / Hamming לאותות בדידים)
בהינתן זוג רמות עיוות ממוצעות D_1,D_2, זוג קצבים R_1,R_2 ייקרא "בר השגה", אם קיימת מערכת קידוד-פענוח, עבורה מתקיים $\frac{1}{n}d_1(\hat{\underline{X}},\underline{X})\le D_1;\frac{1}{n}d_2(\hat{\underline{Y}},\underline{Y})\le D_2$.
השאלה, בדומה לבעיה המקורית:
מהו תחום הקצבים R_1,R_2 ברי ההשגה, ביחס לזוג רמות עיוות ממוצעות D_1,D_2.
צפוי שהתחום ייראה כך:



ציור 2: תחום הקצבים ברי ההשגה עם ובלי עיוות

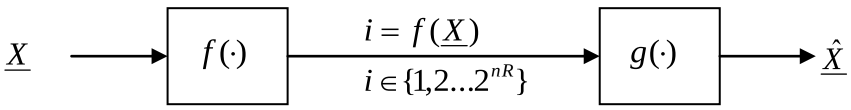
הבעיה הכללית של SW עם עיוות פתוחה כיום (גם למקורות גאוסיים עם מדד עיוות ריבועי).
בסיכום זה יוצגו שתי תתי-בעיות פתורות:

1. בעיית קידוד ללא עיוות עם מסייע (WAK, 1975)
2. פונקצית קצב-עיוות עם מידע-צד במפענח (Wyner-Ziv, 1976)

תחילה – תזכורת בנושא קצב-עיוות:

<u>משפט קצב-עיוות</u>

- נתון **מקור אינפורמציה** $\underline{X} = (X_1, X_2,,,, X_n)$, i.i.d.. מקור זה מקודד ע"י מקודד מקור $f(\cdot)$ בקצב R, ומפוענח (או "משוחזר") ע"י מפענח $g(\cdot)$.



ציור 3 – סכימת קידוד-פענוח מקור

- מוגדר **מדד עיוות:** $d(\hat{\underline{X}}, \underline{X}) = \frac{1}{n}\sum_{i=1}^{n} d(\hat{X}_i, X_i)$, המכמת בכמה הפענוח רחוק מהמקור.

דוגמאות למדדי עיוות נפוצים:

א"ב רציף: עיוות ריבועי: $d(\hat{\underline{X}}, \underline{X}) = \frac{1}{n}\left\|\hat{\underline{X}} - \underline{X}\right\|^2$

א"ב בינארי: עיוות Hamming: $d(\hat{\underline{X}}, \underline{X}) = \frac{1}{n} W_H(\hat{\underline{X}} \oplus \underline{X})$

מדד נוסף : $d(\hat{\underline{X}}, \underline{X}) = W(\underline{X}) \cdot \left\|\hat{\underline{X}} - \underline{X}\right\|^2$ (מדד זה, בניגוד לשני המדדים הקודמים, אינו תלוי רק בהפרש)
קיימים מדדי עיוות נוספים.

- קצב R ייקרא **"בר-השגה"** ביחס לעיוות ממוצע נתון D, אם קיימת מערכת f,g בקצב R, המקיימת את אילוץ העיוות: $E[d(\hat{\underline{X}}, \underline{X})] \le D$. ($R = \frac{1}{n}\log\|f\| \frac{bits}{sample}$)
- **הגדרה אופרטיבית לפונקצית קצב-עיוות:** $R(D) = \inf\{R \mid R - achievable\}$
במלים – R(D) הוא הקצב המינימאלי בו ניתן לקודד עם עיוות ממוצע D בשחזור.
- **הגדרה אינפורמציונית לפונקצית קצב-עיוות** של מקור חסר זיכרון:
$R^*(D) = \inf_{p(\hat{X}/X); E[d(X,\hat{X})] \le D} I(X, \hat{X})$
- **משפט קצב העיוות** (Shannon, 1948, 1959): $R^*(D) = R(D)$

תוצאות:

- מקור גאוסי, עיוות ריבועי:

$$R(D)=\begin{cases}\frac{1}{2}\log(\frac{\sigma^2}{D}) & 0\le D<\sigma^2\\ 0 & D\ge\sigma^2\end{cases}$$

- מקור Bernoulli(p) , עיוות Hamming:

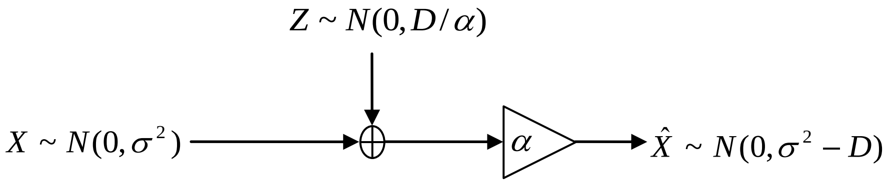
$$R(D)=\begin{cases}H_2(p)-H_2(D) & 0\le D\le\min(p,(1-p))\\ 0 & D\ge\min(p,(1-p))\end{cases}$$

הפילוג המותנה $p^*(\hat{X}\mid X)$ המתאר את הקשר בין המקור לבין הפענוח לאחר העיוות, המשיג את המינימום עבור פונקצית הקצב-עיוות האינפורמציונית, נקרא Optimal test-channel.

לדוגמא:

$D<\sigma^2\ ,X\sim N(0,\sigma^2)$

ה-optimal test-channel שמשיג עיוות D בקצב של $\frac{1}{2}\log(\frac{\sigma^2}{D})$, הוא:



ציור 4 – Optimal test-channel עבור המקרה הגאוסי-ריבועי

כאשר Z,X הינם בת"ס, ו- $\alpha=1-\frac{D}{\sigma^2}$.

עבור פילוג זה, מתקיים : $I(X,\hat{X})=\frac{1}{2}\log(\frac{\sigma^2}{D})$, וזהו הערך המינימאלי המושג.

- **החסם של שנון**: עבור מדד עיוות ריבועי, מתקיים $R(D)\ge h(X)-\frac{1}{2}\log(2\pi eD)$, כאשר h(x) מציין את האנטרופיה הדיפרנציאלית של המקור.
- קיימות גם גרסאות לחסם עבור מדדי עיוות הפרשיים כלליים.

הוכחת משפט הקצב-עיוות:

נתון $p(\hat{X}\mid X)$.

1) ניצור ספר קוד אקראי $\underline{\hat{X}}(i);i=1,2,...,2^{nR}$, לפי הפילוג השולי $\hat{X}\sim p(\hat{X})$, i.i.d. בתוך מילות הקוד וביניהן.
2) קידוד אופייניות משותפת(חזקה): בהינתן x^n, נקודד את אותו i שעבורו מתקיים ש- $\underline{\hat{X}}(i),x^n$ אופייניים במשותף במובן החזק ביחס לפילוג המשותף: $p(\hat{X},X)=p(\hat{X}\mid X)p(X)$. אם אין i כזה, נקודד "ESC". (נראה שההסתברות לכך זניחה)
3) פענוח – לפי ספר הקוד $\underline{\hat{X}}(i);i=1,2,...,2^{nR}$.

ניתוח הסכמה:

א. מאורע שגיאה: אף מילה $\underline{\hat{X}}(i)$ אינה אופיינית במשותף עם מלת המקור:

לכל i, ההסתברות שמלת הקוד $\underline{\hat{X}}(i)$ אופיינית חזק במשותף עם $\underline{X}$ גדולה מ-

$2^{-nI(X,\hat{X})}$ (עד כדי ε באקספוננט). לכן הסיכוי שאף אחת מ-$M=2^{nR}$ מילות הקוד

תהיינה אופיינית חזק במשותף עם $\underline{X}$ קטנה מ-$(1-2^{-nI(X,\hat{X})})^M$, או

$p_e \le (1-2^{-nI(X,\hat{X})})^M$.

נפעיל את החסם $1-t \le e^{-t}$, ונקבל:

$$p_e \le (1-2^{-nI(X,\hat{X})})^M \le (e^{-2^{-nI(X,\hat{X})}})^M = e^{-2^{-nI(X,\hat{X})}2^{nR}} = e^{-2^{-n(I(X,\hat{X})-R)}} \xrightarrow[n\to\infty]{} 0$$

כאשר מתקיים $R > I(X,\hat{X})$.

כלומר – הסיכוי לשגיאה במקודד שואף ל-0 עם n.

ב. העיוות המתקבל:

כאמור, ה- $\underline{\hat{X}}(i)$ המתקבל, אופייני במשותף (אופייניות חזקה) עם מלת

המקור - x^n. העיוות המתקבל, אם כן, הוא:

$$\frac{1}{n}\sum_{i=1}^{n} d(x_i,\hat{X}_i) = \frac{1}{n}\sum_{a\in\chi}\sum_{b\in\hat{\chi}} N_{ab}(x^n,\underline{\hat{X}})\cdot d(a,b) \approx \sum_{x,\hat{x}} p(x,\hat{x})d(x,\hat{x}) = E_{x,\hat{x}}\left[d(x,\hat{x})\right] \le D$$

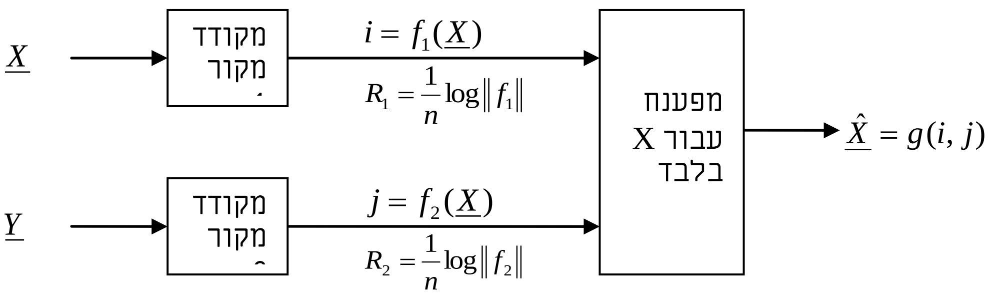
כאשר המעבר השני נובע מהאופייניות החזקה, והשלישי - מהאילוץ על הפילוג המשותף.

כיוון שבממוצע על פני כל ספרי הקוד, קיימת עמידה בתנאי העיוות, אזי קיים לפחות ספר קוד אחד העומד בתנאי העיוות (במובן שכמעט לכל סדרת מקור סבירה תהיה בספר זה מלת מקור במקיימת את תנאי העיוות).

בעיית קידוד מקור ללא עיוות עם מסייע (WAK - Wyner, Ahlswede, Körner, 1975)

נתונה מערכת של שני מקורות קורלטיביים: $\underline{X}=(X_1,X_2,,,,X_n),\underline{Y}=(Y_1,Y_2,,,,Y_n)$

המקורות מקודדים באופן נפרד, בקצבים R_1,R_2 בהתאמה. המטרה היא לפענח את X בלבד, עם הסתברות שגיאה קטנה כרצוננו (Lossless in the Shannon sense).



ציור 5: מערכת קידוד מקור עם מסייע

ניתן לחשוב על Y המשודר כעל מעין מסייע לפענוח X. Y מעביר את ה"הקשר" של אות המקור X, ובכך מסייע לפענוח.

זוהי למעשה תת-בעיה של בעיית SW הכללית:

העיוות המותר עבור X הוא 0, כאשר פונקצית העיוות של X מקיימת $\underline{X} = \underline{\hat{X}} \Leftrightarrow d_1(\underline{\hat{X}}, \underline{X}) = 0$ (העיוותים הנפוצים מקיימים תכונה זו).

העיוות המותר עבור Y הוא המקסימאלי, לדוגמא ${\sigma_Y}^2$ עבור עיוות ריבועי, $\frac{1}{2}$ עבור עיוות המינג.

<u>משפט הקידוד:</u>

זוג קצבים R_1, R_2 ייקרא "בר השגה", אם קיימת מערכת קידוד-פענוח, עבורה מתקיים $\Pr(\underline{\hat{X}} \neq \underline{X}) \xrightarrow{n\to\infty} 0$. נגדיר את $\Re_{WAK}$ בתור תחום הקצבים ברי ההשגה (הגדרה אופרטיבית).

הגדרה אינפורמציונית:

נגדיר: $\Re^*_{WAK}(V) = \left\{(R_1, R_2) \mid R_1 \geq H(X/V); R_2 \geq I(Y;V)\right\}$,

ואז: $\Re^*_{WAK}(V) = \bigcup_{V: X \leftrightarrow Y \leftrightarrow V} \Re^*_{WAK}(V)$, עבור

המשפט: $\Re^*_{WAK} = \Re_{WAK}$

הוכחת המשפט: (Achievability)

1) יצירת ספר קוד, E, לפי $p(v/y)$, בקצב R_2. v הוא למעשה y מעוות. יצירת ספר הקוד הינה בדיוק כמו במשפט הקצב-עיוות הרגיל.
יצירת ספר קוד, E_2, לפי Binning אקראי ואחיד, של וקטורי X בקצב R_1.
2) קידוד:
מקודד 1 מחפש $v^n(i) \in E$, האופייני במשותף עם y^n, לפי $p(v,y)$, ומשדר את i.
מקודד 2 מחפש את הBin ה-j שבו נמצא x^n, ומשדר את j.
3) פענוח:
מפענחים את v^n לפי i: $v^n = g_2(i)$, לפי ספר הקוד E.
מפענחים את x^n לפי v^n ו-j: $\hat{x}^n = g_1(v^n, j)$ - נחפש בBin ה- j x^n אופייני במשותף עם v^n, לפי הפילוג $p(x,v) = \sum_y p(x,y)p(v/y)$.

ניתוח מאורעות השגיאה:

מאורע א. הזוג x^n, y^n שנוצר ע״י זוג המקורות אינו טיפוסי במשותף. ידוע שההסתברות לכך דועכת ל-0 עם n, כיוון ש X,Y נוצרו מה״טבע״ לפי הפילוג המשותף הנ״ל.

מאורע ב. המלה y^n טיפוסית, אבל לא קיים $v^n(i) \in E$ שטיפוסי איתו במשותף. גם הסתברות זו קטנה כרצוננו עם הגדלת n, כי $R_2 \geq I(Y;V)$, כלומר יש ״מספיק״ מלות קוד ב-E (לפי תורת הקצב-עיוות).

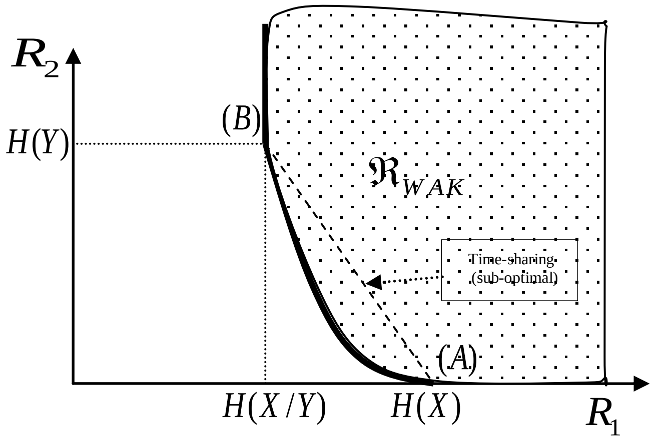
מאורע ג. מלת הקוד $v^n(i) \in E$ אינה טיפוסית במשותף עם x^n. כיוון ש- $X \leftrightarrow Y \leftrightarrow V$, ולפי למת מרקוב* – חלק א', ההסתברות למקרה כנ״ל שואפת ל-0.

מאורע ד. ישנה מלה $\tilde{x}^n$ נוספת באותו ה-Bin, שטיפוסית במשותף עם $v^n(i)$.
ההסתברות שמלה אחרת תהיה טיפוסית במשותף עם $v^n(i)$ חסומה ע״י $2^{-nI(X,V)}$, (למת מרקוב*, חלק ב') ולכן ההסתברות לשגיאה חסומה ע״י:

$$|Bin_j \cap A_\varepsilon^{*(n)}| \cdot 2^{-nI(X,V)} \leq 2^{nH(X)} 2^{-nR_1} 2^{-nI(X,V)} = 2^{-n(R_1 - I(X/V))}$$

וכיוון שמתקיים $R_1 \geq H(X/V)$, הביטוי הנ״ל דועך ל-0.

הצגה גראפית של הפתרון:



ציור 6: התחום $\Re_{WAK}$

הנקודה (A): לא מעבירים מידע על Y – לכן (Shannon) יש להעביר מידע בקצב H(X).
כאן, V הוא קבוצה ריקה, ומתקיים I(Y;V)=0.

הנקודה (B): מעבירים את כל המידע שניתן להעביר על Y – בקצב H(Y), ולכן (-Slepian Wolf) נותר להעביר מידע על X בקצב של H(X/Y). כאן למעשה V=Y, ומתקיים I(Y,V)=H(Y).

קידוד בשיטת Time-Sharing בין (A) ל-(B) יהיה תת-אופטימאלי, כפי שניתן לראות בשרטוט.

***למת מרקוב**: אם $\underline{v}$ אופייני-ε חזק במשותף עם $\underline{y}$ לפי $p(v,y)=p(y)p(v|y)$, וכן $\underline{x},\underline{y}$ מתפלגים במשותף i.i.d. לפי $p(x,y)$, אזי:

א. בהסתברות גבוהה, $\underline{v}$ אופייני חזק במשותף עם $\underline{x}$ לפי הפילוג $p(x,v)=\sum_{y} p(x,y)p(v|y)$ (כלומר – פילוג משותף מרקובי: $X \leftrightarrow Y \leftrightarrow V$).

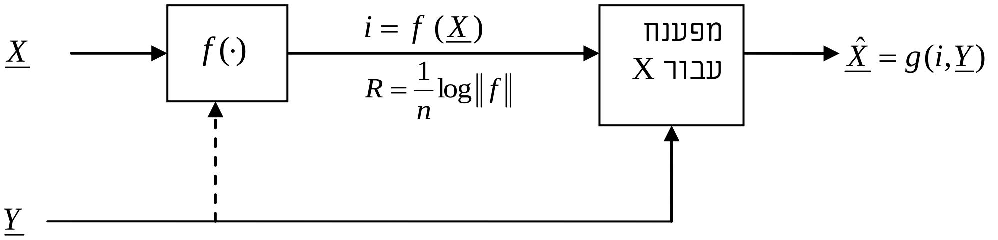
ב. הסיכוי ש-$\underline{v}$ יהיה אופייני במשותף עם וקטור $\tilde{\underline{x}}$, המוגרל i.i.d. לפי p(x), באופן בת"ס ב-$\underline{x}$ הוא $\approx 2^{-nI(X,V)}$, כאשר האינפורמציה ההדדית I(X,V) מחושבת לפי הפילוג $p(x,v)$ שהוגדר לעיל.

<u>פונקצית קצב-עיוות עם מידע-צד במפענח (Wyner-Ziv, 1976)</u>

תיאור הבעיה:

נתונה מערכת של שני מקורות קורלטיביים: $\underline{X}=(X_1,X_2,,,,X_n),\underline{Y}=(Y_1,Y_2,,,,Y_n)$

המקור X מקודד בקצב R. המטרה הינה לפענח את $\hat{\underline{X}}$, בעיוות ממוצע D.



ציור 7: מערכת קידוד מקור עם מידע צד

גם כאן מוגדר מדד עיוות: $d(\hat{\underline{X}},\underline{X})=\frac{1}{n}\sum_{i=1}^{n} d(\hat{X}_i,X_i)$.

השאלה הנשאלת היא, מהו הקצב המינימאלי, בו ניתן לקודד את X, עבור עיוות ממוצע נתון D.

מקרה א' – המקודד והמפענח יודעים את Y. נסמן קצב זה ב-$R_{X/Y}(D)$ ("פונקצית הקצב-עיוות המותנית").

מקרה ב' (המקרה המעניין יותר) – המפענח בלבד יודע את Y. נסמן קצב זה ב-$R_{X/Y}^{WZ}(D)$.

התוצאות במקרה הכללי:

$$R_{X/Y}(D)=\min_{E[d(X,\hat{X})\le D} I(X;\hat{X}|Y)$$

$$R_{X/Y}^{WZ}(D)=\min_{U:U\leftrightarrow X\leftrightarrow Y;\hat{X}=g(U,Y);E[d(X,\hat{X})\le D} I(X;U|Y)$$

ומתקיים $R_{X/Y}^{WZ}(D)\ge R_{X/Y}(D)$. (זאת בניגוד לבעיית SW [D=0], שם מתקיים $R_{X/Y}^{SW}(D)=H(X|Y)$)

תוצאות פרטיות:

במקרה הגאוסי-ריבועי[1]: $X,Y \sim N(\underline{\mu},\Lambda)$, $d(\underline{\hat{X}},\underline{X})=\frac{1}{n}\left\|\underline{\hat{X}}-\underline{X}\right\|^2$.

$$R_{X/Y}(D)=R^{WZ}_{X/Y}(D)=\begin{cases}\frac{1}{2}\log\left(\frac{VAR(X|Y)}{D}\right) & if\ 0\le D\le VAR(X|Y)\\ 0 & o.w.\end{cases}$$

במקרה הבינארי-המינג: $X=\begin{cases}0 & w.p.0.5\\ 1 & w.p.0.5\end{cases}$, $d(\underline{\hat{X}},\underline{X})=\frac{1}{n}W_H(\underline{\hat{X}}\oplus\underline{X})$

Y,X מחוברים דרך BSC, עם הסתברות חילוף p_0 .

$$R_{X/Y}(D)=\begin{cases}H_2(p_0)-H_2(D) & 0\le D\le p_0\\ 0 & D>p_0\end{cases}$$

פתרון עבור $R^{WZ}_{X/Y}(D)$:

נגדיר: $g(D)=\begin{cases}H_2(p_0*D)-H_2(D) & 0\le D\le p_0\\ 0 & o.w.\end{cases}$,

כאשר $a*b\triangleq a(1-b)+b(1-a)$, עבור $0\le a,b\le 1$. ("קונבולוציה בינארית")

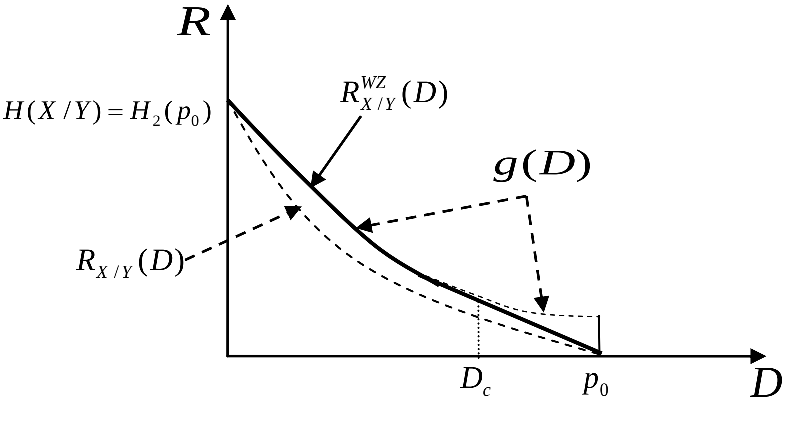
הפתרון: $R^{WZ}_{X/Y}(D)=\inf_{\theta,\beta}\left[\theta(H_2(p_0*\beta)-H_2(\beta))\right]$, כאשר מתקיים $D=\theta\beta+(1-\theta)p_0$.

או לפי מקרים: $R^{WZ}_{X/Y}(D)=\begin{cases}g(D) & 0\le D\le D_c\\ \frac{g(D_c)}{D_c-p_0}(D-p_0) & D_c\le D\end{cases}$

כאשר נקודת ההשקה $(D_c,g(D_c))$ של הישר המסתיים ב $(p_0,0)$ עם הפונקציה $g(D)$,

מוגדרת ע"י הפתרון למשוואה: $\frac{g(D_c)}{D_c-p_0}=g'(D_c)$.

הצגה גראפית של הפיתרון:



ציור 8: $R^{WZ}_{X/Y}(D)$ במקרה הבינארי-המינג

נציג סקיצה של המשפט הישר: $R^{WZ}_{X/Y}(D)=\min_{U:U\leftrightarrow X\leftrightarrow Y;\hat{X}=g(U,Y);E[d(X,\hat{X})\le D} I(X;U|Y)$

נתונים: מ"א U, המקיים $U\leftrightarrow X\leftrightarrow Y$, וכן פונקציה $g(\bullet,\bullet)$. נראה סכמה המשיגה כל קצב גדול מ- $I(X;U|Y)$.

[1] לדיון מפורט על המקרה הגאוסי (Gaussian WZ) ראה חוברת הרצאות 2006.

1) ספר קוד: צור ספר קוד, $\underline{u}(i); i=1,2,...,2^{nR_1}$, לפי הפילוג p(u), בקצב $R_1 = I(X;U)+\varepsilon$. פזר את מילות הקוד באופן אקראי בין 2^{nR} בינים ($R \le R_1$).
יידע את המקודד ואת המפענח לגבי ספר הקוד והחלוקה לבינים.

2) קידוד: מצא $\underline{u}(i)$, שאופיינית חזק במשותף עם $\underline{x}$ לפי p(x,u), ושדר את האינדקס j של הבין שמכיל את $\underline{u}(i)$.

3) פענוח: מצא $\underline{u}(i)$ בתוך בין j, שאופיינית במשותף עם אינפורמציית הצד $\underline{y}$. שחזר את $\underline{x}$ איבר-איבר לפי g(u,y), כלומר $\hat{x}_k = g(u(i)_k, y_k)_{k=1..n}$.

מאורע שגיאה עיקרי: כדי למנוע רב-משמעות, צריך (לפי הלמה המרקובית) שמספר במילים בבין ה-j לא יעלה על $2^{n[I(U;Y)-\varepsilon]}$. כלומר – נדרוש $R_1 - R \le I(U;Y) - \varepsilon$:

$$R \ge R_1 - I(U;Y) + \varepsilon = I(X;U) - I(U;Y) + 2\varepsilon = H(U/Y) - H(U/X) + 2\varepsilon =$$
$$H(U/Y) - H(U/X,Y) + 2\varepsilon = I(X;U/Y) + 2\varepsilon$$

ולכן הדרישה מתקיימת אם $R \ge I(X;U/Y)$.

מקורות נוספים בהם נעזרתי בסיכום השיעור:

[1] Elements of Information Theory – Cover & Thomas, 1991
[2] The Rate-Distortion Function for Source Coding with Side Information an the Decoder – Wyner & Ziv, 1976

הרצאה 8-9

The Broadcast Channel

Summarized by Zak Levi.

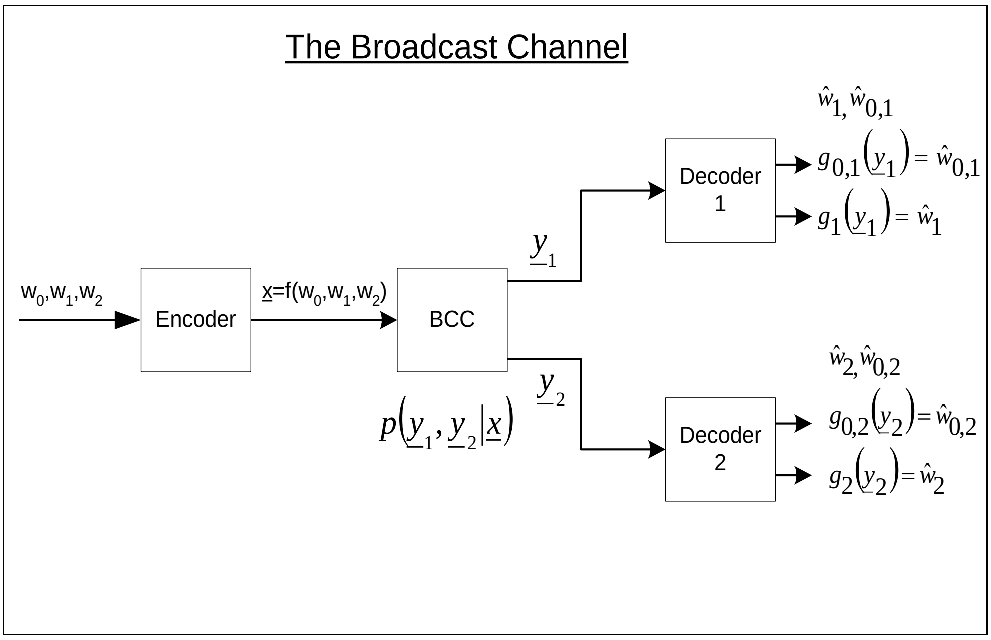
The Broadcast Channel an Overview

The Broadcast Channel (BCC) scenario occurs when a single transmitter wishes to transmit information to several distinct users. For simplicity we shall introduce some limiting assumptions:

- The broadcast transmitter can transmit a single stream of information (a scalar transmitter)
- Only two distinct scalar receivers are assumed

In the sequel we shall introduce several more limiting assumptions since unfortunately (or fortunately) the general BCC problem remains unsolved till this day. Figure 1gives an illustration of the BCC

Figure 1



Where:

$w_0 \in \{1,\ldots,2^{nR_0}\}$ – common message

$w_1 \in \{1,\ldots,2^{nR_1}\}$ – private message for user 1

$w_2 \in \{1,\ldots,2^{nR_2}\}$ – private message for user 2

R_0, R_1, R_2 – rates $\left[{}^{bit}\!/\!_{channel\ use}\right]$

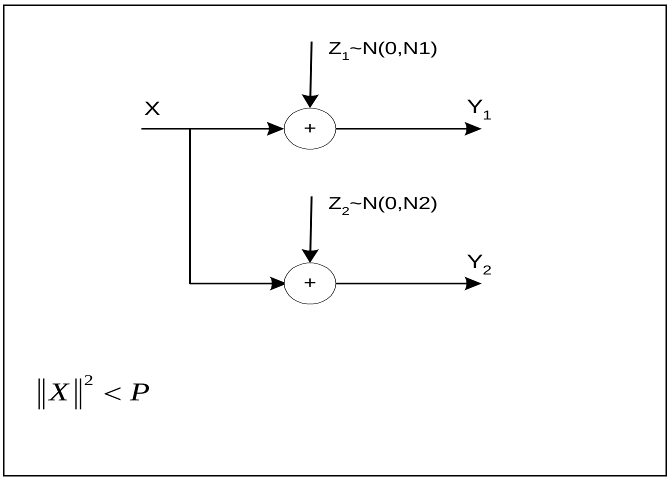
We define the probability of error as

$$P_e = \Pr\{\hat{w}_{0,1} \neq w_0 \cup \hat{w}_1 \neq w_1 \cup \hat{w}_{0,2} \neq w_0 \cup \hat{w}_2 \neq w_2\}$$

Let us consider two examples before going on with the analysis

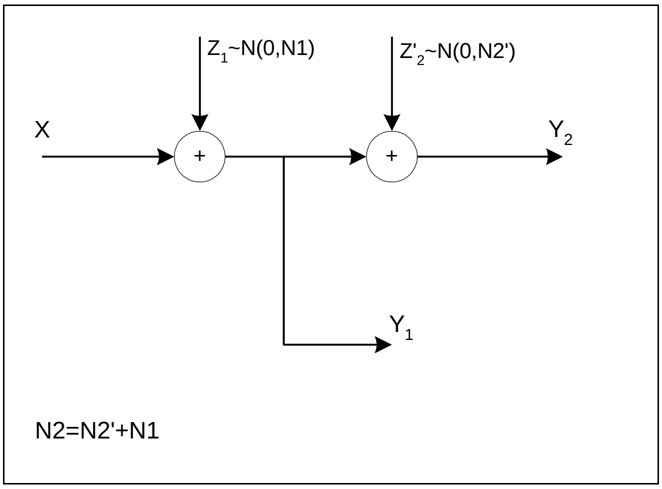
Example 1 Gaussian BCC with power constraint

Figure 2



The noise terms Z1 and Z2 may or may not be independent (only the marginal distributions are of interest since the receivers cannot cooperate). With no loss of generality N2>N1 and assume Z2=Z1+Z'2, where Z1 and Z'2 are independent. Since the two receivers cannot cooperate one may consider the following statistically equivalent communication scenario:

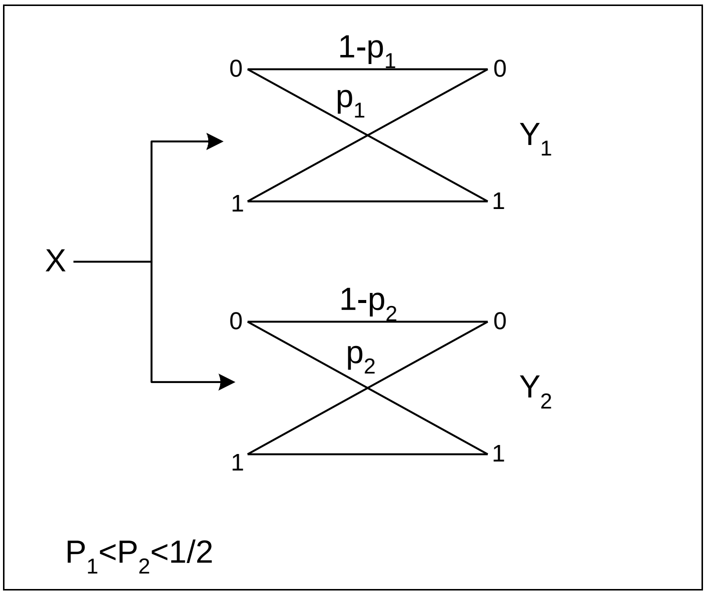
Figure 3



The above scenario is referred to as a **Physically Degraded BCC** since Y2 is a degraded version of Y1

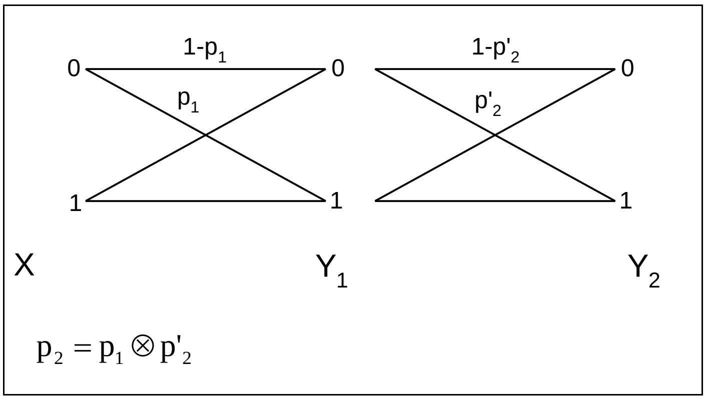
Example 2 The Binary BCC

Figure 4



Once again whether or not the two BSC's are independent, since the rwo receivers cannot cooperate, we can consider a physically degraded model depicted in Figure 5, which is statistically equivalent to the channel in Figure 4.

Figure 5



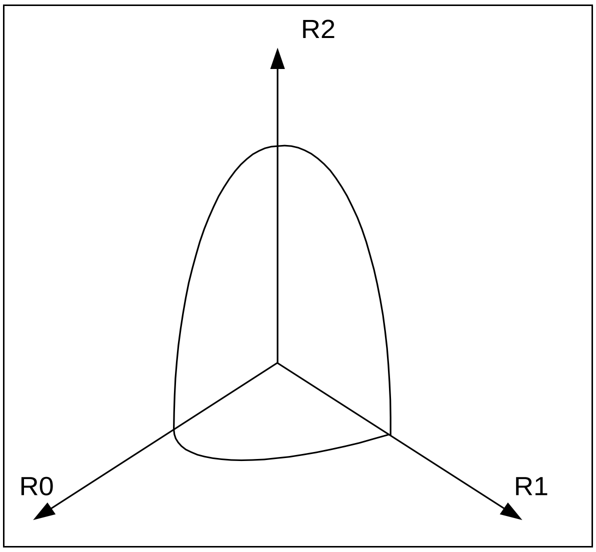
Operative Capacity Region

Let us define the probability of error to be:

$$P_E = \Pr\{\hat{w}_{0,1} \neq w_0 \cup \hat{w}_1 \neq w_1 \cup \hat{w}_{0,2} \neq w_0 \cup \hat{w}_2 \neq w_2\}$$

A rate triplet (R0,R1,R2) is said to be achievable if there exist a series of systems $(f, g_{0,1}, g_1, g_{0,2}, g_2)$ with a dimension (block length) going to infinity such that $P_E \xrightarrow[n\to\infty]{} 0$. **The operative capacity region C_{Bcc} is defined as the closure of all achievable rate triplets**.

Figure 6: Capacity Region Illustration



Let's highlight some problematic issues that arise due to the nature of the BCC

- The channels between X and Y1 and between X and Y2 can be completely different thus their optimal codebooks can be completely different. The common codebook must then make a compromise between the two channels.
- If both channels are of the same type and one has a higher capacity then the other. If one wishes to transmit common information only, then the channel with the higher capacity will not be able to benefit from his superiority.

One may think of time-sharing as a logical solution, such that the transmitter transmits information to receiver 1 and 2 in a TDMA fashion. This approach turns out to be sub-optimal since it does not span the entire capacity region. It turns out that for degraded channels one can span the entire capacity region using superposition coding. In the general non-degraded scenario superposition coding although superior to TDMA still is only sub-optimal. To give a notion of what superposition coding is about consider the following example.

Spanish and Dutch speaker Example (Cover&Thomas Ex 14.6.4)

Consider a speaker who can speak both Spanish and Dutch. There are two listeners: one understands only Spanish and the other understands only Dutch. We assume that a Dutch listener, even though he does not understand Spanish, can recognize when the word is Spanish. Similarly, the Spanish speaker can recognize when the word is in Dutch. The speaker can then convey extra information intelligible to both listeners by the timing of the use of Spanish or Dutch in each word.

The Degraded BCC

The channel transition probability law defines the BCC and is given by

$$P(y_2, y_1|x)$$

If the channel transition probability can be written as

$$(1)\quad P(y_2|x) = P(y_1|x)\cdot P(y_2|y_1)$$

Then the channel is said to be statistically degraded. Note that the fact that a channel is statistically degraded does not mean that it is physically degraded. To illustrate the difference the reader is referred to Figure 2 and Figure 3. Figure 3 depicts a non-degraded physical channel, however since (1) holds, figure 2 is statistically equivalent to figure 3, which is degraded. Thus the channel in figure 2 is statistically degraded where the one in figure 3 is physically degraded.

It turns out that one can prove the following theorem: The capacity region of a statistically degraded channel and its physically degraded equivalent is identical given that receivers at each end cannot cooperate.

This implies that only the marginal pdf's

$$P(y_1|x) = \sum_{y_2} P(y_1, y_2|x)$$
$$P(y_2|x) = \sum_{y_1} P(y_1, y_2|x)$$

Have effect on the capacity region.

Coding Theorem for the statistically Degraded BCC

Define the information capacity region such that:

$$C^*_{Bcc}(U) = \left\{ (R_1, R_2) : \begin{matrix} R_2 \le I(U;Y_2) \\ R_1 \le I(U;Y_1|U) \end{matrix} \right\}$$
$$C^*_{Bcc} = closureconvexhall\{\cup C^*_{Bcc}(U)\}$$
$$\{U : U \leftrightarrow X \leftrightarrow (Y_1, Y_2)\}$$
$$|U| \le \min\{|X|, |Y_1|, |Y_2|\}$$

Where with no loss of generality receiver 1 is assumed to be the better receiver and any common message is encoded with the codebook intended for receiver 2, and so can be decoded by both receivers.

Theorem: For a Statistically Degraded BCC

$C_{Bcc} = C^*_{Bcc}$

And thus

- **Converse**: Any achievable rate pair $(R_0, R_1) \in C^*_{Bcc}$
- **Direct**: Any $(R_0, R_1) \in \underline{C}^*_{Bcc}$, where $\underline{C}^*_{Bcc}$ is C^*_{Bcc} without the boundary points.

Description of an achieving system

Assume P(u,x), we need to show that there exists a scheme that can achieve any rate pair in $C^*_{Bcc}(U)$ for any random variable U satisfying the conditions stated in the theorem. The proof was not given in class however a description of a system that achieves the capacity region is given in the sequel

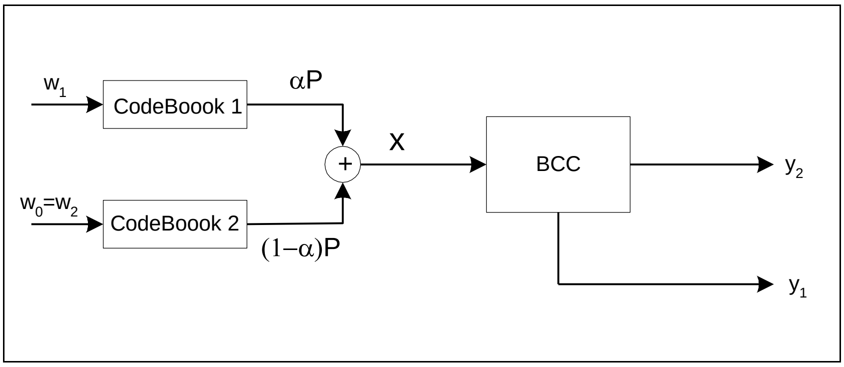
Codebook Construction

Generate 2^{nR2} words such that each word is generated randomly in an i.i.d fashion from the probability law P(u). The resulting codebook shall be denoted by U(1),U(2), . . . U(M_2) where $M_2=2^{nR2}$

For each codeword U(i) in the codebook generate an individual codebook in a random i.i.d fashion using the probability law P(x|U(i)). The resulting codebook shall be denoted by X(i,1),X(i,2), . . .,X(i,M_1) where $M_1=2^{nR1}$

The above encoding is termed Superposition Coding illustrated in the following figure.

Figure 7



The encoder employs two separate codebooks that sum up together at the encoder output

Transmission of the (i = W_2, j =W_1) message

Transmit $\underline{x}$ = X(i,j).

Decoding

<u>Receiver 2 (The bad receiver)</u>

The receiver searches for the codeword U(i) which is jointly typical with $\underline{y}$2 according to the probability law P(u,$\underline{y}$2). The decoding will succeed if R2≤I(U;Y2)

Receiver 1 (The good receiver)
The receiver searches for the pair (U(i),Xj) that are jointly typical with y1 according to the probability law P(y1,x,u). This is equivalent to searching for the codeword U(i) which is jointly typical with y1 according to the probability law P(u,y1) and then searching for for Xj that is jointly typical with y1 with respect to the probability law P(x,y1|U(i)). The first step will succeed since R2<I(U,Y2) implies that R1<I(U,Y1) the second step will succeed if R1≤I(x;y1|U).

Achievability Proof
Without loss of generality assume that the message pair $(W_1,W_2)=(1,1)$ was sent. We denote as P(.) the conditional probability of an event given that (1,1) was sent. Since that channel from U to Y_2 is essentially a single user channel we will be able to decode the U code words with high probability as n->∞ if $R_2<I(U;Y_2)$. To prove this define the events

$$E_{Y_i} = \{U(i), Y_2 \in A_\varepsilon^{(n)}\}$$

The probability of error at receiver 2 is given by

$$P_e^{(n)}(2) = P\left(E_{Y_1}^C \cup \cup_{i\neq 1} E_{Y_i}\right)$$
$$(1) \leq P\left(E_{Y_1}^C\right) + \sum_{i\neq 1} E_{Y_i}$$
$$(2) \leq \varepsilon + 2^{nR_2} 2^{-n(I(U;Y_2))-2\varepsilon} = \varepsilon + 2^{-n(I(U;Y_2)-R_2)-2\varepsilon}$$
$$(3) \leq 2\varepsilon$$

Where
1. Follows from the union bound
2. Since the probability that a wrong message be jointly typical with the channel output is uniform and given by $2^{-nI(U;Y2)-2e}$ (AEP)
3. Since $R_2<I(U;Y_2)$ and n is large enough

Similarly, for decoding of receiver 1, we define the following events
$$\tilde{E}_{Y_i} = \{(U(i), Y_1) \in A_\varepsilon^{(n)}\}$$
$$\tilde{E}_{Y_{ij}} = \{(U(i), X(i,j), Y_1) \in A_\varepsilon^{(n)}\}$$

The error probability is given by

$$P_e^{(n)}(1) = P\left(\tilde{E}_{Y_1}^C \cup \cup_{i\neq 1} \tilde{E}_{Y_i} \cup \cup_{j\neq 1} \tilde{E}_{Y_{1j}}\right)$$
$$(1) \leq P\left(\tilde{E}_{Y_1}^C\right) + \sum_{i\neq 1} P\left(\tilde{E}_{Y_i}\right) + \sum_{j\neq 1} P\left(\tilde{E}_{Y_{1,j}}\right)$$

Where (1) follows from the union bound. By the same arguments as for receiver 2, we can bound $P\left(\tilde{E}_{Y_i}\right) \leq 2^{-n(I(U;Y_1)-3\varepsilon)}$. And so the second term goes to 0 if R2<I(U;Y1). But by the data processing inequality and the degraded nature of the channel I(U;Y1)≥I(U;Y2), and hence the conditions of the theorem imply that the second term goes to 0.

The third term in the error probability can be bounded by

$$
\begin{aligned}
P\left(\tilde{E}_{Y_{1,j}}\right) &= P\left(\left(U(1), X(1,j), Y_1\right) \in A_\varepsilon^{(n)}\right) \\
&= \sum_{(U,X,Y_1)\in A_\varepsilon^n} P\left(\left(U(1), X(1,j), Y_1\right)\right) \\
&= \sum_{(U,X,Y_1)\in A_\varepsilon^n} P\left(\left(U(1), X(1,j)\right) \middle| U(1)\right) P\left(Y_1 \middle| U(1)\right) \\
&\le \sum_{(U,X,Y_1)\in A_\varepsilon^n} 2^{-n(H(U)-\varepsilon)} 2^{-n(H(X|U)-\varepsilon)} 2^{-n(H(Y_1|U)-\varepsilon)} \\
&\le 2^{n(H(U,X,Y_1)+\varepsilon)} 2^{-n(H(U)-\varepsilon)} 2^{-n(H(X|U)-\varepsilon)} 2^{-n(H(Y_1|U)-\varepsilon)} \\
&= 2^{-n(I(X;Y_1|U)-4\varepsilon)}
\end{aligned}
$$

Thus if R1<I(X;Y1|U), the third term in the probability of error goes to zero. Thus error probability can be bounded by:

$$
P_e^{(n)}(1) \le \varepsilon + 2^{-n(I(U;Y_1)-R_2-3\varepsilon)} + 2^{-n(I(X;Y_1|U)-R_1-4\varepsilon)}
$$

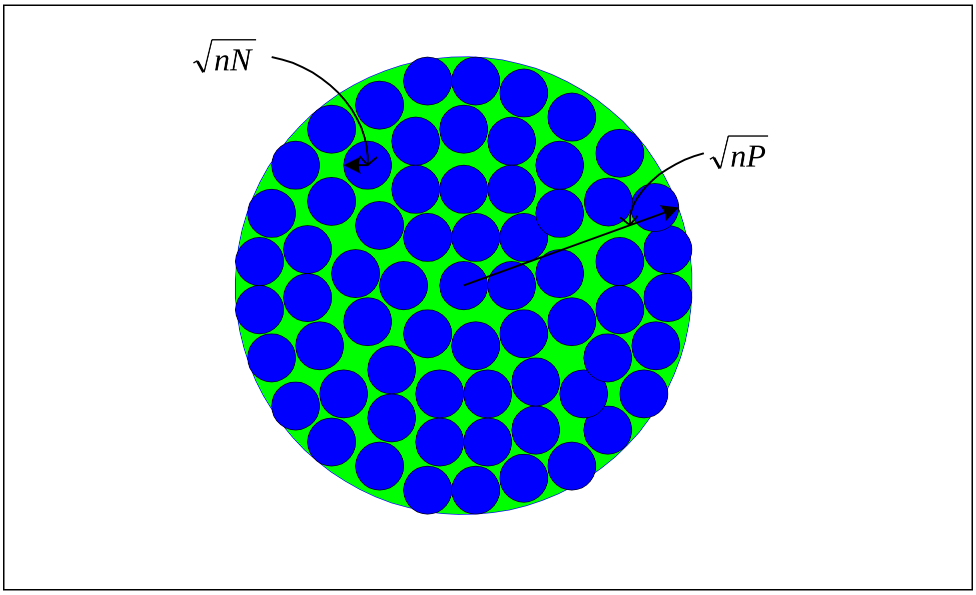
And so if n is large enough and R2≤I(U;Y1) and R1≤I(X;Y1|U) then the probability of error goes to zero. Thus the conditions on R1 and R2 following from the above is that the R2≤I(U;Y2) and R1≤I(X;Y1|U).

To get a better understanding of superposition encoding it is instructive to look at a geometric interpretation of the two codebooks.

Geometric Interpretation to superposition coding

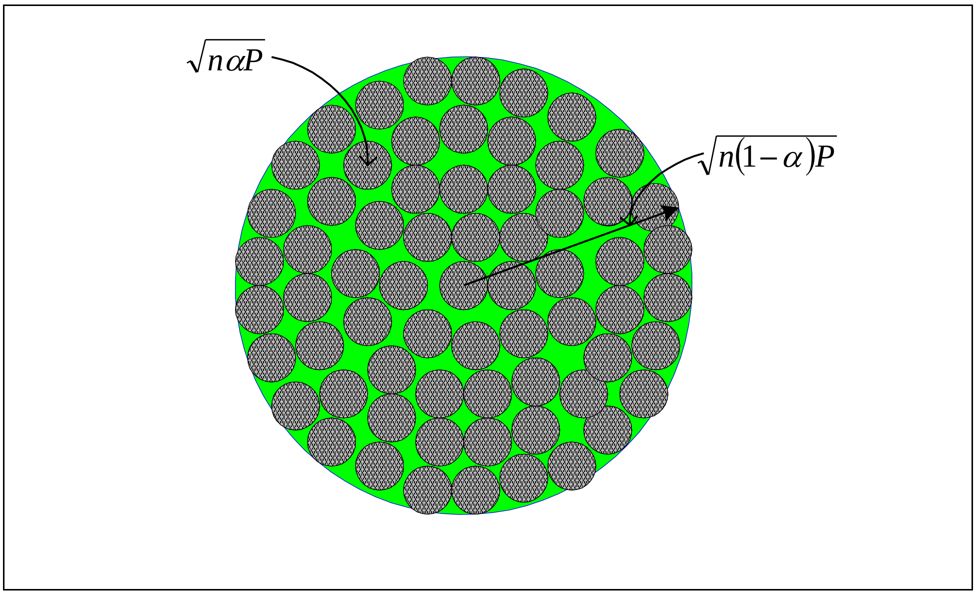
For the Gaussian channel with power constraint P the capacity achieving codebook can be thought of as made up of 2^{nC} code words. Each code word can be thought of as a point in the n dimensional vector space. These points that make up the codebook are distributed uniformly inside an n dimensional sphere with a radius of √nP. When a codeword/point is transmitted through the channel it is corrupted by the AWGN. The AWGN displaces the transmitted point. With high probability the corrupted point will be found inside an n dimensional sphere with radius √nN (N is the noise variance) centered on the original codeword. The following figure illustrates the above

Figure 8: point to point signal after AWGN corruption



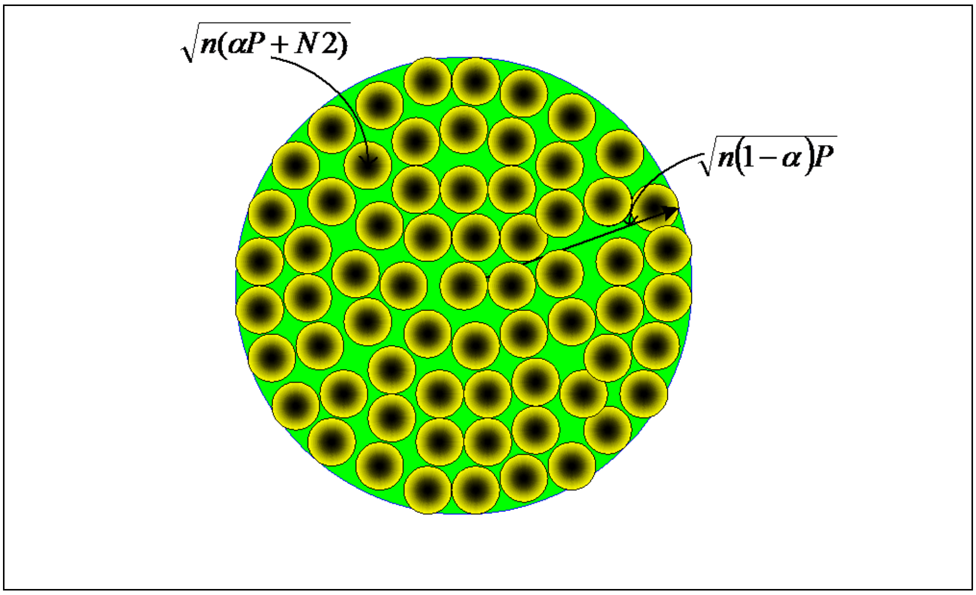
In superposition coding the picture gets a little more complicated as there are two codebooks. One codebook has a total of 2^{nR1} code words while the other has 2^{nR2} code words where R1 rate of the 'good' receiver and R2 of the 'bad' receiver. The 'bad' codebook has code words distributed uniformly in an n dimensional sphere with a radius of $\sqrt{n(1-\alpha)P}$ while the 'good' codebook is uniformly distributed in an n dimensional sphere with a radius of $\sqrt{n\alpha P}$. Now these two codebooks are summed up. This forms a 'cloud' of 'good' code words surrounding each one of the 'bad' code words. The 'could' is of course the n dimensional sphere with radius of $\sqrt{n\alpha P}$ centered on the 'bad' codeword. The following figure illustrates the above

Figure 9: Signal after superposition encoder



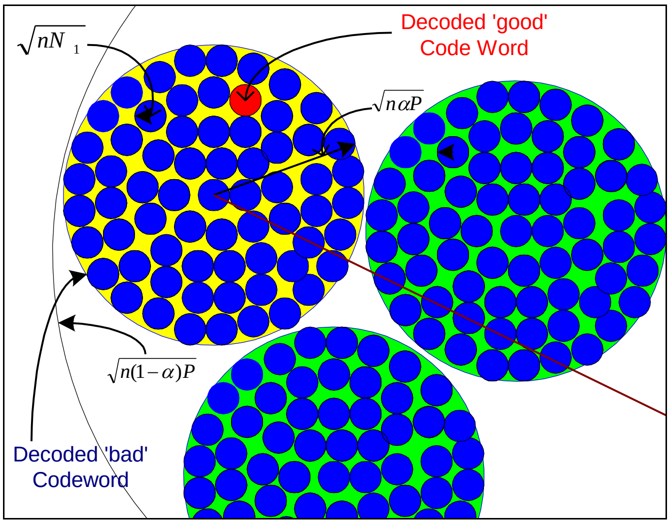
Now each receiver sees a corrupted version of the transmitted code words. The 'bad' receiver can only decode the 'bad' code words and cannot distinguish between the AWGN and the 'good' code words and thus sees that the 'bad' code words are corrupted by a spherical noise with a radius of $\sqrt{n(\alpha P+N2)}$. This is illustrated in the following figure

Figure 10:Superposition signal at the 'bad' receiver



The 'good' receiver first decodes the 'bad' codeword and then subtracts it from the signal. This centers the sphere surrounding the 'bad' codeword around the origin. Once this is done the receiver decodes the 'good' codeword in the presence of the AWGN. This is illustrated in the following figure

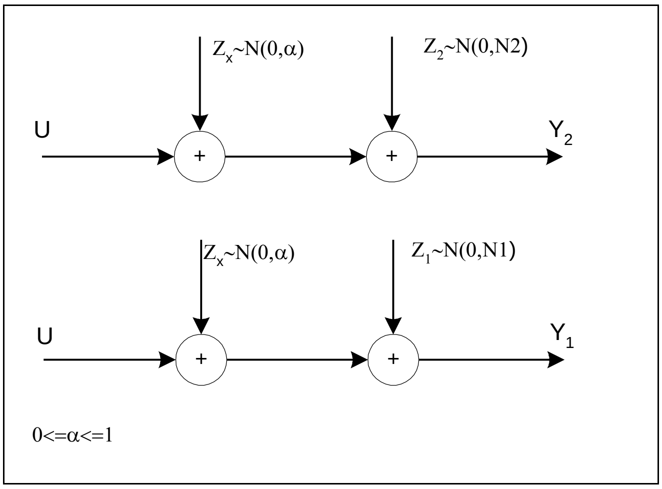
Figure 11: Superposition signal at the 'good' receiver



Revisiting Example 1 The Degraded Gaussian BCC with power constraint
Cover solved this problem in 1972. It was proved that U that achieves capacity is Gaussian.
The capacity achieving scheme is given by:

$X=U+Z_X$
$U \perp\!\!\!\perp Z_X$
$U \sim N(0,(1-\alpha)P)$
$Z_X \sim N(0,\alpha P)$

Figure 12



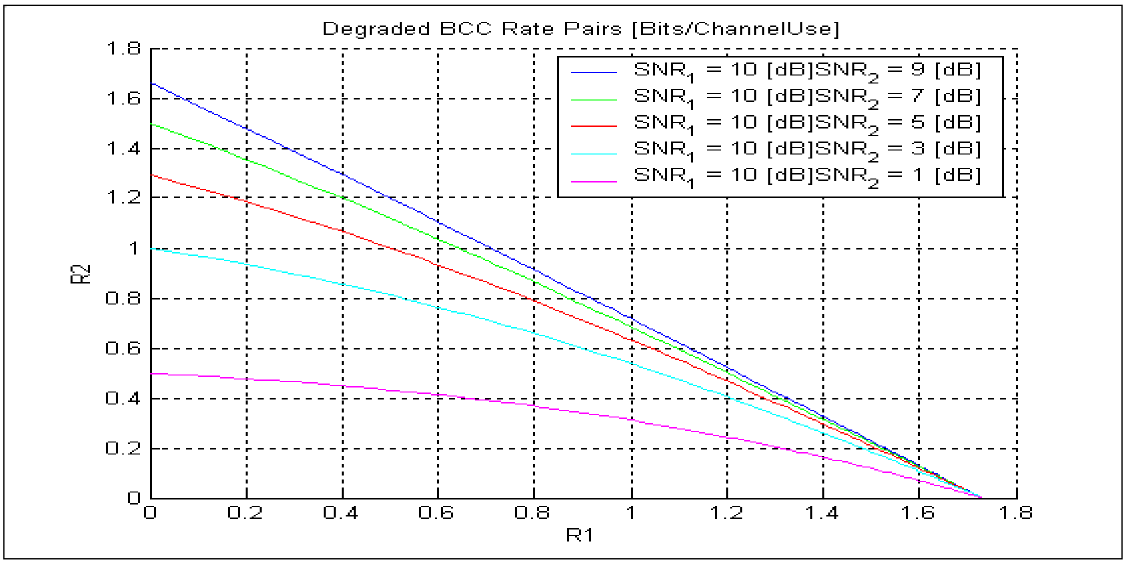
And so

$$I(U;Y_2)=C\left(\frac{(1-\alpha)P}{\alpha P+N2}\right)$$

$$I(X;Y_1|U)=I(Z_x;Y_1-U|U)=I(Z_x;Z_x+Z_1)=C\left(\frac{\alpha P}{N1}\right)$$

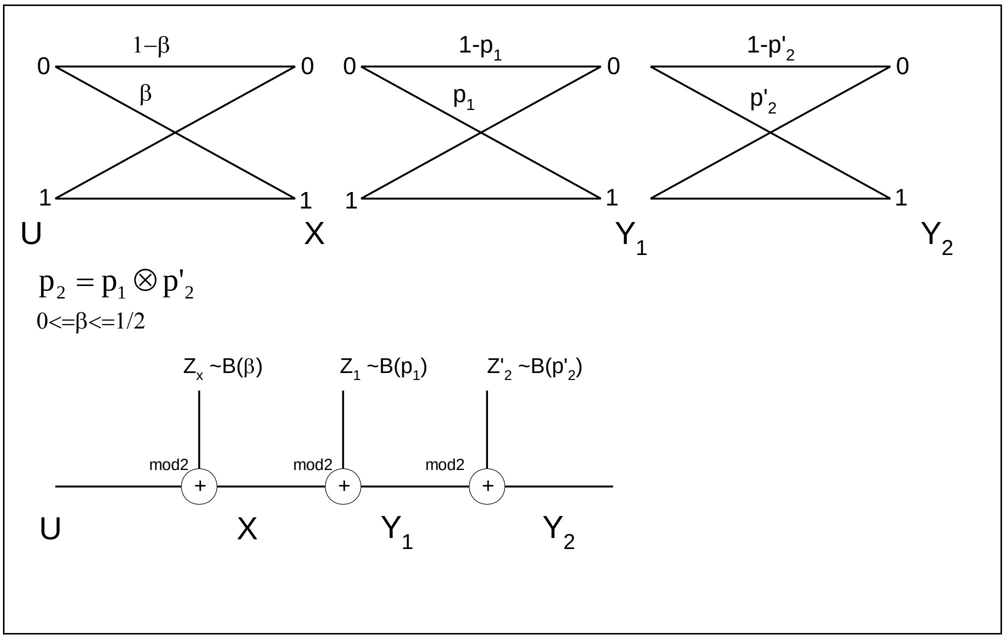
The following figure plots the capacity region for several SNR_1 and SNR_2 values where

SNR_1 = P/N1 > SNR_2 = P/N2



Revisiting Example 2 The Degraded Binary BCC

Figure 13

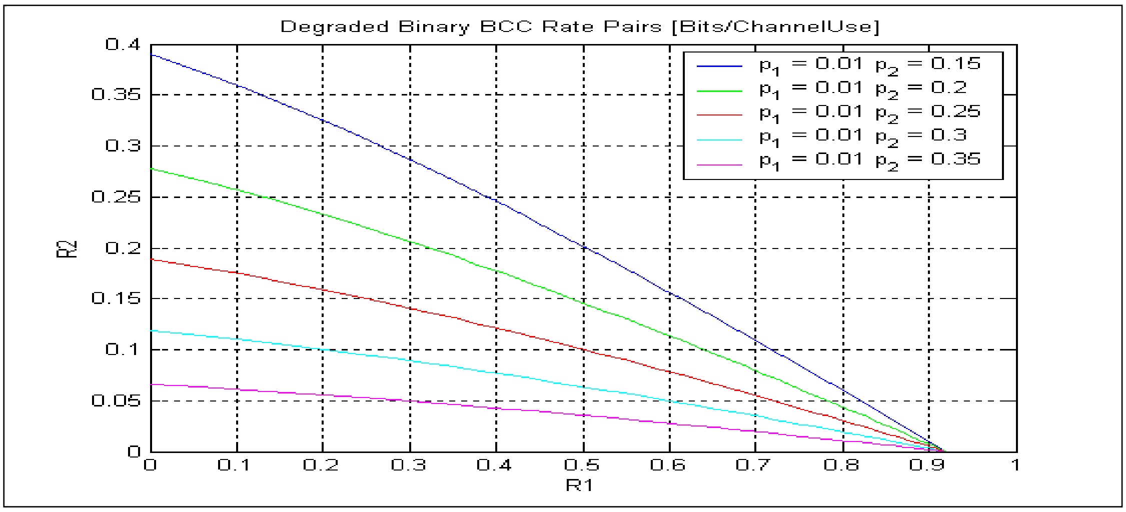


$$R_2 \le I(U;Y_2) = 1 - H_B(\beta \otimes p_2)$$

$$R_1 \le I(X;Y_1|U) = I(U \oplus Z_x; U \oplus Z_x \oplus Z_1|U) = I(Z_x; Z_x \oplus Z_1)$$

$$= H_B(\beta \otimes p_1) - H_B(p_1)$$

The following figure plots the capacity region for several p_1 and p_2 values where p2>p1



Alternative Interpretation For the BCC

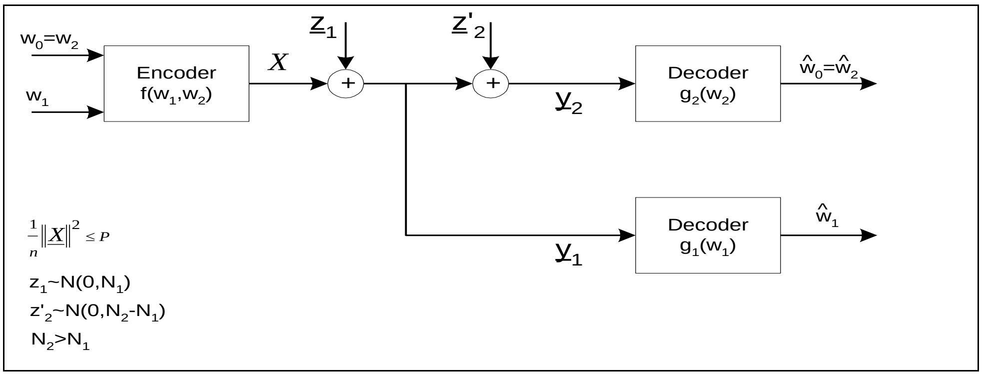
An alternative interpretation for the BCC is unequal error protection. Such a scenario occurs when the noise level of the channel is not known. The transmitter partitions the data stream into two streams a low rate stream that makes pessimistic assumptions on the channel noise, and a refinement stream that makes optimistic assumptions on the channel noise. The low rate stream is received with high probability while the refinement stream is received correctly only if channel conditions allow it. One may think of transmitting audio or video in such a fashion. When the noise is strong only a low-resolution version of the video or audio is received while the high-resolution video or audio is received only when channel conditions are good enough allowing the correct decoding of both streams.

Converse for the Gaussian Degraded BCC

Although the converse can be proved for the degraded BCC the proof for the Gaussian degraded BCC is less general but gives some more insight and shall be presented in the sequel. The proof uses the Entropy Power Inequality that is hereby presented

The converse coding theorem for the Gaussian Degraded BCC

Figure 14



The Capacity region for the degraded Gaussian BCC is given by:

$C_{Bcc} = convex\ hall\ \{closure(R_1, R_2)\}$

$$(R_1, R_2) = \begin{cases} R_1 < I(X;Y_1|U) = C\left(\frac{\alpha P}{N1}\right) \\ R_2 < I(U;Y_2) = C\left(\frac{(1-\alpha)P}{\alpha P + N2}\right) \\ 0 \le \alpha \le 1 \end{cases}$$

We need to show that any rate pair (R1,R2) that result in an error probability that goes to zero as the block length goes to infinity belong to $C_{BCC.}$

Proof of the Converse coding theorem

We need to show that any other codebook generated using a non-Gaussian probability law is worst then the Gaussian one.

Let $\underline{x} = f(w_0, w_1)$ denote the encoder and assume that W_0 and W_1 are statistically independent. Let us assume that the decoders result in $P_E<\varepsilon$ were P_E is defined to be

$$P_E = \Pr\{\hat{w}_{0,1} \neq w_0 \cup \hat{w}_1 \neq w_1 \cup \hat{w}_{0,2} \neq w_0\}$$

We shall proof that for any arbitrary $\underline{x} = f(w_0, w_1)$ obeying the power constraint P the following inequalities hold

$$R_1 \le C\left(\frac{\alpha P}{N1}\right) + \delta'$$

$$R_2 \le C\left(\frac{(1-\alpha)P}{\alpha P + N2}\right) + \delta''$$

where $\varepsilon \to 0 \Rightarrow (\delta' \to 0, \delta'' \to 0)$

<u>Proof</u>

(1) $nR_1 = H(W_1)$

$(2) = H(W_1|W_0)$

$(3) = H(W_1|W_0) - H(W_1|W_0, Y_1) + H(W_1|W_0, Y_1)$

$(4) = I(W_1; Y_1|W_0) + H(W_1|W_0, Y_1)$

$(5) = I(W_1; Y_1|W_0) + n\delta'$

Where

(1) - Since W_1 is transmitted using nR_1 bits
(2) - Since W_1 and W_0 are statistically independent
(3) - Adding and subtracting the same term
(4) - From the properties of mutual information
(5) - Using the Fano inequality (since an arbitrary small probability of error is assumed the uncertainty in W_1 given Y_1 and W_0 is small)

$$(6) = h(Y_1|W_0) - h(Y_1|W_0, W_1) + n\delta^{'}$$
$$(7) = h(Y_1|W_0) - h(Y_1|X) + n\delta^{'}$$
$$(8) = h(Y_1|W_0) - nh(Z_1) + n\delta^{'}$$
$$(9) = \frac{n}{2}\log\left(2\pi eP(Y_1|W_0)\right) - \frac{n}{2}\log\left(2\pi eN_1\right) + n\delta^{'}$$
$$(10) = \frac{n}{2}\log\left(P(Y_1|W_0) \Big/ N_1 \right) + n\delta^{'}$$
$$\Downarrow$$
$$R_1 = \frac{1}{2}\log\left(P(Y_1|W_0) \Big/ N_1 \right) + \delta^{'}$$

Where:

(6) random variable
(7) – From the data processing inequality since $(W_0,W_1)\leftrightarrow X\leftrightarrow Y_1$
(8) – Since $y_1 = x+z_1$
(9) – **By defining $h(Y_1|W_0)$ to be $n/2\cdot\log(2\pi eP(Y_1|W_0))$**
(10) – Algebra
(11) – Algebra

Similarly

$$(1)\ nR_2 = H(W_0)$$
$$(2) = H(W_0) - H(W_0|Y_2) + H(W_0|Y_2)$$
$$(3) = I(W_0;Y_2) + H(W_0|Y_2)$$
$$(4) = I(W_0;Y_2) + n\delta^{''}$$

Where

(1) - Since W_0 is transmitted using nR_2 bits
(2) - Adding and subtracting the same term
(3) - From the properties of mutual information
(4) - Using the Fano inequality (since an arbitrary small probability of error is assumed the uncertainty in W_0 given Y_2 is small)

$$(5) = h(Y_2) - h(Y_2|W_0) + n\delta^{''}$$
$$(6) \le \frac{n}{2}\log\left(2\pi e(P + N_2)\right) - h(Y_2|W_0) + n\delta^{''}$$

(5) – From the properties of mutual information and since y_2 is a continues random variable
(6) – Since the entropy of a random variable with a given variance is always smaller than the entropy of a Gaussian random variable with the same variance

Now we shall use the vector Entropy Power Inequality

$$h\left(Y_2\middle|W_0\right)=h\left(Y_1+Z_2^{'}\middle|W_0\right)\geq\frac{n}{2}\log\left(2^{\frac{2}{n}h\left(Y_1|Y_0\right)}+2^{2h\left(Z_2^{'}\right)}\right)$$

Substituting the above into (6)

$$(7)\leq\frac{n}{2}\log\left(2\pi e\left(P+N_2\right)\right)-\frac{n}{2}\log\left(2^{\frac{2}{n}h\left(Y_1|W_0\right)}+2^{2h\left(Z_2^{'}\right)}\right)+n\delta^{''}$$

$$(8)=\frac{n}{2}\log\left(\frac{P+N_2}{P\left(Y_1\middle|W_0\right)+N_2^{'}}\right)+n\delta^{''}$$

$$\Downarrow$$

$$R_2\leq\frac{1}{2}\log\left(\frac{P+N_2}{P\left(Y_1\middle|W_0\right)+N_2^{'}}\right)+\delta^{''}$$

Where

(7) – Using the Vector EPI. Equality holds if $Y_1|W_0$ is Gaussian i.i.d

(8) – **Again since $h(Y_1|W_0)$ is defined to be $n/2\cdot\log(2\pi eP(Y_1|W_0))$** + Algebra

Now following our definition that $h(Y_1|W_0)=n/2\cdot\log(2\pi eP(Y_1|W_0))$ it follows that

$$P(Y_1|W_0)=\frac{1}{2\pi e}\cdot 2^{\frac{2}{n}h\left(Y_1|W_0\right)}$$

$$\Downarrow$$

$$N_1\leq P(Y_1|W_0)\leq N_1+P$$

$\uparrow$ holds if all the uncertinty in Y_1 given W_0 is due to N_1

$\uparrow$ holds if W_0 is not transmitted and $\underline{X}$ is Gaussian i.i.d

Now define

$$\alpha\equiv\frac{P(Y_1|W_0)-N_1}{P}$$

$$\Downarrow$$

$$0\leq\alpha\leq 1$$

Substituting the above into the inequalities developed for R1 and R2 we obtain

$$R_1\leq\frac{1}{2}\log\left(1+\frac{\alpha P}{N1}\right)+\delta^{'}$$

$$R_2\leq\frac{1}{2}\log\left(1+\frac{\left(1-\alpha\right)P}{\alpha P+N2}\right)+\delta^{''}$$

This concludes the proof and thus any system achieving an error probability arbitrary small is contained in $C_{BCC.}$

Entropy Power Inequality (EPI)

Let X be a continues real random variable such that:

$$X \sim f_x(x)$$
$$E\{X\} = \mu$$
$$Var(X) = \sigma^2$$
$$h(X) = E\{-\log(f_x(x))\} = -\int f(x)\log f(x)\partial x$$

Let X^* be a continues real Gaussian random variable such that:

$$X^* \sim N(0, \sigma^2)$$
$$h(X^*) = \frac{1}{2}\cdot\log(2\pi e\sigma^2)$$

Consider the relative entropy between X and X^*

$$D(f_x \| f_x^*) = \int f(x)\log\frac{f(x)}{f^*(x)}\partial x$$

It can be shown that in this case

$$D(f_x \| f_x^*) = h(X^*) - h(X)$$

Since the relative entropy is non negative

$$h(X^*) - h(X) = D(f_x \| f_x^*) \geq 0$$
$$\Downarrow$$
$$h(X^*) \geq h(X) \quad \forall f_x(x)$$

Let us define $\tilde{X}$ to be a continues real Gaussian random variable such that its entropy equals that of X thus

$$\tilde{X} \sim N(0, P(X))$$
$$h(\tilde{X}) = h(X)$$
$$\Downarrow$$
$$P(X) = \frac{1}{2\pi e}2^{2h(X)} \leq \sigma^2$$

Where P(X) is defined as the entropy power of X which is simply the variance of a gaussian random variable with an entropy equal to that of X. Consider a continues real random variable Y such that that:

X and Y are independent.

Thus

$$Var(X+Y)=Var(X)+Var(Y)$$

now we are interesetd in

$$P(X+Y)=?$$

Theorem (Shannon 1948)

$$P(X+Y) \geq P(X)+P(Y)$$
$$\uparrow$$

equality holds $\Leftrightarrow$ X, Y are Gaussian

Some insight into this theorem may be gained by recalling the Central Limit Theorem (CLT) that states that: Given a series of i.i.d random variables x_i

$$E\{X_i\}=0$$
$$Var\{X_i\}=\sigma^2$$

then

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n} X_i \xrightarrow[\text{in distributin}]{n\to\infty} X^* \sim N(0,\sigma^2)$$

And so for i.i.d random variables X_i one can intuitively imagine that

$$P\left(\frac{1}{\sqrt{n}}\sum_{i=1}^{n} X_i\right) \xrightarrow[n\to\infty]{} P(X^*)$$

This gives intuition into why the entropy power of the sum is greater than the sum of entropy powers.
The sum of i.i.d random variables tends to be ‘more’ Gaussian and thus has larger entropy power. The proof was not given in class. The interested reader is referred to [1].
The EPI can also be stated for the random vector case and the random process case.

For the random vector case:
Consider a continues random vector, $\underline{X} = [X_1\ X_2 \ldots X_n]$ with a covariance matrix K_X.

We define the entropy power of $\underline{X}$ as:

$$P(\underline{X}) = \frac{1}{(2\pi e)^n} 2^{2h(\underline{X})}$$

It can be proved that

$$P(\underline{X}+\underline{Y}) \geq P(\underline{X}) + P(\underline{Y})$$

The Conditional EPI
Let X,U,Y be continues time real random variables such that (X,U) are independent of Y. since

$$\frac{1}{2}\log(2\pi e P(X)) = h(X) \quad \Rightarrow P(X) = \frac{1}{2\pi e} 2^{2h(X)}$$

Now using the EIP one has the following

$$\frac{1}{2\pi e} 2^{2h(X+Y)} \geq \frac{1}{2\pi e} 2^{2h(X)} + \frac{1}{2\pi e} 2^{2h(Y)}$$

now since $y \perp (x,u)$

$$\frac{1}{2\pi e} 2^{2h(X+Y|U)} \geq \frac{1}{2\pi e} 2^{2h(X|U)} + \frac{1}{2\pi e} 2^{2h(Y)}$$

$$\uparrow$$

equality holds $\Leftrightarrow$ x | u and y are gaussian

Where

$$h(X|U) = -\mathrm{E}\{\log f_{x|u}(X,U)\} = -\iint_{x,u} f_u(u) f_{x|u}(x|u) \log f_{x|u}(x,u) \partial x \partial u$$

Similarly for the vector case:

$$\frac{1}{(2\pi e)^n} 2^{2h(\underline{X}+\underline{Y}|\underline{U})} \geq \frac{1}{(2\pi e)^n} 2^{2h(\underline{X}|\underline{U})} + \frac{1}{(2\pi e)^n} 2^{2h(\underline{Y})}$$

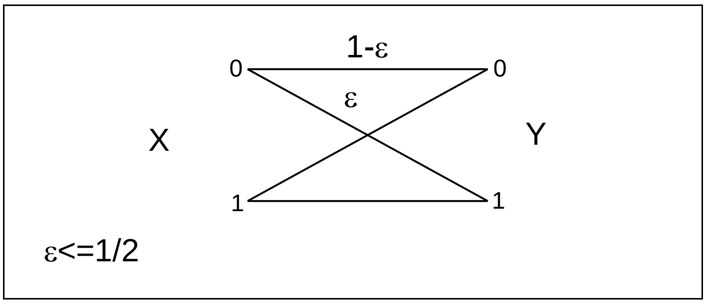
$$\uparrow$$

equality holds $\Leftrightarrow$ $\underline{x}$ | $\underline{u}$ and $\underline{y}$ are gaussian

Mrs Gerber's Lemma (Wyner-Ziv 1973)

A similar role played by the EPI in proving the converse of the degraded Gaussian BCC coding theorem is played by Mrs Gerber's lemma in proving the converse of the degraded binary BCC coding theorem. The theorem is hereby given.

Consider a binary random vector $\underline{X} = [X_1 \; X_2 \ldots X_n]$ and the following BSC



Where Y can be written as:

$$\underline{Y} = X \oplus \underline{N}$$

where

$$\underline{N} = [N_1 \; N_2 \ldots \mathrm{N_n}]$$
$$N_i \sim Bernulli(\varepsilon)$$

Denote the average probability for a coordinate in $\underline{X}$ to equal 1:

$$p(X) = \frac{1}{n}\sum_{i=1}^{n} \Pr(X_i = 1)$$

And thus

$$P(\underline{Y}) = P(\underline{X}) \otimes P(\underline{N}) = P(\underline{X}) \otimes \varepsilon$$
$$\uparrow x_i \text{ i.i.d}$$

Define

$$\underline{X}^* = [X_1^* \; X_2^* \ldots X_n^*] \text{ where } X_i^* \sim Bernulli(p(x))$$

and

$$\underline{\tilde{X}} = [\tilde{X}_1 \; \tilde{X}_2 \ldots \tilde{X}_n] \text{ where } \tilde{X}_i \sim Bernulli(q(x))$$
$$q(x) = H_B^{-1}\left(\frac{1}{n} H(\underline{X})\right)$$

i.e , $\underline{\tilde{X}}$ has the same entropy as $\underline{X}$

It can be proved that using the Jensen Inequality that

$$\frac{1}{n} H(\underline{x}^*) \geq \frac{1}{n} H(\underline{x}) = \frac{1}{n} H(\underline{\tilde{x}})$$

Mrs. Gerber's lemma

$$H(\underline{Y}) \geq nH_B(q(\underline{X}) \otimes \varepsilon) = H(\underline{\tilde{X}} + \underline{N})$$

$$\uparrow \qquad \uparrow$$

$$\text{equality} \Leftrightarrow x_i \sim \text{Bernulli i.id}$$

An intuitive interpretation on the lemma is that if a binary random vector $\underline{x}$ that is not Bernulli i.i.d is passed through a BSC, the BSC output $\underline{y}$ will tend to be 'more' Bernulli like.

Conditional version of Mrs. Gerber's lemma

Given a binary random vector $\underline{X}$, a random variable u and binary random vector $\underline{Y}$ that is the outcome of passing $\underline{x}$ through a BSC then

$$if\ (X,U) \perp N$$

$$H(\underline{Y}|U) \geq nH_B(q(\underline{X}|U) \otimes \varepsilon)$$

where

$$q(\underline{X}|U) \equiv H_B^{-1}\left(\frac{1}{n}H(\underline{X}|U)\right)$$

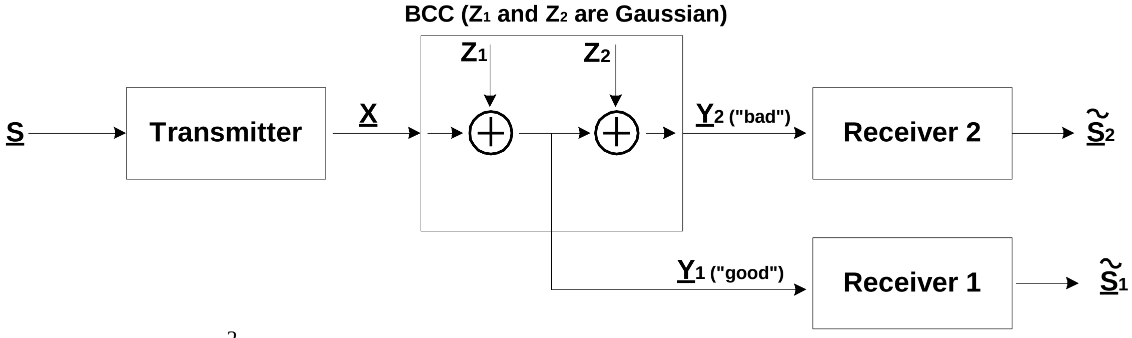
10 – הרצאה

Joint Source / Channel coding over the Gaussian BCC Channel

Summarized by Ori Finkelman.

The degraded Broadcast Channel – analog transmission vs. digital transmission

Following is an example for a case where the source / channel coding separation principle does not work for an information network.



$S \sim N(0, \sigma_s^2)$

$\frac{1}{n} E \| X \|^2 \le P$

The individual capacities of the cannels are:

$$C_1 = \frac{1}{2}\log(1+\frac{P}{N_1}) \qquad C_2 = \frac{1}{2}\log(1+\frac{P}{N_1+N_2})$$

$$D_1 = E(\tilde{S}_1 - S)^2 \qquad D_2 = E(\tilde{S}_2 - S)^2$$

The rate distortion function of **S** is: $R(D) = \frac{1}{2}\log\frac{\sigma_s^2}{D}, 0 \le D \le \sigma_s^2$, hence the optimal distortion we can reach for each of the cannels individually is:

$$D_1^{opt} = R^{-1}(C_1) = \sigma_s^2 2^{-2C_1} \qquad D_2^{opt} = R^{-1}(C_2) = \sigma_s^2 2^{-2C_2}$$

The Analog case:

In the analog case the optimal distortion can be achieved simply by using MSE estimator.
Given the output $\underline{Y}$, we can give an optimal estimation of $\underline{X}$ in the MSE sense. Since we have a power limitation on the transmitted signal, we can amplify $\underline{S}$ up to the allowed power *P*.

1. Multiply the signal **S** by a constant **α** to get **X** such that $\frac{1}{n}E\|\underline{X}\|^2 = P$
2. Use an optimal Wiener estimator *R*, to get the estimation $\tilde{S} = \underline{Y}\cdot\frac{1}{\alpha}\cdot\frac{P}{P+N}$.

Following is a proof for the optimality of the coefficients used by the Wiener filter.

$$X = \alpha S$$
$$\tilde{S} = (X+Z)\beta = (\alpha S + Z)\beta$$
$$E[e^2] = E[(S-\tilde{S})^2] = E[(S-(\alpha S+Z)\beta)^2] = \ldots = E[S^2(1-\alpha\beta)] - E[Z^2\beta^2] =$$

Assuming $\mu_s = 0 \quad \mu_z = 0$ (the means do not change the mse)

$$= 2\sigma_s^{\ 2}(1-\alpha\beta)^2 + 2\sigma_z^{\ 2}\beta$$

It is clear that the minimum value will be when $\alpha \to \infty$ and $\beta = \frac{1}{\alpha} \to 0$ but since we have power limitation we know that α can be no more than $\frac{P}{\sigma_s^{\ 2}}$. For this maximal α we calculate the optimal β.

$$\frac{\partial}{\partial\beta}E[e^2] = \frac{\partial}{\partial\beta}[2\sigma_s^{\ 2}(1-\alpha\beta)^2 + 2\sigma_z^{\ 2}\beta] = 0$$

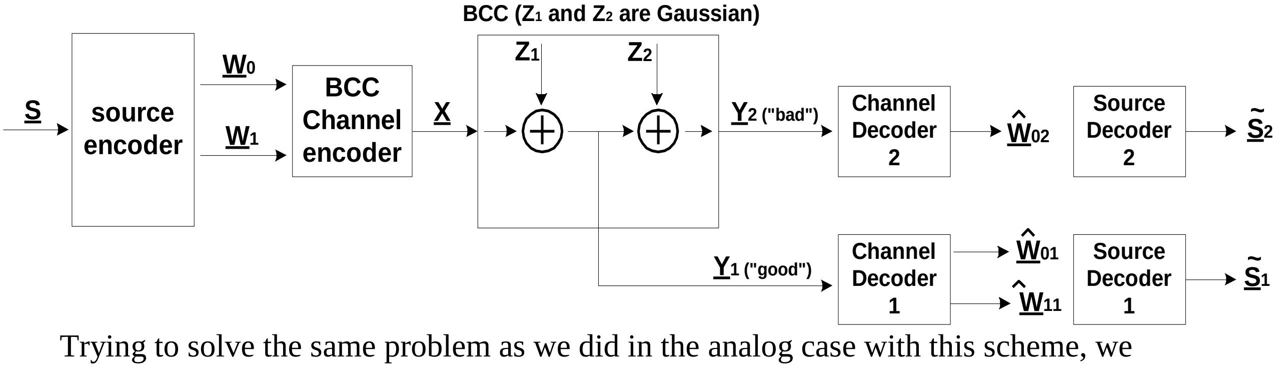
$$\beta = \frac{\alpha\sigma_s^{\ 2}}{\alpha^2\sigma_s^{\ 2}+\sigma_z^{\ 2}} = \frac{1}{\alpha}\frac{\alpha^2\sigma_s^{\ 2}}{\alpha^2\sigma_s^{\ 2}+\sigma_z^{\ 2}} = \frac{1}{\alpha}\frac{\sigma_x^{\ 2}}{\sigma_x^{\ 2}+\sigma_z^{\ 2}} = \frac{1}{\alpha}\frac{P}{P+N}$$

It is clear that in the analog case, since the transmitter behaves the same for both individual receivers and that there are no mutual dependencies between the receivers, they could both achieve the optimal distortion for their channel capacity rates.

The digital case:

Now let us see what are the achievable distortions for the digital case, using a source/channel separation scheme.

Our system may be described by the following drawing:

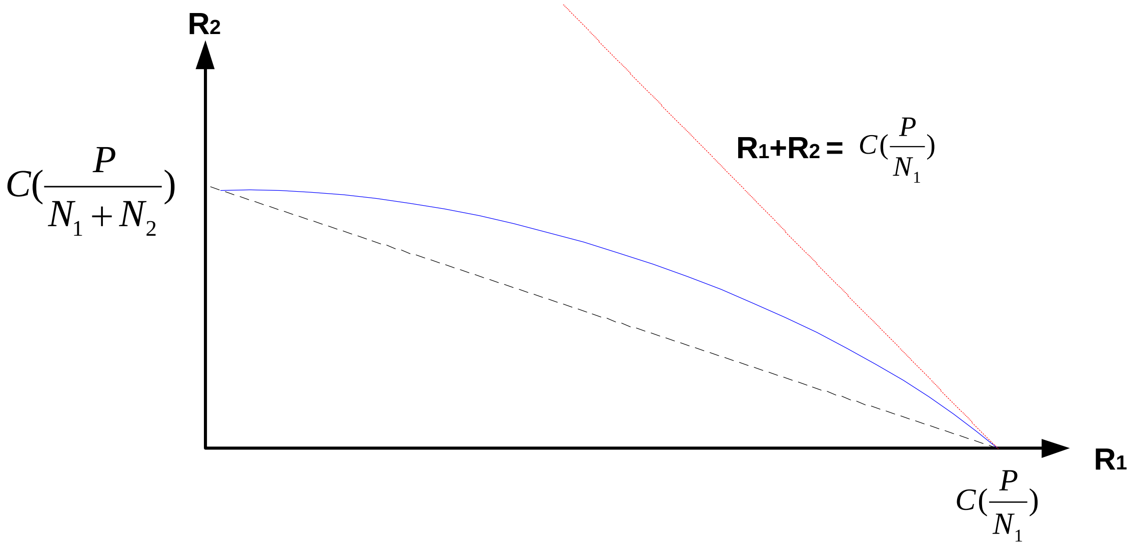


Trying to solve the same problem as we did in the analog case with this scheme, we would like to think of $\underline{\tilde{S}_1}$ and $\underline{\tilde{S}_2}$ as two estimators of $\underline{S}$, where $\underline{\tilde{S}_1}$ is finer than $\underline{\tilde{S}_2}$.

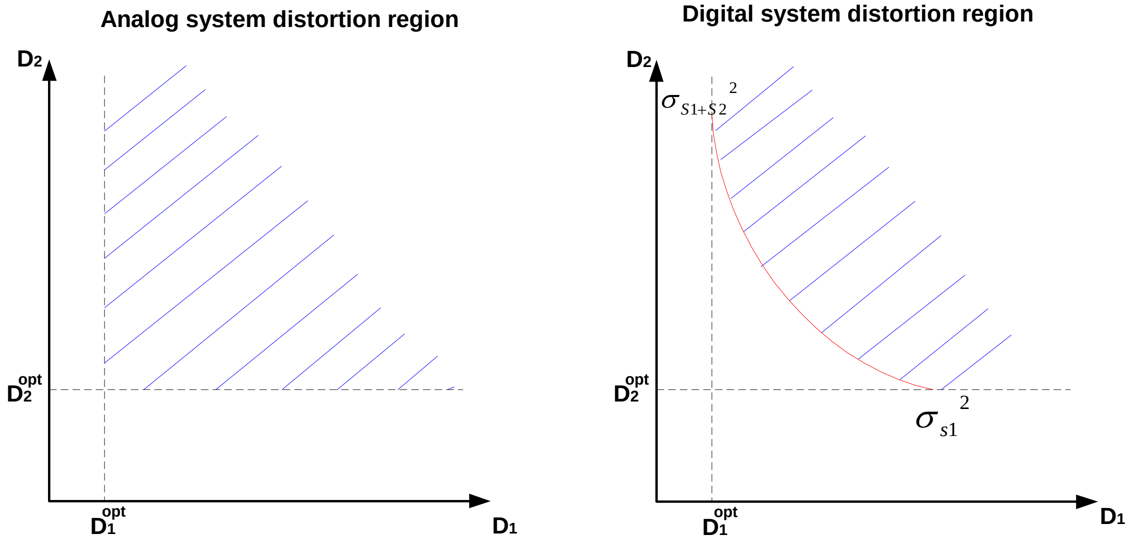
Thus $\underline{W_0}$ is a coarse description of the source $\underline{S}$ and $\underline{W_1}$ is a refinement for $\underline{W_0}$, allowing receiver 1 to decode a finer description of the source than receiver 2.
If it is possible to divide $\underline{S}$ to $\underline{W_0}$ and $\underline{W_1}$ such that the sum rate would be no higher than the rate it would take to encode $\underline{S}$ in a single word, achieving the same distortion for receiver 1, we would say that $\underline{S}$ is successive refinable.

Assuming $\underline{S}$ is successive refinable (further discussion on successive refinement is in the last section of this lecture notes), what would be the capacity and distortion regions of this solution?

We have seen Cover's solution for the degraded BCC channel problem from 1972 (see lecture notes from 28/4/2004).
The capacity region is described by the following drawing:



The blue line is the solution for the degraded broadcast channel in the Gaussian case; the black dashed line is the solution using TDM, and the red dashed line is the line $R_1 + R_2 = C(\frac{P}{N_1})$. It is clear that the maximum achievable rate for receiver 1 is $C(\frac{P}{N_1})$, which can only be achieved when $R_1 = C(\frac{P}{N_1})$ and $R_2 = 0$. Trying to set $R_2 > 0$ reduces R_1 in more than R_2, that is $R_1 + R_2 < C(\frac{P}{N_1})$.
From this we can draw the achievable distortion graphs of the two cases (digital vs. analog).



In the digital case, trying to reduce the distortion of message $\underline{W}_0$ below the variance of the noise of the "bad" channel raises the distortion of $\underline{W}_1$ in more than the reduction of the $\underline{W}_0$ distortion.

Achieving the bounds for the digital case using a successive refinement scheme:

Successive refinement:

We are given a source X and two descriptions of X, a coarse description $\hat{X}_1$ and a finer description $\hat{X}_2$, and distortion values $D_1 = d(X, \hat{X}_1), D_2 = d(X, \hat{X}_2)$ where $D_1 \geq D_2$ for some distortion measure D.

We know that in order to transmit $\hat{X}_1$ we will need a rate of $R_1 = R(D_1)$, and the same, for $\hat{X}_2$ we will need a rate of $R_2 = R(D_2)$, obviously $R_1 \leq R_2$.

Instead of choosing either $\hat{X}_1$ or $\hat{X}_2$, we would like to send the information in two phases. In the first phase we would like to send $\hat{X}_1$ in a rate of R_1, such that at the end of the first phase the receiver may decode $\hat{X}_1$ with no error (in the Shannon sense).

In the second phase, we would like to send some encoded data in a rate of (R_1-R_2) and that the receiver, once getting this data may now decode $\hat{X}_2$.

This process is called *successive refinement*.

I will describe the basic ideas of successive refinement and the conditions for a successive refinable source, with no proof. For further reading, please refer to [1].

Example:

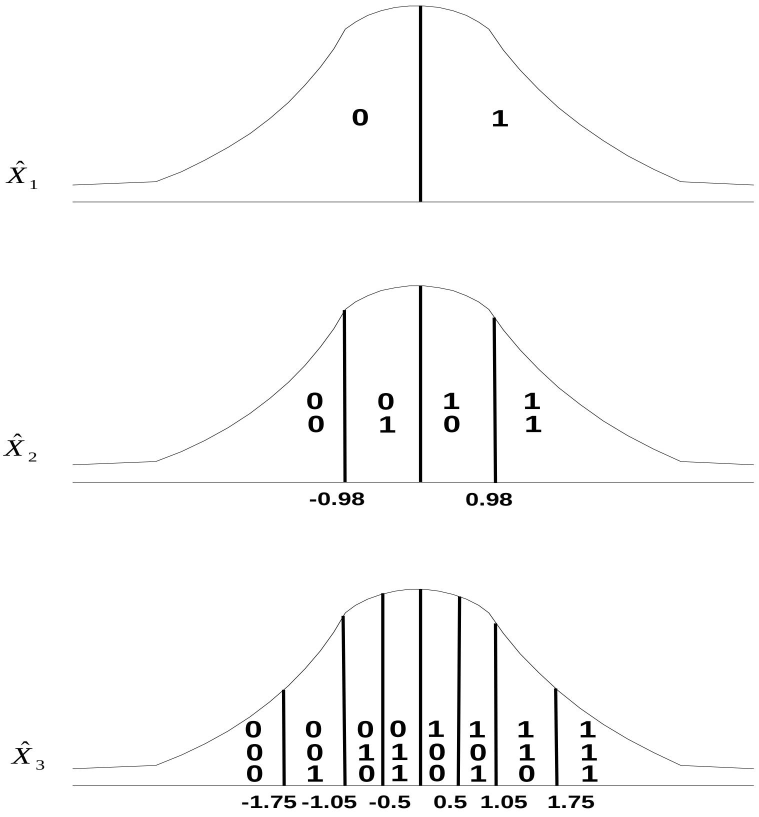
Let us take a simple case of X drawn from a standard normal distribution where the distortion measure is taken as the mean square error.

We would like to minimize the error resulting from describing X~N(0,1) using a finite number of bits.

It is obvious that if we have only one bit of description the optimal description would be to specify whether X is positive or negative. The reconstruction of $\hat{X}_1$ at the receiver would be the centroid of the partition. Thus, $\hat{X}_1 = -\sqrt{2/\pi}$ if $X < 0$, and $\hat{X}_1 = \sqrt{2/\pi}$ if $X \geq 0$.

The resulting squared error distortion is $D = E(X - \hat{X}_1)^2 = (\pi - 2)/\pi \approx 0.3634$
If there are 2 bits of description then there is an optimal quantization of the interval (-∞,∞). The interval is quantized into 4 regions and $\hat{X}_2$ is given as the centroid of the bin in which *X* happens to fall. Here it is clear that the 2-bit description is a refinement of the 1 bit description.

However, trying to add another bit we find that the optimal description for 3 bits is not a refinement of the 2-bit description, since it requires a different quantization then the one we used for $\hat{X}_2$.
The following drawing shows the optimal descriptions for 1, 2, and 3 bits, and it is clear from it that the single Gaussian variable case is not successive refinable. The results are given here in a sketch. The calculations were omitted, but are straightforward.



When can we use successive refinement?

It is clear from the previous example that successive refinement cannot be always achieved.
So, when can we use successive refinement?
In [1], it was shown that that successive refinement from a coarse description $\hat{X}_1$ to a fine description $\hat{X}_2$ is possible if and only if the individual rate distortion solutions $p(\hat{x}_1 | x)$ and $p(\hat{x}_2 | x)$ for $D_1 \geq D_2$ are such that we can write $X \to \hat{X}_2 \to \hat{X}_1$ as a Markov chain.
Specifically it is proven in [1] that:

Successive refinement with distortions D_1 and D_2 $(D_1 \geq D_2)$ can be achieved if and only if there exist a conditional distribution $p(\hat{x}_1, \hat{x}_2 \mid x)$ with

$$Ed(X, \hat{X}_1) \leq D_1 \tag{1}$$

and

$$Ed(X, \hat{X}_2) \leq D_2 \tag{2}$$

such that

$$I(X; \hat{X}_1) = R(D_1) \tag{3}$$

$$I(X; \hat{X}_2) = R(D_2) \tag{4}$$

and

$$p(\hat{x}_1, \hat{x}_2 \mid x) = p(\hat{x}_2 \mid x) p(\hat{x}_1 \mid \hat{x}_2)$$

Note that although we have seen an example where successive refinement fails, and in [1] another counterexample is provided, however, in many cases, when taking $\underline{X}$ to be a vector of i.i.d variables, successive refinement is asymptotically achievable.

Applying successive refinement to our problem:

As described above, the problem of the degraded BCC source encoder is to encode the input signal $\underline{S}$ into the words W_0 and W_1, where W_0 is a public message for both receivers and W_1 is a private message for receiver 1 which is that “good” receiver.

In this case we may apply successive refinement in the following way:
W_0 will be the coarse description $\hat{X}_2$ of the source $\underline{S}$ transmitted in a rate R_2 and achieving the distortion $D_2 = D(R_2)$.
W_1 together with W_0 will be the finer description $\hat{X}_1$, where W_1 is transmitted in a rate $R_1=R_0-R_2$ and the achieved rate distortion in the “good” receiver is
$D_1 = D(R_1 + R_2) = D(R_0)$.
As we’ve seen in class, transmitting W_0 as a public message to both receivers and W_1 as a private messages to receiver 1, concurrently, is possible in the degraded BCC within the distortion / rate regions as described above.

References:

[1] W.H.R Eqiutz and T.M. Cover. Successive Refinement of Information. *IEEE Trans. Information Theory,* Vol.37, No.2, March 1991

הרצאה – 11

אקספוננטי שגיאה לפי שיטת הטיפוסים (Method of types)

סוכם ע"י אסף בן ישי

מוטיבציה

שאנון, במאמרו המקורי משנת 1948 הגדיר את מושג "קיבול הערוץ" כמדד לטיב ביצועיו של ערוץ תקשורת. זהו המדד העיקרי בו משתמשים לבחינה של ערוצים, עם זאת, למרות חשיבותו, ישנן תכונות של הערוץ אותן אינו מצליח לתאר. מדד שנותן אינפורמציה נוספת הוא אקספוננט השגיאה. ישנן שתי שיטות לחישוב אקספוננט השגיאה - השיטה של Gallager ושיטת הטיפוסים (Csiszár & Körner). אנו נראה את השיטה השניה, היות והיא יותר אינפורמטיבית מזו של Gallager.
ראשית נבהיר בדוגמא את החסרון של מדד הקיבול בתאור תכונותיו של ערוץ:

דוגמא 1

נתונים שני ערוצים מודולו אדיטיביים מעל א"ב $\{0,1,2,3\}$. הקשר בין הכניסה למוצא נתון ע"י $Y=(X+N)\bmod 4$.

ערוץ א'

זהו ערוץ מכונת כתיבה רועשת.
הרעש N מאופיין ע"י הפילוג הבא

$$\Pr(N=0)=\Pr(N=1)=1/2$$
$$\Pr(N=2)=\Pr(N=3)=0$$

בערוץ מודולו אדיטיבי פילוג הכניסה המגשים הוא אחיד והקיבול ניתן ע"י הנוסחא

$$C=\log(|X|)-H(N)=\log(4)-H(N)=1bit/channel\ use$$

($|X|$ הוא גודל הא"ב – 4 במקרה שלנו. $H(N)$ היא אנטרופית הרעש)

ערוץ ב'

זו מעיין הכללה של ערוץ בינארי סימטרי לבסיס 4. כעת פילוג הרעש הוא

$$\Pr(N=0)=1-\delta$$
$$\Pr(N=1)=\Pr(N=2)=\Pr(N=3)=\delta/3$$

נוסחת הקיבול היא עדיין כמו בסעיף הקודם. ניתן לראות כי עבור $\delta\approx 0.2$ נקבל קיבול של 1 ביט לשימוש ערוץ.
כלומר, לשני הערוצים אותו הקיבול. אולם יש הבדל עקרוני ביניהם. כפי שלומדים בקורס בתורת האינפורמציה, בערוץ א' אפשר לשדר בקצב 1 ביט לשימוש ערוץ ע"י שימוש בכניסות 0 ו 2 בהסתברות שווה. אין צורך בקוד לתיקון שגיאות (כלומר, משתמשים בקוד באורך בלוק 1). הסתברות השגיאה המתקבלת היא 0 ממש!. בערוץ ב', יש צורך בקוד בלוק באורך $n\to\infty$. הסתברות השגיאה לעולם איננה ממש 0, אלא רק שואפת ל-0 עם הגדלת n.
ננסח מחדש את ההבדל בין הערוצים ע"י הגדרת מושג "קיבול אפס שגיאה".
ראשית, שגיאת הפענוח האופטימלית של ספר קוד באורך n, בקצב R (ביט לשימוש ערוץ) מוגדרת כ

$$P_e^{opt}(n,R)=\min\{\overline{P}_e(\beta):|\beta|\geq 2^{nR}\}$$

כאשר $\overline{P}_e(\beta)$ היא שגיאת הפענוח הממוצעת בספר קוד β על פני מילות הקוד ואקראיות הערוץ (בהנחת שידור מילים בהסתברות שווה).
קיבול אפס השגיאה מסומן ב C_0 ומוגדר כך

$C_0 := \max\left\{R : P_e^{opt}(n,R) = 0\, for\ some\ n\right\}$

כעת ניתן לומר שההבדל בין הערוצים בדוגמא הוא שבערוץ א' קיבול אפס השגיאה הוא 1 (ביט לשימוש ערוץ) ובערוץ ב' הוא 0.

נגדיר את אקספוננט השגיאה $E^{opt}(R)$ (עבור $R > C_0$)

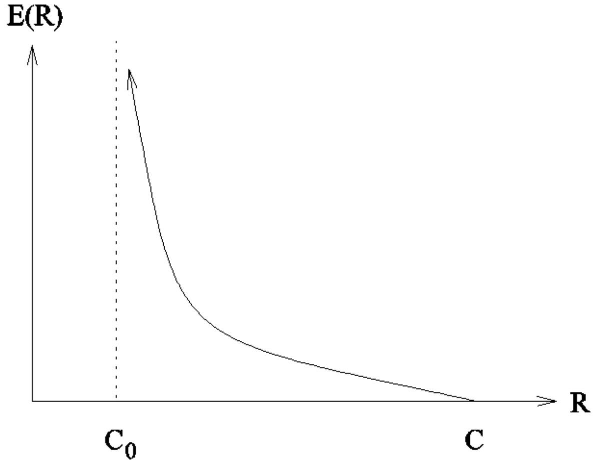
$$E^{opt}(R) = \lim_{n\to\infty} -\tfrac{1}{n}\log\left\{P_e^{opt}(n,R)\right\}$$

עבור $R > C$ נקבל $P_e^{opt}(n,R) = 1$ (כאשר $n \to \infty$) ולכן $E^{opt}(R) = 0$. אם נצליח לבטא את $E^{opt}(R)$ כפונקציה single letter של R וסטטיסטיקת הערוץ, נוכל לומר שבתחום $C_0 < R < C$ הסתברות השגיאה יורדת ל-0 אקספוננציאלית עם אורך הבלוק.

מכאן והלאה לא נתייחס לאקספוננט השגיאה של ספר הקוד האופטימלי, $E^{opt}(R)$, אלא לאקספוננט השגיאה עבור קוד אקראי אותו קל יותר לחשב. אקספוננט זה מסומן ב $E(R)$ ומוגדר בהתאם ע"י

$$E(R) = \lim_{n\to\infty} -\tfrac{1}{n}\log\left\{\overline{P}_e(n,R)\right\}$$

$\overline{P}_e(n,R)$ היא הסתברות השגיאה הממוצעת ע"פ אקראיות הערוץ, מילות הקוד, וספרי הקוד. ברור מההגדרות ש $E(R) \le E^{opt}(R)$, אולם מעניין לדעת שעבור קצבים מסוימים מתחת לקיבול $E(R)$ מתלכד עם חסם עליון לאקספוננט השגיאה ואז גם $E(R)$ מתלכד גם עם $E^{opt}(R)$.



דוגמא 2

ערוצי רעש חיבורי רציפים $Y = X + Z$, נניח $SNR >> 1$.

מקרה 1 רעש גאוסי

$Z \sim N(0,\sigma^2)$

מקרה 2 רעש תערובת גאוסית

$Z \sim p_0 N(0,{\sigma_0}^2) + p_1 N(0,{\sigma_1}^2)$

נניח שלשני הרעשים אותו ההספק : $\sigma^2 = p_0{\sigma_0}^2 + p_1{\sigma_1}^2$.

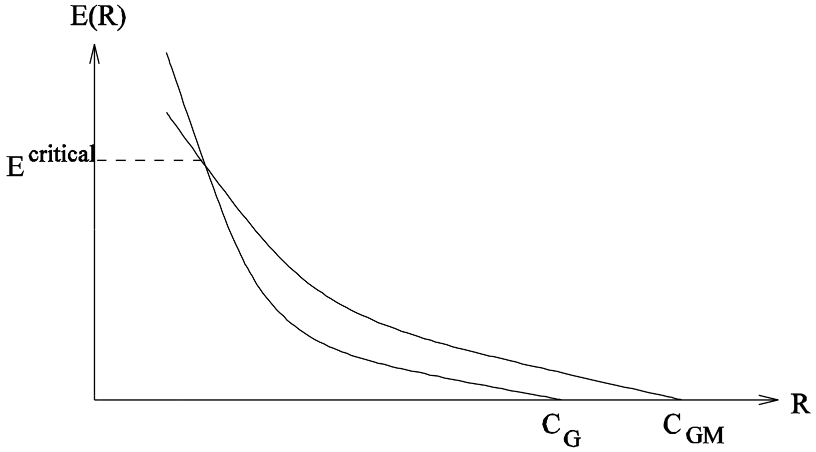
הקיבול של הערוצים (בקירוב SNR גבוה, לכן אנטרופית האות+הרעש היא בקירוב אנטרופית האות) הוא

$C \approx \tfrac{1}{2}\log(2\pi eP) - h(N)$

כידוע, אנטרופית הרעש, $h(N)$, גדולה יותר בערוץ הגאוסי ולכן קיבול הערוץ הגאוסי קטן יותר. אם נתבונן באקספוננטי השגיאה נקבל את התמונה הבאה (באופן סכימטי):

ניתן לראות שיש תחום שבו לערוץ בעל הקיבול הקטן יותר יש אקספוננט שגיאה טוב (גדול) יותר.

בתכנון של מערכת תקשורת, נתונים הסתברות השגיאה P_e, ואורך הבלוק n, מהם אפשר לגזור את אקספוננט השגיאה $E = \frac{1}{n}\log P_e$. עבור E נתון, נרצה את הקצב R הגבוה ביותר. כיצד נעשה



זאת בדוגמא? נסמן את נקודת החיתוך בין הגרפים ב- $E^{critical}$. עבור $E > E^{critical}$ נשתמש בערוץ הגאוסי ועבור $E < E^{critical}$ נשתמש בערוץ התערובת הגאוסית. זו תוצאה לא שגרתית, משום שיש כאן סיטואציה בה נעדיף דווקא את הערוץ בעל הקיבול הקטן יותר.

שיטת הטיפוסים – The Method of Types

נתבונן בוקטור $\underline{x} = (x_1, x_2, \cdots, x_n)$ מעל א"ב בדיד X.
וקטור הטיפוס הוא

$$P_x = \left(\frac{N(0\,|\,\underline{x})}{n}, \frac{N(1\,|\,\underline{x})}{n}, \cdots, \frac{N(|X|\,|\,\underline{x})}{n} \right)$$

כאשר $N(a\,|\,\underline{x})$ הוא מספר ההופעות של סימבול a בוקטור $\underline{x}$.

1. ρ_n מוגדר כאוסף הטיפוסים האפשריים של וקטורים באורך n, כלומר אוסף הפילוגים הרציונליים עם מכנה n. במקרה הבינארי אפשר לתאר את הטיפוס ע"י מספר יחיד והוא יחס האחדים בוקטור. לכן במקרה הבינארי $\rho_n = \{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n}\}$, ומכך נובע ש $|\rho_n| = n+1$.
2. במקרה הכללי $|\rho_n| \le (n+1)^{|X|}$ (הגורם בצד ימין הוא מספר הוקטורים באורך $|X|$ מעל א"ב $\{0,1,\ldots,n\}$).
3. קבוצת הטיפוס T_ρ היא אוסף כל הוקטורים מטיפוס ρ. דוגמא בינארית $T_{2/4} = \{1100, 0011, 1010, 0101, 1001, 0110\}$.
4. גודל קבוצת הטיפוס $|T_\rho|$ הוא

במקרה הבינארי $2^{nH_B(\rho)} \cong \left|T_\rho\right| = \binom{n}{n\rho}$.

במקרה הלא בינארי $2^{nH(\underline{\rho})} \cong \left|T_\rho\right| = \binom{n}{n\rho_1, n\rho_2, \cdots, n\rho_{|X|}}$.

הסימן "$\cong$" מייצג שוויון עד כדי $n\varepsilon$ באקספוננט.

כמו כן $H(\underline{\rho}) = \sum_{i=0}^{|X|-1} \rho_i \log \rho_i$.

ליתר דיוק

$$(n+1)^{-|X|} 2^{nH(\underline{\rho})} \leq |T_p| \leq 2^{nH(\underline{\rho})}$$

5. ההסתברות שסדרה שהוגרלה בפילוג Q היא מטיפוס (כלומר, בפילוג אמפירי) ρ (המתאים לשכיחויות $N(a \mid \underline{x})$):

$$Q^n(\underline{x}) = \prod_{i=1}^{n} Q(x_i) = \prod_{a \in X} Q(a)^{N(a|\underline{x})}$$

במקרה הבינארי (כאשר הסתברות הגרלת 1 היא q):

$$Q^n(\underline{x}) = q^{N(1|\underline{x})}(1-q)^{N(0|\underline{x})} = q^{\rho n}(1-q)^{(1-\rho)n} = 2^{n\rho \log \rho} \times 2^{n(1-\rho)\log(1-\rho)}$$

עבור גודל א"ב כללי, ניתן להראות ש- $Q^n(\underline{x}) = 2^{-nD(\rho\|q)} \times 2^{-nH(\rho)}$, כאשר $D(\rho \| q)$ הוא ה Divergence המוגדר ע"י $D(\rho \| q) := \sum_{i=0}^{|X|-1} \rho_i \log \frac{\rho_i}{q_i}$.

הסתברות זו זהה לכל הסדרות בקבוצת הטיפוס.

6. הסתברות קבוצת הטיפוס T_ρ ביחס לפילוג יוצר Q

$$Q^n(T_\rho) \cong \left|T_\rho\right| 2^{-nD(\rho\|Q)} \times 2^{-nH(\rho)} = 2^{-nD(\rho\|Q)}$$

כידוע $D(\rho \| Q) \geq 0$ עם שוויון כאשר $\rho = Q$. כלומר הסתברות טיפוס יורדת ל- 0 אלא אם כן $\rho = Q$. משמעות המשפט היא AEP במובן חזק.

7. טיפוסיות מותנית של צמד $(\underline{x}, \underline{y})$:

$v := V_{y|x}$ הוא הפילוג האמפירי המותנה של y בהנתן x המחושב מתוך השכיחויות המשותפות של בוקטורים $\underline{x}$ ו- $\underline{y}$.

מספר הטיפוסים המותנים $|v| \leq (n+1)^{|X||Y|}$.

8. קבוצת טיפוס מותנה $T_v(\underline{x})$: היא קבוצת כל הסדרות $\underline{y}$ שהטיפוס המותנה שלהן בהנתן $\underline{x}$ (מטיפוס ρ) הוא v. גודל קבוצת הטיפוס המותנית

$$\left|T_v(\underline{x})\right| \cong 2^{nH(v|\rho)}$$

שימו לב ש $H(v \mid \rho) = H(y \mid x)$.

ליתר דיוק

$$(n+1)^{-|X||Y|} 2^{nH(v|\rho)} \leq |T(\underline{x})_v| \leq 2^{nH(v|\rho)}$$

9. הסיכוי שערוץ (בדיד וחסר זכרון) W יוציא $\underline{y}$ לא אופייני מטיפוס מותנה v עבור כניסה $\underline{x}$ מטיפוס ρ:

$$w^n(\underline{y} \mid \underline{x}) \cong 2^{-n[D(v\|w|\rho)]} \times 2^{-nH(v|\rho)}$$

זאת כאשר

$$D(v \| w \mid p) = \sum_{x \in X} p(x) \sum_{y \in Y} v(y \mid x) \log \frac{v(y \mid x)}{w(y \mid x)}$$

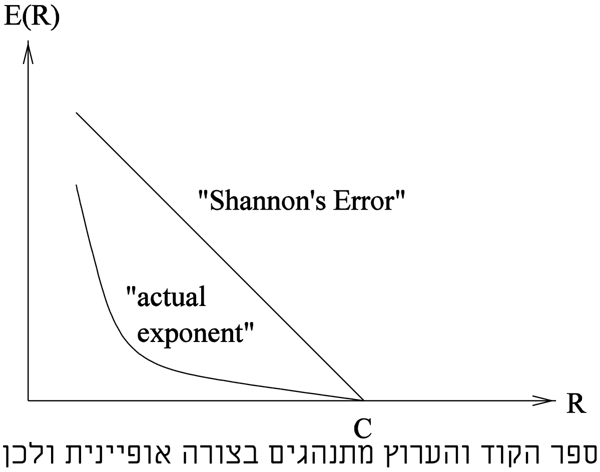
(p מייצג את פילוג הכניסה $p(x)$ ו- v מייצג את הפילוג המותנה $p(y|x)$)
גורם זה הוא ה divergence בין ערוץ v לערוץ w עבור פילוג הכניסה p .
הערה: ההסתברות המחושבת בסעיף זה היא בעצם הסיכוי שערוץ w יתנהג כמו v עבור כניסה המפולגת p .

ה"טעות" של שאנון (1948)

ממאמרו הקלאסי של שאנון משנת 1948 ניתן להבין את הטענה (השגויה) הבאה:
הסתברות השגיאה למילת אינפורמציה עבור קוד אקראי (המוגרל לפי פילוג p) העובר בערוץ w ומפוענח פענוח אופייניות משותפת היא בקירוב (לאורך בלוק n גדול):

$$P_e \cong 2^{-n[I(p,w)-R]^+}$$

(כאשר $[a]^+$ שווה ל a עבור a חיובי, ו-0 אחרת.)
ה"טעות" מתוארת באופן סכימטי בגרף הבא:



הצדקה של שאנון – ספר הקוד והערוץ מתנהגים בצורה אופיינית ולכן

$$1-\left(1-2^{-nI(p,w)}\right)^{2^{nR}} \le 2^{-n[I(p,w)-R]^+}$$

בצד שמאל זוהי ההסתברות שלא פענחנו אחת מ 2^{nR} המילים האחרות מספר הקוד. אי השוויון נובע מאי השוויון $1-ax \le (1-a)^x$, עבור $0 \le a < 1$ ו- $x > 1$.
הסבר לטעות: הזנחנו כאן את ההסתברות למאורעות לא אופייניים. בפועל חסמנו הסתברות זו מלמעלה ב ε והזנחנו את ε , בלי לדעת איך הוא שואף ל-0 עם אורך הבלוק.

שיטת ניתוח חליפית (Csiszár & Körner)

כיצד נתגבר על חוסר האופייניות?

1. נשתמש אך ורק במילות קוד אופייניות. נעשה זאת ע"י הגרלת מילות הקוד בהסתברות שווה מקבוצת הטיפוס T_ρ .
2. פענוח אוניברסלי – Maximum Mutual Information = MMI – מפענח ללא ידיעת הערוץ וכך יוכל לפענח גם כאשר הערוץ מתנהג בצורה בלתי אופיינית (היות והמפענח לא מניח שהוא יודע מה התנהגות הערוץ).

האקספוננט שמתקבל הוא

$$E(R)=E(p,w,R)=\min_v E(v)$$

כאשר

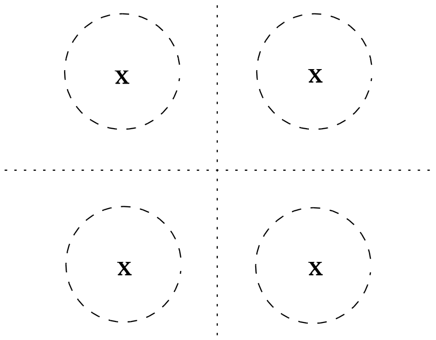
$$E(v):=D(v\,\|\,w\,|\,p)+[I(p,v)-R]^+$$

הגורם השמאלי באגף ימין הוא ההסתברות להתנהגות ערוץ v, הגורם הימני הוא הסתברות השגיאה בהנתן התנהגות v.

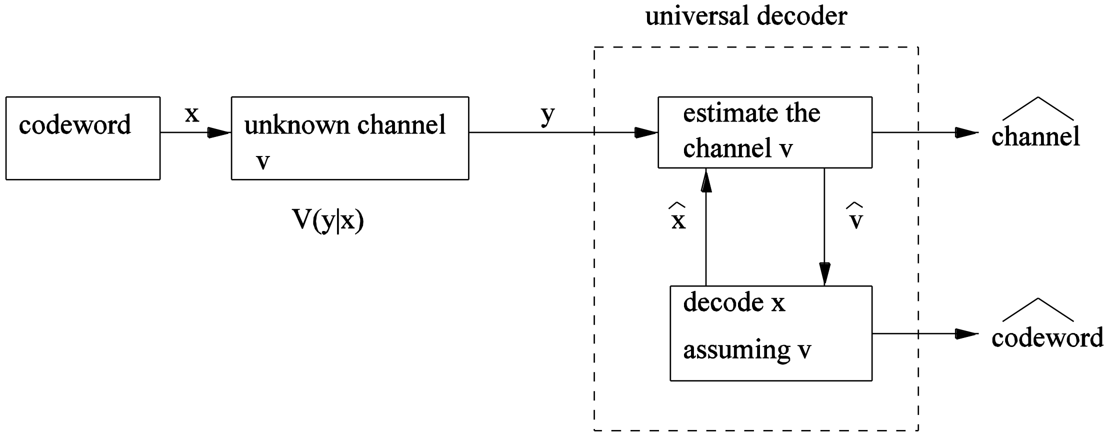
הערה : הביטוי הנ"ל לא בהכרח מתלכד עם הביטוי של Gallager, אבל הוא כן מתלכד ב p אופטימלי.

מהו פענוח אוניברסלי?

הסכימה הבאה היא במרחב רב מימדי של וקטורי מילות הקוד עבור ערוץ גאוסי. x מייצגים את נקודות הקונסטלציה (מילות הקוד), הקווים הישרים הם תחומי ההחלטה לפי כלל סבירות מירבית, והעיגולים הם תחומי ההחלטה בפענוח אופייניות משותפת



מפענח אוניברסלי עובד באופן סכימטי כמו בתרשים הבא – הוא כולל משערוך של הערוץ ומשערוך של מילות הקוד בהנתן הערוץ שמזינים זה את זה:



מהי הסתברות השגיאה בפענוח אוניברסלי

$$P_e = \Pr(erroneous decoding) =$$
$$\sum_v \Pr(channel\ behaviour\ is\ v) \times \Pr(error\ in\ universal\ decoder \mid channel\ behavior\ is\ v)$$

<u>מהי התנהגות ערוץ מסוג v?</u>

הכוונה היא להתנהגות ה"ערוץ האמפירי", כלומר לטיפוס המותנה של מוצא הערוץ $\underline{y}$ בהינתן כניסת הערוץ $\underline{x}$. כפי שראינו קודם, ההסתברות להתנהגות v של ערוץ היא

$$\Pr(channel\ behaviour\ is\ v) \cong 2^{-nD(v\|w|p)}$$

אנו טוענים (ונוכיח בהמשך) שהסתברות השגיאה כאשר הערוץ מתנהג v היא

$$\Pr(error\ in\ universal\ decoder \mid channel\ behavior\ is\ v) \cong 2^{-n[I(p,v)-R]^+}$$

נמשיך בניתוח Pe , נזכור שסכומם של גורמים אקספוננציאליים נשלט ע"י הגורם הגדול ביותר. לכן

$$P_e \cong \max_v 2^{-nD(v\|w|p)} \times 2^{-n[I(p,v)-R]^+} = 2^{-n\min_v\left[D(v\|w|p)+[I(p,v)-R]^+\right]} = 2^{-nE(R,p)}$$

פענוח Maximum Mutual Information (MMI)

הגדרה

אינפורמציה הדדית אמפירית בין שתי סדרות $\underline{x}$, $\underline{y}$

$$I(\underline{x} \wedge \underline{y}) := I(p_{\underline{x}}, V_{\underline{y}|\underline{x}})$$

כאשר $V_{\underline{y}|\underline{x}}$ הוא טיפוס המעבר האמפירי, ו- $p_{\underline{x}}$ הוא טיפוס המבוא.

פענוח MMI:

הגדרה

$$i = \arg\max_{i=1,2,\dots,2^{nR}} I(\underline{x}_i \wedge \underline{y})$$

אינטואיציה

במקרה האדיטיבי הקריטריון יהיה מינימום על $H(\underline{y} - \underline{x}_i)$, כלומר, מלה עבורה הרעש בערוץ הוא מינימלי (במובן מינימום אנטרופיה).

ניתוח הסתברות השגיאה במפענח MMI

נניח שידור מילה $\underline{x}_0$ וקליטת מילה $\underline{y}$. $\underline{x}$ היא מלה המוגרלת בהסתברות שווה מתוך קבוצת הטיפוס T_p. נסמן

$$p' := \Pr\{I(\underline{x} \wedge \underline{y}) > I(\underline{x}_0 \wedge \underline{y})\}$$

זו ההסתברות שמילת קוד אחרת שהגרלנו, $\underline{x}$, מפוענחת במקום $\underline{x}_0$. נסמן $I(p,v) := I(\underline{x}_0 \wedge \underline{y})$. שימו לב, שבהגדרה, ההסתברות p' זהה לכל $\underline{y}$ עבורה $I(p,v) := I(\underline{x}_0 \wedge \underline{y})$.

טענה

$$p' \le 2^{-n[I(p,v)-\delta]^+}$$

הוכחה

ראשית נחשב את ההסתברות שמילה $\underline{y}$ שייכת לקבוצת הטיפוס המותנה $T_{\hat{v}}(\underline{x})$, עבור $\underline{x}$ המוגרל בהסתברות שווה מתוך T_p:

$$\Pr\{\underline{y} \in T_v(\underline{x})\} = \frac{|\{\underline{x} : \underline{x} \in T_p, \underline{y} \in T_{\hat{v}}(\underline{x})\}|}{|T_p|}$$

השוויון נובע מהעובדה שכל המילים בקבוצת הטיפוס T_p הן שוות הסתברות. נסמן את פילוגי ה"ערוץ ההפוך" : נסמן ב $\hat{v}$ את פילוג המעבר $p(x|y)$, וב P את הפילוג השולי של y המתאימים ל- $\hat{v}$ ו p . אזי,

$$|\{\underline{x} : \underline{x} \in T_p, \underline{y} \in T_{\hat{v}}(\underline{x})\}| \le 2^{nH(\hat{v}|p)}$$

כמו כן, אנו יודעים ש

$$|T_p| \ge (n+1)^{|X|} 2^{nH(p)}$$

אם נציב נקבל

$$\Pr\{\underline{y} \in T_{\hat{v}}(\underline{x})\} \le (n+1)^{|X|} 2^{-nI(p,\hat{v})}$$

כעת נפנה לחישוב p' . מתוך חסם האיחוד נובע ש

$$p' \le \sum_{\hat{v}:I(p,\hat{v})\ge I(p,v)} \Pr\{\underline{y} \in T_{\hat{v}}(\underline{x})\} \le |V| \times \max_{\hat{v}:I(p,\hat{v})\ge I(p,v)} \left(\Pr\{\underline{y} \in T_{\hat{v}}(\underline{x})\}\right)$$

$|V|$ הוא מספר טיפוסי המעבר החסום ע"י $|V| \le (n+1)^{|X||Y|}$. כמו כן

$$\max_{\hat{v}:I(p,\hat{v})\ge I(p,v)} \left(\Pr\{\underline{y} \in T_{v}(\underline{x})\}\right) \le \max_{\hat{v}:I(p,\hat{v})\ge I(p,v)} (n+1)^{|X|} 2^{-nI(p,\hat{v})} \le (n+1)^{|X|} 2^{-nI(p,v)}$$

לכן

$$p' \le (n+1)^{|X|+|X||Y|} 2^{-nI(p,v)} \le 2^{-n[I(p,v)-\delta]^+}$$

לקיחת הערך החיובי היא מתוך חסם טרוויאלי $p' \le 1$, וזו הוכחת הטענה.

הסתברות השגיאה הכוללת היא 1 פחות ההסתברות שאף מילה אחרת שהגרלנו לא מפוענחת במקום $\underline{x}_0$. כלומר

$$\Pr(error\ in\ universal\ decoder |\ channel\ behavior\ is\ v) = 1 - (1-p')^{2^{nR}}$$

נציב את p' ונשתמש באי השוויון $1 - ax \le (1-a)^x$

$$\Pr(error\ in\ universal\ decoder |\ channel\ behavior\ is\ v) \le 2^{-n[I(p,v)-R-\delta]^+}$$

כעת, אם נציב גורם זה בביטוי שקיבלנו קודם (הכולל מיצוע של הסתברות השגיאה על פני התנהגויות הערוץ) נקבל

$$P_e \le 2^{-n[E(R,p)-\delta]}$$

כאשר $E(R,p)$ הוא אקספוננט השגיאה הרצוי.

<u>הערה</u>

ניתוח מתמטי מפורט יותר מבוסס על "למת האריזה" של Csiszár & Körner ונמצא ב [1] פרק 5, עמודים 162-166.

<u>בבליוגרפיה</u>

[1] I. Csiszár and J. Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press, 1981.

[2] I. Csiszár, "The Method of Types," Trans. Info. Theory, Vol. 44, No. 6, pp. 2505--2523, Oct. 1998

[3] T. M. Cover and J. A. Thomas, "Elements of Information Theory", John Wiley & Sons, Inc., 1991, Chapter 12

הרצאות 12-13

משפט Gelfand & Pinsker או Writing on Dirty Paper Theorem[2]

סוכם ע"י יוסי קדישביץ

ערוצים תלויי מצב

ערוץ תלוי מצב הוא ערוץ בו הסתברות המעבר מכניסת הערוץ $\underline{x}$ למוצאו $\underline{y}$ תלויה בוקטור פרמטרים נוסף $\underline{s}$ שניקרא מצב המערכת. במילים אחרות $\underline{y}$ נקבע ע"י חוק ההסתברות $p\left(\underline{y}|\underline{x},\underline{s}\right)$. ניתן מספר דוגמאות לערוצים תלויי מצב.

א. המצב תלוי באינפורמציה המשודרת דוגמת ערוץ ISI בו הסתברויות המעבר תלויות באינפורמציה ששודרה בערוץ במשך הסימבולים הקודמים. (הפתרונות הנפוצים במקרה זה הם אלגוריתם ויטרבי equalizers למיניהם, מעבר לציר התדר כמו ב OFDM וכו.) ערוצים אלו מכונים ערוצים עם זכרון ומשתנה המצב שלהם הוא הזיכרון האגור בערוץ

ב. סוג נוסף הוא ערוצים בהם המצב נקבע ע"י הטבע דהינו הוא תהליך אקראי שדגמי התהליך הם משתני המצב והם קובעים את הסתברויות המעבר. גם כאן ניתן להבחין בין ערוצים בהם יש תלות בין משתני המצב של הסימבולים השונים (שנקראים ערוצים בעלי זיכרון) לבין המקרה בו משתני המצב של הסימבולים השונים הם בלתי תלויים (שיקראו חסרי זיכרון). להלן דוגמאות לערוצים תלויי מצב (בהם המצב נקבע ע"י הטבע) בעלי זיכרון

a. פרמטרי הערוץ קבועים לאורך מפרק זמן שיכונה בלוק. ומשתנים בין בלוק לבלוק. דוגמא לערוץ כזה הוא ערוץ מקלט משדר (מקמ"ש) מדלג תדר איטי השוהה בכל פרוסת תדר זמן ממושך. פרוסות התדר נבדלות ביניהן ביחס האות לרעש (SNR) . פרמטר זה הוא משתנה המצב (במקרה זה נבצע לימוד ה SNR מהאות הנקלט ולאחר מכן פיענוח ע"פ הפרמטר המשוערך)

b. דוגמא נוספת היא כאשר המצב הוא דגימות של תהליך מרקובי (דוגמת רעש פאזה וכו,) במקרים אלו ניתן לנצל את הזיכרון של התהליך על מנת ללמוד את חלקו או כולו ולשפר בכך את בצועי הגילוי כי המקלט יכול לפעול כאילו משתני המצב ידועים. ערוצים אלו טופלו ע"י Gallager.

בהמשך נתייחס רק לערוצים תלויי מצב ללא זיכרון כאשר המצב נקבע ע"י הטבע.

אינפורמציית צד וקיבולת של ערוצים בעלי אינפורמציית צד

אם קיים מידע על משתנה המצב של ערוץ תלוי מצב נקרא למידע זה אינפורמציית צד. נניח במהלך הדיון כי אינפורמציית הצד מתאפשרת לשחזר את משתני המצב במדויק ללא שגיאות. לשם פשטות נניח כי הכניסה לערוץ המוצא מהערוץ ומשתנה המצב הם בעלי א"ב סופי.

$$x \in X$$

$$y \in Y$$

$$s \in S$$

ניבחן מספר מיקרים של אינפורמציית צד והשפעתם על קיבולת הערוץ.

אינפורמציית הצד אינה ידועה לא למקלט ולא למשדר

במקרה זה הערוץ האקוויוולנטי מיוצג ע"י ערוץ סטציונרי בעל הסתברויות מעבר

$$p\left(\underline{y}|\underline{x}\right)=\sum_{s} p\left(\underline{y}|\underline{x},\underline{s}\right)p\left(\underline{s}|\underline{x}\right)=\sum_{s} p\left(\underline{y}|\underline{x},\underline{s}\right)p\left(\underline{s}\right)$$

[2] ראה גם סיכומי הרצאות 2006, "בעיית GP" ו-"בעיית Costa"

והקיבול נתון ע"י

$$C = \sup_{p(x)} I(Y;X)$$

אינפורמציית הצד ידועה הן למקלט והן למשדר

במקרה זה לכל ערך של משתנה מצב ניתן לבחור ספר קוד אופטימלי ואז ניתן להראות כי

$$C = E\left\{ \sup_{p(x|s)} I(X;Y|S) \right\}$$

$$I(X;Y|S) = \sum_{x\in X}\sum_{y\in Y} p(x,y|s)\log\left[p(x,y|s)\right]$$

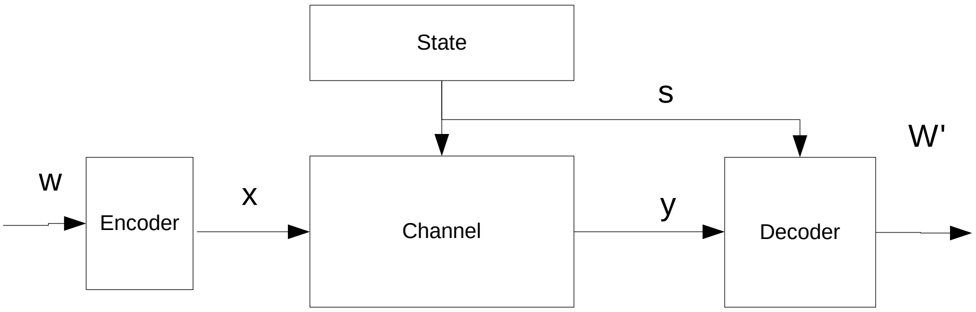
אינפורמציית הצד ידועה למקלט אך לא למשדר

במקרה זה יש לנו ערוץ אקוויוולנטי הנראה בציור 1 שלו יש כניסה אחת x ו 2 מוצאים y,s.
הקיבולת של ערוץ זה נתונה ע"י

$$C = \sup_{p(x)} I(X;Y,S) = \sup_{p(x)} E\left\{\log\left[\frac{p(y,s)}{p(y,s|x)}\right]\right\} = \sup_{p(x)} E\left\{\log\left[\frac{p(y,s)}{p(y|x,s)\,p(s|x)}\right]\right\} =$$

$$= \sup_{p(x)} E\left\{\log\left[\frac{p(y,s)}{p(y|x,s)\,p(s)}\right]\right\} = \sup_{p(x)} E\left\{\log\left[\frac{p(y|s)}{p(y|x,s)}\right]\right\} = \sup_{p(x)} I(X;Y|S)$$

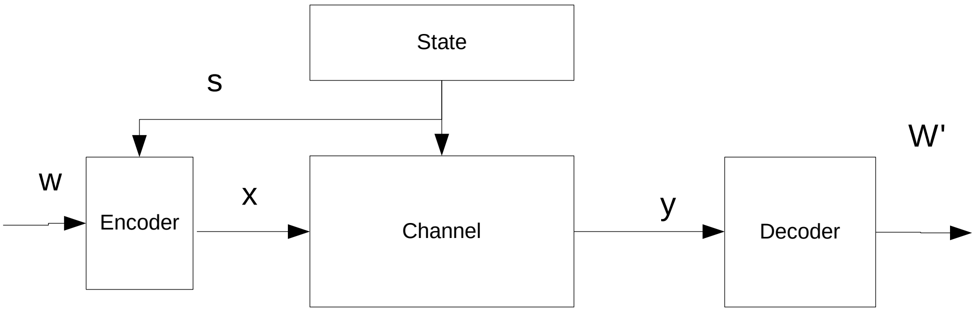
$$p(y|s) = \sum_{x\in X} p(y|x,s)\,p(x)$$



ציור 1

אינפורמציית הצד ידועה למשדר אך לא למקלט

במקרה זה לא ניתן להתייחס לערוץ זה כערוץ עם 2 כניסות x,s ומוצא y היות ולמשדר אין שליטה על המצב. מקרה זה דורש לכן התייחסות נפרדת. הערוץ מתואר בציור 2.



ציור 2

הפתרון לערוץ זה מתחלק ל 2 מקרים: המקרה בו אינפורמציית הצד ידועה למשדר בצורה סיבתית (כגון מקרה של מפריע חזק זר המתווסף לערוץ ואינפורמציית הצד היא המדידות

שלו אותן אנו יודעים רק ברגע המדידה) ומקרה בו אינפורמציית הצד ידועה למשדר באופן לא סיבתי (לדוגמא מקרה של ערוץ Broadcast כאשר אינפורמציית הצד היא השידור למקלט השני. במקרה זה המקודד יודע את ההודעה המשודרת מראש ולכן הוא יודע גם את האות המשודר למקלט השני עוד לפני ששודר וניתן לעשות בידע זה שימוש לצורך קידוד)

אינפורמציית צד סיבתית במשדר

בעיה זו נפתרה ע"י Shannon בשנת 1958 והפיתרון הוא

$$C^{causal}=\sup_{p(u)} I(U;Y)$$

$$F=\left\{f(1,s),f(2,s),\dots f\left(|X|^{|S|},s\right)\right\}$$

$$u\in\left[1,|X|^{|S|}\right]$$

$$u\perp s$$

$$x=f(u,s)$$

$$p(u,s,x,y)=p(s)\,p(u)\,p(y|x,s)$$

כאשר f(u,s) היא פונקציה דטרמיניסטית של u,s והיא האסטרטגיה הנבחרת עליה הוחלט מראש. בתור אסטרטגיה נגדיר מיפוי מ S→X. יש $|X|^{|S|}$ מיפויים כאלה. האינפורמציה אותה רוצים להעביר נמצאת בבחירת המיפוי והפילוג שעליו עושים את האופטימיזציה הוא פילוג ההסתברות של בחירת המיפוי.

אינפורמציית צד לא סיבתית במשדר בעייתGelfand & Pinsker

בעיה זו ניפתרה ע"י Gelfand & Pinsker בשנת 1980 והפתרון הוא

$$C_{GP}=\sup_{p(u,x|s)}\left\{H(U|S)-H(U|Y)\right\}=\sup_{p(u,x|s)}\left\{I(U;Y)-I(U;S)\right\}$$

כאשר U,X,S,Y יוצרים שלשה מרקובית

$$U\leftrightarrow(X,S)\leftrightarrow Y$$

הערות:

א. האופטימום מושג כאשר x הוא פונקציה דטרמיניסטית של s,u $x=f(u,s)$.

ב. נשים לב שבפתרון יש תלות בין u ל s וזה השוני בינה לבעיית Shannon. אם נאלץ תנאי U⊥S אזי נקבל את התוצאה של Shannon

ג. בד"כ הבעיה מופיעה עם אילוצי כניסה כדוגמת אילוץ הספק $\frac{1}{n}E\left\{\sum_{i=0}^{n}C(x_i)\right\}\le P$ כאשר $C(x_i)$ היא פונקצית מחיר של אות בודדת, או אילוץ עוות $\frac{1}{n}E\left\{\sum_{i=0}^{n}d(s_i,s_i+x_i)\right\}\le D$ אילוצים אלו הופכים את הבעיה ללא טריוויאלית.

דוגמאות לישומי בעיתGelfand & Pinsker

1. בעית מפריע אדיטיבי ללא רעש מעל שדה בינארי (Shannon 1958)

$y=x\oplus s$ במקרה זה הפיתרון הוא טריוויאלי $x=w\oplus s$ אך הוא מסתבך אם יש אילוץ על מספר ה "1" ב x .

2. <u>שדור אות BPSK בערוץ עם הפרעה שלמה</u>

במקרה זה

$$x\in[-1,1]$$

$$s\in\mathbb{Z}\quad s\in[0,\pm1,\pm2,\ldots,\pm N,\ldots]$$

$$y=x+s$$

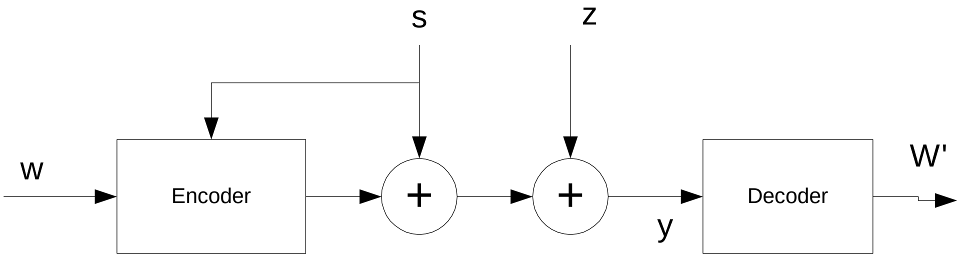
נתבונן במשוואה שלמעלה מודולו 4 , $y \mod 4=(x+s) \mod 4$ ובטבלת הקדוד הבאה

s mod 4	x	y mod 4	
		w=-1	w=1
0	x=w	3	1
1	x=w	0	2
2	x=-w	3	1
3	x=-w	0	2

מעיון בטבלה נקבל כי עבור $y\in[0,3]$ w=-1 ועבור $y\in[1,2]$ w=1 והפיענוח התבצע ללא שגיאה. במקרה זה הקיבול עם הפרעה זהה לקיבול בלי הפרעה.

3. <u>בעיית Costa</u>

בבעיה זו נתון ערוץ עם רעש גאוסי אדיטיבי והפרעה אדיטיבית. הבעיה מתוארת בציור 3



ציור 3

הספק השידור של המקור בבעיה זו מוגבל ל P . ללא מגבלה זו הפיתרון הוא טריוויאלי המשדר פשוט מחסיר את ההפרעה (משדר סיגנל x=w-s ולאחר תוספת s ע"י הערוץ ההפרעה מתבטלת). מגבלת הספק השידור גורמת לכך שלא ניתן להחסיר את סיגנל השידור במלואו. בעיה זו נקראת כתיבה על ניר מלוכלך (Writing on Dirty Paper). נתבונן במקרה בו פילוג ההפרעה הוא גאוסי

$$y=x+s+z$$

$$s\sim N(0,Ps)$$

$$z\sim N(0,\sigma^2)$$

$$z\perp s$$

נבחר $x\perp s\perp z$ $x\sim N(0,P)$ כמו כן נבחר $u=\alpha s+x$ כאשר α קבוע. אנו נראה בהמשך כי $h(u|s)-h(u|y)$ עבור בחירה זו זהה לקיבול של הערוץ ללא הפרעה מכאן האופטימום מתקבל עבור בחירה זו של פילוג גאוסי עבור x שהוא בלתי תלוי ב s. היות ו u היא פונקציה דטרמיניסטית של s,x אזי מתקיים בהכרח התנאי

$$u\leftrightarrow(x,s)\leftrightarrow y$$

ע"פ Gelfand & Pinsker

$$C=\sup_{p(u,x|s)}\left\{h(u|s)-h(u|y)\right\}$$

$$h(u|s)=h(\alpha s+x|s)=h(x)=\frac{1}{2}\log(2\pi eP)$$

$$h(u|y)=h(u,y)-h(y)$$

בבחירה שלנו u,y הם גאוסיים במשותף (כי הם קומבינציה לינארית של מ"א גאוסיים x,s,z)
אזי האנטרופיה המשותפת שלהם

$$h(u,y)=\frac{1}{2}\log\left[(2\pi e)^2\left|R_{u,y}\right|\right]$$

$$R_{u,y}=E\left\{\begin{bmatrix}u\\y\end{bmatrix}\begin{bmatrix}u & y\end{bmatrix}\right\}=\begin{bmatrix}E\left\{u^2\right\} & E\{uy\}\\E\{uy\} & E\left\{y^2\right\}\end{bmatrix}$$

$$E\left\{u^2\right\}=E\left\{(\alpha s+x)^2\right\}=\alpha^2E\left\{s^2\right\}+E\left\{x^2\right\}=\alpha^2Ps+P$$

$$E\{uy\}=E\left\{(\alpha s+x)(s+x+z)\right\}=\alpha E\left\{s^2\right\}+E\left\{x^2\right\}=\alpha Ps+P$$

$$E\left\{y^2\right\}=E\left\{(x+y+z)^2\right\}=E\left\{x^2\right\}+E\left\{s^2\right\}+E\left\{z^2\right\}=P+Ps+\sigma^2$$

$$\left|R_{u,y}\right|=\left|\begin{bmatrix}\alpha^2Ps+P & \alpha Ps+P\\\alpha Ps+P & Ps+P+\sigma^2\end{bmatrix}\right|=\left(\alpha^2Ps+P\right)\left(Ps+P+\sigma^2\right)-\left(\alpha Ps+P\right)^2=$$

$$=\alpha^2Ps^2+\left(1+\alpha^2\right)PsP+P^2+\sigma^2\left(\alpha^2Ps+P\right)-\alpha^2Ps^2-2\alpha PsP-P^2=$$

$$=(1-\alpha)^2PsP+\sigma^2\left(\alpha^2Ps+P\right)$$

$$h(u,y)=\frac{1}{2}\log\left\{(2\pi e)^2\left((1-\alpha)^2PsP+\sigma^2\left(\alpha^2Ps+P\right)\right)\right\}$$

$$h(y)=\frac{1}{2}\log\left\{2\pi e\left(Ps+P+\sigma^2\right)\right\}$$

נסמן ב *C את הערך המתקבל במשואת Gelfand & Pinsker כשמציבים בתוכה את הבחירה שלנו עבור x ומבצעים מכסימיזציה על α.

$$C^*=\max_{\alpha}\frac{1}{2}\log\left\{\frac{P\left(P+Ps+\sigma^2\right)}{(1-\alpha)^2PsP+\sigma^2\left(\alpha^2Ps+P\right)}\right\}$$

מכסימום של *C מתקבל כאשר המכנה הוא מינימלי לכן

$$\frac{\partial}{\partial\alpha}\left((1-\alpha)^2PsP+\sigma^2\left(\alpha^2Ps+P\right)\right)=0$$

$$-(1-\alpha)PsP+\sigma^2\alpha Ps=0$$

$$\alpha=\frac{P}{P+\sigma^2}$$

מהצבת α האופטימלי לתוך המשואה של *C נקבל

$$C^* = \frac{1}{2}\log\left\{\frac{P\left(P+Ps+\sigma^2\right)}{\left(1-\alpha^*\right)^2 PsP+\sigma^2\left(\alpha^{*2} Ps+P\right)}\right\} =$$

$$= \frac{1}{2}\log\left\{\frac{P\left(P+Ps+\sigma^2\right)}{\left(\frac{\sigma^2}{P+\sigma^2}\right)^2 PsP+\sigma^2\left(\left(\frac{P}{P+\sigma^2}\right)^2 Ps+P\right)}\right\} =$$

$$= \frac{1}{2}\log\left\{\frac{\left(P+Ps+\sigma^2\right)\left(P+\sigma^2\right)^2}{\sigma^4 Ps+\sigma^2\left(PPs+\left(P+\sigma^2\right)^2\right)}\right\} = \frac{1}{2}\log\left\{\frac{\left(P+Ps+\sigma^2\right)\left(P+\sigma^2\right)^2}{\sigma^2 Ps\left(\sigma^2+P\right)+\sigma^2\left(P+\sigma^2\right)^2}\right\} =$$

$$\frac{1}{2}\log\left\{\frac{\left(P+Ps+\sigma^2\right)\left(P+\sigma^2\right)^2}{\sigma^2\left(\sigma^2+P\right)\left(Ps+P+\sigma^2\right)}\right\} = \frac{1}{2}\log\left\{1+\frac{P}{\sigma^2}\right\} = \tilde{C}$$

$\tilde{C}$ הוא קבול הערוץ כאשר ההפרעה ידועה הן למשדר והן למקלט (היות וההפרעה היא אדיטיבית זה שקול למקרה בו ההפרעה אינה קימת). ברור כי קיבול הערוץ כאשר ההפרעה ידועה גם למשדר וגם למקלט גדול שווה לקיבול כאשר ההפרעה ידועה רק למשדר היות ואינפורמציה נוספת אינה יכולה לקלקל לכן אינה מקטינה את הקיבול.

$$C \ge C^*$$
$$\tilde{C} \ge C \quad \Rightarrow C = C^* = \tilde{C}$$
$$\tilde{C} = C^*$$

מכאן שהבחירה שלנו בפילוג המשתנים u,x היא אופטימאלית. כמו כן מסקנה נוספת היא שאין כל הפסד מאי ידיעת ההפרעה במקלט, או במילים אחרות קיבול ערוץ גאוסי עם הפרעה אדיטיבית הידועה למשדר זהה לקיבול הערוץ הגאוסי ללא כל הפרעה.

4. בעיית Digital Water Marking או Information Embedding

בבעיה זו נתון סיגנל כלשהוא (אנלוגי או דיגיטאלי) ורוצים להטמין בתוכו מידע דיגיטאלי. המקלט משחזר את הסיגנל המקורי וכן מחלץ את המידע הדיגיטאלי. שמושים לבעיה זו יכולים להיות בהטמנת מידע זכויות יוצרים בתוך סרט וכו' . בעיה זו מתוארת בציור 4.

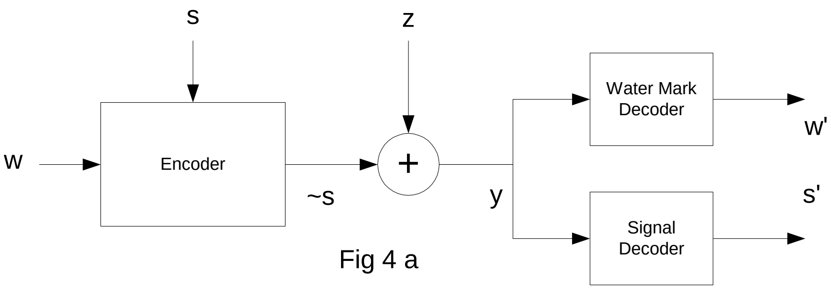


Fig 4 a

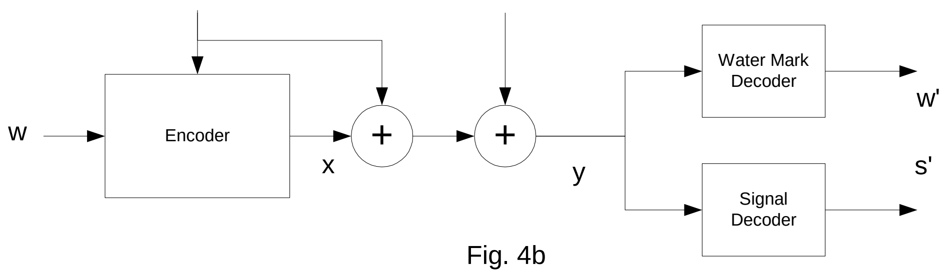


Fig. 4b

ציור 4

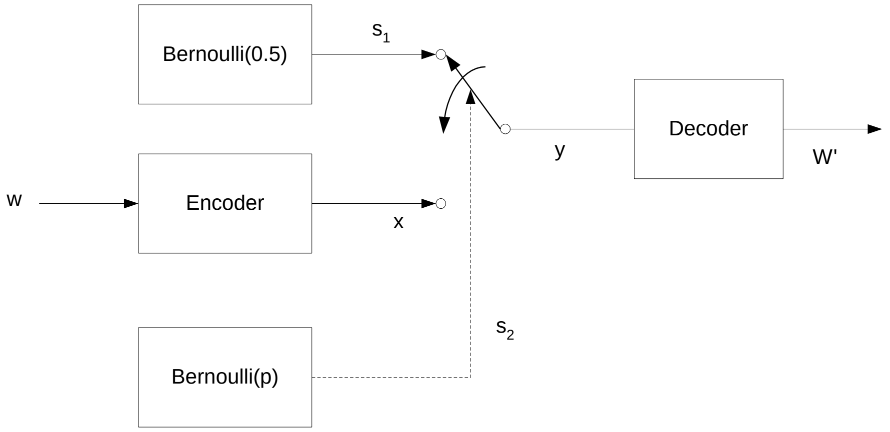
במקרה זה נרצה שהעיוות שנגרם לסיגנל המקורי במוצא המקלט לא יהיה גדול מהעיוות המכסימלי הנסבל D. השאלה היא מה גודל האינפורמציה אתה נוכל להטמין כך שהעיוות לא יעלה על D. ז"א

$$\frac{1}{n}E\left\{\left|s-\tilde{s}\right|^{2}\right\}\leq D$$

מודל זה שקול למודל בציור 4b כאשר $x=s-\tilde{s}$. תאור זה זהה לתאור של בעיית Costa ואם פילוג s הוא גאוסי בעיה זו שקולה לבעיית Costa .

5. <u>בעית זיכרון עם תאים תקולים</u>

נתון מערך זיכרון שיש לו תאים תקולים. כאשר פונים לתא תקול הוא מוצא במוצאו "1" או "0" בהסתברות 0.5. תא תקין מוציא במוצאו את אשר נכתב בו. הכותב יודע מי התאים התקולים ואילו הקורא אינו יודע וקורא באופן רציף. ניתן לתאר מערכת זו כמערכת עם מקודד ותהליך Bernoulli 1/2 ומתג הבוחר ביניהם המפוקד ע"י תהליך Bernoulli אחר שהוא משתנה המצב S. תאור זה נראה בציור 5.



ציור 5

תאור זה מבוטא ע"י המשוואה

$$y=x\left(1-s_{2}\right)+s_{1}s_{2}$$

$$y,x,s_{1},s_{2}\in\left[0,1\right]$$

$$S=\left(s_{1},s_{2}\right)$$

כאשר S הוא משתנה המצב. נניח כי p היא ההסתברות לתא תקול. אם גם הכותב וגם הקורא יודעים מי הם התאים התקולים הם אינם משתמשים בהם ומשתמשים רק בתאים התקינים. במקרה זה כמות האינפורמציה האגורה במערך ע"פ חוק המספרים הגדולים N(1-p) בהסתברות השואפת ל 1 כאשר N מספר התאים שואף לאינסוף או הקיבולת הממוצעת לתא

$$\tilde{C}\triangleq\frac{N\left(1-p\right)}{N}=1-p$$

נתבונן במקרה בו אינפורמציית הצד ידועה רק לכותב. נסמן את הקיבולת במקרה בו אינפורמציית הצד ידועה רק למשדר ב C. ברור כי $\tilde{C}\geq C$. נבחר u=y . תנאי השרשרת המרקובית $u\leftrightarrow\left(x,S\right)\leftrightarrow y$

מתקיים היות ויש תלות דטרמיניסטית בין y לזוג (x,S) . נסמן את הקיבולת המתקבלת ע"פ משוואת GP (Gelfand Pinsker) כשמציבים את הבחירה שלנו עבור u ב *C

$$C^*=H(u|S)-H(u|y)$$
$$u=y$$
$$H(y|y)=0$$
$$s_2=0\rightarrow y=x$$
$$x\perp S$$
$$s_2=1\rightarrow y=s_1$$
$$C^*=H(y|S)=p(s_2=0)H(x|S)+p(s_2=1)H(s_1|S)=(1-p)H(x)=1-p$$
$$\tilde{C}\geq C$$
$$C\geq C^*$$
$$C^*=\tilde{C}\Rightarrow C^*=C=\tilde{C}$$

מכאן הבחירה שלנו עבור u היא אופטימלית וכן הקיבולת הממוצעת לביט זהה עבור 2 המקרים כאשר יש אינפורמציית צד בשני הצדדים וכאשר יש אינפורמציית צד אצל הכותב בלבד.

הוכחת השגת הקצב של Gelfand & Pinsker

אלגוריתמי הקידוד והפענוח

נניח כי נתונה פונקציה דטרמיניסטית המקודדת את x כך ש x=f(u,s) והפילוג המותנה p(u|s). במקרה זה u,x,s,y הם שלשה מרקובית מהצורה $u\leftrightarrow(x,s)\leftrightarrow y$ היות לכל u כך ש

$$p(u)\neq 0$$
$$p(s|u)=\frac{p(u|s)p(s)}{p(u)}$$
$$p([x,s]|u)=\sum_{s\ \ s.t.\ \ x=f(u,s)}p(s|u)=\sum_{s\ \ s.t.\ \ x=f(u,s)}\frac{p(u|s)p(s)}{p(u)}=\sum_{s\ \ s.t.\ \ x=f(u,s)}\frac{p(u|s)p(s)}{\sum_s p(u|s)p(s)}$$

והערוץ נתון ע"י p(y|x,s).

בניית ספר קוד

נתענין בזוג האופייני (u,s) ע"פ משפט הגבול המרכזי יש זוגות כאלה וההסתברות לזוג אופייני שואפת ל 1 כאשר n אורך הבלוק שואף לאינסוף. נגריל $2^{nR'}$ מילות קוד של u האופייניות במשותף עם s. נחלק את $2^{nR'}$ מילות קוד של u ל 2^{nR} בינים באופן אקראי ולכל בין נתאים הודעת מקור w. כאן נכנסת דרישת הקידוד הלא סיבתי היות ואנו דורשים למצוא u ובהתאם לכך גם x שאופייני במשותף עם כל הווקטור s ולא רק עם החלק הסיבתי שלו.

הקידוד

בהנתן w,s נבחר מספר הקוד מילה u השייכת לבין w האופיינית במשותף עם s. באם s המתקבל מהערוץ אינו אופייני או בין w אינו מכיל מילה u שאופיינית במשותף עם ווקטור משתנה המצב s המתקבל מהערוץ המקודד יעביר הודעת שגיאה. נקרא למאורע זה "שגיאת משדר"

הפענוח

הפילוג המותנה $p(y|u)$ נתון ע"י

$$p\left(y,x,s\middle|u\right)=p\left(y\middle|x,s,u\right)p\left(x,s\middle|u\right)=p\left(y\middle|x,s\right)p\left(x,s\middle|u\right)=p\left(y\middle|x,s\right)p\left(x\middle|u,s\right)p\left(s\middle|u\right)$$

$$p\left(x\middle|u,s\right)=\delta\left(f\left(u,s\right)\right)$$

$$p\left(y\middle|s\right)=\sum_s\sum_x p\left(y\middle|x,s\right)p\left(x\middle|u,s\right)p\left(s\middle|u\right)=\sum_s p\left(y\middle|f\left(u,s\right),s\right)p\left(s\middle|u\right)=$$

$$=\sum_s p\left(y\middle|f\left(u,s\right),s\right)\frac{p\left(u\middle|s\right)p\left(s\right)}{\sum_s p\left(u\middle|s\right)p\left(s\right)}$$

מכאן ישנם זוגות $(\underline{y},\underline{u})$ שאופייניים במשותף וההסתברות לזוג אופייני שואפת ל 1 כאשר n שואף לאינסוף. המפענח מחפש את הווקטור $\underline{u}$ שאופייני במשותף עם הווקטור הנקלט $\underline{y}$. ההודעה המשודרת $\underline{w}$ היא מספר הבין בו נמצא $\underline{u}$. מאורע שגיאה קורה באם הווקטור $\underline{y}$ אינו אופייני או שיש יותר מווקטור $\underline{u}$ אחד שאופייני במשותף עם $\underline{y}$ או שהתקבל מהמשדר קוד שגיאה. נקרא למאורע זה "שגיאת מקלט"

חישוב הסתברות השגיאה

עבור ε נתון קיים n_1 כך שלכל $n>n_1$ ההסתברות ל $\underline{s}$ לא טיפוסי היא $\Pr\left(\underline{s}\notin A_n^{\varepsilon}\left(\underline{s},\underline{u}\right)\right)\le\varepsilon$ וקיים n_2 כך שלכל $n>n_2$ ההסתברות ל $\underline{y}$ לא טיפוסי $\Pr\left(\underline{y}\notin A_n^{\varepsilon}\left(\underline{y},\underline{u}\right)\right)\le\varepsilon$. עבור n מספיק גדול בהנחה שמגרילים ספר קוד אקראי תוכלת ההסתברות למאורע שגיאה היא

$$\bar{P}_e=\Pr\left(Rx_error\bigcup Tx_error\right)$$

$$Rx_error=\left(\underline{y}\notin A_n^{\varepsilon}\left(\underline{u},\underline{y}\right)\right)\bigcup_{\underline{\hat{u}}\ne\underline{u}}\left(\underline{\hat{u}},\underline{y}\right)\in A_n^{\varepsilon}\left(\underline{u},\underline{y}\right)$$

$$Tx_error=\left(\underline{s}\notin A_n^{\varepsilon}\left(\underline{s},\underline{u}\right)\right)\bigcup_{\underline{w}}\left(\bigcap_{\underline{u}}\underline{u}\notin bin\left(\underline{w}\right)\right)$$

$$\bar{P}_e\le\Pr\left(Tx_error\right)+\Pr\left(Rx_error\right)$$

$$\Pr\left(Rx_error\right)\le\varepsilon+\sum_{\substack{\underline{\hat{u}}\ne\underline{u}\\ \underline{\hat{u}}\in A_n^{\varepsilon 2}\left(\underline{u},\underline{y}\right)}}\Pr\left(\underline{\hat{u}}\right)\le\varepsilon+2^{nR'}2^{-n\left(I\left(U;Y\right)-3\varepsilon\right)}=\varepsilon+2^{n\left(R'-I\left(U;Y\right)+3\varepsilon\right)}$$

$$\Pr\left(\underline{\hat{u}}\in bin\left(\underline{w}\right)\bigcap\underline{\hat{u}},\underline{s}\in A_n^{\varepsilon}\right)\le 2^{-nR}2^{-n\left(I\left(U;S\right)-3\varepsilon\right)}=2^{-n\left(R+I\left(U;S\right)-3\varepsilon\right)}$$

$$\Pr\left(Tx_error\right)\le\varepsilon+\sum_{\underline{w}}\prod_{\underline{u}}\left(1-2^{-n\left(R+I\left(U;S\right)-3\varepsilon\right)}\right)\le\varepsilon+2^{nR}\left(1-2^{-n\left(R+I\left(U;S\right)-3\varepsilon\right)}\right)^{2^{nR'}}=$$

$$=\varepsilon+2^{nR}\left[\left(1-2^{-n\left(R+I\left(U;S\right)-3\varepsilon\right)}\right)^{2^{n\left(R+I\left(U;S\right)-3\varepsilon\right)}}\right]^{\frac{2^{nR'}}{2^{n\left(R+I\left(U;S\right)-3\varepsilon\right)}}}\approx\varepsilon+e^{-2^{n\left(R'-R-I\left(U;S\right)+3\varepsilon\right)}+nR\ln\left(2\right)}=$$

$$=\varepsilon+e^{-2^{n\left(R'-R-I\left(U;S\right)+3\varepsilon\right)}\left(1-\frac{nR\ln\left(2\right)}{2^{n\left(R'-R-I\left(U;S\right)+3\varepsilon\right)}}\right)}$$

כאשר $R'-R-I\left(U;S\right)+3\varepsilon<0$ ניתן למצוא n מספיק גדול כך ש $\frac{nR\ln\left(2\right)}{2^{n\left(R'-R-I\left(U;S\right)+3\varepsilon\right)}}<\varepsilon$

$$\bar{P}_e \le \Pr\left(Tx_error\right)+\Pr\left(Rx_error\right)\le 2\varepsilon + e^{-2^{n\left(R'-R-I(U;S)+3\varepsilon\right)}(1-\varepsilon)} + 2^{n\left(R'-I(U;Y)+3\varepsilon\right)}$$

הסתברות השגיאה שואפת ל0 כאשר n שואף לאינסוף כאשר

$$R'-I\left(U;Y\right)+3\varepsilon<0$$

$$R'-R-I\left(U;S\right)+3\varepsilon>0$$

משני אלה נקבל

$$R<I\left(U;Y\right)-I\left(U;S\right)$$

מכאן כל קצב המקיים $R<I\left(U;Y\right)-I\left(U;S\right)$ הוא בר השגה. הוכחת המשפט ההפוך לא תובא כאן.

הערה: הסבר אינטואיטיבי מדוע הקצב אינו I(u;y): המשתנה u הוא פונקציה לא רק של w אלא גם של s שהוא בלתי תלוי ב w. האינפורמציה העוברת למקלט היא אינפורמציה על u שחלקה הוא אינפורמציה על s שאינו מלמד דבר על ההודעה ששודרה לכן אינטואיטיבית יש להפחית מהאינפורמציה שהמקלט לומד על u שהיא I(u;y) את החלק שתלוי ב s כדי לקבל את כמות האינפורמציה שנלמדה על w.

מימוש אלגברי של קידוד לערוצים עם אינפורמציית צד הידועה למשדר בלבד

בסעיפים הקודמים מצאנו את הקיבולת של ערוצים שונים עם אינפורמציית צד הידועה למשדר בלבד ע"פ משפט GP שהוכח ע"י שמוש בקידוד אקראי. קידוד אקראי אינו טכניקת קידוד מעשית. בסעיפים הבאים נציג טכניקות קידוד מעשיות לבעיית Costa ולבעיית הזיכרון עם התאים התקולים שהוצגה קודם.

קידוד אלגברי לבעיית הזיכרון עם תאים תקולים

נניח מודל של זיכרון בגודל n עם k תאים תקינים ו n-k תאים תקולים. התאים התקולים תקועים ב"1" או ב"0" ללא קשר לערך שנכתב לתוכם. שיטת הקידוד היא כדלקמן: המקודד שיודע את תבנית השגיאה (מקום וערך התא התקול) יכתוב לזיכרון מילה שערכה שבמקום התאים התקולים יהיו ביטים הזהים לתבנית השגיאה כך שבזמן קריאה הקורא יקרא בדיוק את המילה שנכתבה ללא כל שנויים. נבחר קוד ליניארי בינארי עם מטריצה יוצרת G ומטריצת בדיקה H. נניח כי דרגת H היא k דרגת G היא n-k ו GH=0. נחלק את כל 2^n הוקטורים הבינאריים באורך n ל 2^k מחלקות $A_0, A_1, \ldots, A_{2^k-1}$ בגודל 2^{n-k} וקטורים כל אחת על פי

$$A_w=\left\{y\in\left[0,1\right]^n, w\in\left[0,1\right]^k \middle| yH=w\right\}$$

(יש 2^k מחלקות כאלה כי H היא מטריצה k x n שורותיה בלתי תלויות לכן לכל w קיים לפחות y אחד שעבורו yH=w). נגדיר תבנית שגיאה: תבנית השגיאה היא זוג וקטורים ($\underline{i}$,$\underline{s}$) כאשר $\underline{i}$ מציין את מקום השגיאה ו $\underline{s}$ מציין את הערך שהתא המצוין ע"י $\underline{i}$ תקוע בו.

$$\underline{i}=\left(i_1,i_2,\ldots,i_u\right)\quad s.t.\quad 1\le i_j\le n$$

$$\underline{s}=\left(s_{i_1},s_{i_2},\ldots,s_{i_u}\right)\quad s.t.\quad s_{i_j}\in\left[0,1\right]$$

$$u\le n-k$$

נניח כי ההודעה שאותה רוצים לשדר היא w ונתונה תבנית השגיאה של הזיכרון בתאים בהם רוצים לאכסן את ההודעה. נבחר וקטור כל שהוא $x\in A_w$. אם $\left(x_{i_j}=s_{i_j}\right)\forall i_j\in\underline{i}$ ז"א ערכי הוקטור x במקומות התאים התקולים זהים לערך בו התאים תקועים אזי הוקטור x ייכתב לזיכרון. אם יש שוני נחפש וקטור d כך ש

$$dG' = \left[s_{i_1} - x_{i_1}, s_{i_2} - x_{i_2}, \ldots, s_{i_u} - x_{i_u} \right]$$
$$G' = \left[\underline{g}_{i_1}, \underline{g}_{i_2}, \ldots, \underline{g}_{i_u} \right]$$
$$when \quad G = \left[\underline{g}_1, \underline{g}_2, \ldots, \underline{g}_n \right]$$

ניתן תמיד למצוא וקטור d אם דרגת 'G היא לפחות u. המספר המינימאלי של העמודות הבלתי תלויות של G הוא $d_{min}(C\perp)-1$ כאשר $C\perp$ הוא הקוד הדואלי הנפרש ע״י העמודות של H ו $d_{min}(C\perp)$ הוא משקל Haming המינימאלי של מילות הקוד הדואלי. לכן $u \le d_{\min}(C\perp)-1$. במקרה זה הוקטור שייכתב לזיכרון הוא

$$y = x + dG$$
$$yH = xH + dGH = xH = w$$

היות והביטים של y במקומות של התאים התקולים זהים לערכי התאים התקולים הקורא יקרא את הוקטור שנכתב. הקורא מכפיל את הוקטור שנקרא במטריצת הבדיקה ומקבל את ההודעה שנשלחה שהיא הסינדרום.

נניח שקיים קוד ליניארי בינארי בעל תכונת MDS (Minimum Distance Separable) דהינו מרחק הקוד d (מינימום מספר הביטים השונים מאפס ע״פ כל מילות הקוד) קשור עם אורך מילת הקוד בביטים n, ואורך מילת המקור בביטים k ע״י הקשר הבא d=n-k+1. נניח כי H היא מטריצה יוצרת של קוד MDS בינארי וG תהיה המטריצה היוצרת של הקוד הדואלי שלו. אזי ע״פ הבניה שלמעלה ניתן לאחסן בזיכרון הודעות בנות k ביטים במקטע זיכרון של n ביטים כאשר במקטע זה יש עד n-k ביטים תקולים התקועים באיזו תבנית שהיא. בהנחה כי אורך המקטע הוא ארוך וההסתברות לביט תקול היא p אזי בממוצע יש לנו n-k=np ביטים תקולים וקצב הקוד הממוצע במקרה זה הוא 1-p

הערות:

1) סכימה זו מבוססת על המצאות קוד MDS בינארי (שבפועל לא קיים) או קוד קרוב ככל האפשר לMDS בינארי. דרך סיסטמטית אחרת היא שימוש בקודי MDS מעל שדות בעלי א״ב גדול יותר $GF(2^m)$. קודי Reed Solomon הם קודים בעלי תכונת MDS (Minimum Distance Separable) דהינו מרחק הקוד d (מינימום מספר הסימבולים השונים מאפס ע״פ כל מילות הקוד) קשור עם אורך מילת הקוד בסימבולים n ואורך מילת המקור בסימבולים k ע״י הקשר הבא d=n-k. ההסתברות לסימבול תקול היא $p_s = 1-(1-p)^m$ כאשר p היא הסתברות לביט תקול. גודל זה גדול מ p כך שיש אובדן קצב אם משתמשים בקודים מעל א״ב גדול יותר לערוץ בינארי. מאידך אם הבעיה הפיזיקאלית מוגדרת בא״ב גבוה יותר לדוגמא אם כל ה byte תקול דהינו תקוע בערך מסויים שימוש בקוד Reed Solomon אינו גורם לאיבוד קצב.

2) קוד לינארי לתקון שגיאות יכול לתקן עד $\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ שגיאות כל שהן שמקומם אינו ידוע וכן לתקן עד $d_{min}-1$ מחיקות שהן שגיאות שמקומן מסומן למפענח. באלגוריתם שהוצג כאן ניתן לפענח כל הודעה שמכילה תבנית בת עד $d_{min}-1$ ביטים תקולים שמקומם ידוע למשדר אך לא למקלט. המקלט אינו מפענח את מילת הקוד המקורית x אלא ישר מפענח את ההודעה w.

3) שיטה זו הוצגה במאמר

C. Heegard "Partitioned Linear Block Codes for Computer Memory with "Stuck at" Defects"IEEE Trans. On Inform. Theory Vol-29 No.6 Nov. 1983

יחד עם הרחבות לזיכרונות עם רעש.

קידוד אלגברי לבעייתCosta

הפתרון האלגברי לבעיה זו משתמש ברעיון שהוצג ע״י Tomlinson & Harashima ב 1971. הם עסקו במימוש Equalizer במשדר עם מגבלת הספק. הרעיון הוא הרחבה מחזורית של א״ב הערוץ ע״י פעולת המודולו. כדי להדגים את הרעיון ולהסביר את התועלת בו נתייחס כרגע לבעיית Costa ללא רעש $y=x+s$ כאשר s ידוע למשדר. אם המשדר יחסיר את s המקלט יקבל סיגנל נקי אך אם s גדול הספק השידור יהיה גדול ונחרוג ממגבלת ההספק של המשדר. נניח כי x מוגבל בין [0,L] . Tomlinson & Harashima הציעו שהמקלט יבצע את הפעולה $y'=y \mod L$ אזי התקון שהמשדר יצטרך להוסיף לא יהיה s אלא ערך המביא את הכניסה לערך $y'=x+kL$ כאשר k שלם כלשהוא. מכאן אם המשדר ישדר $\hat{x}=(x-s) \mod L$ נקבל $y'=x$ והספק השידור יקטן בצורה משמעותית עבור s גדול. נשתמש ברעיון זה כאן.

בשלב ראשון נעסוק בערוץ שהא״ב שלו הוא L רמות אמפליטודה [-(L-1)/2:(L-1)/2] (L-PAM).

נגדיר פונקצית מודולו

$$x \mod^* L=\left(\left(x+\frac{L}{2}\right) \mod L\right)-\frac{L}{2}$$

שזו היא בעצם פונקצית מודולו רגילה המחזירה תוצאה בין 0 ל L אך ממורכזת סביב 0 כך שהיא מחזירה תוצאה בין [-L/2,L/2]. כמו כן נניח שההודעה אותה אנו רוצים לשדר מורכבת מסימבולים מאותו הא״ב (PAM-L). המשדר ישלח לערוץ את האות הבא

$$x_n=(v_n-\alpha s_n-u_n) \mod^* L$$

כאשר v_n הוא סימבול המקור s_n היא ההפרעה הידועה למשדר, ו u_n הוא אות ריטוט (dither) הידוע גם למקלט וגם למשדר ונועד לגרום לאי תלות סטטיסטית בין v_n ל x_n. היות ואות זה ידוע לשני הצדדים תוספת שלו לסיגנל המשודר לא משנה את קיבולת הערוץ.

במוצא הערוץ יתקבל

$$y_n=x_n+s_n+z_n$$

כאשר z_n הוא רעש גאוסי לבן אדיטיבי עם שונות σ^2. מאות זה המקלט מיצר אות y_n'

$$y_n'=(\alpha y_n+u_n) \mod^* L$$

$$y_n'=(\alpha x_n+\alpha s_n+\alpha z_n+u_n) \mod^* L=(x_n+\alpha s_n+\alpha z_n+u_n-(1-\alpha)x_n) \mod^* L=$$

$$=((v_n-\alpha s_n-u_n) \mod^* L+\alpha s_n+\alpha z_n+u_n-(1-\alpha)x_n) \mod^* L=$$

$$=((v_n) \mod^* L+\alpha z_n-(1-\alpha)x_n) \mod^* L=$$

$$=(v_n+\alpha z_n-(1-\alpha)x_n) \mod^* L$$

נבחר u_n מ״א i.i.d. מפולג אחיד על פני אינטרוואל [-L/2:L/2]. x_n הוא בלתי תלוי ב v_n היות ו u_n משתנה ע״פ כל האינטרוואל [-L/2:L/2]. כמו כן x_n מתפלג אחיד ע״פ כל האינטרוואל. נגדיר רעש אקוויוולנטי 'N.

$$N' \triangleq (\alpha z_n-(1-\alpha)x_n) \mod^* L$$

$$y_n'=(v_n+N') \mod^* L$$

$$E\left\{(N')^2\right\}\le E\left\{(\alpha z_n \mod^* L)^2\right\}+E\left\{(1-\alpha)^2 x_n^2\right\}\le E\left\{\alpha^2 z_n^2\right\}+E\left\{(1-\alpha)^2 x_n^2\right\}$$

$$E\left\{x_n^2\right\}=P=\frac{L^2}{12}$$

נניח כי 'N הוא קטן ונחפש ערך α המביא למינימום את החסם על $E\left\{\left(N'\right)^2\right\}$. מגזירת החסם והשוואת הנגזרת לאפס מתקבל

$$\alpha^* = \frac{P}{P+\sigma^2}$$

$$E\left\{N'^2\left(\alpha^*\right)\right\} \le \left(\frac{\sigma^2}{P+\sigma^2}\right)^2 P + \left(\frac{P}{P+\sigma^2}\right)^2 \sigma^2 = \frac{P\sigma^2}{P+\sigma^2} \le \sigma^2$$

הספק הסיגנל המקורי v_n בהנחת פילוג אחיד של המקור מקיים

$$E\left\{v_n^2\right\} = \frac{2}{L}\sum_{i=0}^{L/2-1}\left(\frac{2i+1}{2}\right)^2 = \frac{2}{L}\sum_{i=0}^{L/2-1} i^2+i+\frac{1}{4} = \frac{1}{4}+\frac{2}{L}\frac{\left(\frac{L}{2}-1\right)\frac{L}{2}\left(\frac{L}{2}+1\right)}{3} = \frac{1}{4}+\frac{L^2-4}{12} = \frac{L^2-1}{12} = P-\frac{1}{12}$$

יחס האות לרעש המתקבל

$$SNR = \frac{E\left\{v_n^2\right\}}{E\left\{N'^2\right\}} = \frac{P-\frac{1}{12}}{\frac{\sigma^2 P}{\sigma^2+P}} = \frac{P}{\sigma^2}\left(1-\frac{1}{12P}\right)\left(1+\frac{\sigma^2}{P}\right)$$

לכאורה יוצא שיחס האות לרעש טוב יותר לאחר המניפולציה שהוצגה כאן מאשר ללא הפרעה אך סטטיסטיקת הסיגנל והרעש אינן גאוסיות כך שיחס האות לרעש אינו מדד לקיבולת. המדד לקיבולת היא האינפורמציה ההדדית I(y;x) . עבור המקרה של PAM-L (המקרה בו א״ב השידור הוא חד ממדי) חישוב האינפורמציה ההדדית מסובך. נתבונן במקרה הרב מימדי דהינו השדור x הוא וקטור שהוא נקודה בשריג רב מימדי ופעולת המודולו מבוצעת מודול השריג. (כדוגמא פשוטה נניח שריג שנקודותיו הם וקטורים במימד n שכל אחת מהקואורדינאטות שלו היא מספר שלם בין [L/2,-L/2] במקרה זה מודולו השריג הוא בעצם ביצוע פעולת מולו בכל אחת מהקואורדינאטות). עבור שריג רב מימדי טוב פילוג 'v,y,N שואף לפילוג גאוסי ככל שהמימד עולה. עקב פעולת המודולו 'y ו x מפולגים באופן זהה ע״פ כל השריג. לכן $E\left\{v^2\right\} \approx E\left\{y'^2\right\} = E\left\{x^2\right\} = P$ כאשר ככל שהמימד עולה הספק v מתקרב ל P והפילוג מתקרב לגאוסי. היות 'y,v,N הם כולם ערכים בשריג הבסיסי (במקרה החד מימדי כולם בין [L/2,-L/2]) אזי בהינתן y',v קיים 'N יחיד המקיים $y' = \left(v+N'\right) \mod^* L$. לכן $p\left(y'|v\right) = p\left(N'\right)$. קיבולת הערוץ בין v ל 'y נתונה ע״י

$$R \le I\left(y';v\right) = H\left(y'\right) - H\left(y'|v\right) = H\left(y'\right) - H\left(N'\right) =$$

$$= \frac{1}{2}\log\left(2\pi eP\right) - \frac{1}{2}\log\left(2\pi e\frac{\sigma^2 P}{P+\sigma^2}\right) = \frac{1}{2}\log\left(1+\frac{P}{\sigma^2}\right)$$

שזו בדיוק הקיבולת ע״פי Costa .

2006

מרצה: פרופ' רם זמיר

עורך: אנטולי חינה

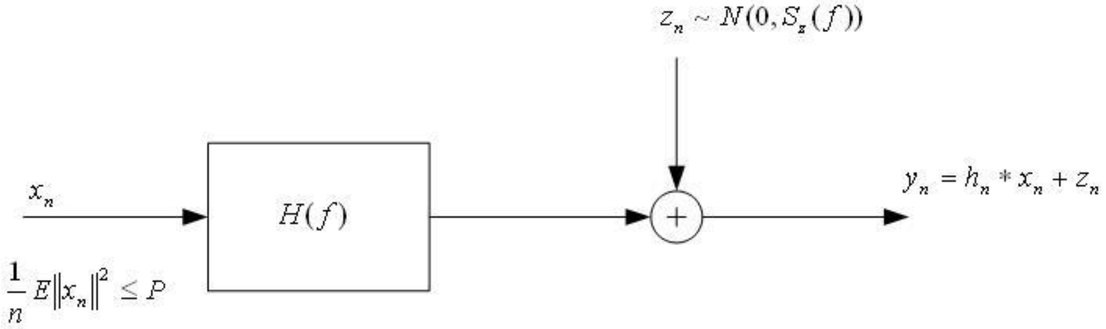
הרצאה - 1

משוונים, חיזוי וכלל השרשרת לאינפורמציה הדדית בעולם הגאוסי

סוכם ע"י ניר וינברגר

ערוץ רעש גאוסי עם הפרעה בין סימנית (ISI)

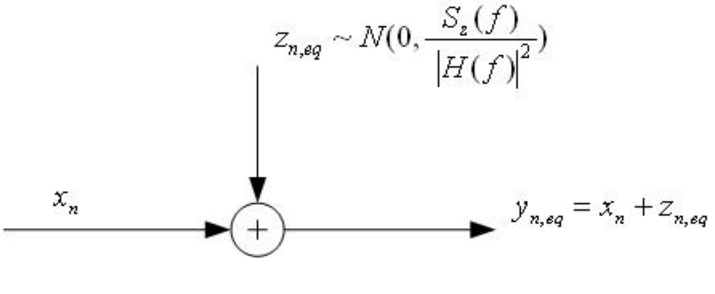
נעסוק במודל זמן בדיד הבא לערוץ עם הפרעה בין סימנית (Inter-symbol interference, ISI).



המוצא מתואר ע"י $y_n = h_n * x_n + z_n$ כאשר

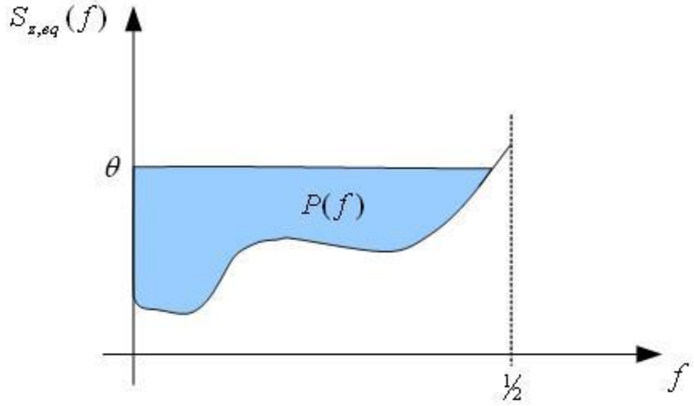
- הכניסה x_n מוגבלת הספק, $\frac{1}{n}E\|x_1^n\|^2 \le P$.
- הערוץ מכיל מסננת ליניארית קבועה בזמן בעלת תגובת הלם h_n, ותגובת תדר $H(f)$.
- מתווסף רעש חיבורי גאוסי z_n, בעל ספקטרום הספק $S_z(f)$.

ע"י הוספת מסננת הופכית ל $H(f)$ במוצא הערוץ ניתן לעבור לערוץ השקול הבא,



כך שכעת המוצא מתואר ע"י $y_n = x_n + z_{eq,n}$ כאשר הרעש החיבורי השקול $z_{eq,n}$ הוא גאוסי עם ספקטרום הספק $S_{z,eq}(f) = |H(f)|^{-2} \cdot S_z(f)$.

מציאת קיבול הערוץ – לפי כלל מזיגת מים



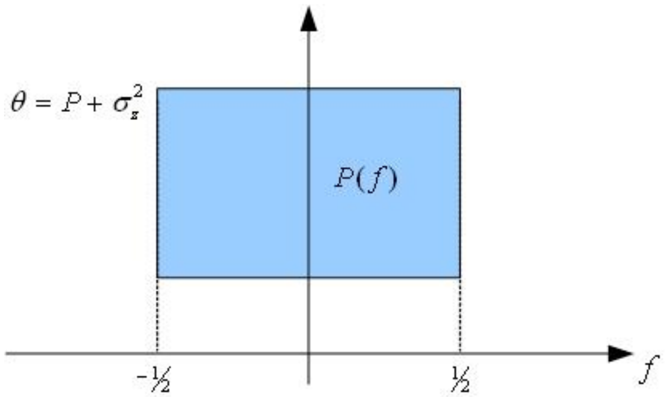
$$C=\int_{-1/2}^{1/2}\frac{1}{2}\log_2\left(1+\frac{P(f)}{S_{z,eq}(f)}\right)df=\int_{f:\ \theta>S_{z,eq}(f)}\frac{1}{2}\log_2\left(\frac{\theta}{S_{z,eq}(f)}\right)df\quad\left(\frac{bits}{channel\,use}\right)$$

כאשר θ הוא "גובה המים" וההספק בכל תדר נקבע כך ש $\int_{-1/2}^{1/2}P(f)\,df=P$.

<u>מקרים פרטיים ותכונות:</u>

- ערוץ AWGN – $y_n=x_n+z_n$. הקיבול נתון ע"י

$$C_{AWGN}=\frac{1}{2}\log_2\left(1+\frac{P}{\sigma_z^2}\right)\quad\left(\frac{bits}{channel\,use}\right)$$



- החסם העליון של Shannon –

$$C\le\int_{-1/2}^{1/2}\frac{1}{2}\log_2\left(\frac{P+\sigma_{z,eq}^2}{S_{z,eq}(f)}\right)df$$

כאשר $\sigma_{z,eq}^2$ הוא שונות הרעש השקול, $\sigma_{z,eq}^2=\int_{-1/2}^{1/2}S_{z,eq}(f)\,df$. החסם מתקבל בשוויון כאשר המים מכסים את כל הרעש, דהיינו $\theta\ge S_{z,eq}(f)$ לכל $|f|\le 1/2$ (מצב זה מתקבל בד"כ כאשר יחס האות לרעש גבוה).

* המבוא האופטימלי - מכיוון ש
$$C = \sup \bar{I}(\{x_n\};\{y_n\}) = \bar{I}(\{x_n^*\};\{y_n\})$$

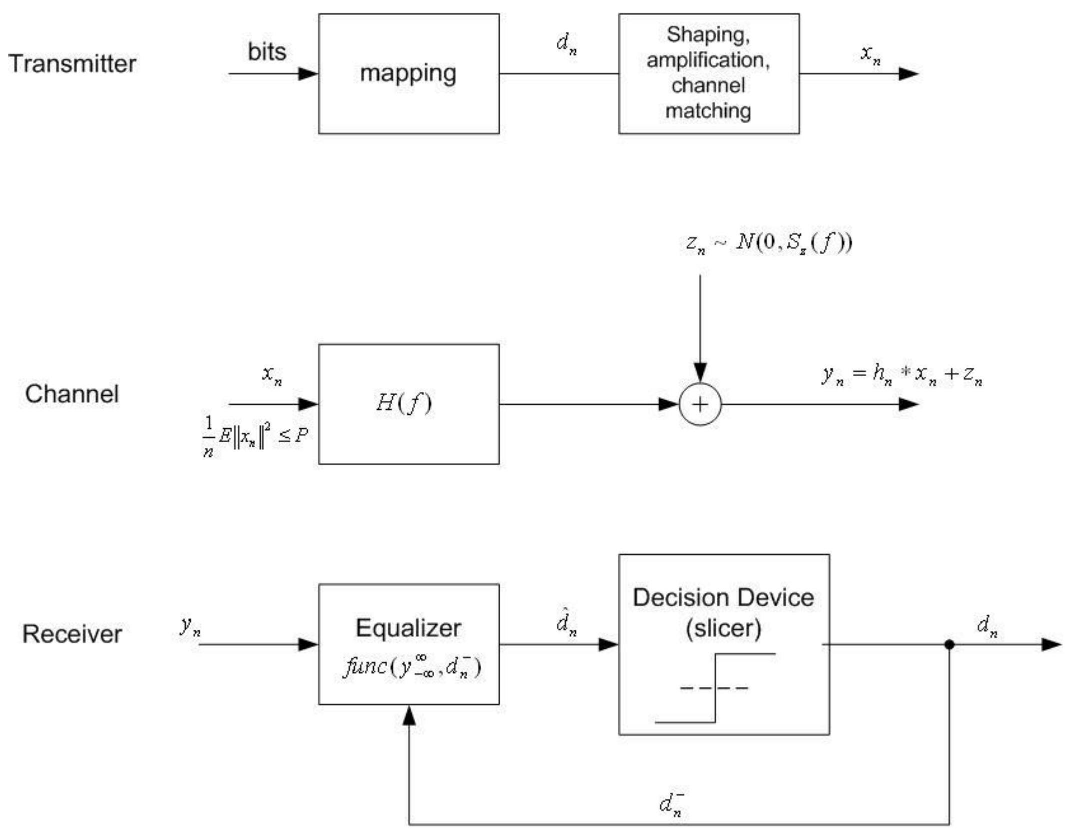
כאשר הסופרימום נלקח על פני כל התהליכים האקראיים הסטאציונריים שמקיימים את אילוץ ההספק, $E(x_n^2) \le P$, הגודל $\bar{I}(\{x_n\};\{y_n\})$ הוא האינפורמציה הדדית הממוצעת בין $\{x_n\}$ ל $\{y_n\}$,

$$\bar{I}(\{x_n\};\{y_n\}) = \lim_{N\to\infty} \frac{1}{N} I(x_1^N ; y_1^N)$$

ו$\{x_n^*\}$הוא תהליך אקראי גאוסי עם ספקטרום הספק $P(f)$, הנקבע באמצעות כלל מזיגת המים.

שימוש במשוון עם משוב החלטה לשידור וגילוי בערוץ ISI גאוסי

משוון עם משוב קדמי (Feed forward equalizer) ומשוב החלטה (Decision feedback equalizer) מתואר ע"י המערכת הבאה.



כאשר עבור סדרה d_n , עברה מסומן ע"י $d_n^- \equiv \{d_{-\infty}^{n-1}\}$.

<u>הנחה :</u> החלטות העבר ב slicer נכונות, ולכן סימבולי העבר ידועים במקלט.

מטרת המערכת היא להגיע למצב שבו קיבול הערוץ עם הזיכרון שווה לאינפורמציה ההדדית הסקלארית על פני יחידת ההחלטה, דהיינו $C = \sup \bar{I}(\{x_n\};\{y_n\}) = I(\hat{d}_n ; d_n)$.

נסמן את שגיאת המשוון ב $e_n = d_n - \hat{d}_n$ ואז $I(\hat{d}_n; d_n) = I(\hat{d}_n; \hat{d}_n + e_n)$.

<u>תזכורות :</u>

- כלל השרשרת לאינפורמציה הדדית - לכל שלושה משתנים אקראיים a,b,c מתקיים

$$I(a;b,c) = I(a;b) + I(a;c|b)$$

עבור המקרה שלנו נזדקק לפיתוח

$$\bar{I}(\{x_n\};\{y_n\}) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-N}^{N} I(x_{-N}^{N}; y_{-N}^{N})$$

$$= \lim_{N\to\infty} \frac{1}{2N+1} \sum_{n=-N}^{N} I(x_n; y_{-N}^{N} | x_{-N}^{n-1}) = I(x_n; y_{-\infty}^{\infty} | x_n^{-})$$

כאשר השוויון השני נובע מכלל השרשרת, והשוויון השלישי נכון עבור תהליכים אקראיים סטאציונריים במצב היציב, כאשר מגדירים $x_n^{-} = \{x_{n-1}, x_{n-2}, \ldots\}$.

- משפט אי שוויון עיבוד הנתונים - לכל שני משתנים אקראיים a,b ופונקציה $\varphi(\cdot)$ מתקיים

$$I(a;\varphi(b)) \le I(a;b)$$

ושוויון אם $\varphi(\cdot)$ הפיכה.

ננתח את שני הגדלים $\bar{I}(\{x_n\};\{y_n\})$ ו $I(\hat{d}_n; d_n)$.

הגודל הראשון

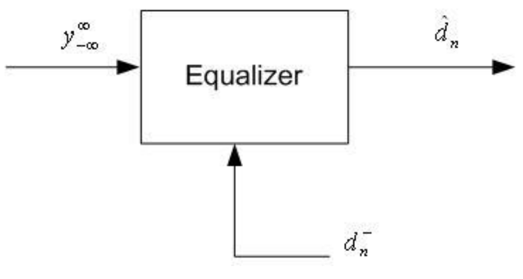
$$\bar{I}(\{x_n\};\{y_n\}) = \bar{I}(\{d_n\};\{y_n\}) = I(d_n; y_{-\infty}^{\infty} | d_n^{-}) = h(d_n | d_n^{-}) - h(d_n | y_{-\infty}^{\infty}, d_n^{-})$$

$$= h(d_n) - h(d_n - \hat{d}_n | y_{-\infty}^{\infty}, d_n^{-}) = h(d_n) - h(e_n | y_{-\infty}^{\infty}, d_n^{-})$$

כאשר :

- השוויון הראשון נכון תמיד משום שמצד אחד לפי אי-שוויון עיבוד הנתונים מתקיים $\bar{I}(\{x_n\};\{y_n\}) \ge \bar{I}(\{d_n\};\{y_n\})$, ומצד שני, מכיוון ש x_n נקבעים דטרמיניסטית ע"י d_n , ובאמצעות כלל השרשרת וחיוביות האיפורמציה ההדדית מתקיים אי שוויון הפוך $\bar{I}(\{d_n\};\{y_n\}) = \bar{I}(\{d_n\},\{x_n\};\{y_n\}) = \bar{I}(\{x_n\};\{y_n\}) + \bar{I}(\{d_n\};\{y_n\}|\{x_n\}) \ge \bar{I}(\{x_n\};\{y_n\})$.
- השוויון השני נכון מכלל השרשרת והפיתוח אחריו.
- השוויון השלישי מתקבל מפירוק האינפורמציה הדדית להפרש אנטרופיות.
- השוויון הרביעי מתקבל כאשר d_n היא סדרה i.i.d. , ומכיוון שהמשערך $\hat{d}_n$ הוא פונקציה של המדידות $\{y_{-\infty}^{\infty}, d_n^{-}\}$.

כעת נשתמש בכלל האורתוגונליות של משערך MMSE, האומר שאם $\hat{d}_n$ הוא משערך MMSE של d_n מתוך המדידות $\{y_{-\infty}^{\infty}, d_n^{-}\}$, אזי שגיאת השערוך $e_n = d_n - \hat{d}_n$ ניצבת למדידות. במקרה הגאוסי הניצבות (חוסר קורלציה) גוררת אי תלות סטטיסטית, ולכן e_n המתקבל משערוך אופטימלי במובן MMSE, בת"ס במדידות $\{y_{-\infty}^{\infty}, d_n^{-}\}$.



מכאן נובע שכאשר המשוון הוא משערך אופטימלי במובן MMSE מתקבל

$h(e_n \,|\, y_{-\infty}^{\infty}, d_n^{-}) = h(e_n)$ ולכן בסה"כ מתקבל $\bar{I}(\{x_n\};\{y_n\}) = h(d_n) - h(e_n)$.

הגודל השני הוא

$$I(\hat{d}_n; d_n) = h(d_n) - h(d_n \,|\, \hat{d}_n) = h(d_n) - h(e_n \,|\, \hat{d}_n) = h(d_n) - h(e_n)$$

כאשר השוויון השני נכון מכיון ש $\hat{d}_n$ הוא פונקציה (ליניארית) של המדידות $\{y_{-\infty}^{\infty}, d_n^{-}\}$

ומכיוון ש e_n בת"ס במדידות אלו הרי שהוא בת"ס גם ב. $\hat{d}_n$

מהשוואת שני הביטויים ניתן לראות שקיבלנו את התוצאה הרצויה, המסוכמת במשפט הבא.

משפט (Cioffi, Dudevoir, Eyuboglu, Forney) :

אם:

- d_n סדרה i.i.d. גאוסית, בעלת שונות σ_d^2 .
- $\{x_n\} = \{x_n^*\}$, כלומר מתאם הערוץ הוא מסנן $G(f)$ המקיים $|G(f)|^2 = \dfrac{P(f)}{\sigma_d^2}$.
- המשוון הוא מסננת וינר האופטימלית לשערוך d_n מתוך המדידות $\{y_{-\infty}^{\infty}, d_n^{-}\}$ (דהיינו מסדר אינסופי).
- החלטות העבר ב slicer נכונות.

מקבלים $C = I(\hat{d}_n; d_n)$.

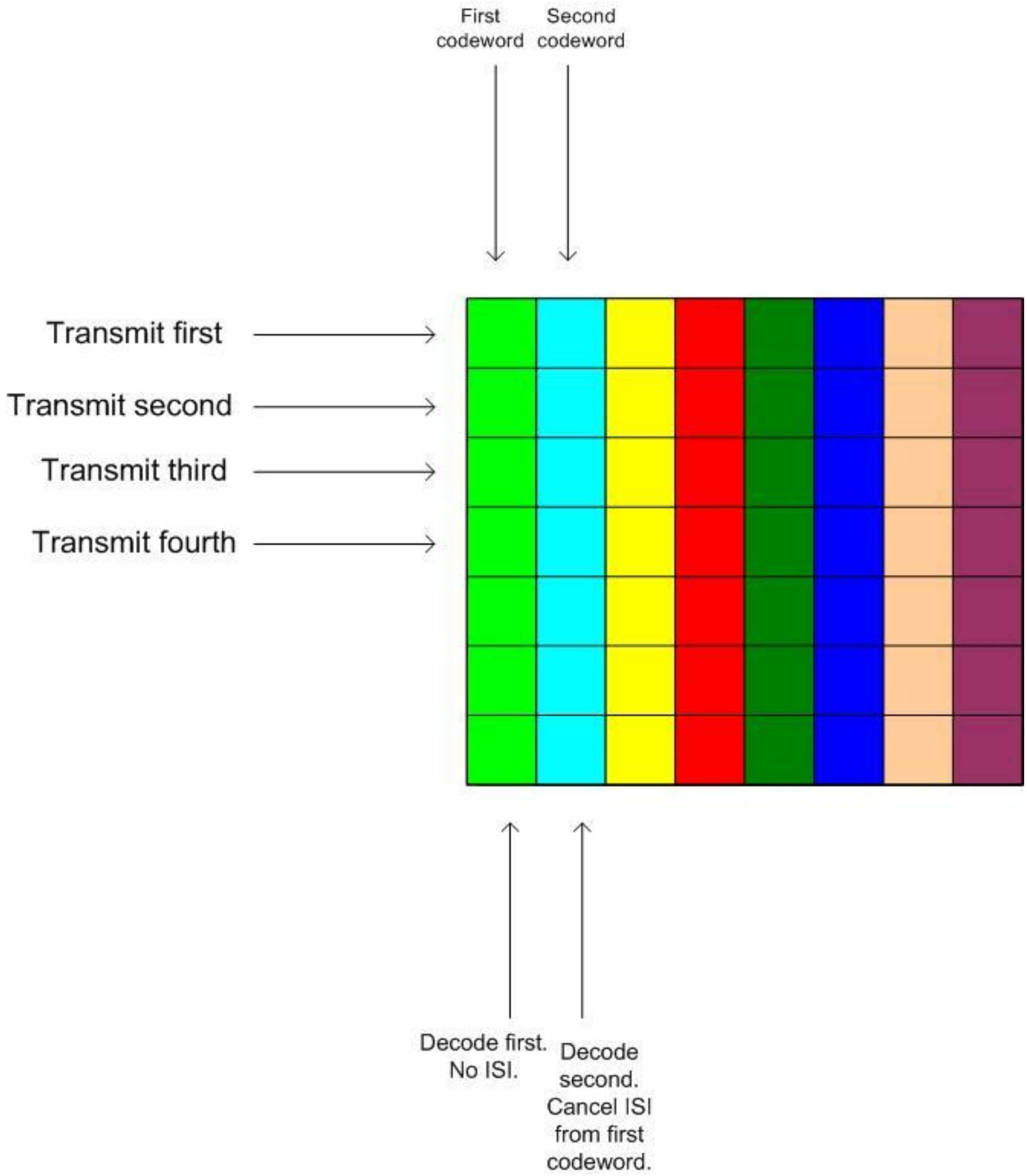
משמעות המשפט היא שכאשר רוצים לשדר בערוץ גאוסי צבעוני ניתן להפריד בין החלק של הקידוד והחלק של שיוויון הערוץ ללא הפסד בקצב השידור. הקידוד יתבצע עבור ערוץ גאוסי לבן, ובאמצעות כלים של עיבוד אותות, כגון מסנן וינר ומתאם הערוץ, ניתן לטפל בצבעוניות הערוץ.

נדון כעת בקיום הנחות המשפט. ההנחה על מתאם הערוץ נכונה תמיד, וההנחה על משערך וינר מתקיימת בקירוב כאשר מספר המקדמים של המסננת גדול מספיק כך שההפסד ביחס למסננת אינסופית זניח.

לעומת זאת, ההנחות לגבי גאוסיות הסימבולים d_n, וההנחה שהחלטות העבר נכונות, נראות סותרות את המבנה הסדרתי של המערכת. בכדי שהסימבולים d_n יראו כמ"א גאוסיים i.i.d. יש צורך בקוד עיצוב (shaping), ובפענוח לא סיבתי. כמו כן, ההנחה שהחלטות העבר נכונות, והשימוש באינפורמציה הדדית כמדד לביצועים מחייבים שימוש בקוד טוב עבור ערוץ AWGN , ובהכרח פענוח לא סיבתי.

נתיר כעת את הסתירה באמצעות שימוש בשזירה (Interleaving). נניח בשלב ראשון שאין לנו ערוץ צבעוני בודד יחיד, אלא מספר ערוצים בלתי תלויים במקביל. הקידוד יתבצע על פני הערוצים הבלתי תלויים, ולא על פני ציר הזמן. כאשר הקוד טוב, ההנחות לגבי גאוסיות d_n וידיעת סימבולי העבר במקלט יתקיימו והאינפורמציה ההדדית אכן תהיה מדד לקצב השידור. כאשר אין מספר ערוצים במקביל ניתן להשתמש בשזירה. נבנה מטריצה כך שכל עמודה היא מילת קוד, ומספר השורות גדול כך שניתן לקבל קוד באורך מספיק גדול. נשדר את המטריצה שורה שורה, וכאשר תתקבל כל המטריצה במקלט נתחיל בפענוח. ראשית נפענח את העמודה הראשונה. מכיוון שזוהי מילה מקוד טוב עבור ערוץ AWGN , הסימבולים הם בקירוב גאוסיים i.i.d. , והפענוח מדויק. כעת, כאשר באים לפענח את העמודה השנייה ניתן לבטל את ה ISI מהעמודה הראשונה. נמשיך בצורה דומה ונפענח כל עמודה בנפרד כאשר מבטלים את ה ISI מעמודות קודמות. הבעייתיות בגישה זו היא ההשהיה הגדולה שנוצרת, מכיוון שמספר השורות צריך להיות גדול בכדי שהקוד יהיה טוב וגם מספר העמודות צריך להיות גדול.הסיבה שגם מס' העמודות צריך להיות גדול היא שבכדי שלא נקבל ISI מהסימבול האחרון בשורה מסוימת לסימבול הראשון בשורה הבאה יש להקדים ולשדר בכל שורה אפסים באורך תגובת הערוץ. בכדי שההפסד בקצב יהיה קטן

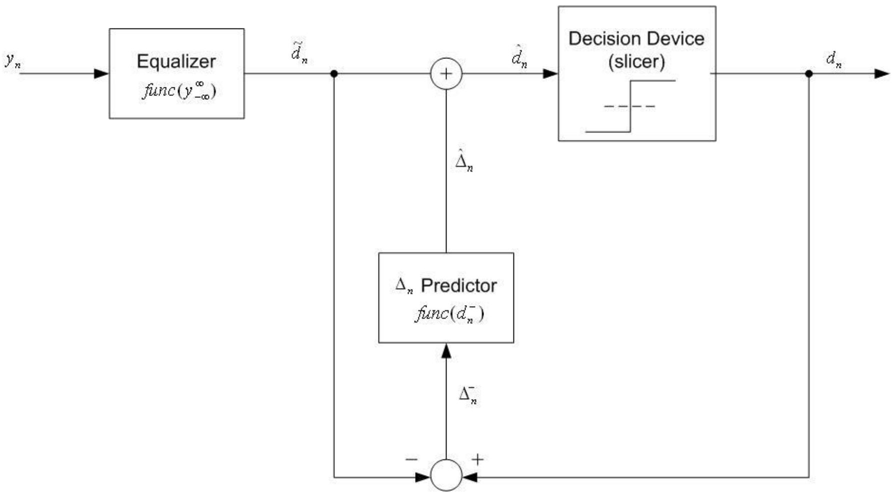
יש לשדר מס' עמודות גדול, וכאשר מס' העמודות שואף לאינסוף לא נפסיד בקצב כלל והקיבול יושג.



משוון ה FFE/DFE שהתקבל הוא משערך של סימבולי השידור d_n מתוך המדידות $\{y_{-\infty}^{\infty}, d_n^{-}\}$. תוך שימוש בעקרון האורתוגונליות ניתן להראות, שמבלי לאבד מאופטימליות המשערך, ניתן להציג אותו כמשערך בעל שני שלבים.[3] בשלב הראשון המדידות $\{y_{-\infty}^{\infty}\}$ משמשות לשערוך אופטימלי $\tilde{d}_n$, של סימבול השידור d_n, ויוצרות שגיאת שערוך $\Delta_n = d_n - \tilde{d}_n$. כעת, בשלב השני, משום שהנחנו שהעבר של הסדרה d_n ידוע במדויק במקלט, גם העבר של הסדרה Δ_n ידוע במקלט וניתן להשתמש בו בכדי לחזות את הערך הנוכחי של Δ_n, וכך להקטין את שונות השגיאה בשערוך של d_n.

[3] נכונות אלגוריתם Levinson – Durbin מעיבוד אותות מוכחת בצורה דומה. ההוכחה של פירוק המשוון ניתנה כתרגיל בית.

המערכת המתקבלת נראית כך,



נפתח כעת ביטוי מפורש לאינפורמציה ההדדית על פני יחידת ההחלטה ונראה שהיא שווה לקיבול הערוץ הצבעוני. נראה עבור המקרה שחסם Shannon הדוק, למרות שמשיקולי עיבוד אותות הפירוק נכון תמיד.

נסמן ב $S_\Delta(f)$ את ספקטרום שגיאת השערוך האופטימלי של d_n מתוך $\{y_{-\infty}^{\infty}\}$ (בלבד), כאשר $y_n = h_n * g_n * d_n + z_n$. לפי הביטוי לספקטרום שגיאת השערוך של מסננת ווינר נקבל,

$$S_\Delta(f) = \frac{\sigma_d^2 \cdot \dfrac{S_z(f)}{|G(f)|^2 |H(f)|^2}}{\sigma_d^2 + \dfrac{S_z(f)}{|G(f)|^2 |H(f)|^2}} = \frac{\sigma_d^2 \cdot S_{z,eq}(f)}{P(f) + S_{z,eq}(f)} = \frac{\sigma_d^2 \cdot S_{z,eq}(f)}{\theta} = \frac{\sigma_d^2 \cdot S_{z,eq}(f)}{P + \sigma_d^2}$$

כאשר $S_d(f) = \sigma_d^2$, השוויון השני נכון משום ש $S_{z,eq}(f) = |H(f)|^{-2} \cdot S_z(f)$ ו $P(f) = \sigma_d^2 \cdot |G(f)|^2$, והשוויונות השלישי והרביעי נכונים כאשר חסם Shannon הדוק.

שגיאת החיזוי של הסדרה Δ_n מתוך העבר שלה תסומן כעת $e_n = \Delta_n - \hat{\Delta}_n$ והיא שגיאת השערוך הכוללת בשערוך d_n מתוך כל המדידות $\{y_{-\infty}^{\infty}, d_n^-\}$. שגיאה זו נתונה ע"י הספק האנטרופיה (entropy power) של Δ_n , המסומן $P_e(\Delta_n)$. נקבל,

$$\sigma_e^2 = Var(e_n) = P_e(\Delta_n) = \exp\left(\int_{-1/2}^{1/2} \log S_\Delta(f)\, df \right)$$
$$= \frac{\sigma_d^2}{P + \sigma_z^2} \exp\left(\int_{-1/2}^{1/2} \log S_{z,eq}(f)\, df \right)$$

האינפורמציה ההדדית הסקלארית המתקבלת על פני יחידת ההחלטה היא

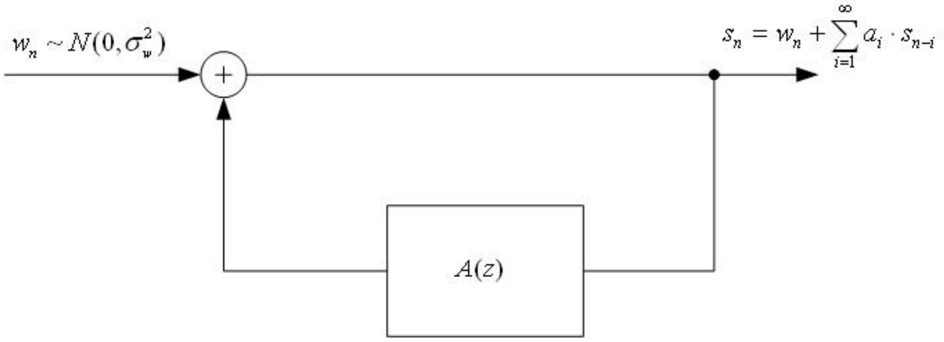
$$I(\hat{d}_n;d_n)=h(d_n)-h(e_n)=\frac{1}{2}\log_2(2\pi e\cdot\sigma_d^2)-\frac{1}{2}\log_2(2\pi e\cdot\sigma_e^2)$$

$$=\int_{-1/2}^{1/2}\frac{1}{2}\log_2\left(\frac{\sigma_d^2}{\frac{\sigma_d^2}{P+\sigma_z^2}\cdot S_{z,eq}(f)}\right)df=\int_{-1/2}^{1/2}\frac{1}{2}\log_2\left(\frac{\theta}{S_{z,eq}(f)}\right)df=C$$

כאשר חסם Shannon הדוק. מכיוון שהשגנו את קיבול הערוץ הרי שהפירוק לשני שלבים של מערכת
ה FFE/DFE שהצענו שומר על אופטימליות.

<u>דחיסה עם עיוות ריבועי של מקור גאוסי צבעוני</u>

נעסוק במודל זמן בדיד הבא למקור גאוסי צבעוני מסוג Auto – regressive (AR) .



המקור מתואר ע"י s_n כאשר

- תהליך החידושים (אינובציות) w_n הוא תהליך גאוסי לבן בעל תוחלת אפס ושונות σ_w^2.
- המקור נבנה ע"י מסננת ליניארית קבועה בזמן וסיבתית בעלת התמרת z ,
  $A(z)=\sum_{i=1}^{\infty}a_i\cdot z^{-i}$.
- ספקטרום המקור נתון ע"י $S_S(f)=\frac{\sigma_w^2}{|1-A(f)|^2}$. כמו כן מתקיים הקשר

$$\sigma_w^2=P_e(s_n)=\exp\left[\int_{-1/2}^{1/2}\log S_s(f)\ df\right]$$

כאשר $P_e(s_n)$ מסמן את הספק האנטרופיה של המקור s_n.

מציאת פונקצית קצב עיוות – לפי כלל מזיגת מים

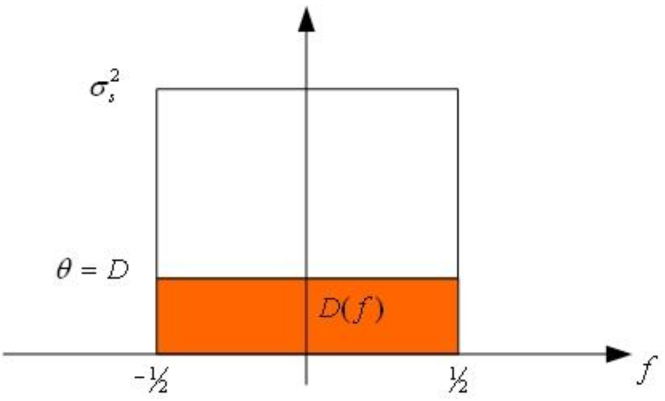
$$R=R(D)=\int_{-1/2}^{1/2}\frac{1}{2}\log_2(\frac{S_s(f)}{D(f)})df=\int_{f:\ \theta<S_s(f)}\frac{1}{2}\log_2(\frac{S_s(f)}{\theta})df\quad(\frac{bits}{sample})$$

כאשר θ הוא "גובה המים" והעיוות בכל תדר נקבע כך ש $\int_{-1/2}^{1/2}D(f)df=D$.

מקרים פרטיים ותכונות :

- מקור גאוסי לבן – כאשר למקור שונות σ_s^2 פונקצית קצב עיוות נתונה ע"י

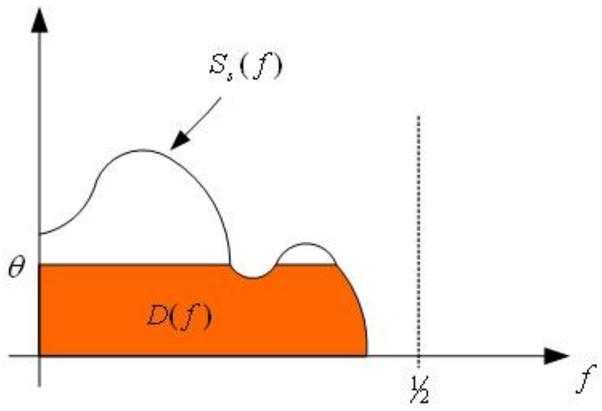
$$R(D)=\frac{1}{2}\log_2(\frac{\sigma_s^2}{D})\ \ (\frac{bits}{sample})$$



- החסם התחתון של Shannon –

$$R(D)\ge\int_{-1/2}^{1/2}\frac{1}{2}\log_2(\frac{S_s(f)}{D})\,df=\frac{1}{2}\log_2(\frac{\sigma_w^2}{D})$$

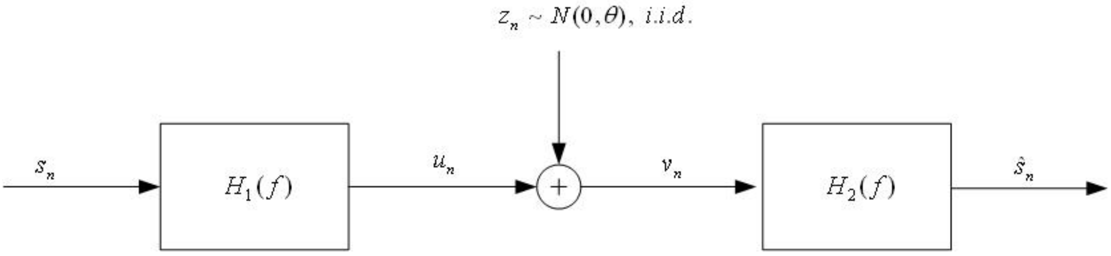
כאשר σ_w^2 הוא שונות תהליך החידושים ונתון ע"י הספק האנטרופיה של המקור. החסם מתקבל בשוויון כאשר גובה המים נמצא מתחת לנקודת ספקטרום המקור המינימלית, דהיינו $S_s(f)\ge\theta$ לכל $|f|\le 1/2$ (מצב זה מתקבל בד"כ כאשר העיוות קטן).



- "הערוץ" האופטימלי - מכיוון ש

$$R(D)=\inf\ \bar{I}(\{s_n\};\{\hat{s}_n\})$$

כאשר האינפימום נלקח על פני כל הפילוגים $p(\{\hat{s}_n\}|\{s_n\})$ היוצרים תהליכים אקראיים סטאציונריים $\{\hat{s}_n\}$ שמקיימים את אילוץ העיוות, $E(\hat{s}_n-s_n)^2\le D$.
מפתרון מזיגת המים נובע שהערוץ ההפוך $\{\hat{s}_n\}\to\{s_n\}$, המגשים את פונקצית קצב עיוות מקיים ש $s_n=\hat{s}_n+e_n$, כאשר e_n גאוסי בת"ס ב $\hat{s}_n$, וספקטרום ההספק שלו נתון ע"י $D(f)$, כך ש $S_s(f)=S_{\hat{s}}(f)+D(f)$.
במקרה שלנו ניתן לקבל גם ערוץ מגשים קדמי:



כאשר המסננות נתונות ע"י

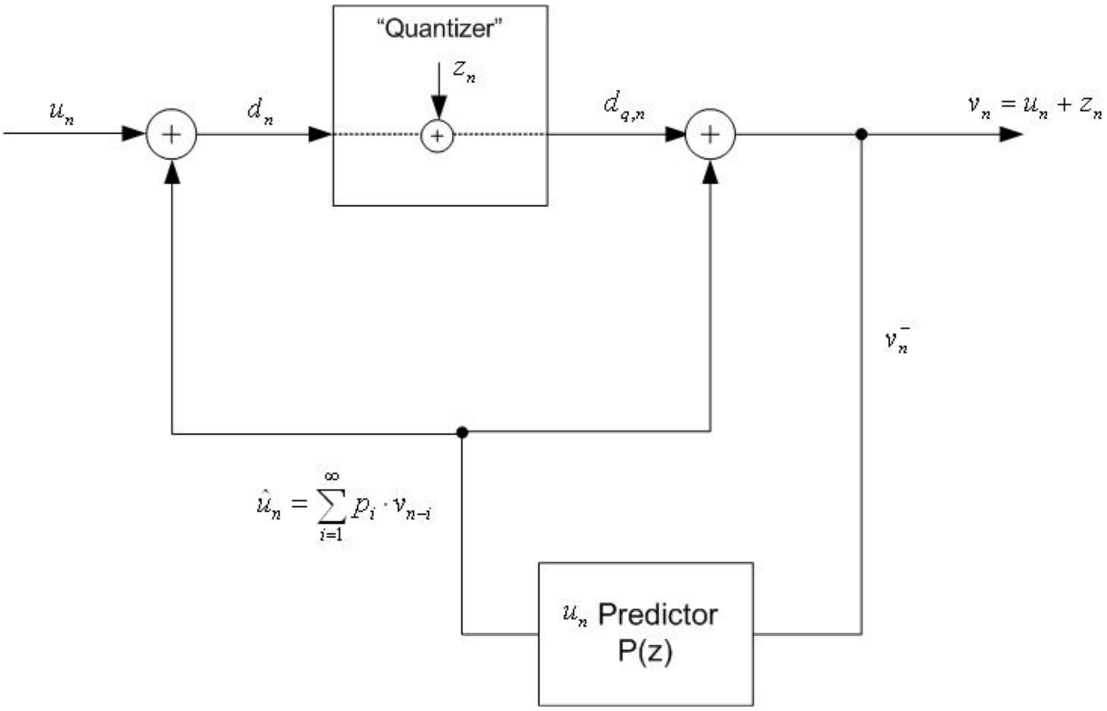
$$\left|H_1(f)\right|^2 = 1 - \frac{S_s(f)}{D(f)}$$

$$H_2(f) = H_1^*(f)$$

, וניתן לוודא שאכן האינפורמציה ההדדית היא $\bar{I}(\{s_n\};\{\hat{s}_n\}) = \bar{I}(\{u_n\};\{v_n\}) = R(D)$,
כאשר אילוץ העיוות נשמר $E(\hat{s}_n - s_n)^2 \le D$, ע"י מציאת האינפורמציה ההדדית והעיוות בכל תדר בנפרד.

שימוש בחיזוי לדחיסת מקור AR גאוסי צבעוני

מערכת של קוונטייזר עם חיזוי מתוארת ע"י



המסנן $P(z)$ הוא חזאי ל u_n מתוך v_n^- , ו"הרעש" הנוצר בקונטייזר z_n הוא רעש גאוסי לבן, בת"ס בתהליך $\{u_n\}$ וב v_n^- , העבר של התהליך $\{v_n\}$.

מטרת המערכת היא להגיע למצב שבו פונקצית קצב עיוות של המקור הצבעוני שווה לאינפורמציה ההדדית הסקלארית על פני הקוונטיזר, דהיינו

$$R(D)=\inf\ \bar{I}(\{s_n\};\{\hat{s}_n\})=I(d_n;d_{q,n})\ .$$

בדומה לפיתוח בחלק הקודם עבור קידוד ערוץ נפתח,

$$R(D)\overset{(1)}{=}\bar{I}(\{u_n\};\{v_n\})\overset{(2)}{=}I(v_n;u_{-\infty}^{\infty}|v_n^-)\overset{(3)}{=}I(v_n-\hat{u}_n;u_n-\hat{u}_n,u_{-\infty}^{n-1},u_{n+1}^{\infty}|v_n^-)$$

$$\overset{(4)}{=}I(d_{q,n};d_n,u_{-\infty}^{n-1},u_{n+1}^{\infty}|v_n^-)\overset{(5)}{=}h(d_{q,n}|v_n^-)-h(d_{q,n}|d_n,u_{-\infty}^{n-1},u_{n+1}^{\infty},v_n^-)$$

$$\overset{(6)}{=}h(d_{q,n}|v_n^-)-h(z_n)\overset{(7)}{=}h(d_{q,n})-h(z_n)\overset{(8)}{=}I(d_n;d_n+z_n)=I(d_n;d_{q,n})$$

כאשר :

- השוויון הראשון נכון כאשר משתמשים במסננים $H_1(f)$ ו $H_2(f)$.
- השיויון השני נובע מכלל השרשרת למקרה הסטאציונרי והפיתוח אחריו.
- השוויון השלישי מתקבל מכיון שהחזאי $\hat{u}_n$ הוא פונקצית של המדידות v_n^- בלבד.
- השוויון הרביעי מתקבל ממבנה המערכת.
- השיויון החמישי מתקבל מפירוק האינפורמציה הדדית להפרש אנטרופיות.
- השיויון השישי מתקבל מכיון ש z_n בת"ס בתהליך $\{u_n\}$ וב v_n^-.
- השיויון השביעי מתקבל כאשר $d_{q,n}$ בת"ס ב v_n^-.
- השיויון השמיני מתקבל ע"י חזרה מהפרש אנטרופיות לאינפורמציה הדדית.

התוצאה המבוקשת מתקבלת לאחר השיויון התשיעי ממבנה המערכת.

נרצה לבדוק מתי מתקיים השיויון השביעי. מכיון ש $v_n=u_n+z_n$ ו z_n הוא רעש גאוסי לבן, בת"ס בתהליך $\{u_n\}$ וב v_n^-, הרי שהחזאי הטוב ביותר ל v_n מתוך v_n^- הוא החזאי הטוב ביותר ל u_n מתוך v_n^-, ולכן שגיאת החיזוי ל v_n שהיא $d_{q,n}$ מקימת את עיקרון האורתוגונליות, דהיינו ניצבת למדידות v_n^-. מכיוון שהתהליכים הם גאוסיים, חוסר קורלציה שקול לאי תלות סטטיסטית, ולכן כאשר $P(z)$ הוא החזאי האופטימלי במובן שגיאה ריבועית ממוצעת ל u_n (ולכן גם ל v_n) מתוך v_n^-, נקבל ש $d_{q,n}$ בת"ס ב v_n^-.
במצב זה פונקצית קצב עיוות של המקור הצבעוני שווה לאינפורמציה ההדדית הסקלארית על פני הקוונטייזר.

בדומה לבעיית הערוץ הצבעוני, גם עבור מקור צבעוני ניתן להפריד בין הטיפול בצבעוניות המקור לבין הטיפול בקוונטיזציה. צבעוניות המקור תטופל באמצעות המסננים $H_1(f)$, $H_2(f)$ והחזאי $P(z)$, והקוונטייזר צריך להתאים למקור גאוסי לבן בלבד.

כמו כן ניתן להסביר את הסתירה בין העובדה שהמערכת חוזה באופן סדרתי, לבין העובדה שרעש הקוונטיזציה הוא גאוסי ולכן בהכרח ישנו שימוש בקוד (שאינו סיבתי), משיקולים דומים לשיקולים של בעיית הערוץ – הנחה של מספר מקורות שרוצים לקודד במקביל או שימוש בשוזר במקרה של מקור יחיד.

קריאה נוספת:

[1] Cioffi J. M. , Dudevoir G. P. , Eyuboglu M. V., and Forney G. D. , Jr. ; “MMSE decision-feedback equalizers and coding- Part I: Equalization results” ; IEEE Trans. Commun., vol. 43, no. 10, pp. 2582–2594, Oct. 1995.

[2] -- ; “MMSE decision-feedback equalizers and coding- Part II: Coding results” ; IEEE Trans. Commun., vol. 43, no. 10, pp. 2595–2604, Oct. 1995.

[3] Guess T. Varanasi M.K. ; "A new successively decodable coding technique for intersymbol-interference channels" ; Proceedings. IEEE International Symposium on Information Theory , 2000, 25-30 June 2000, Page 102.

[4] Forney G. David, Jr. ; Shannon meets Wiener II: On MMSE estimation in successive decoding schemes

[5] Zamir R. , Kochman Y. , Erez U. ; Achieving the Gaussain Rate-Distortion function by prediction, to appear in ISIT 2006 , Seattle, Washington.

הרצאה – 2

קידוד ערוץ גאוסי עם אינפורמציית צד - Writing on Dirty Paper (Costa)

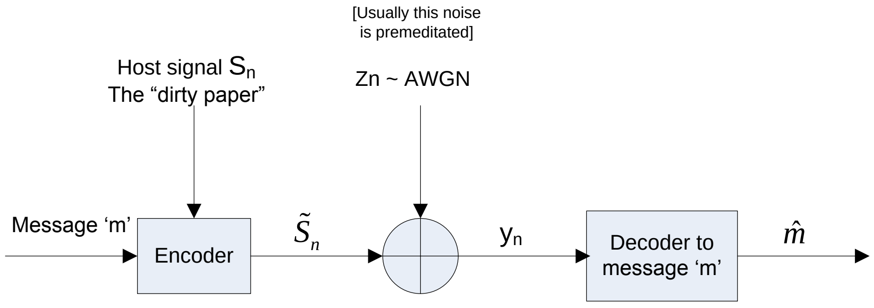
סוכם ע"י עידן אלרוד

נראה דואליות של אינפורמצית צד בין אינפורצית צד לקידוד מקור ואינפורמצית צד לקידוד ערוץ כלומר נראה שזו אותה בעייה תיאורטית. נדגים את הנושא בעזרת בעיית כתיבה על נייר מלוכלך (Writing on dirty paper).

הבעייה מוגדרת כך: יש לנו נייר מלוכלך ורוצים לכתוב עליו כך שמאוחר יותר ניתן יהיה לקרוא את הכתוב. יש שתי אפשרויות:

- למחוק את הנייר המלוכלך כך שיהיה נקי ואז לכתוב על הנייר הנקי.
- ברור כי פעולת ניקוי הנייר היא קשה ודורשת אנרגייה ולכן נרצה להימע ממנה. לכך ניתן לכתוב על הנייר המלוכלך כמות שהוא אולם להסכים עם הקורא על דרך הקריאה כך שיקל עליו לקרוא.

בשנת 1983 הוכיח COSTA כי ניתן להשתמש בצורה השנייה ללא אובדן אינפורמציה. אחת האפליקציות כיום לשימוש בשיטתו של COSTA היא הגנה על זכויות יוצרים בהפצת מוזיקה, וידאו ותמונות. למי שרוכש את המוצר ניתנת אינפורמצית צד שבעזרתה יוכל לקרוא/לנגן את האינפורמציה שהיא גלויה לכל. מודל זה ניקרא Digital Water Marking (DWM). מודל המערכת נבנה באופן הבא:



האות לאחר המקודד אינו מעוות מידי כלומר קימת המגבלה כי:

$$E\left\{d\left(S,\tilde{S}\right)\right\}\le D \quad (0.1)$$

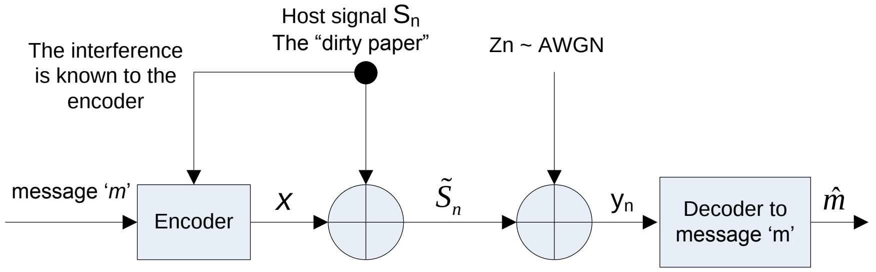
כאשר בדרך כלל d(.) הוא מדד עיוות ריבועי. מכאן יש עיוות מקסימלי בהטבעה או לחלופין אנרגיה סופית של ההודעה הנכתבת. נגדיר:

$$x \triangleq \tilde{S}-S \quad (0.2)$$

לפי הגדרה(0.2) נקבל כי:

$$y=s+x+z \quad (0.3)$$

המודל של COSTA ניקרא קידוד ערוץ עם אינפורמצית צד, והוא שונה רק במקצת מ DWM:



מגבלת ההספק השקולה היא:

$$E\left\{x^2\right\} \le P \qquad (0.4)$$

עתה בעיית DWM ובעיית קידוד הערוץ עם אינפורמצית צד שלנו לפי הגדרת 'x' במשוואה (0.3) הן שקולות כאשר הספק הערוץ P שווה לעיוות הריבועי המותר בהטבעה D כלומר D=P. נסתכל עתה מה ידוע על הבעייה של COSTA ומזה נלמד על בעיית קידוד המקור שלנו. למעשה בעייה זו היא בעיית ערוץ . ובכן COSTA הוכיח את משפט COSTA בשנת 1983 בהתבססו על מאמר של Gelfand Pinsker משנת 1980. המשפט שהוכיח COSTA הוא:

$$C_{SI@Tx} = C_{SI@both} = C_{zero\ \text{int}erference} = \frac{1}{2}\cdot log_2\left(1+\frac{P}{\sigma_z^2}\right) \qquad (0.5)$$

כאשר:

- $C_{SI@TX}$- קיבול הערוץ כאשר ידועה ההפרעה S למקודד בלבד.
- $C_{SI@Both}$- קיבול הערוץ כאשר ידועה ההפרעה S למקודד ולמפענח גם יחד.
- $C_{zero\ interference}$ – *קיבול הערוץ* כאשר אין הפרעה S כלל.

למעשה כאשר S ידוע במקלט ניתן לחסרו ולכן זה שקול למצב שהוא לא קיים כלל . כלומר גם אם המפענח לא יודע את ה "ליכלוך על הנייר" שכתבנו עליו עדיין ניתן לפענח את מה שניכתב כאילו כן ידע המפענח מה היה הליכלוך המקורי . כלומר אין כל צורך למחוק את הנייר וקיבול האינפורמציה תלוי רק בהספק ההודעה שניכתבה ביחס לרעש הלבן במערכת.

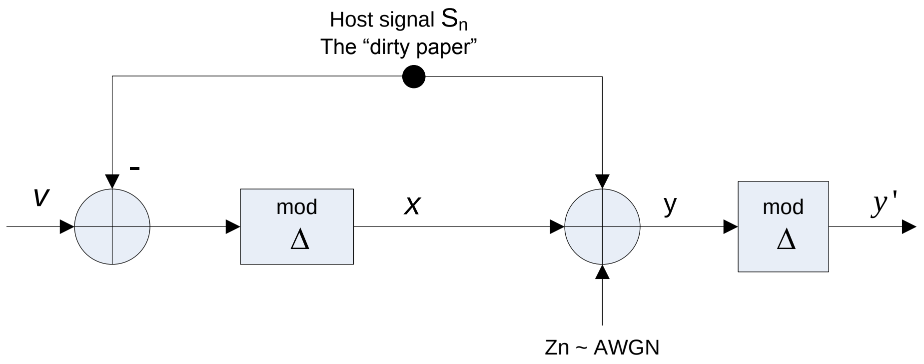
נראה עתה את החלק היותר מסובך בשיויון COSTA כלומר נראה כי:

$$C_{SI@Tx} = C_{SI@Both} \qquad (1.1)$$

נראה כי ניתן להתקרב לכך על ידי ביטול ההפרעה בעזרת אריטמטיקת Modulo סקאלרית. נגדיר את הפעולה של modulo:

$$x\ modulo\ \Delta = x - \Delta\cdot\left[\frac{x}{\Delta}\right] = min\left\{\left|x - i\cdot\Delta\right| \ : i\in\mathbb{Z}\right\} = \left\{\begin{matrix} error\ in\ rounding\ x \\ to\ the\ nearest \\ multiple\ of\ \Delta \end{matrix}\right\} \qquad (2.1)$$

נסתכל עתה על פתרון קידוד ערוץ עם אינפורמצית צד לפי מודל COSTA כאשר המקודד מבצע פעולת *modulo* לאחר חיסור ההפרעה שהוא יודע כי תתוסף ובדרגת הכניסה של המפענח קיימת אותה פעולת *modulo*.



עדיין לפי המודל הספק המשדר מוגבל כלומר:

$$E\left\{x^2\right\} \le P \qquad (1.3)$$

נסכל על האינפורמציה ההדדית בין ***y'*** ו - ***v.*** לאחר דרגת הכניסה יש במפענח מערכת ML שמשערכת את '***v***'. כמובן שלפי הגדרת בעיית COSTA ה"לכלוך" S ידוע למשדר אבל לא למקלט. נסתכל על ***y'*** ***במונחי*** v ו z:

$$y' = y \; mod \; \Delta = \underbrace{x}_{(v-s)\; mod \;\Delta} + s + z \; mod \; \Delta = \left[\left(v-s\right) \; mod \; \Delta + s + z\right] \; mod \; \Delta \qquad (1.4)$$

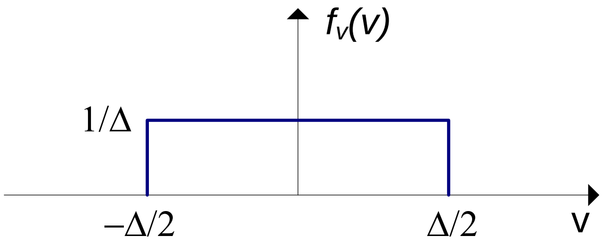
כיוון שהפעלת פעולות *modulo* בטור שקולה להפעלת פעולת *modulo* אחת בסיום אזי נקבל:

$$y' = \left(v+z\right) \; mod \; \Delta \qquad (1.5)$$

המסקנה מ - (1.5) היא כי:

$$I\left(v; y'\right) = I\left[v \; ; \; \left(v+z\right) \; mod \; \Delta\right] \qquad (1.6)$$

שזהו ערוץ רעש חיבורי *modulo* . בקורס הבסיסי למדנו כי הקיבול בערוץ רעש חיבורי *modulo* מתקבל על ידי פילוג מבוא אחיד או הפילוג המגשים בכניסה הינו אחיד . במקרה כזה כלומר הכניסה מתפלגת אחיד בין $-\Delta/2$ ל - $\Delta/2$ בגובהה $1/\Delta$. הפילוג ניראה כך:



התוחלת היא אפס והשונות היא:

$$E\left\{v^2\right\} = \frac{\Delta^2}{12} \qquad (2.1)$$

נשיב לב שלכל 's' (קבוע או אקראי) מתקיים $x=v-s \;\; mod \;\; \Delta$ גם כן אחיד . ומכאן $E\left\{x^2\right\} = \frac{\Delta^2}{12}$ גם כן. כיוון שהספק הכניסה מוגבל כלומר $E\left\{x^2\right\} = P$ אזי נקבל כי:

$$\Delta = \sqrt{12 \cdot P} \qquad (2.2)$$

הקיבול של ערוץ רעש חיבורי *modulo* הוא מקסימלי כאשר פילוג המבוא אחיד . נסמן את הפרמטר של הפילוג האחיד ב - Δ הקיבול נתון ע"י:

$$C_{eq} = h(out) - h(equivalent\ noise) = log(\Delta) - h(Z\ mod\ \Delta) \qquad (2.3)$$

נציב את (2.2) לתוך (2.3) נקבל:

$$C_{eq} = \frac{1}{2} \cdot log(12 \cdot P) - h(Z\ mod\ \Delta) \qquad (2.4)$$

לכל משתנה אקראי Z ובפרט גאוסי פעולת ה – *mod* מקטינה את האנטרופיה ולכן:

$$h(Z\ mod\ \Delta) \le h(Z) \qquad (2.5)$$

נשתמש ב – (2.5) ונקבל מ - (2.4) חסם תחתון לקיבול הערוץ:

$$C_{eq} \ge \frac{1}{2} \cdot log(12 \cdot P) - h(Z) \qquad (2.6)$$

נשים לב כי ב – SNR גבוה מתקיים:

$$\Delta \gg \sigma_z \ \rightarrow\ Z\ mod\ \Delta \ \approx Z \qquad (2.7)$$

ומכאן שב – SNR גבוה החסם (2.6) הוא הדוק. נציב ב - (2.6) את הביטוי לאנטרופיה של משתנה גאוסי ונקבל:

$$C_{eq} \ge \frac{1}{2} \cdot log(12 \cdot P) - \frac{1}{2} \cdot log(2 \cdot \pi \cdot e \cdot \sigma_z^2) = \underbrace{\frac{1}{2} \cdot log\left(\frac{P}{\sigma_z^2}\right)}_{A} - \underbrace{\frac{1}{2} \cdot log\left(\frac{2 \cdot \pi \cdot e}{12}\right)}_{B} \qquad (2.8)$$

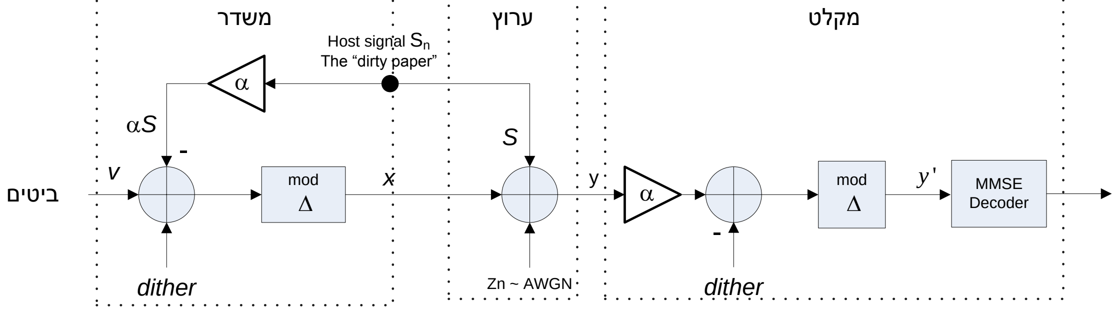
ביטוי A במשוואה (2.8) הינו הקיבול של ערוץ AWGN ללא ה – '1' כלומר כמעט אופטימלי ובמצב של SNR גבוה הם קרובים כלומר:

$$C_{AWGN} = \frac{1}{2} \cdot log\left(1 + \frac{P}{\sigma_z^2}\right) \underset{High\ SNR \rightarrow \frac{P}{\sigma_z^2} \gg 1}{\approx} \frac{1}{2} \cdot log\left(\frac{P}{\sigma_z^2}\right) = A \qquad (2.9)$$

ביטוי B הוא הפסד כיוון שלא עשינו Shaping ומהווה 0.254~ [ביט לשימוש ערוץ]. הוא נובע מכך שביצענו פעולת ח יסור modulo ולמעשה בגלל זה איבדנו אינפורמציה . כדי להרוויח בחזרה את ה – Shaping Gain צריך לשדר סיגנל על שריג רב ממדי בהמשך נילמד על שריגים ונירא כיצד ניתן לשפר את הסיגנל המשודר . כדי להרוויח בחזרה את ה – '1' בנוסחת הקיבול (2.9)כלומר לעבור מביטוי 'A' ל- (2.9) חלק שמאלי צריך לבצע סינון MMSE במקלט ולהיעזר ברנדמיזציה משותפת (common randomness) בצורה של dither.

הגדרה: <u>dither</u> הוא משתנה אקראי שמתפלג אחיד על תא השריג בין Δ/2- ל Δ/2. זהוא רעש ידוע גם למקודד וגם למפענח ובד"כ מבוסס על מעגל פסאודו אקראי.

הסכמה עם ה – dither נקראת lattice pre-coding ונראית כך:



הוספנו הכפלה בקבוע של האות המארח בחיבורו בכניסת המקודד וכן הכפלה באותו קבוע לפני החסרת ה - dither במפענח. נסתכל עתה על הרעש השקול ונראה שכאשר מכפילים בקבוע (α) אות שטבול ברעש אזי ניתן להוריד את הרעש השקול . לפני החסרת ה – dither במקלט נקבל:

$$\alpha \cdot y = \alpha \cdot (x + s + z) = x + \alpha \cdot s + \underbrace{\left[(1-\alpha)\cdot x + \alpha \cdot z\right]}_{Z_{eq}} \tag{3.1}$$

ניתן ע"י ידי שינוי α להביא גודל זה (Z_{eq}) למינימום אנרגיה, המינימום הוא:

$$Var\left(Z_{eq}\right) = (1-\alpha)^2 \cdot P + \alpha^2 \cdot \sigma_z^2 \Big|_{\alpha_{opt} = \frac{P}{P+\sigma_z^2}} = \frac{P \cdot \sigma_z^2}{P + \sigma_z^2} \tag{3.2}$$

כאשר כמובן X ו – Z הם בלתי תלויים סטטיסטית I - Z עם תוחלת אפס וכן:

$$E\left\{x^2\right\} = P \quad , \quad E\left\{Z^2\right\} = \sigma_z^2 \tag{3.3}$$

עבור SNR גבוה $P \gg \sigma_z^2$ ואז $\alpha_{opt} \approx 1$ כלומר חוזרים לסכמה המקורית ואין צורך ב – dither. לא הראיינו זאת אולם אם 's' הוא "חזק וחלק" (כלומר בעל פילוג שטוח ורחב בייחס למשרת של 'x') אזי אין צורך ב – dither גם עבור α<1.

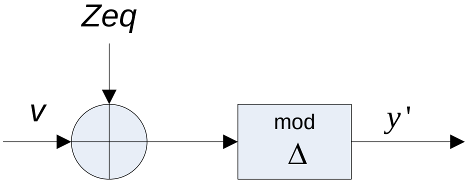
<u>**טענה**</u>: עבור משתנה אחיד dither כלומר $dither \sim Unif\left(-\frac{\Delta}{2}, \frac{\Delta}{2}\right)$ אזי לכל ערך דטרמיניסטי 'a' מתקיים:

$$\boxed{(a + dither)\ mod\ \Delta \sim Unif\left(-\frac{\Delta}{2}, \frac{\Delta}{2}\right)} \tag{4.3}$$

מהטענה נובע כי לכל משתנה אחיד w שאינו תלוי ב - dither הפעולה של הוספת dither ואח"כ ביצוע mod Δ לא תלויה ב – w בסימונים שלנו:

$$\boxed{(w + dither)\ mod\ \Delta \ \underline{\perp}\ w} \tag{3.5}$$

<u>**משפט**</u>: סכמת ה – lattice pre-coding שקולה לערוץ האדיטיבי הבא:



כאשר Z_{eq} הוא בת"ס בכניסה, ומקיים:

$$Z_{eq} = \alpha \cdot Z + (1-\alpha)\cdot dither \quad ; \quad Z \sim N\left(0, \sigma_z^2\right) \quad ; \quad dither \sim Unif\left(-\frac{\Delta}{2}, \frac{\Delta}{2}\right) \tag{4.1}$$

הוכחה: נסתכל על היציאה של המערכת המקורית כלומר ה lattice pre-coding ונראה כי היא זהה לבסוף לערוץ האדיטיבי השקול. הכניסה למקלט ML בסכמה המקורית היא:

$$\begin{aligned} y' &= (\alpha \cdot y + dither)\ mod\ \Delta = (\alpha \cdot [x + Z + S] - dither)\ mod\ \Delta = \ldots \\ \ldots &= (\alpha \cdot Z + \alpha \cdot S + x + [\alpha - 1]\cdot x - dither)\ mod\ \Delta \end{aligned} \tag{4.2}$$

כאשר:

$$x = (v - \alpha \cdot S + dither)\ mod\ \Delta \tag{4.3}$$

לתוך משוואה (4.2) נציב את (4.3) נקבל:

$$y' = \left(\alpha \cdot z + \alpha \cdot S + \left[(v - \alpha \cdot S + dither)\ mod\ \Delta\right] + [\alpha - 1]\cdot x - dither\right)\ mod\ \Delta \tag{4.4}$$

נשתמש בעובדה כי במקום שתי פעולות *modulo* בטור ניתן לבצע רק אחת בסוף ונקבל:

$$y' = \left(v + \alpha \cdot z + [\alpha - 1] \cdot x\right)\ mod\ \Delta \qquad (4.5)$$

נשתמש במסקנה מהטענה כלומר אם מחברים למשתנה אחיד עם פרמטר Δ (dither) במיקרה שלנו) משתה אחר כלשהו (במיקרה שלנו v-αS) ועושים Δ modulo לאחר מכן (משתנה 'x' במקרה שלנו) אזי התוצאה 'x' אינה תלוייה בכניסה כלומר אינה תלוייה ב - v-αS ולכן אינה תלוייה ספציפית גם ב- 'v'. כלומר לפי המסקנה מהטענה 'x' אינו תלוי ב – 'v'.

נסתכל עתה על (4.5) ונסמן את החלק הימני שלו כ - Z_{eq} כלומר:

$$y' = \left(v + \underbrace{\alpha \cdot z + [\alpha - 1] \cdot x}_{Z_{eq}}\right)\ mod\ \Delta = \left(v + Z_{eq}\right)\ mod\ \Delta \qquad (4.6)$$

כיוון ש – 'x' אינו תלוי ב – 'v' וכן 'Z' אינו תלוי ב – 'v' אזי Z_{eq} אינו תלוי ב 'v' בכתיב מתמטי:

$$x \perp v \rightarrow Z_{eq} \perp v \qquad (4.7)$$

לפי החלק הראשון בטענה 'x' מתפלג כמו dither ומכאן:

$$Z_{eq} = \alpha \cdot z + [\alpha - 1] \cdot x = \alpha \cdot z + [\alpha - 1] \cdot dither \qquad (4.8)$$

משוואה (4.8) יחד עם (4.6) מהווה הוכחה של המשפט. עתה נשתמש בסכמה השקולה לסכמת lattice pre-coding כדי לחשוב את הקיבול של מערכת ה – lattice pre-coding. נניח כי 'v' מתפלג אחיד עם פרמטר כלשהוא אז הקיבול של המערכת השקולה נתון על ידי:

$$C_{lattice\ pre-coding} = I\left(v; y'\right)\Big|_{v\sim uniform} = h(out) - h(equivalent\ noise) = log\left(\Delta\right) - h\left(Z_{eq}\right) \qquad (4.9)$$

נשים לב כי כי פילוג אחיד בכניסה משיג קיבול ללא אילוצי הספק, במידה ויש אילוצי הספק צריך לבחור Δ (גודל הקונסטלציה הבסיסי) שיקיים $P = \Delta^2/12$. נחשב עתה חסם תחתון לקיבול על ידי כך שידוע כי אנטרופיה של משתנה כלשהו עם שונות σ^2 תמיד קטנה מאנטרופיה של משתנה גאוסי בעל אותה שונות. כלומר בשונות נתונה למשתנה גאוסי יש את האנטרופיה המקסימלית.

בכתיב מתמטי:

$$h\left(Z_{eq}\right) \le h\left(Z_{eq}^{*}\right)\ \ ;\ \ Var\left(Z_{eq}\right) = \sigma_{zeq}^2\ \ ;\ \ Z_{eq}^{*} \sim N\left(0, \sigma_{zeq}^2\right) \qquad (5.1)$$

אנטרופיה של משתנה גאוסי היא ידועה:

$$h\left(Z_{eq}^{*}\right) = \frac{1}{2} log\left(2 \cdot \pi \cdot e \cdot \sigma_{zeq}^2\right) \qquad (5.2)$$

הגודל σ_{zeq}^2 חושב כבר קודם לכן עבור $\alpha = \alpha_{opt}$ במשוואה (3.2) נציב אותו ונקבל:

$$h\left(Z_{eq}^{*}\right) = \frac{1}{2} log\left(2 \cdot \pi \cdot e \cdot \frac{P \cdot \sigma_z^2}{P + \sigma_z^2}\right) \qquad (5.3)$$

נציב את (5.3) ב - (5.1) ונקבל בעזרת (4.9) כי החסם התחתון לקיבול הוא:

$$C_{lattice\ pre-coding} \ge log\left(\Delta\right) - \frac{1}{2} log\left(2 \cdot \pi \cdot e \cdot \frac{P \cdot \sigma_z^2}{P + \sigma_z^2}\right) \qquad (5.4)$$

נציב את (2.2) ב- (5.4) ונקבל:

$$C_{lattice\ pre-coding} \geq \frac{1}{2} \cdot log\left(12 \cdot P\right) - \frac{1}{2} log\left(2 \cdot \pi \cdot e \cdot \frac{P \cdot \sigma_z^2}{P + \sigma_z^2}\right) \quad (5.5)$$

ע"י כינוס איברים נגיע ל:

$$C_{lattice\ pre-coding} \geq \frac{1}{2} \cdot log\left(1 + \frac{P}{\sigma_z^2}\right) - \frac{1}{2} \cdot log\left(\frac{2 \cdot \pi \cdot e}{12}\right) \quad (5.6)$$

כלומר הצלחנו אכן להחזיר את ה – '1' לביטוי 'A' במשוואה (2.8). איבר ההפסד הנותר, כלומר ביטוי 'B' במשוואה (2.8) נובע מאי ביצוע shaping על אות הכניסה, דבר זה ייפתר כאשר נעבור לפעולת modulo ביחס לסריג רב מימדי טוב.

<u>ביבליוגרפיה</u>:

- ISI pre-coding from the books of Gitlin, or Proakis, or Lee-Messerschmidt
- Chen, B. Wornell, G.W. / Quantization index modulation: a class of provably good methods fordigital watermarking and information embedding, IEEE Transactions on Information Theory, May 2001 vol. 47, issue 4, pg. 1423-1443.
- Erez, U. Shamai, S. Zamir, R "Capacity and lattice strategies for canceling known interference", IEEE Transactions on Information Theory, Nov. 2005 vol 51, Issue: 11 pg. 3820- 3833.

הרצאה 3-4

סריגים ושימושם במערכות תקשורת

סוכם ע״י י אמיר סלומון

"כתיבה על נייר מלוכלך"

Costa הוכיח שבערוץ הכולל אות הפרעה הידוע למשדר בלבד ניתן להגיע לקיבול. חיסור-מודולו Δ במשדר משיג אנפורמציה הדדית הקרובה לקיבול. שימוש ב dither במשדר (חיבור) ובמקלט (חיסור) ושיערוך MMSE במוצא נותן חסם לאנפורציה ההדדית בין הכניסה למוצא:

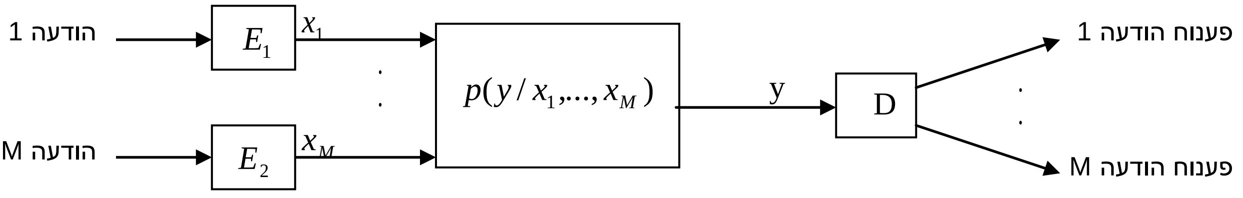
$$I(y';v) \geq \frac{1}{2}\log\left(\frac{p+\sigma_z^2}{\sigma_z^2}\right) - \frac{1}{2}\log\left(\frac{2\pi e}{12}\right)$$

כאשר החסם די הדוק. קיים הפסד של $\frac{1}{2}\log\left(\frac{2\pi e}{12}\right) \approx 0.255bit$ פר שימוש ערוץ לעומת הביטוי לקיבול של ערוץ AWGN (ללא אות הפרעה). הפסד זה נובע כתוצאה ממעבר לשימוש בפילוג אחיד $\left[-\frac{\Delta}{2},\frac{\Delta}{2}\right]$ בכניסה (המביא למקסימום אינפורמציה הדדית בערוץ מודולו) במקום פילוג גאוסי. כדי ל "החזיר" הפסד זה יש להשתמש בקונסטלציות שידור רב מימדיות בכניסה, למשל ע״י שימוש בסריגים. ראשית, נראה מספר בעיות בתקשורת הקשורות לבעיית ה"כתיבה על נייר מלוכלך" הנותנות מוטיבציה לשימוש בסריגים ע"מ להגיע לקיבול בבעייה זו.

תורת אינפורמציה למערכות מרובות משתמשים

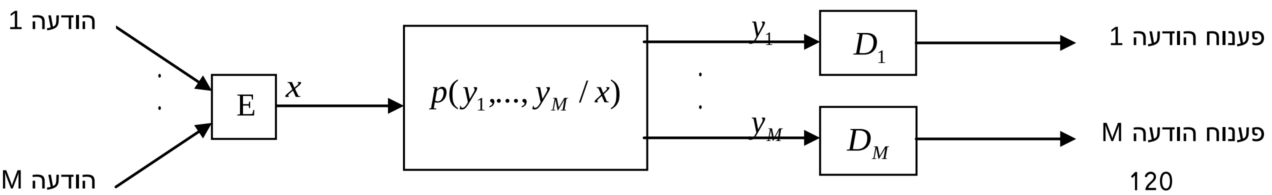
קידוד ערוץ

1) M.A.C - מקלט אחד, ריבוי משדרים:



המטרה היא לפענח מתוך המוצא הבודד את כל M ההודעות באופן תוך שידור בקצבי שידור כמה שיותר גבוהים.

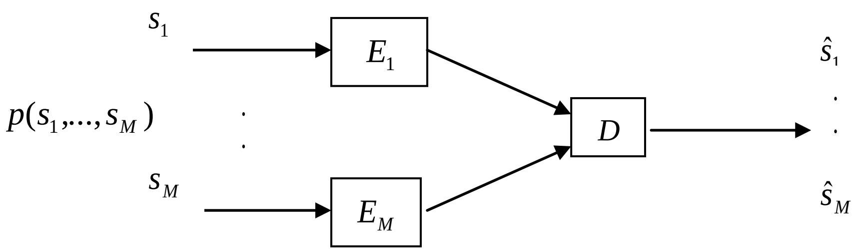
2) B.C - משדר אחד, ריבוי מקלטים:



המטרה היא לפענח מתוך כל מוצא את ההודעה המיועדת לו תוך שידור בקצבי שידור כמה שיותר גבוהים.

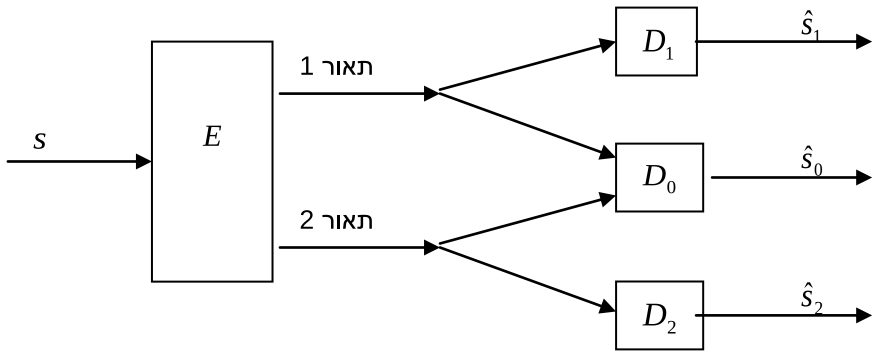
קידוד מקור

1) בעיית קידוד מקור מבוזר:



נתונים M מקורות. המטרה היא לשחזר (בד"כ עם עוות) מתוך אוסף הכניסות המקודדות את M המקורות, תוך ניצול ידיעת ההתפלגות המשותפת שלהן.

2) ריבוי תאורים:



המטרה היא ליצור קידוד יעיל תוך שימוש במספר תאורים שונים של האות s כך שישוחזר במספר מקלטים נפרדים באופן האופטימלי (כלומר עם מינימום עוות).

<u>ייצוג בעיות תקשורת כבעיות "כתיבה על נייר מלוכלך"</u>

ניתן לייצג את בעיות ה- Broadcast Channel וקידוד מקור מבוזר כבעיות שחזור אות בהנתן אינפורמציית צד. נניח למשל כי בבעיית ה- B.C ישנם שני מוצאים, y_1, y_2. ניתן לרשום $x = x_1 + x_2$ כך ש x_1 "מותאם" למקלט y_1 ו- x_2 "מותאם" למקלט y_2. באופן זה, ניתן להתייחס לפענוח מתוך y_1 כערוץ בעל רעש ו "הפרעה"
בלתי-ידועה x_2, ולפענוח מתוך y_2 כערוץ בעל רעש ו "הפרעה" **ידועה** x_1.

עבור בעיית קידוד מקור מבוזר, ניתן לראות בפענוח של כל אחד מהאותות s_i כפענוח תוך שימוש באינפורמציית צד הכוללת את כל שאר הכניסות (המקודדות), תוך ניצול התלות ביניהן כפי שבאה לידי ביטוי בהסתברות המשותפת $p(s_1,\ldots,s_M)$.

לסיכום, בעיית ה "כתיבה על נייר מלוכלך" מייצגת תחום נרחב של בעיות בעולם התקשורת. עובדה זו נותנת מוטיבציה לנסות להגיע לקיבול עבור סכימה זו. נושא זה יידון בהרחבה בסעיפים הבאים.

סריגים

מטרה – להתגבר על ההפסד של $\frac{1}{2}\log\left(\frac{2\pi e}{12}\right)$ הנגרם עקב שימוש במבוא בעל פילוג אחיד בסכימת ה "כתיבה על נייר מלוכלך". מרויחים הפסד זה ע"י שימוש בקונסטלציות שידור רב מימדיות המדמות פילוג רצוי ולכן נקרא Shaping gain.
דרך נוספת להתבונן בבעיה היא אם נרשום את "נפח הרעש" לפי שאנון במונחי אנטרופיה כ- $h(z)=\frac{1}{2}\log(2\pi e\sigma_z^2)$ ואת גודל תא האות המשודר בפועל במונחים של אנטרופיה כ- $\log(\Delta)$. נגדיר "שולי רעש" (המציין פי כמה חזק הספק האות המשודר ביחס לרעש) כ- $\mu=\frac{\Delta^2}{\sigma_z^2}$ להשגת הסתברות שגיאה מסויימת P_e עבור שידור לא מקודד בנוכחות רעש גאוסי:

$$P_e=\int_{\frac{\Delta}{2}}^{\infty}P_z(z)dz=Q\left(\frac{\Delta/2}{\sigma_z}\right)=Q(\sqrt{\mu}/2)$$

"הפער מהקיבול" של שידור אות לא מקודד ניתן לרישום כ- $h(z)-\log(\Delta)=-\frac{1}{2}\log\left(\frac{\mu}{2\pi e}\right)$. ככל ש- μ גדל (כלומר נדרש Pe קטן יותר) כך גם גדל הפער. תוצאה זו נותנת מוטיבציה לפירוש התפלגות הרעש הגאוסי כבעל פילוג גיאומטרי "אופטימלי" במרחב.

משפט (שקילות רעש גאוסי לבן לפילוג אחיד על פני כדור)

א. אם $\underline{x}=(x_1,...,x_n)$ מתפלגים $N(0,\sigma^2)$ i.i.d אזי

$$\underline{x}\xrightarrow[n\to\infty]{dist}Unif(n-\dim.\ Ball\quad with\quad R=\sqrt{n\sigma^2})$$

ב. אם $\underline{u}=(u_1,...,u_n)$ מתפלג אחיד על פני n-dim. Ball ברדיוס $\sqrt{n\sigma^2}$ אזי הפילוג המשותף של כל קבוצה
סופית של דגימות של $\underline{u}$ שואף ל- i.i.d גאוסי עם שונות σ^2 עבור $n\to\infty$.

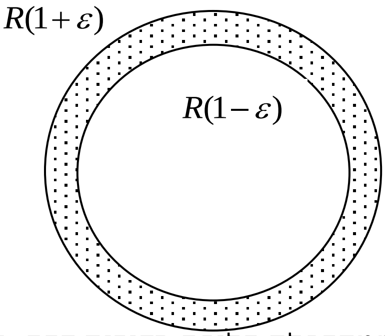
הוכחת א':

1. $f_x(\underline{x})=\left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^n\cdot e^{-\frac{\|\underline{x}\|^2}{2\sigma^2}}$ היא צפיפות משותפת איזוטרופית (כלומר תלויה רק בנורמת הוקטור).
2. ע"פי חוק המספרים הגדולים $\frac{1}{n}\|\underline{x}\|^2=\frac{1}{n}\sum_{i=1}^{n}x_i^2\xrightarrow[n\to\infty]{}\sigma^2$ כאשר ההתכנסות היא במובן Mean square $\Leftarrow$ $\|\underline{x}\|^2\underset{n\to\infty}{\approx}\sqrt{n\sigma^2}$.

מ- 1 ו- 2 נובע כי עבור n גדול $\underline{x}$ מתפלג בקירוב אחיד על פני קליפה כדורית ברדיוס $R=\sqrt{n\sigma^2}$.

3. עבור n גדול, פילוג אחיד על פני קליפה כדורית ≈ פילוג אחיד על פני הכדור כולו:
נפח כדור n מימדי הוא $Vol(n-\dim\ \ Ball)=V_nR^n$, כאשר V_n הוא נפח כדור עם רדיוס יחידה.

נבנה כדור חיצוני ופנימי באופן הבא:



כאשר ε קטן כרצוננו, כך שמתקבלת קליפה כדורית דקה. היחס בין נפח הכדור הפנימי לחיצוני הוא:

$$\frac{[R(1-\varepsilon)]^n V_n}{[R(1+\varepsilon)]^n V_n} = \frac{(1-\varepsilon)^n}{(1+\varepsilon)^n} \xrightarrow[n\to\infty]{} 0$$ עבור כל $\varepsilon > 0$.

לכן, מבחינת תורת ההסתברות, עבור n מאוד גדול פילוג אחיד על פני כל הכדור שקול לפילוג על הקליפה.

סיכום של 1, 2 ו- 3 נותן את התוצאה המבוקשת. ■

להוכחה של חלק ב׳ ראה למשל מאמר "On Lattice Quantization Noise" מאת רמי זמיר ומאיר פדר,

IEEE Transactions on Information Theory, 1996, ורשימת הביבליוגרפיה במאמר.

סריג – הגדרה:

סריג Λ במרחב האוקלידי R^n הוא אוסף בדיד של נקודות $\underline{l}_i \in R^n$, $\Lambda = \{\underline{l}_i\}_{i=-\infty}^{\infty}$. את נקודות הסריג ניתן ליצור בעזרת מטריצה יוצרת $\underline{\underline{G}}(n\times n)$:

$$\Lambda = \left\{ \underline{\underline{G}} \cdot \underline{i} \quad : \quad \underline{i} \in Z^n \right\}$$

ניתן גם לייצג כל נקודת סריג בתור $l_i = \sum_{k=1}^{n} i_k \cdot \underline{g}_k$ כאשר $\underline{g}_k$ העמודה ה- k של $\underline{\underline{G}}$ (אוסף העמודות הוא וקטורי הבסיס של הסריג).

סריג הוא מרחב ליניארי דיסקרטי: $\underline{l}_i \in \Lambda,\ \underline{l}_j \in \Lambda \Rightarrow \underline{l}_i + \underline{l}_j \in \Lambda$, וכולל תמיד את האפס $\underline{l}_0 = \underline{0}$.

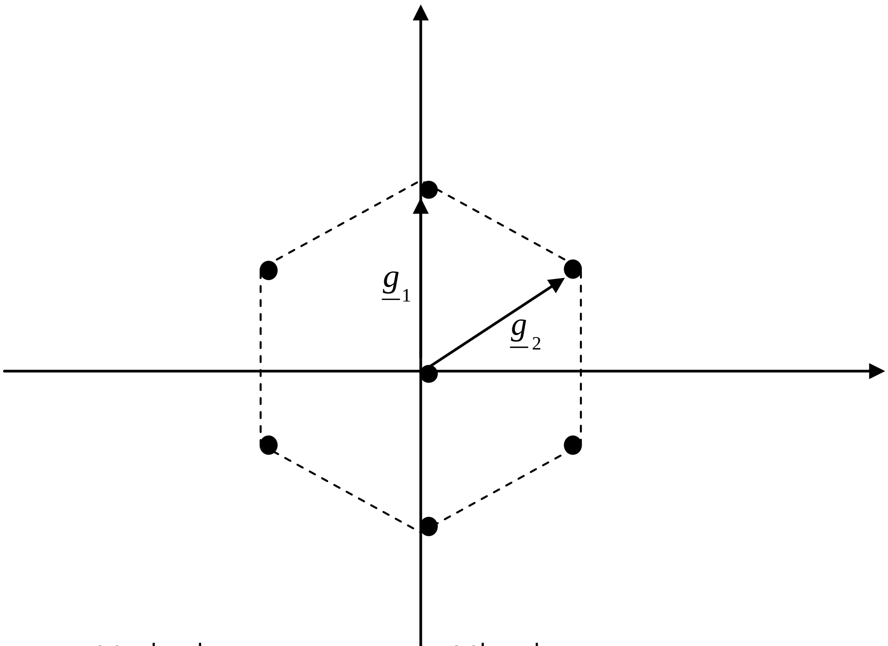
<u>דוגמאות:</u>

1. סריג השלמים $\underline{\underline{G}} = \underline{\underline{I}}_n \Leftarrow \Lambda = Z^n$, מתקבל Cubic lattice. סריג שקול לסריג השלמים הוא הסריג $\Lambda = \{0, \pm\Delta, \pm 2\Delta \ldots\}$.

2. סריג המשושה עבור n=2:

$$G=\begin{pmatrix}0 & \sqrt{3}\\ 2 & 1\end{pmatrix}$$

נתבונן בחלק מהסריג (רק הנקודות הקרובות ביותר לראשית):

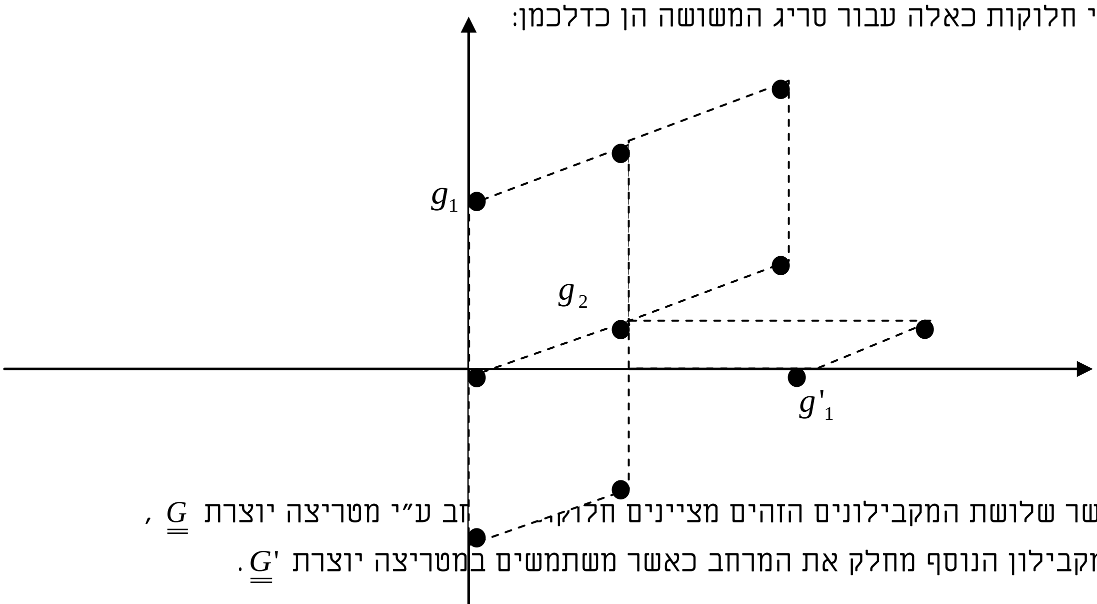


עבור כל סריג, ישנם אינסוף ייצוגים שקולים למטריצה היוצרת – כפל של המטריצה היוצרת במטריצת מספרים שלמים בעלת דטרמיננטה ± 1 , $\underline{\underline{G}}'=\underline{\underline{G}}\cdot\underline{\underline{J}}$ נותנת את אותו הסריג. למשל

$$\underline{\underline{G}}'=\begin{pmatrix}0 & \sqrt{3}\\ 2 & 1\end{pmatrix}\cdot\begin{pmatrix}-1 & 0\\ 2 & 1\end{pmatrix}=\begin{pmatrix}2\cdot\sqrt{3} & \sqrt{3}\\ 0 & 1\end{pmatrix}$$

חלוקה סריגית של המרחב:

ניתן לחלק את המרחב R^n ע״י מקבילונים שצלעותיהם הם עמודות (וקטורי הבסיס) של המטריצה היוצרת. קיימות אינסוף חלוקות כאלה בהתאם למטריצה היוצרת איתה עובדים. שתי חלוקות כאלה עבור סריג המשושה הן כדלכמן:



כאשר שלושת המקבילונים הזהים מציינים חלוקת המרחב ע״י מטריצה יוצרת $\underline{\underline{G}}$, והמקבילון הנוסף מחלק את המרחב כאשר משתמשים במטריצה יוצרת $\underline{\underline{G}}'$.

הגדרה: חלוקה סריגית (lattice partition) של המרחב $p_i = p_0 + \underline{l}_i \overset{\Delta}{=} \left\{ \underline{x} + \underline{l}_i \;:\; \underline{x} \in p_0 \right\}$, כך ש p_0 היא כל

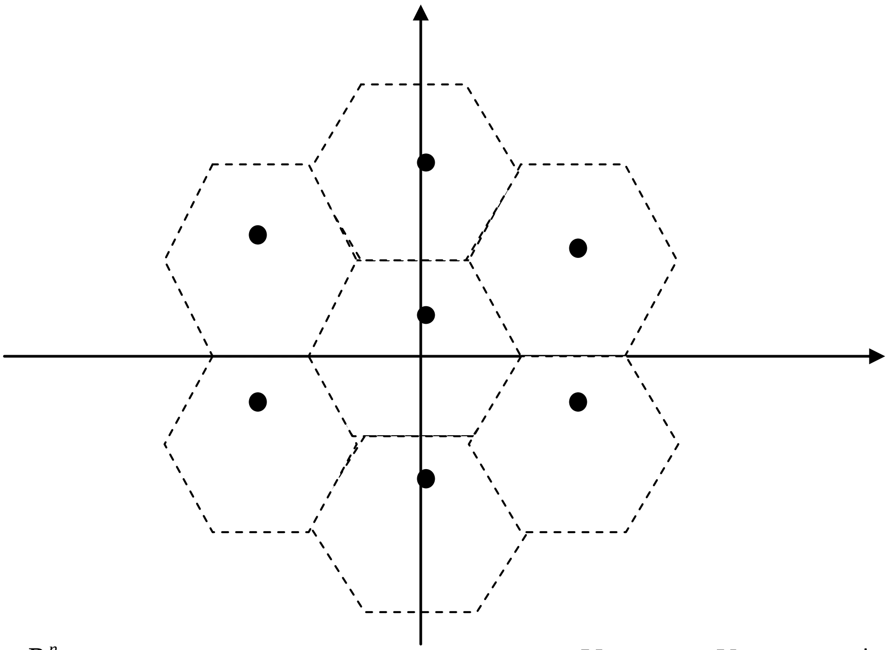
צורה המאפשרת ריצוף מושלם של R^n (ללא חפיפות ו $\bigcup_{i=-\infty}^{\infty} p_i = R^n$). צורה כזאת נקראת
"space filling polytop".

חלוקה למקבילונים התחומים ע"י עמודות המטריצה היוצרת $\underline{g}_1, \underline{g}_2, ..., \underline{g}_n$ נותנת p_0 מהצורה $\left\{ \underline{x} = \sum_{i=1}^{n} \alpha_i \underline{g}_i \;:\; 0 \le \alpha_i \le 1 \right\}$.

נפח המקבילון (וכל חלוקה סריגית אחרת) זהה בכל חלוקה אפשרית ושווה לערך המוחלט של דטרמיננט המטריצה היוצרת $Vol(p_0) = Vol(p_i) = Const = \det(\underline{\underline{G}})$.

אוסף הנקודות הקרובות לנקודת האפס יותר מכל נקודת סריג אחרת נקרא **<u>תא וורונוי</u>**. תא וורונוי הוא "space filling polytop" . חלוקת וורונוי ניתנת לביטוי באופן $\|\underline{l}_i - \underline{x}\| \le \|\underline{l}_j - \underline{x}\| \Rightarrow \underline{x} \in p_i$ עבור כל j.

למשל, עבור סריג המשושה חלוקת וורונוי נראית באופן הבא:



מסמנים חלוקה זו ב- V_i, כאשר V_0 הוא תא וורונוי בסיסי – אוסף הנקודות ב R^n הקרובות לראשית יותר מכל נקודת סריג אחרת.

חלוקת וורונוי היא החלוקה היעילה ביותר, ובעזרתה מגדירים:

1. קוונטייזר סריג (ביחס למרחק אוקלידי):
$Q_\Lambda(\underline{x}) = \underline{l}_i$ אם לכל $i \ne j$,$\underline{l}_i, \underline{l}_j \in \Lambda$ מתקיים $\|\underline{x} - \underline{l}_i\| \le \|\underline{x} - \underline{l}_j\|$.
2. תא וורונוי של $\underline{l}_i$ - $V_i = \left\{ \underline{x} \;:\; Q(\underline{x}) = \underline{l}_i \right\}$.
3. נפח הסריג $V \overset{\Delta}{=} \left|\det(\underline{\underline{G}})\right| = Vol(\text{מקבילון}) = Vol(V_0)$.
4. מומנט שני (פר מימד) $\sigma^2 = \frac{1}{n} \cdot \frac{1}{V} \cdot \oint_{\underline{x} \in V_0} \|\underline{x}\|^2 d\underline{x}$.

ניתן להגדיר את המומנט השני גם כ- $\sigma^2 = \frac{1}{n}\cdot E\|\underline{z}\|^2$ כאשר $\underline{z}$ מתפלג אחיד על פני V_0:

$f_{\underline{z}}(\underline{z}) = \left\{\begin{matrix} \frac{1}{V}, & \underline{z}\in V_0 \\ 0, & o.w \end{matrix}\right\}$.

5. רדיוס חוסם וחסום:
רדיוס חוסם R_{out} הוא רדיוס הכדור המינימלי המכיל את V_0.
רדיוס חסום R_{in} הוא רדיוס הכדור המקסימלי המוכל בתוך V_0.

6. קל לראות ש- $\frac{1}{n}\cdot R_{in}^2 \le \sigma^2 \le \frac{1}{n}\cdot R_{out}^2$.

ראוי לציין כי קיימות שיטות פענוח תת אופטימליות השקולות לחלוקות סריגיות שאינן תאי וורונוי.

<u>גורמי טיב לקידוד</u>

1. <u>לקוונטיזציה:</u> מומנט שני מנורמל $G(\Lambda)\overset{\Delta}{=}\frac{\sigma^2}{V^{2/n}}$. זהו גודל חסר יחידות שאינווריאנטי למתיחה,
סיבוב, שיקוף.

נגדיר $G_n \overset{\Delta}{=} \inf_{\Lambda} G(\Lambda)$ כמומנט השני המנורמל המינימלי הניתן להשגה ב R^n .

המוטיבציה להגדרה זו היא
שעבור מקור המתפלג "אחיד במרחב" על פני נפח>>V, ו- V מוחזק קבוע (שקול לקצב קבוע), העיוות המתקבל
כתוצאה מהקוונטיזציה שווה בקירוב ל $\sigma^2 = V^{2/n}G(\Lambda)$, לכן מעוניינים ב $G(\Lambda)$ קטן.
<u>אי-שיוויון איזו-פרימטרי:</u> מבין כל הצורות במרחב עם נפח נתון, המומנט השני הכי קטן הוא של כדור.

$$G(\Lambda) \ge G_n^* = G(n-\dim.\quad Ball) = \frac{\frac{1}{n}\cdot\frac{1}{V_{Ball}}\cdot\oint_{\underline{x}\in Ball}\|\underline{x}\|^2 d\underline{x}}{V_{Ball}^{2/n}}$$

<u>דוגמאות:</u>

$$G_1 = G(Z) = \frac{1}{12}$$

עבור סריג המשושה הוכח בשנות ה- 80:

$$G_2 = G(hexa-lattice) = \frac{5}{36\cdot\sqrt{3}} \approx \frac{1}{12.5}$$

תמיד מתקיים $G_n, G_n^* > \frac{1}{2\pi e}$.

משפט (סריגי קוונטיזציה טובים אסימפטוטית):

$G_n, G_n^* \underset{n\to\infty}{\to} \frac{1}{2\pi e} \approx \frac{1}{17}$ $\Leftarrow$ במובן קוונטיזדציה תאי וורונוי של סריגים אופטימליים שואפים
לכדורים.

2. **לקידוד ערוץ AWGN:**

$$y = x + N \ , \ N \ is \ N(0,\sigma^2) \ distributed$$

אם $\underline{x}$ שייך לסריג לא מוגבל (ללא שפה) אזי:

$$\hat{\underline{x}}_{M.L} = \arg\max_{\underline{x}\in\Lambda} P(\underline{y}/\underline{x}) \overset{\Delta}{=} \arg\min_{\underline{x}\in\Lambda} \left\|\underline{y}-\underline{x}\right\|$$

שזה שקול לפעולת הקוונטייזר: $\hat{\underline{x}}_{M.L} = Q_\Lambda(\underline{x})$

הסתברות השגיאה לפענוח זה היא:

$$P_e = \Pr(\underline{N} \notin V_0) = \oint_{\underline{x}\notin V_0} \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^n \cdot \exp\left(-\frac{\left\|\underline{x}\right\|^2}{2\sigma^2}\right)$$

שולי רעש (noise margin) של סריג Λ מוגדרים באופן:

$$\mu(\Lambda, P_e) \overset{\Delta}{=} \left.\frac{V^{2/n}}{\sigma^2}\right|_{@\Pr(\underline{N}\notin V_0)=P_e}$$

ברור שעל מנת להשיג $P_e \to 0$ נדרש $\mu(\Lambda, P_e) \to \infty$.

נגדיר את החסם התחתון (עבור מימד ספציפי n) של $\mu(\Lambda, P_e)$ הנדרש להשגת P_e כלשהוא:

$$\mu_n(P_e) \overset{\Delta}{=} \inf_{\Lambda} \mu(\Lambda, P_e)$$

מגדירים: $\mu_n^*(P_e) \overset{\Delta}{=} \mu(n-\dim. \quad Ball)$

מתקיים: $\mu_n^*(P_e) < \mu_n(P_e)$

משפט (סריגים טובים לערוץ AWGN):

עבור כל $P_e > 0$, $\mu_n(P_e), \mu_n^*(P_e) \underset{n\to\infty}{\to} 2\pi e$.

$$\Leftarrow \quad \frac{1}{n}\log(V) = \frac{1}{2}\log(\mu\cdot\sigma^2) \underset{n\to\infty}{\to} \frac{1}{2}\log(2\pi e\sigma^2) = h(N(0,\sigma^2))$$

קצב השידור שווה בקירוב ל- $R = \frac{1}{n}\log\left(\frac{constellation \ volume}{V}\right) \Leftarrow$ סריגים טובים

במובן הנ"ל מבטיחים קצב שידור מקסימלי:

$$R = constant(transmitted \ \ power) - \frac{1}{n}\log(V) \underset{n\to\infty}{\to} constant - h(N) = C$$

סריגים מקוננים

__הגדרה:__ סריגים Λ_1, Λ_2 הם סריגים מקוננים אם מתקיים $\Lambda_2 \subset \Lambda_1 \Leftrightarrow \underline{\underline{G}}_2 = \underline{\underline{G}}_1 \cdot \underline{\underline{J}}$, כאשר $\underline{\underline{J}}$ מטריצה של שלמים.

קבוצת הוקטורים המובילים את הקוסטים היחסיים של Λ_1 ביחס ל- Λ_2 מוגדרת באופן:

$\Lambda_1 \mod \Lambda_2 \overset{\Delta}{=} \left\{\underline{l} \mod \Lambda_2 : \underline{l} \in \Lambda_1\right\} \in V_2$, כאשר V_2 הוא תא הוורונוי של סריג Λ_2 .

פעולת "מודולו סריג" מוגדרת באופן: $\underline{x} \mod \Lambda \overset{\Delta}{=} \underline{x} - Q(\underline{x}) \in V_0$.

קוסט מוגדר כאוסף הנקודות של Λ_1 הנמצאות באותו מיקום יחסית ל- Λ_2 :

$\cos et(\underline{v}) \overset{\Delta}{=} \left\{\underline{l} \in \Lambda_1 : \underline{l} \mod \Lambda_2 = \underline{v}\right\}$, כאשר $\underline{v} \in \Lambda_1 \mod \Lambda_2$.

סריגים מקוננים טובים אסימפטוטית

אם Λ_2 הוא סריג קוונטיזציה עם מומנט שני σ_2^2, ($V_2^{2/n} = \sigma_2^2 / G(\Lambda_2)$) Λ_2 ייקרא "סריג גס") ו- Λ_1 הוא סריג לקידוד ערוץ AWGN עם שונות רעש σ_1^2 ושולי רעש $\mu(\Lambda_1, P_e)$, ($V_1^{2/n} = \mu(\Lambda_1, P_e) \cdot \sigma_1^2$) Λ_1 ייקרא "סריג עדין") אזי מתקיים ש:

$$R \overset{\Delta}{=} \frac{1}{n} \log \left| \Lambda_1 \mod \Lambda_2 \right| = \frac{1}{n} \log \left(\frac{V_2}{V_1} \right) = \frac{1}{2} \log \left(\frac{\sigma_2^2}{\sigma_1^2} \right) - \frac{1}{2} \log \left(G(\Lambda_2) \cdot \mu(\Lambda_1, P_e) \right)$$

כאשר הגודל $-\frac{1}{2} \log \left(G(\Lambda_2) \cdot \mu(\Lambda_1, P_e) \right)$ הוא "הפסד הקיבול".

<u>טענה:</u> עבור כל $P_e>0$, קיימים זוגות $\Lambda_1 \subset \Lambda_2$ כך ש- $\log \left(G(\Lambda_2) \cdot \mu(\Lambda_1, P_e) \right) \underset{n \to \infty}{\to} 0$.

קיימת גם טענה למקרה ההפוך של דחיסת אות, כלומר Λ_2 סריג לקידוד ערוץ AWGN ו- Λ_1 סריג לקוונטיזציה – במקרה הזה איבר ההפסד עם סימן חיובי ולכן מציין הפסד דחיסה.
מטענה זו נובע כי עבור כל קצב הקטן מהקיבול (או קצב הגדול מאנטרופיית המקור במקרה של קידוד מקור), ניתן למצוא צמדי סריגים (סריג קוונטיזציה וסריג לערוץ AWGN) כך שנקבל הסתברות שגיאה קטנה כרצוננו.

<u>**ביבליוגרפיה:**</u>

1. M.H.M. Costa. "Writing on dirty paper". IEEE Trans. Information Theory, IT-29:439-441, May 1983.

2. J.H. Conway and N.J.A. Sloane. "Sphere Packings, Lattices and Groups". Springer-Verlag, New York, N.Y., 1988.

3. R.Zamir, S.Shamai and U.Erez, "Nested Linear/Lattice Codes for Structured Multiterminal Binning", IEEE Transactions on Information Theory, pp. 1250-1276, June 2002.

הרצאה - 5

בעיית קידוד מקור עם אינפורמציית-צד למקרה הגאוסי

(Gaussian Wyner-Ziv)

סוכם ע"י אנטולי חינה

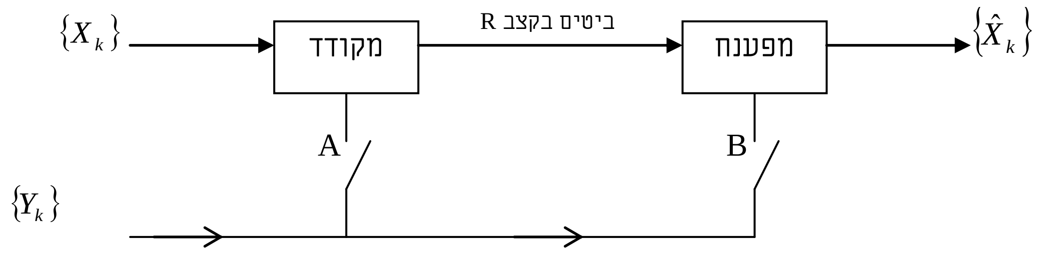
הגדרת הבעיה:

נניח $\{(X_k, Y_k)\}_{k=1}^{\infty}$ סדרה של הגרלות בת"ס של משתנים גאוסיים במשותף קורלטיביים X, Y.

נגדיר מדד עיוות ריבועי: $d(\underline{x}, \underline{y}) = \frac{1}{n}\sum_{k=1}^{n}(x_k - y_k)^2$.

המטרה היא למצוא את הקצב המינימלי R בו ניתן לקודד את X כך ש: $E(X-\hat{X})^2 \le D$ עבור D נתון.

נתבונן בשלושה מקרים:



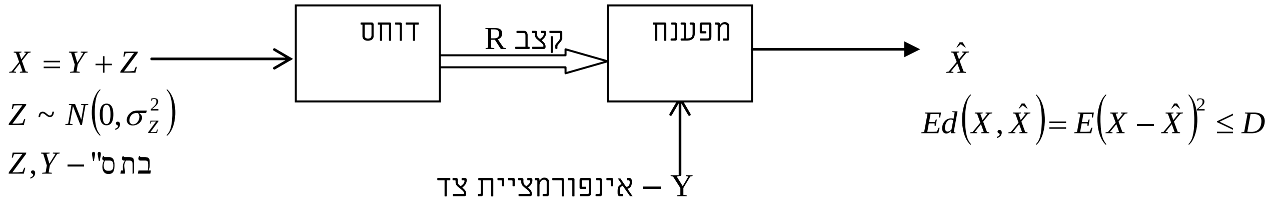
1. מפסקים A,B פתוחים. כלומר אין אינפורמציית-צד "זמינה".
הפיתרון במקרה זה הוא הפיתרון הרגיל מתורת שנון: $\boldsymbol{R_X(D) = \min_{p(X,Y,\hat{X}):\, Ed(X,\hat{X}) \le D} I(X;\hat{X})}$.

2. מפסקים A,B סגורים. כלומר הן המקודד והן המפענח בעלי גישה לאינפורמציית-הצד $\{Y_n\}$.
הפיתרון עבור מקרה זה יהיה: $\boldsymbol{R_{X|Y}(D) = \min_{p(X,Y,\hat{X}):\, Ed(X,\hat{X}) \le D} I(X;\hat{X}\,|\,Y)}$.

3. A פתוח, B סגור. כלומר רק למפענח יש גישה לאינפורמציית-הצד.
נסמן את הפיתרון עבור מקרה זה ב-$R^*(D) \equiv R_{X|Y}^{WZ}(D)$.

אנו נתמקד במקרה השלישי (שני המקרים הראשונים טריויאליים).

היות ואנו מסתכלים על המקרה הגאוסי, נתמקד בסכימה הבאה:



נשים לב כי סכימה זו תקפה עבור כל מקרה של (X,Y) גאוסיים במשותף. היות ונוכל להמיר מקרה זה תמיד לבעיית WZ שקולה שבה: $X = \tilde{Y} + \tilde{Z}$.
לשם פשטות נסתכל על המקרה שבו כל התוחלות הן אפס (אחרת בסכימת השידור נוכל להחסיר ולהוסיף את התוחלות המתאימות...).
עבור מקרה זה ידוע כי שיערוך אופטימלי במובן MMSE (אשר במקרה הגאוסי מזדהה עם שיערוך אופטימלי במובן LMMSE) של X מתוך Y הינו: $\alpha = \frac{\sigma_{XY}}{\sigma_Y^2}$ $\qquad \tilde{Y} \triangleq \hat{X}(Y) = \alpha Y,$
.
ומעיקרון האורתוגונליות מתקיים: $Z \triangleq X - \hat{X} = X - \tilde{Y} \perp \tilde{Y}$, והיות וכל המ"א גאוסיים במשותף ובעלי תוחלת אפס, מתקיים כי $Z, \tilde{Y}$ בת"ס וכן ש:
$\sigma_Z^2 = E\left(X - \hat{X}\right)^2 = E\left\{\mathrm{Var}\left(X \mid \tilde{Y}\right)\right\}$. וקיבלנו את הדרוש.

נראה כיצד ניתן להרוויח את ה-Shaping Gain בבעיה זו.

משפט Wyner-Ziv (1976, 1978):

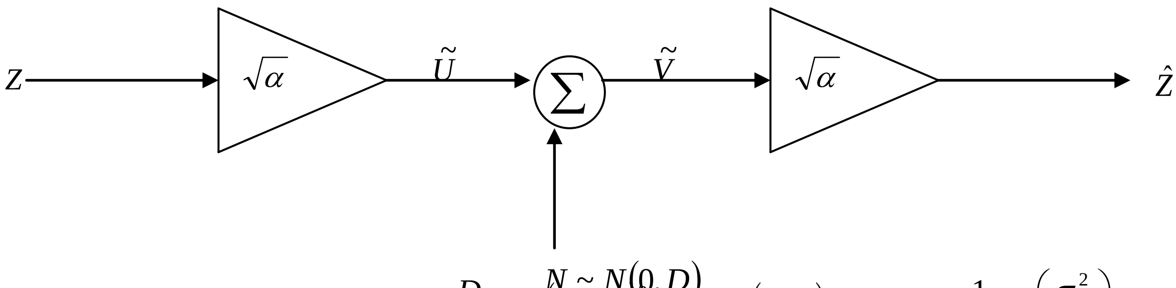
$$R^*(D) \equiv R_X^{WZ}(D) = R_{X|Y}(D) = R_Z(D) = \frac{1}{2}\log\left(\frac{\sigma_Z^2}{D}\right)$$

(הוכיחו משיקולי אינפורמצייה בעזרת random binning).

נראה כי ניתן להגיע למה שמבטיחים WZ ע"י שריגים מקוננים (Nested Lattices).

פתרון ע"י שריגים מקוננים:

הערוץ (הקידמי) המגשים לפונקציית קצב-עיוות של $Z \sim N\left(0, \sigma_Z^2\right)$:



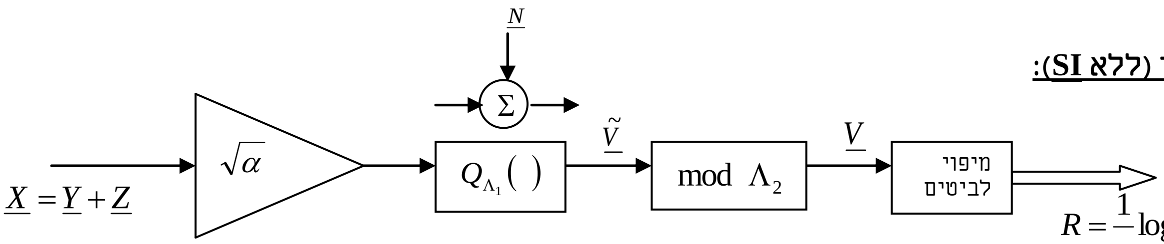
כאשר: $\alpha = \alpha_{opt} = 1 - \frac{D}{\sigma_Z^2}, \quad E\left(Z - \hat{Z}\right)^2 = D, \quad I\left(Z; \hat{Z}\right) = R_Z(D) = \frac{1}{2}\log\left(\frac{\sigma_Z^2}{D}\right)$

($0 \le D \le \sigma_Z^2$ אחרת אין טעם לדחוס)

נשים לב גם כי מתכונות האינפורמציה ההדדית: $I\left(Z; \hat{Z}\right) = I\left(\tilde{U}; \tilde{V}\right) = I\left(\tilde{U}; \tilde{U} + N\right)$
(היות והכפלה בקבוע שונה מאפס אינה משפיעה על אינפורמציה הדדית)

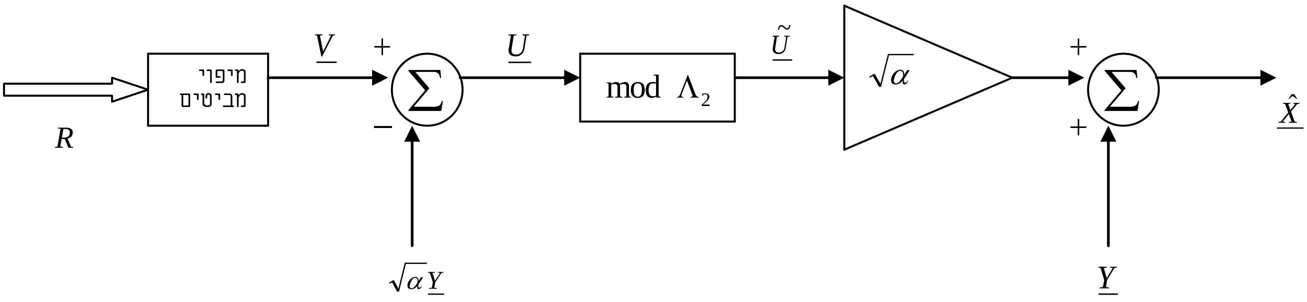
נבנה דיאגרמה שמתבססת על הערוץ הנ"ל בשילוב עם שריגים מקוננים, ונראה כי אנו משיגים את $R_Z(D)$ בהשאפת מימד השריג לאינסוף ($n \to \infty$).

המקודד (ללא SI):



$$R = \frac{1}{n}\log\left(\frac{V_2}{V_1}\right)\left[\frac{bits}{sample}\right]$$

המפענח (עם SI):



לפי משפט, שריגי קוונטיזציה "טובים אסימפטוטית" ושואפים לכדורים עם נפח זהה לתאי הוורונוי של השריגים. יתר על כן, פילוג אחיד ע"פ כדור ⇔ רעש גאוסי i.i.d. ועל כן אסימפטוטית Q_{Λ_1} בעצם מבצע פעולה השקולה לתוספת רעש $\underline{N}$ אשר אסימפטוטית הינו רעש גאוסי "לבן".

נבחר את השריג Λ_1 ("השריג העדין") כך שיהיה שריג קוונטיזציה טוב לעיוות $\sigma_1^2 = D$.

כלומר, הרעש האפקטיבי $\underline{N}$ מתפלג לפי: $\underline{N} \sim N(0, D \cdot I_n)$ (כאשר $n \to \infty$).

על מוצא הקוונטייזר נבצע פעולת מודולו Λ_2 (כאשר $\Lambda_2 \subset \Lambda_1 \Leftrightarrow G_2 = G_1 J$, J – מטריצת שלמים. כלומר אנו מדברים על "שריגים מקוננים"). פעולה זו בעצם אומרת כי אנו "עובדים" בתוך התא של השריג הגס, כאשר מתוך אינפורמציית הצד נדע במפענח באיזה תא של השריג הגס אנו נמצאים.

ממשפט, "שריגים טובים לקידוד ערוץ AWGN", ידוע כי עבור כניסה גאוסית (וכאמור קודם, מוצא הקוונטייזר $Q_{\Lambda 1}$ הינו אסימפטוטית גאוסי) שימוש בשריג בתור ספר קוד אסימפטוטית שקול לתוספת רעש גאוסי לבן עם שונות σ_2^2: $\frac{1}{n}\log(V_2) = \frac{1}{2}\log\left(\mu_n {\sigma_2}^2\right)$

(כאשר μ_n הינו "שולי הרעש").

אנו נבחר $\sigma_2^2 = \sigma_Z^2$.

עבור שריגים מקוננים (טובים) ידוע כי, אם Λ_2 הוא שריג לקידוד ערוץ AWGN ("גס") עם מומנט שני σ_2^2 $\left(V_2^{\frac{2}{n}} = \mu_n \sigma_2^2\right)$ וְ-Λ_1 הוא שריג קוונטיזציה ("עדין") עם שונות רעש σ_1^2 ושולי רעש $\mu(\Lambda_1, P_e)$ $\left(V_1^{\frac{2}{n}} = \frac{\sigma_1^2}{G_n(\Lambda_1)}\right)$, אזי:

$$R \triangleq \frac{1}{n}\log\left(\frac{V_2}{V_1}\right) = \frac{1}{2}\log\left(\frac{\sigma_2^2}{\sigma_1^2}\right) + \frac{1}{n}\log(G_n \mu_n).$$

כאשר: $G_n \triangleq \inf_{\Lambda} G(\Lambda)$ הינו המומנט השני המנורמל המינימלי בר-ההשגה ע"י שריג ב-$\Re^n$;
$\mu_n \triangleq \inf_{\Lambda} \mu(\Lambda, P_e)$ הינו שולי הרעש האופטימליים ברי-ההשגה ע"י שריג ב-$\Re^n$ עבור הסתברות שגיאה P_e.[4]

האיבר $\frac{1}{n}\log(G_n\mu_n)$ הינו בעצם הפסד קצב דחיסה, כאשר לפי משפט: $\mu_n > 2\pi e$, $G_n > \frac{1}{2\pi e}$

. אך בגבול ($n \to \infty$): $\mu_n \to 2\pi e$, $G_n \to \frac{1}{2\pi e}$, ולכן: $\frac{1}{n}\log(G_n\mu_n) \to 0$ (לכל הסתברות שגיאה, קטנה כרצונינו $P_e > 0$).

מכאן שבגבול מתקיים: $R \triangleq \frac{1}{n}\log\left(\frac{V_2}{V_1}\right) = \frac{1}{2}\log\left(\frac{\sigma_2^2}{\sigma_1^2}\right) - \frac{1}{n}\log(G_n\mu_n) \to \frac{1}{2}\log\left(\frac{\sigma_2^2}{\sigma_1^2}\right)$,[5]

כך שבעצם משיגים אסימפטוטית את מה שמבטיחים WZ ע"י הסכימה שהצגנו מבחינת קצב.

נסתכל עתה מה מתקבל בכל שלב בסכימה (ונראה שהעיוות הממוצע $\frac{1}{n}\sum_{k=1}^{n} E\left(X_k - \hat{X}_k\right)^2$ אכן שווה ל-D).

לאחר הכפלה ב-$\sqrt{\alpha}$ וקוונטיזציה (אשר כאמור שקולה לתוספת רעש גאוסי לבן במקרה זה), נקבל:

$$\underline{\tilde{V}} = \left(\sqrt{\alpha}\,\underline{Y} + \sqrt{\alpha}\,\underline{Z} + \underline{N}\right).$$

נשים לב כי שונות החלק ה"מעניין" הינה: $Var\left(\sqrt{\alpha}\,\underline{Z} + \underline{N}\right) = \alpha\sigma_Z^2 + D = \left(1 - \frac{D}{\sigma_Z^2}\right)\sigma_Z^2 + D = \sigma_Z^2$

(N ו-Z רעשים בת"ס).

לאחר מודולו השריג הגס, נקבל: $\underline{V} = \left(\sqrt{\alpha}\,\underline{Y} + \sqrt{\alpha}\,\underline{Z} + \underline{N}\right) \bmod \Lambda_2$. וזה גם האות שנמפה לביטים ונשלח למפענח.

במפענח אנו מבצעים החסרת מודולו של החלק ה"לא מעניין" ולפי חוקי מודולו[6]:

$$\underline{\tilde{U}} = \left[\left(\sqrt{\alpha}\,\underline{Y} + \sqrt{\alpha}\,\underline{Z} + \underline{N}\right) \bmod \Lambda_2 - \sqrt{\alpha}\,\underline{Y}\right] \bmod \Lambda_2 = \left[\sqrt{\alpha}\,\underline{Y} + \sqrt{\alpha}\,\underline{Z} + \underline{N} - \sqrt{\alpha}\,\underline{Y}\right] \bmod \Lambda_2 = \left[\sqrt{\alpha}\,\underline{Z} + \underline{N}\right] \bmod \Lambda_2$$

אך כבר ראינו כי שונות $\sqrt{\alpha}\,\underline{Z} + \underline{N}$ הינה σ_Z^2 וכן קבענו את השריג הגס Λ_2 להיות שריג טוב לקידוד ערוץ AWGN עם מומנט שני $\sigma_Z^2 = \sigma_2^2$. ניזכר כי תא וורונוי של שריג (טוב לקידוד ערוץ AWGN) שואף לכדור n-מימדי עם רדיוס $\sqrt{n\sigma^2}$ וכן רעש גאוסי שואף לפילוג אחיד בתוך כדור n-מימדי עם רדיוס $\sqrt{n\sigma^2}$ (הן במובן a.e. והן במובן m.s.). ולכן בגבול, פעולת המודולו לא תשפיע על $\sqrt{\alpha}\,\underline{Z} + \underline{N}$, ולכן: $\underline{\tilde{U}} = \left[\sqrt{\alpha}\,\underline{Z} + \underline{N}\right] \bmod \Lambda_2 \overset{n\to\infty}{=} \sqrt{\alpha}\,\underline{Z} + \underline{N}$.

לאחר הכפלה (נוספת) ב-$\sqrt{\alpha}$ והוספת מידע הצד $\underline{Y}$ נקבל (בגבול $n \to \infty$):

$$\underline{\hat{X}} = \underline{Y} + \alpha\underline{Z} + \sqrt{a}\,\underline{N} = \underline{Y} + \underline{\hat{Z}}$$

וקיבלנו את אותה השר"מ כמו בערוץ (הקידמי) המגשים לפונקציית קצב-עיוות של $Z \sim N\left(0, \sigma_Z^2\right)$ (שאותו גם ניסינו בעצם לממש) <= $E\left(X - \hat{X}\right)^2 = E\left(Z - \hat{Z}\right)^2 = D$.

---

[4] כפי שהוגדר והוסבר בפרק "סריגים ושימושם במערכות תקשורת".

[5] לפי משפט: קיימים זוגות $\Lambda_2 \subset \Lambda_1$ כך ש: $\frac{1}{n}\log(G_n\mu_n) \to 0$

[6] $[(A \bmod C) \pm B] \bmod C = [A \pm B] \bmod C$

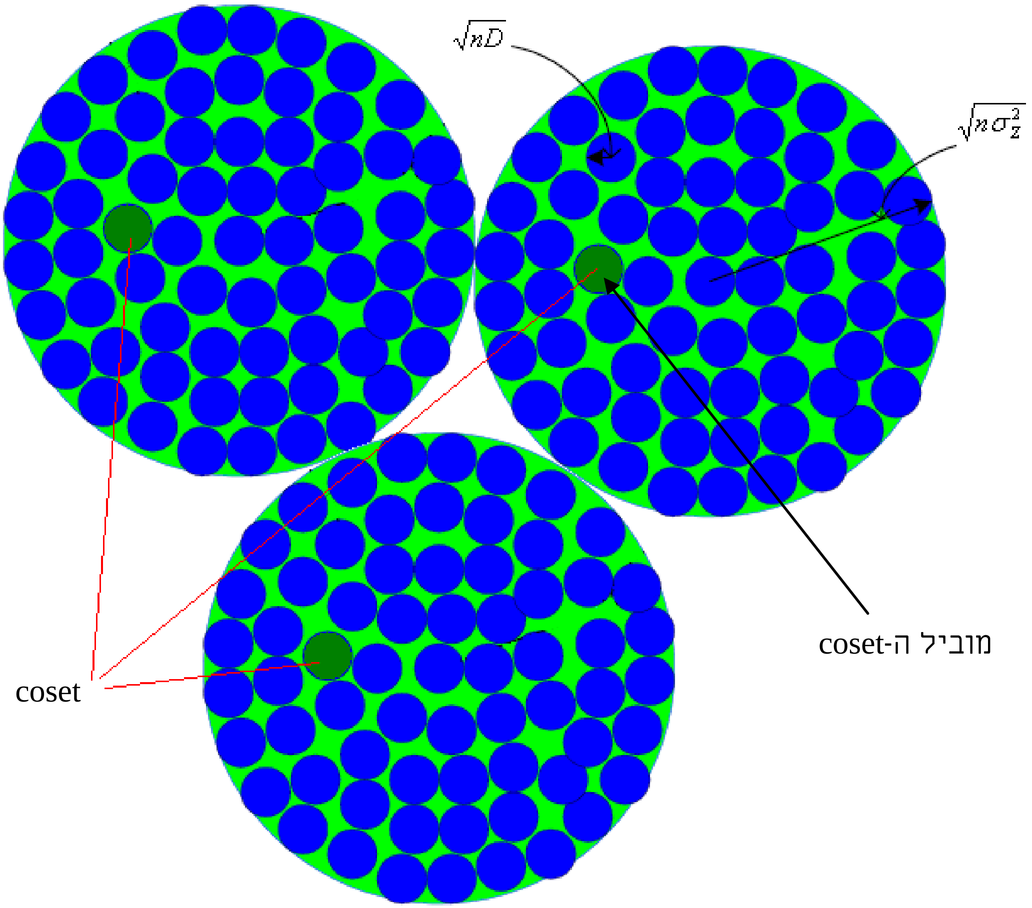
כלומר הצלחנו להעביר בקצב $R \hat{=} \frac{1}{2}\log\left(\frac{\sigma_2^2}{\sigma_1^2}\right)$ ולשמור על עיוות שלא עולה על D. ובעצם השגנו (אסימפטוטית) את מה שמבטיחים WZ.

הסבר אינטואיטיבי וגרפי לגבי בחירת השריגים:

בחרנו את השריג הגס בתוך שריג לקידוד ערוץ AWGN, היות ו"לא נרשה" חפיפה/בילבול בין התאים של שריג זה. כי במקרה כזה תהיה טעות גדולה...
לעומת זאת, השריג העדין קובע לנו את העיוות, ולכן למשל "חפיפה" בין תאים עדינים לא תגדיל את העיוות אך תגרור כמובן הפסד בקצב...
בפועל אנו משדרים את האינדקס של מוביל ה-coset, כאשר מידע הצד Y קובע את האיבר המדוייק
בתוך ה-coset. לשם שידור האינדקס דרושים $\left[bits\right]$ $\log\left(\frac{V_2}{V_1}\right) \overset{n\to\infty}{=} \frac{n}{2}\log\left(\frac{\sigma_Z^2}{D}\right)$ ולכן הקצב פֵּר מימד הינו:

$$\frac{1}{n}\log\left(\frac{V_2}{V_1}\right) \overset{n\to\infty}{=} \frac{1}{2}\log\left(\frac{\sigma_Z^2}{D}\right)\left[bits\right].$$

נוכל לחשוב על השריגים המקוננים גרפית בצורה הבאה:



<u>הערות:</u>

1. בשרטוט הכל משורטט בדו-מימד, אך בפועל אנו עובדים כמובן ב-$n \to \infty$. לכן גם המרווחים בין הכדורים לא קיימים במציאות...

2. השרטוט הנ"ל מתייחס לתמונה שאחרי ה-Pre Filter ולפני ה-Post Filter (כלומר לאחר ההכפלה הראשונה ב- $\sqrt{\alpha}$ - במשדר, ולפני ההכפלה השנייה ב- $\sqrt{\alpha}$ - במקלט).

דואליות:

בעיית WZ הגאוסית הינה הבעייה הדואלית לבעיית Costa, אשר הוצגה בפרק "קידוד ערוץ גאוסי עם אינפורמצית צד". בפרק המדובר, היה הפסד Shaping gain ממנו ניתן להיפטר בצורה זהה כמעט לזו שהוצגה בפרק זה.
בבעיה הדואלית, המשדר והמקלט "מחליפים תפקידים" ובשריגים המקוננים השריג העדין הינו שריג טוב לקידוד ערוץ AWGN, בעוד שהערוץ הגס הינו ערוץ טוב לקוונטיזצייה (בדיוק הפוך מבעיית WZ).
וזאת היות ושם לא נרשה חפיפה/בילבול בין מילים/תאים של השריג העדין (אחרת נשגה בפיענוח).
לעומת זאת, השריג הגס קובע לנו את ה-coset, כאשר אם מילה אחת תשוייך ליותר מ-S אחד, זה ייצור יתירות בקצב (אם נסתכל על האינפורמצייה ההדדית היא תגדל עקב החפיפה)...

קריאה נוספת:

[1] A. D. Wyner, J. Ziv, "The Rate-Distortion Function for Source Coding with Side-Information at the Decoder", *IEEE Trans. Inform. Theory*, vol. 22, pp. 1-10, Jan. 1976.
[2] A. D. Wyner, " The Rate-Distortion Function for Source Coding with Side Information at the Decoder II: General Sources", *Information and Control*, vol. 38, pp. 60-80, July 1976
[3] R. Zamir, S. Shamai, U. Erez, "Nested Linear/Lattice Codes for Structured Multiterminal Binning", *IEEE Trans. Inform. Theory*, special A.D. Wyner issue, pp. 1250-1276, June 2002.
[4] S.S. Pradhan, K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction", *IEEE Trans. Inform. Theory*, vol. 49, pp. 626-643, March 2003.
[5] S.S. Pradhan, K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction", *IEEE DCC '99* , pp. 158-167, 29-31 March 1999.

הרצאה - 6

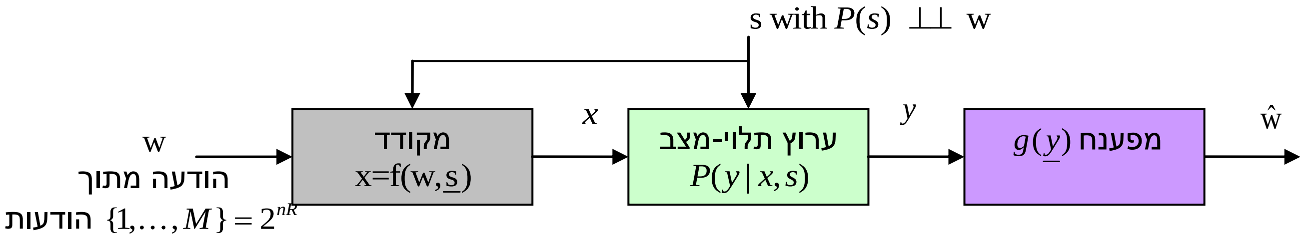
בעית גלפנד-פינסקר (Gel'fand-Pinsker)

קידוד עם אינפורמצית צד (לא סיבתית) במשדר

סוכם ע"י אורי שנטל

הגדרת הבעיה

נתון ערוץ כללי תלוי-מצב מהצורה (איור 1)



איור 1

אינפורמציית הצד (**S**ide **I**nformation) s מקורה "מהטבע" ואינה תלויה בהודעות w. נניח שאינפורמציית הצד המסופקת למקודד (המשדר) אינה סיבתית. כמו כן נניח שכל המידע בבלוק השידור ידוע למקודד . בנוסף ניתן (אופציונלי) לאלץ פונקצית מחיר לכניסה , $E\rho(x)\le c$.

נשתמש בסימונים הבאים:

- n = אורך בלוק השידור
- R = קצב השידור (ביט לשימוש ערוץ)
- $f(\cdot)$ = פונקצית המקודד
- $g(\cdot)$ = פונקצית המפענח
- P_e = הסתברות השגיאה ($\Pr(\hat{w}\neq w)$)
- $C_{SI@Tx} = func(P(y|x,s),P(s),(\rho(\cdot),c))$ = הקצב R המקסימאלי (במובן סופרמום) כך שלכל $P_e>0$ קיימת מערכת של $(u,R,f(\cdot),g(\cdot))$ הנותנת הסתברות שגיאה כזו.

רקע היסטורי

בעית גלפנד-פינסקר (להלן GP) הוצגה לראשונה ב-1980 [1] ומתבססת למעשה על בעיה שטופלה במקור ע"י שאנון עוד בשנת 1958 [2]. שאנון פתר את בעית הערוץ עם אינפורמציית צד **סיבתית**, דהיינו $i=0,1,\cdots,n$ $x_i = func(w,s_1,\dots,s_i)$. GP פתרו את הבעיה למקרה הלא-סיבתי, כלומר x_i תלוי בכל הוקטור $\underline{s}$. יש לציין שעבודתם המקורית של GP לא קושרה לזו של שאנון.

קיבולים נוספים - הגדרות

בנוסף לקיבול עבור אינפורמציית צד במשדר ניתן להגדיר גם:

- המקרה "הקלאסי": קיבול עם אינפורמציית צד במקלט בלבד (ז"א s הוא כמו כניסה נוספת למקלט) ל- $C_{SI@Rx}=\max_{P(x)} I(x;s,y) \underset{\substack{I(x,s)=0 \\ +\text{chain rule for M.I.}}}{=} I(x;y\,|\,s)$.
- קיבול עם אינפורמציית צד בשני צדי המערכת $C_{SI@Both}=\max_{P(x|s)} I(x;y\,|\,s)$.
במקרה זה האופטימיזציה היא על פילוגי כניסה התלויים ב- s שידוע למשדר (סיבתית או לא-סיבתית), ולכן ניתן לקבל קיבול גבוה יותר מאשר במקרה הקודם.
- קיבול ללא אינפורמציית צד $C_{\text{no ISI}}=\max_{P(x)} I(x;y)$. זהו הפתרון הקלאסי של שאנון עבור ערוץ המוגדר ע"י $P(y\,|\,x)$ ($\sum_s P(s,y\,|\,x)=\sum_s P(s)P(y\,|\,x,s)=$).

משפט GP (1980)

קיבול הערוץ תלוי- המצב, כפי שתואר לעיל, בהינתן אינפורמצית צד לא- סיבתית במשדר, $C_{SI@Tx}$, מתקבל ע"י

$$C_{SI@Tx}=\max_{u,x:\,u\leftrightarrow(s,x)\leftrightarrow y}[I(u;y)-I(u;s)]=\max_{u,x:\,u\leftrightarrow(s,x)\leftrightarrow y}[H(u\,|\,s)-H(u\,|\,y)]$$

כאשר $u\leftrightarrow(s,x)\leftrightarrow y$ מסמל שלשה מרקובית [7], ואילו השוויון האחרון מניח בעיה דיסקרטית ומתקבל מפירוק לאנטרופיות וקיזוז אנטרופית u. המשתנה u הינו משתנה עזר מעל אלפבית כללי, כאשר הפילוג המשותף מקיים

$$P(u,s,x,y)=P(s,u,x)P(y\,|\,u,s,x)=P(s)P(u\,|\,s)P(x\,|\,u,s)P(y\,|\,s,x)$$

כאשר השוויון האחרון מתקבל בזכות המרקוביות. במקרה של אילוץ מחיר כניסה (cost function), דוגמת אילוץ על הספק השידור, אזי נדרוש גם $E\rho(x)\le c$.

הערות על משפט GP

א. נשאלת השאלה מהי המשמעות הפיזיקלית של משתנה העזר u שאינו מופיע בתיאור הבעיה המקורית.

ב. ניתן להראות שהפתרון האופטימלי, דהיינו זה שמביא את שמביא את קצב השידור למקסימום, יהיה פונקציה דטרמיניסטית של u,s. ז"א x נקבע חד-ערכית ע"י u ו-s לפי פונקציה דטרמיניסטית $x=\varphi(u,s)$. הסבר היוריסטי ניתן למצוא בכך שאם x האופטימלי יהיה תלוי במשתנה אקראי נוסף z שאינו משפיע על הערוץ, ז"א $x=\varphi(u,s,z)$, אזי אקראיות זו יכולה רק להקטין את האינפורמציה ההדדית. לפיכך, במקום מציאת מקסימום על פני (u,x), מספיק לבצע מקסימיזציה ביחס ל- u בלבד שיקבע באופן דטרמיניסטי גם את x המיטבי.

ג. נקודת אזהרה: ייתכן u "לא-טוב". בחירת u "לא-טוב" תגרור תוצאה לא פיזיקלית של "קיבול שלילי" $I(u;y)-I(u;s)<0$.

ד. במקרה של בעיה דיסקרטית ניתן להראות כי גודל האלפבית של u חסום ע"י סכום האלפבית של x ו-s, דהיינו $|u|\le|x|+|s|$.

---

[7] $A\leftrightarrow B\leftrightarrow C \Rightarrow I(A;C\,|\,B)=0\ ,\ P(A\,|\,B,C)=P(A\,|\,B)$

ה. הקיבול של בעית הערוץ עם אינפורמצית צד סיבתית (שאנון, 1958) מתקבל ע"י משפט GP תחת האילוץ של u,s בת"ס ($u \perp\!\!\!\perp s$). כלומר,

$$C_{SI(Causal)@Tx} = \max_{\substack{u:\, u \perp\!\!\!\perp s \\ x=\varphi(u,s)}} I(u;y)$$

יש לשים לב כי אין צורך באיבר השני של משפט GP משום ש- $u \perp\!\!\!\perp s$. במאמרו מ-1958, שאנון טען כי u יילקח מתוך תת-קבוצה של איחוד האלפבית של s ו-x, ולכן גודל האלפבית של u יהיה חסום ע"י $|u| \le |x|^{|s|}$. ברור כי מתקיים $C_{SI(non-causal)@Tx} \ge C_{SI(causal)@Tx}$. אמנם במקרה הסיבתי איננו מפחיתים את $I(u;s)$ בביטוי הקיבול, אך מנגד אנו דורשים אופטימיזציה מעל $u \perp\!\!\!\perp s$, דרישה המגבילה את סוג התלויות u,s האפשריות.

דוגמאות למקרים פרטיים של בעית GP

ערוץ עם הפרעה אדיטיבית ידועה במשדר (Writing on Dirty Paper או בעית Costa [3])

ערוץ מהצורה

$$y = x + s + z$$

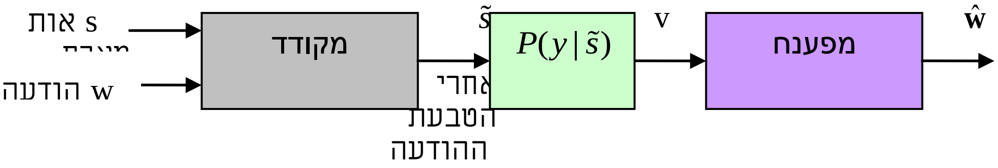
עם אילוץ הספק (פונקצית מחיר) $\frac{1}{n} E \| \underline{x} \|^2 \le P$. ראינו לגבי בעיה זו כי מתקיים

$$C_{SI(non-causal)@Tx} = C_{SI@Both}$$

.

משפחה של בעיות "סימני מים" (digital watermarking)

נסתכל על המודל



איור 2

ונדרוש עיוות ממוצע חסום. $\frac{1}{n}\sum_{i=1}^{n} E\rho(s_i, \tilde{s}_i) \le D$

נסתכל על מקרה פרטי של $\frac{1}{n} E \| \underline{s} - \underline{\tilde{s}} \|^2 \le D$. אזי דוגמא זו (איור 2) מתלכדת עם הדוגמא הקודמת, משום שניתן להסתכל על $\tilde{s}$ למעשה כעל $x+s$ בבעיית Costa.

ערוץ עם דעיכות (fading channel)

ערוץ מהצורה $y = x \cdot s + z$, כאשר s הן הדעיכות (flat fading). במקרה הוקטורי יכול להתקבל ערוץ עם זכרון (fast fading). עבור ערוץ זה ידוע כי

$$C_{SI@Rx} = E_s \frac{1}{2}\log(1+\frac{P \cdot s^2}{\sigma_z^2}).$$

ערוץ עם רעש אימפולסיבי

מהצורה $y = x + s \cdot z$, כאשר s קובע אם הרעש חזק או חלש.

ערוץ קוסטה/שאנון בינארי

ערוץ זה זהה לערוץ Binary Symmetric Channel (BSC) עם סיכוי חילוף p. אולם במקרה זה המשדר יודע אם התרחש חילוף. אזי לכאורה זו בעיה טריוויאלית משום שהמשדר ישדר ביטים הפוכים במקרה של שגיאה. הבעיה הופכת למעניינת אם מוסיפים אילוץ על הכניסה כך שמספר ההיפוכים המותרים חסום. למשל, נדרוש שמספר האחדים בכניסה יהיה קטן ממספר האפסים. ידוע שבמקרה זה עבור אינפורמציית צד לא סיבתית ניתן עדיין לקבל $C_{SI(non-causal)@Tx} = C_{SI@Both} = H_B(x)$ בעזרת קוד. לעומת זאת במקרה של אינפורמציית צד סיבתית נפסיד קיבול.

"זיכרון עם תאים דפוקים"

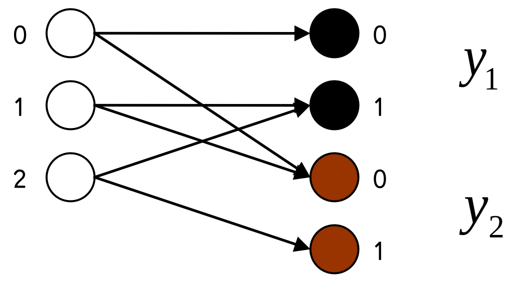
במודל זיכרון זה (המהווה אגב את המוטיבציה המקורית לפתרון בעיית GP) נתון זיכרון מגנטי עם תאים דפוקים. ראש הכתיבה יודע מראש אילו תאים דפוקים ושלא ניתן לאחסן בהם אינפורמציה. הקורא לעומת זאת לא יודע אילו תאים דפוקים ואילו תקינים. ז"א ניתן להסתכל על מודל זיכרון זה כמקיים

$$y = \begin{cases} \text{x if } s = \text{"}ok\text{"} \\ 0 \text{ if } s = \text{"}stuck@0\text{"} \\ 1 \text{ if } s = \text{"}stuck@1\text{"} \end{cases}$$

במקרה והכותב והקורא שניהם יודעים את מיקום התאים התקולים, אזי קיבול הזיכרון יהיה בדיוק ההסתברות שיש לתא לא להיות תקוע (למשל, במקרה הבינארי, אם 90% מהתאים תקינים אזי הקיבול יהיה 0.9 ביט לתא זיכרון). מסתבר כי ניתן להגיע לקיבול זה גם עם ידע על מיקום התאים התקולים **רק** בכותב! ז"א

$$C_{SI(non-causal)@Tx} = C_{SI@Both} = \%\text{Good Cells}.$$

ערוץ Blackwell (ערוץ Broadcast דטרמיניסטי)



איור 3

מה הקשר של ערוץ זה (איור3) לערוץ עם אינפורמציית צד במשדר? ובכן,בעיה זו שקולה למודל הזיכרון עם התאים הדפוקים: נניח ש-x מיעד את השידור ל- y_1 ומשדרת אותו בקצב מלא. אזי מבחינת המשתמש השני הוא מאולץ לקבל 0 במקרים בהם המשתמש הראשון מקבל 0, וחופשי לקבל 0 או 1 במקרים בהם המשתמש הראשון מקבל 1. זה בדיוק כמו תא תקול בבעיית הזיכרון שלעיל, וגם במקרה זה המשדר יודע מהו מצב "התא" בעוד שהמקלט (של y_2) אינו יודע זאת.

הוכחת המשפט הישר בעזרת Random Coding and Random Binning

כרגיל בהוכחות קלאסיות בתורת האינפורמציה, ההוכחה מתבססת על אוסף של קודים אקראיים ולא על קוד ספציפי. נניח שידוע לנו $P(u|s)$ ו- $\varphi(u,s)$, ונרצה להוכיח השגה של הקצב, ז"א עבור קצב R הנמוך מ- $I(u;y)-I(u;s)$ ניתן לקבל הסתברות שגיאה קטנה כרצוננו $P_e \to 0$.

תחילה נגדיר שלושה שלבים:

שלב Offline

- נגריל קוד אקראי $C=\{\underline{u}\}$ בגודל 2^{nR_1} לפי פילוג i.i.d. $P(u)=\sum_s P(u|s)P(s)$ (כאשר R_1 יוגדר בהמשך).
- נפזר את מילות הקוד בין 2^{nR} תאים (bins) בצורה אקראית אחידה.
- נגדיר מיפוי מהודעות לתאים $\text{w} \to \text{bin}$.

שלב הקידוד

בהינתן ההודעה $\text{w}=\text{i}$, וקטור ה-SI $\underline{s}$ וכן $\varepsilon>0$:

- מצא $\underline{u}$ בתא i שהוא אופייני במשותף עם $\underline{s}$ הנתון (ביחס לפילוג $P(u,s)=P(s)P(u|s)$), ז"א $\underline{u}\in A_\varepsilon^n(\underline{u}|\underline{s})$.
- שדר את $x_i=\varphi(u_i,s_i)$, $i=1,\dots,n$.

שלב הפענוח

- מצא $\underline{\hat{u}}\in C$ (כאשר ספר הקוד ידוע למפענח משלב ה- offline) שאופייני במשותף עם $\underline{y}$ שנקלט (ביחס לפילוג המשותף $P(u,y)=\sum_{x,s}P(u,s,x,y)$), ז"א $\underline{\hat{u}}\in A_\varepsilon^n(\underline{\hat{u}}|\underline{y})$.
- מצא לאיזה תא $\underline{\hat{u}}$ שייך, למשל התא j, והכרז על ההודעה המתאימה $\hat{\text{w}}=\text{j}$.

תהיות לגבי המנגנון ומקור לשגיאות:

i. מה מבטיח שיהיה בתא ה- i לפחות $\underline{u}$ אחד מתאים? זהו מקור לשגיאת קידוד (זוהי שגיאה מבוקרת שניתן לזהות ולהכריז עליה במקודד).

ii. מה מבטיח ש- $\underline{u}$ האמיתי הוא אכן אופייני עם $\underline{y}$, ושאכן יהיה יחיד (למרות שעקרונית ניתן להרשות $\underline{u}$ אחר אופייני, העיקר שיהיה באותו התא)?

iii. מה מבטיח שלא יהיו מתחרים ל- $\underline{u}$ האמיתי בתאים אחרים? זהו מקור לשגיאת פענוח משום שאם ה- $\underline{u}$ האמיתי אינו אופייני, וקיים $\underline{u}$ אחר אופייני, אזי לא

נדע כי חלה שגיאה (במקרה של מספר $\underline{u}$-ים אופיינים המפענח יכול להכריז לפחות על בעייה בפענוח).

ובחזרה להוכחה, נזהה תכונות האופייניות הבאות:

א. $\underline{u}$ אופיינית במשות ף עם $\underline{s}$ ומשום ש- $i=1,\cdots,n$ $x_i=\varphi(u_i,s_i)$, גם $(\underline{u},\underline{s},\underline{x})$ אופייניים במשותף ביחס ל-$P(u,s,x)$.

ב. על סמך ה-.A.E.P ביחס לערוץ, נקבל כי, בהסתברות הגבוהה מ- $1-\varepsilon$, $(\underline{x},\underline{s},\underline{y})$ גם הם אופייניים במשותף ביחס לפילוג $P(x,s,y)$.

מתוך שני הסעיפים לעיל , בתוספת תכונת המרקוביות של $(\underline{u},\underline{s},\underline{x},\underline{y})$, נסיק כי גם $(\underline{u},\underline{s},\underline{x},\underline{y})$ אופייניים במשותף.

כעת נגדיר טענת עזר שתסייע בניתוח השגיאות.

טענת עזר: "אכספוננט סף ההצלחה" ([4])

אם הסיכוי ל- "הצלחה" הוא 2^{-nr} ומבצעים 2^{2R} ניסויים בת"ס, אזי הסיכוי שנקבל "הצלחה" בלפחות אחד מהניסויים הוא

$$P_{success}\underset{n\to\infty}{\to}\begin{cases}1 & R>r \quad (I)\\ 0 & R<r \quad (II)\end{cases}$$

הוכחה:

נוכיח את (I) ע"י חישוב המשלים לסיכוי ל- "הצלחה" בלפחות מאחד הניסויים (ז"א הסיכוי ל"אי-הצלחה" בכל הניסויים)

$$P_{\text{fail in all trials}}=(1-2^{-nr})^{2^{nR}}\underset{e^{-x}\ge 1-x}{\le}(e^{-2^{-nr}})^{2^{nR}}=e^{-2^{n(R-r)}}\underset{\substack{R>r\\ n\to\infty}}{\to}0$$

ולגבי (II), לפי חסם האיחוד

$$P_{success}\le\sum_{i=1}^{2^{nR}}\Pr(\text{success in trial i})=2^{nR}\cdot 2^{-nr}\underset{\substack{r<R\\ n\to\infty}}{\to}0$$

יש לשים לב שטענה (I) שקולה למעשה לקידוד מקור – רוצים שלפחות מילה אחת תכסה את המידע ומותר שיהיו יותר ממילה אחת כזו (ז"א "הצלחה"). לעומת זאת, טענה (II) שקולה לקידוד ערוץ – איננו רוצים שמילה מתחרה תצליח . (הערה: אנו כבר יודעים משעורים קודמים כי בבעיות של אינפורמציית צד "מתחבא" הן קי דוד מקור והן קידוד ערוץ).

כעת נחזור ונתייחס לשלושת מקורות השגיאה שזיהינו לעיל (i-iii):

- אם $(\underline{u},\underline{s},\underline{x},\underline{y})$ אופייניים במשותף , כפי שאכן ראינו , אזי בפרט גם $\underline{u}$ ו- $\underline{y}$ אופייניים במשותף, ולכן בהסתברות קרובה ל-1 $\underline{u}$ האמיתי הוא אכן אופייני עם $\underline{y}$. מסקנה: **שגיאה ii** קטנה כרצוננו.

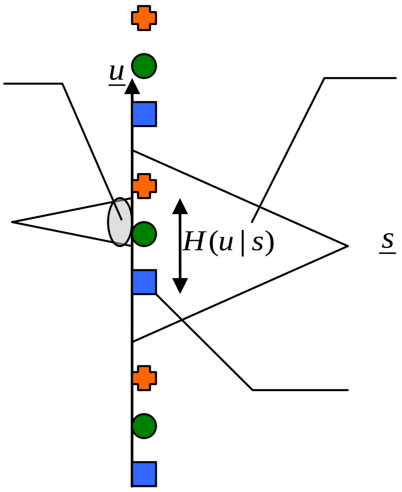
* כדי לאפס את **שגיאה iii** יש לדאוג שלא יהיה $\underline{u}$ אחר אופייני עם $\underline{y}$ (אין מתחרים), בדיוק כמו בקידוד ערוץ. לכן נדרוש ש-$R_1 < I(u;y)$, כך שיובטח (על סמך טענת העזר) שאין מתחרים בהסתברות שואפת ל-1.
* כדי לאפס את **שגיאה i** עלינו לנהוג כמו בבעית קידוד מקור. הסיכוי ש-$\underline{u}$ אקראי יהיה אופייני עם $\underline{s}$ שואף ל-$2^{-nI(u;s)}$. כמו כן, הסיכוי ש-$\underline{u}$ אקראי "ייפול" בתא i הוא 2^{-nR}. מכאן הסיכוי ש-$\underline{u}$ אקראי יהיה גם אופייני עם $\underline{s}$ וגם "ייפול" בתא i הינו (מאחר והמאורעות בלתי תלויים => מכפלה של הסתברויות) $2^{-n[I(u;s)+R]}$. זהו הסיכוי ל-"הצלחה" (ז"א 2^{-nr}). על סמך טענת העזר שהוכחנו, כדי שתהיה לפחות "הצלחה" אחת מתוך 2^{nR_1} ניסויים עבור s נתון, חייב להתקיים $R_1 > I(u;s)+R$

מסיכום שלושת מקורות השגיאה הללו נקבל את התנאי לשגיאה השואפת לאפס:

$$R < I(u;y) - I(u;s)$$

שמסכם את ההוכחה של החלק הישר של משפט GP.

הסתכלות גיאומטרית



4 איור

נרצה שבמניפה של $\underline{u}$ שאופייני עם $\underline{y}$ יהיה נציג אחד מקוסט אחד. תחום הקוסטים האפשריים מוגדר ע"י אי הוודאות $H(u|s)$. נזהה קוסט בודד מתוך הקבוצה ע"י $\underline{y}$. מכאן שקצב השידור הוא $H(u|s)-H(u|y)$.

<u>דוגמא לבעיית GP: קידוד לזיכרון עם תאים תקולים (defective cells)</u>

כזכור במקרה זה

$$y = \begin{cases} x \text{ if } s = \text{"}ok\text{"} \\ 0 \text{ if } s = \text{"}stuck@0\text{"} \\ 1 \text{ if } s = \text{"}stuck@1\text{"} \end{cases}$$

והרחבה ברורה למקרה של אלפבית שאינו בינארי $|X|>2$.

ראינו כי במקרה של אינפורמציית צד בשני צדי המערכת $C_{SI@Both}=\Pr(s=\text{"ok"})\cdot\log_2|X|$. נוכיח כי עבור ערוץ זה מתקיים $C_{GP}=C_{SI@Both}$:

ננחש $u=y$, ו-x האופטימלי להשגת $C_{SI@Both}$. זוהי בחירה לגיטימית משום ש- y הוא פונקציה דטרמיניסטית עם בחירת x ולכן מתקיים הקשר המרקובי הרצוי $u\leftrightarrow(s,x)\leftrightarrow y$.

עבור בחירה זו

$$C_{GP}=\max_{P(x)}H(y|s)=\max_{P(x)}\Pr(s=\text{"ok"})\cdot H(x)+\max_{x}\Pr(S=Stuck@)\cdot 0$$

לפיכך נחפש את $P(x)$ שמביא למקסימום את אנטרופית הכניסה, דהיינו $H(x)=\log|X|$.

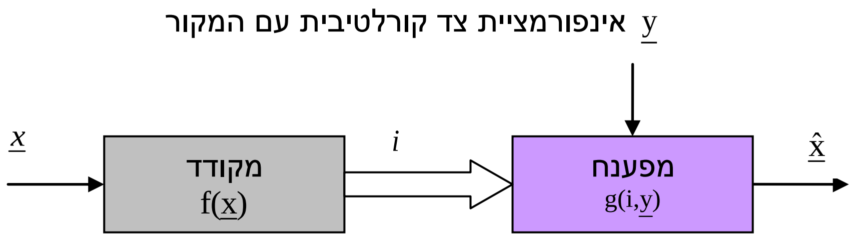
לכן נקבל $C_{GP}=\Pr(s=\text{"ok"})\cdot\log|X|=C_{SI@Both}$.

<u>דוגמא לקוד עבור זיכרון עם תאים תקולים[8]:</u>

למשל קוד ממשפחת קודי MDS (קודי R-S). נסתכל על בלוק קוד באורך n המחולק ל- k ביטי אינפורמציה ו- n-k ביטי יתירות (בדיקת זוגיות). בבניית הקוד לזיכרון נאכסן את המידע דווקא ב- n-k "ביטי היתירות", בעוד יתר k הביטים יתארו את התאים התקולים. לפיכך, ניקח n-k ביטי מידע (הודעות) שברצוננו לאכסן בזיכרון. ביטים אלו ניתן לשייך ל- 2^{n-k} קוסטים של קוד מהצורה $C_w=\{\underline{x}:\underline{\underline{H}}\underline{x}=\underline{w}\}$. דהיינו, כל הודעה מיוצגת ע"י קוסט (סינדרום) מתאים. בכל קוסט ישנן 2^k מילות קוד.

נרצה להראות כיצד ניתן למצוא בקוסט נתון מילת קוד שמתלכדת עם תכולת התאים התקולים. ובכן, מאחר ולמשדר אינפורמציית צד על מיקום התאים התקולים, ניתן לבחור מילת קוד כלשהי x באורך n בתוך הקוסט ולבצע XOR עם מילה באורך n, נסמנה s, המציינת את ערכי k התאים התקולים (ב-k ביטים שונים). אזי $\tilde{e}=x\oplus s$ היא ההבדל בין x ו-s. מתוך תכונות הקוד בהכרח קיימת מילה $\tilde{\tilde{e}}$ בקוסט האפס המתלכדת עם $\tilde{e}$ ב-k התאים התקולים. נבחר לאחסן את $\tilde{x}=x+\tilde{\tilde{e}}$, ולכן מובטח ש- $\tilde{x}$ מתלכד עם ערכי המקומות התקולים. המפענח יחשב (ללא אינפורמציית צד) $\underline{\underline{H}}\tilde{\underline{x}}=\underline{\underline{H}}(\underline{x}+\tilde{\tilde{\underline{e}}})=\underline{\underline{H}}\underline{x}=\underline{w}$ שמייצג את ההודעה שנשלחה. יש לשים לב כי במקרה זה פעולת המקודד היא קשה בעוד פעולת המפענח קלה יותר (בשונה מבדר"כ בקידוד ערוץ).

הדואליות לבעיית Wyner-Ziv



איור 5

ראינו כי עבור בעיה זו של קידוד מקור עם אינפורמציית צד במפענח

$$R_{WZ}(D) = R_{SI@Rx}(D) = \min_{\substack{u \\ u\leftrightarrow x\leftrightarrow y \\ \text{exists } \hat{x}=\varphi(u,y) \\ \text{under } \varphi(x,\hat{x})\le D \\ (\text{e.g. } \varphi(x,\hat{x})=E(x-\hat{x})^2)}} I(x;u\,|\,y)$$

בגלל התנאי המרקובי, ניתן לרשום גם

$$R_{WZ}(D) = \min[I(x;u) - I(y;u)]$$

פונקצית הקצב-עיוות $R_{WZ}(D)$ בצורתה זו דומה מאוד למשפט GP. גם במקרה זה u הוא משתנה עזר והפתרון מקיים דואליות עם הפתרון לבעיית GP:

יש קוד בקצב גבוה עם ספר קוד C_1 של מילות $\underline{u}$ ($|\square| = 2^{nR_1} \approx 2^{nI(x;u)}$), המפוזרות אחיד ל- 2^{nR} תאים (bins).

הקידוד מתבצע באופן הבא : מצא $\underline{u}$ בתוך C_1 שאופייני עם $\underline{x}$, שלח את האינדקס i של התא אליו שייך $\underline{u}$. הפענוח מתבצע באופן הבא: מצא $\underline{\hat{u}}$ בתוך התא i שאופייני במשותף עם אינפורמציית הצד $\underline{y}$, ומכאן $i=1,\ldots,n$ $\hat{x}_i = \varphi(\hat{u}_i, y_i)$.

סכימת עבודה זו היא דואלית (רק הפוך) להליך המקביל בבעיית GP. לדוגמא, בבעיה זו C_1 הוא קוד מקור (קוד כיסוי) טוב, בעוד C_1 המקביל לו בבעיית GP הוא קוד ערוץ טוב.

<u>ביבליוגרפיה</u>

[1] C. E. Shannon, "Channels with side information at the transmitter", IBM Journal, pp. 289--293, October, 1958. 33.

[2] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," Problems of Control and Information Theory 9(1), pp. 19--31, 1980.

[3] M.H.M. Costa, "Writing on dirty paper", IEEE Trans. Information Theory, IT-29, pp. 439—441, May 1983.

[4] Cover & Thomas Book.

הרצאה - 7

ערוצי MAC ו BC וקטוריים - ערוצי MIMO

סוכם ע"י אבינועם לוי על פי הרצאה של טל פילוסוף מה30/05/06 .

ערוץ MIMO כללי נתון ע"י:

$$Y=\begin{bmatrix}y_1\\y_2\\ \\ y_{nr}\end{bmatrix}=\underline{\underline{H}}\cdot\underline{X}+\underline{Z}=\begin{bmatrix}h_{11} & h_{12} & h_{1nt_t}\\ h_{21} & & \\ & & \\ h_{n_r r1} & & h_{nr,nt}\end{bmatrix}\cdot\begin{bmatrix}x_1\\x_2\\ \\ x_{nt}\end{bmatrix}+\begin{bmatrix}z_1\\z_2\\ \\ z_{nr}\end{bmatrix}$$

כאשר:

<u>Y</u> - וקטור מוצא מהערוץ (כניסה למקלטים) במימד n_r (מס' אנטנות קליטה).

<u>X</u> - וקטור כניסה לערוץ (מוצא משדרים) במימד n_t (מס' אנטנות שידור).

<u>Z</u> – וקטור רעש גאוסי לבן במימד n_r, $z\sim N(0,\sigma^2 zI)$.

H – מטריצת מעבר ערוץ. h_{ij} מייצג השפעת ערוץ על כניסה i למוצא j).

<u>הערה:</u> כל רכיב במטריצות שהוגדרו יכול להיות ממשי או קומפלקסי. אנו נניח בניתוח הנוכחי, ללא הגבלת הכלליות, רכיבים ממשיים.

ניתן לחלק בעיות MIMO לבעיות P2P,MAC,BC ע"פ מס' המקלטים והמשדרים הבאים לידי ביטוי בקשרים המתקיימים בין הכניסות למוצאים דרך מטריצת מעבר ערוץ H:

א. <u>MIMO P2P – מקלט אחד ומשדר אחד:</u>

$$\underline{Y}=\underline{\underline{H}}\cdot\underline{X}+\underline{Z}$$

כאשר המשתנים הם כפי שהוגדרו במקרה הכללי. כל n_t הכניסות לערוץ (אנטנות שידור) יוצאות ממשדר אחד וכל n_r היציאות מהערוץ (אנטנות קליטה) נכנסות למקלט אחד.

הקיבול נתון ע"י:

$$C_{p2p}=\max_{\substack{S_{\underline{x}}\\ tr(S_{\underline{x}})\le P}} I(\underline{y};\underline{x})=\max_{\substack{S_{\underline{x}}\\ tr(S_{\underline{x}})\le P}}\frac{1}{2}\log\left(\frac{\left|HS_{\underline{x}}H^T+\sigma^2{}_z I\right|}{\sigma^2{}_z\left|I\right|}\right)$$

כאשר:

$S_{\underline{X}}=E\{\underline{X}\cdot\underline{X}^T\}$ - מטריצת קרוס קורלציה רכיבי שידור ממימד $n_t * n_t$

|.| - אופרטור דטרמיננטת מטריצה.

ב. <u>MIMO MAC – מס' כלשהו n_u (מס' משתמשים) של משדרים ומקלט בודד:</u>

לדוגמא עבור 2 משדרים:

$$\underline{y}=\left[\underline{\underline{h}}_1\quad \underline{\underline{h}}_2\right]\cdot\begin{bmatrix}\underline{x}_1\\ \underline{x}_2\end{bmatrix}+\underline{z}=\underline{\underline{h}}_1\cdot\underline{x}_1+\underline{\underline{h}}_2\cdot\underline{x}_2+\underline{z}$$

כאשר באופן כללי כל משדר i מתוך n_u יכול לשדר ל- n_{ti} אנטנות שידור שממופות ל- n_r אנטנות הקליטה דרך מטריצת מעבר ערוץ hi ממימד $n_r * n_{ti}$. כל אנטנות הקליטה נכנסות למקלט בודד.

$$C_{MAC}^{SUM}=\max_{\substack{tr(S_{\underline{x}1})\le P1\\ tr(S_{\underline{x}2})\le P2}} I\left(\underline{y};\underline{x}_1,\underline{x}_2\right)=\max_{\substack{S_{\underline{x}}\\ tr(S_{\underline{x}})\le P}}\frac{1}{2}\log\left(\frac{\left|HS_{\underline{x}}H^T+\sigma^2{}_zI\right|}{\sigma^2{}_z\left|I\right|}\right)\le C_{p2p}$$

כאשר:

$\underline{\underline{S}}_{\underline{X}1}=E\left\{\underline{X}_1\cdot\underline{X}_1{}^T\right\}$ - מטריצת קרוס קורלציה רכיבי שידור משדר 1 ממימד n_{t1} *n_{t1}.

$\underline{\underline{S}}_{\underline{X}2}=E\left\{\underline{X}_2\cdot\underline{X}_2{}^T\right\}$ - מטריצת קרוס קורלציה רכיבי שידור משדר 2 ממימד n_{t2} *n_{t2}.

$\underline{\underline{S}}_{\underline{X}}=E\left\{\underline{X}\cdot\underline{X}^T\right\}$ - מטריצת קרוס קורלציה כל רכיבי השידור ממימד $n_{t1}+n_{t2}$ *$n_{t1}+n_{t2}$.

הקיבול הכולל נמוך מקיבול p2p כתוצאה מחוסר שיתוף פעולה במשדר - $S_{\underline{x}}$ – אלכסונית (חוסר תלות בין הכניסות ב MAC).

ג. **MIMO BC – משדר בודד ומספר כלשהו n_u של מקלטים:**

לדוגמא עבור 2 מקלטים:

$$\begin{bmatrix}\underline{y}_1\\ \underline{y}_2\end{bmatrix}=\begin{bmatrix}\underline{\underline{h}}_1\\ \underline{\underline{h}}_2\end{bmatrix}\cdot\underline{x}+\begin{bmatrix}z_1\\ z_2\end{bmatrix}$$

כאשר באופן כללי המשדר משדר דרך n_t אנטנות שידור שממופות ל-n_{ri} אנטנות קליטה דרך מטריצת מעבר ערוץ hi ממימד n_{ri} *n_t. כל מקלט i מתוך n_u מקבל n_{ri} אנטנות קליטה.

שוב, הקיבול הכולל נמוך מקיבול p2p כתוצאה מחוסר שיתוף פעולה במקלט.

1. **GDFE – Generalized Decision Feedback Equalizer (P2P)**

בדומה לערוץ ISI, עבורו ניתן להגיע לקיבול עם הפרדה בין קוד לאפנון (הורדת סיבוכיות) באמצעות שימוש בתצורת DFE, נשתמש בתצורת GDFE עבור בעיות MIMO P2P.

נתון ערוץ P2P ווקטורי:

$$\underline{Y}=\underline{\underline{H}}\cdot\underline{X}+\underline{Z}$$

כאשר:

$\underline{X}$~N(0,S_{xx}) ממימד n_t.

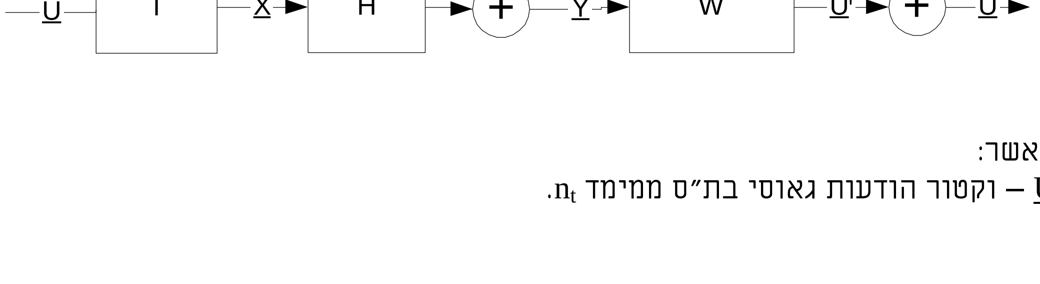
$\underline{Z}$~N(0, I) ממימד n_r.

$\underline{Y}$ ממימד n_r.

המטרה: לאפשר לפענח כל הודעה בנפרד (הורדת סיבוכיות) בלי לפגוע בקיבול.

נניח ללא הגבלת כלליות שתי כניסות סקלריות (n_t=2).

שערוך MMSE לינארי:



כאשר:

$\underline{U}$ – וקטור הודעות גאוסי בת"ס ממימד n_t.

$\underline{X}$ – וקטור שידור גאוסי כללי לא בהכרח בת"ס ממימד n_t המתקבל מ- $\underline{U}$ ע"י $\underline{X}=T\underline{U}$
כאשר T מטריצת מיפוי ממימד n_t*n_t .
W – מטריצת שערוך MMSE ממימד n_t*n_r .
$\underline{E}=\underline{U}-\underline{U}'$ – שגיאת השערוך, ניצבת למדידות $\underline{Y}$ ולמשערך U' (ע"פ עקרון האורתוגנליות של משערך ה – MMSE וגאוסיות) בעלת מטריצת אוטוקורלציה $S_{\underline{E}}$ ולכן הערוץ $\underline{U}=\underline{U}'+\underline{E}$ אדיטיבי עם רעש גאוסי בת"ס.
$\underline{U}$ הינו משתנה עזר שמאפשר להתייחס להודעות כוקטור בת"ס בעל מטריצת קורלציה $S_U=E\{\underline{U}\underline{U}^T\}$ אלכסונית. מאחר ו-$\underline{U},\underline{X}$ קשורים באמצעות מטריצת מיפוי T דטרמיניסטית הערוץ $\underline{X}$->$\underline{Y}$ שקול לערוץ $\underline{U}$->$\underline{Y}$ כאשר H->H'=HT.
קיבול ערוץ עבור פענוח משותף של כל ההודעות:

$$\left.\begin{array}{l} I(\underline{U};\underline{U}')=\frac{1}{2}\log\left(\frac{|S_{\underline{U}}|}{|S_{\underline{E}}|}\right) \\ I(\underline{Y},\underline{U})=\frac{1}{2}\log\left(\frac{|S_{\underline{Y}}|}{|S_{\underline{Z}}|}\right)\end{array}\right\}\xrightarrow{MMSE} I(\underline{U};\underline{U}')=I(\underline{Y},\underline{U})=\frac{1}{2}\log\left(\frac{|S_{\underline{U}}|}{|S_{\underline{E}}|}\right)$$

סכום הקצבים (עבור פיענוח כל הודעה בנפרד):

$$I(u_1;u'_1)+I(u_2;u'_2)=\frac{1}{2}\log\left(\frac{|S_{u1}|}{|S_{e1}|}\right)+\frac{1}{2}\log\left(\frac{|S_{u2}|}{|S_{e2}|}\right)\le\xrightarrow[|S_{\underline{U}}|=S_{U1}S_{U2}]{\substack{hadamard\\ inequality\\ |S_{\underline{E}}|\le S_{E1}S_{E2}}}\frac{1}{2}\log\left(\frac{|S_{\underline{U}}|}{|S_{\underline{E}}|}\right)$$

שוויון מתקבל רק כאשר השגיאות בת"ס - $S_{\underline{E}}$ אלכסונית (עבור המונה הראינו כי ניתן לעבוד עם $S_{\underline{U}}$ אלכסונית ללא הגבלת הכלליות) לכן עבור המקרה הכללי עבורו השגיאות לא בת"ס קיים הפסד בקצב בפענוח כל הודעה בנפרד.

ננסה לשפר את הסכימה:

$$W=S_{\underline{U}\underline{Y}}S_{\underline{Y}\underline{Y}}^{-1}=S_{\underline{U}}H'^T\left(H'S_{\underline{U}}H'^T+I\right)^{-1}=\xrightarrow{MIL}=\underbrace{\left(H'^T H'+S_{\underline{U}}^{-1}\right)^{-1}}_{Rb}\underbrace{H'^T}_{MF}$$

$$\underline{R}=\underbrace{H'^T H'}_{R_f}\underline{U}+\underbrace{H'^T\underline{Z}}_{Z'}=R_f\underline{U}+\underline{Z}'$$

$$\underline{U}=\underbrace{(H^T H+S_{\underline{U}}^{-1})^{-1}}_{R_b}\underline{R}+\underline{E}=R_b\underline{R}+\underline{E}$$

$$S_{\underline{E}}=E\{\underline{E}\underline{E}^T\}=E\{(\underline{U}-\underline{U}')(\underline{U}-\underline{U}')^T\}=E\{(\underline{U}-S_{\underline{U}\underline{Y}}S_{\underline{Y}}^{-1}\underline{Y})(\underline{U}-S_{\underline{U}\underline{Y}}S_{\underline{Y}}^{-1}\underline{Y})^T\}=$$
$$=S_{\underline{U}}-S_{\underline{U}\underline{Y}}S_{\underline{Y}}^{-1}S_{\underline{Y}\underline{U}}-S_{\underline{U}\underline{Y}}S_{\underline{Y}}^{-1}S_{\underline{U}\underline{Y}}+S_{\underline{U}\underline{Y}}^2S_{\underline{Y}\underline{Y}}^{-1}=S_{\underline{U}}-S_{\underline{U}}H'^T(H'S_{\underline{U}}H'^T+I)^{-1}H'S_{\underline{U}}$$
$$=\xrightarrow{MIL}R_b$$

המטרה היא להגיע למטריצת רעש אלכסונית ע"מ להגיע לסכום קצבים מקסימלי לכן נעשה שימוש בפירוק cholesky:

$$R_b = G^{-1}\Delta^{-1}G^{-T}$$

$$G \equiv \begin{bmatrix} I & G_{22} \\ 0 & I \end{bmatrix}$$

$$\Delta \equiv \begin{bmatrix} \Delta_{11} & 0 \\ 0 & \Delta_{22} \end{bmatrix}$$

ונגדיר:

$$\underline{E}' \equiv G\underline{E}$$

$$S_{\underline{E}'} = GR_bG^T = \Delta^{-1}$$

$$\left|S_{\underline{E}'}\right| = \left|S_{\underline{E}}\right|$$

כלומר קיבלנו מטריצת רעש אלכסונית בעלת דטרמינטה זהה למטריצה המקורית.
נבנה סכימה שקולה העושה שימוש בוקטור הרעש החדש:

$$\underline{U} = R_b\underline{R} + \underline{E} = G^{-1}\Delta^{-1}G^{-T}\underline{R} + \underline{E}$$

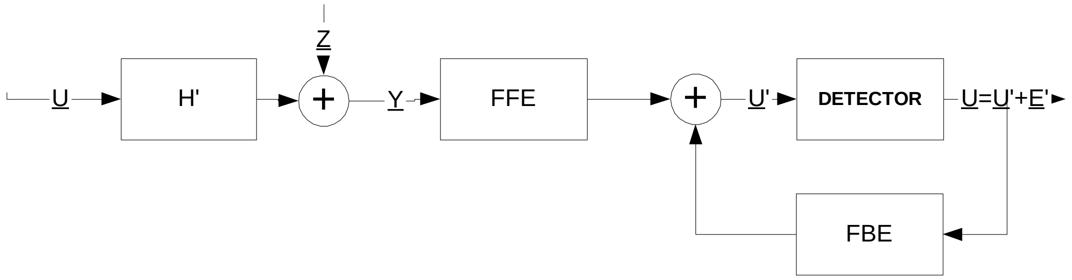
$$G\underline{X} = \Delta^{-1}G^{-T}\underline{R} + G\underline{E} \qquad /+(I-G)\underline{U}$$

$$\Rightarrow \underline{U} = \underbrace{\Delta^{-1}G^{-T}\underline{R} + (I-G)\underline{U}}_{X'} + \underline{E}'$$

$$FFE \equiv \Delta^{-1}G^{-T}H'^{T}$$

$$B = FBE \equiv I - G$$

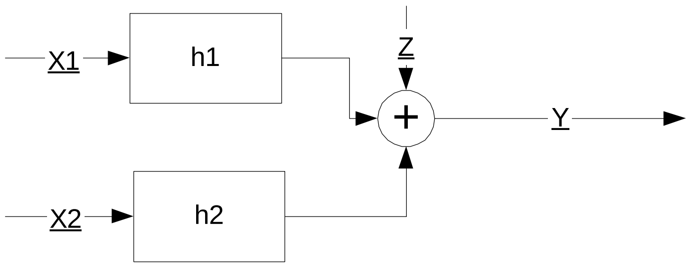
כלומר קיבלנו תצורת DFE:



ומאחר ותצורה זו מבטיחה וקטור רעש אדיטיבי בת"ס בעל רכיבים בת"ס אי שוויון הדמרד מתקיים בשוויון וניתן להגיע לקיבול מקסימלי ע"י פענוח כל הודעה בנפרד.

2. **<u>ערוץ MAC וקטורי</u>**

נניח ערוץ MAC בעל 2 כניסות וקטוריות.



כאשר:

$$\underline{Z} \sim N(0, S_{\underline{Z}})$$
$$S_1 = E\{\underline{X}_1 \underline{X}_1^T)$$
$$S_2 = E\{\underline{X}_2 \underline{X}_2^T)$$
$$tr(S_1) \le P_1$$
$$tr(S_2) \le P_2$$
$$\underline{Y} = \underline{\underline{h}}_1 \cdot \underline{X}_1 + \underline{\underline{h}}_2 \cdot \underline{X}_2 + \underline{Z}$$

תחום הקיבול נתון ע״י:

$$R_1 \le I\left(\underline{X}_1; \underline{Y} \mid \underline{X}_2\right) = h(\underline{Y} \mid \underline{X}_2) - h(\underline{Y} \mid \underline{X}1, \underline{X}_2) = h(\underline{X}_1 \cdot \underline{H}_1) - h(\underline{Z}) \le \frac{1}{2}\log\left(\frac{\left|h_1 S_1 h_1^T + S_Z\right|}{\left|S_Z\right|}\right)$$

$$R_2 \le I\left(\underline{X}_2; \underline{Y} \mid \underline{X}_1\right) \le \frac{1}{2}\log\left(\frac{\left|h_2 S_2 h_2^T + S_Z\right|}{\left|S_Z\right|}\right)$$

$$R_1 + R_2 \le I\left(\underline{X}_1, \underline{X}_2; \underline{Y}\right) \le \frac{1}{2}\log\left(\frac{\left|h_1 S_1 h_1^T + h_2 S_2 h_2^T + S_Z\right|}{\left|S_Z\right|}\right)$$

הקצב המקסימלי עבור כל משדר מתקבל כאשר המשדר השני מנוון.
שוויון אחרון מתקבל עבור כניסה גאוסית.
תחום הקיבול הינו איחוד כל הפנטגונים המתקבלים ע״י כל וקטורי הכניסה המקיימים אילוץ הספק.

נשים לב שערוץ MAC מתאים בדיוק למבנה ה-GDFE שהוצג ותחום הקיבול זהה מאחר וניתן להציג את פענוח ההודעות בתצורת GDFE, בדומה לבעית MAC, בצורה עוקבת:

$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} \Delta_{11}^{-1} & 0 \\ 0 & \Delta_{22}^{-1} \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ -G_{22}^T & I \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} + \begin{bmatrix} 0 & -G_{22} \\ 0 & 0 \end{bmatrix} \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} + \begin{bmatrix} e'_1 \\ e'_2 \end{bmatrix}$$
$$u_2 = \Delta_{22}^{-1}(-G_{22}^T \cdot r_1 + r_2) + e'_2$$
$$u_1 = \Delta_{11}^{-1} \cdot r_1 - G_{22} \cdot u_2 + e'_1$$

כלומר בשלב ראשון פענוח u_2 (u_1 נחשב כרעש) ולאחר מכן שימוש בשערוך של u_2 בפענוח u_1 ומתקבל כי:

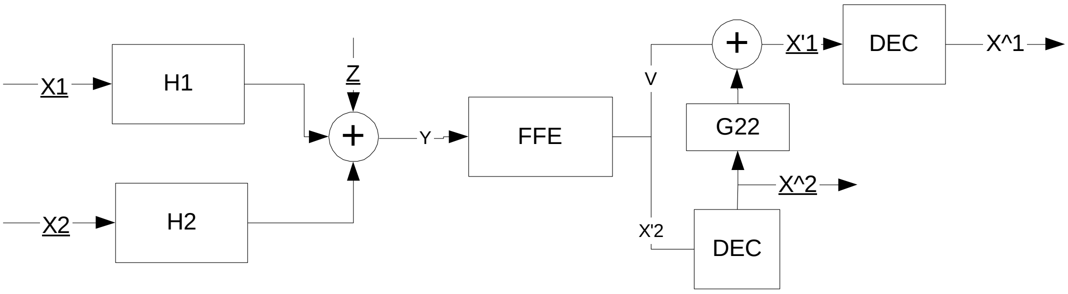
$$\begin{cases} R_1 = I(u'_1, u) = I(u_1; \underline{Y} \mid u_2) \\ R_2 = I(u'_2, u_2) = I(u_2; \underline{Y}) \\ R_1 + R_2 = I(u_1, u_2; \underline{Y}) \end{cases}$$

3. **<u>ערוץ BC וקטורי</u>**

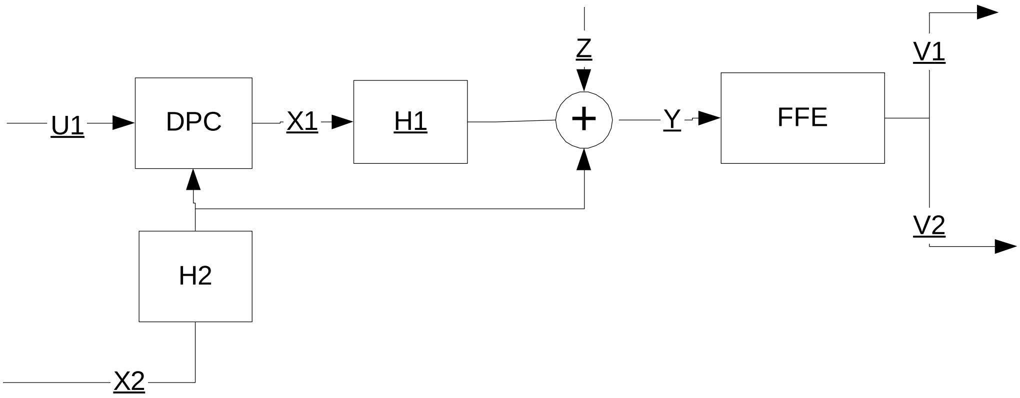
<u>דואליות בין GDFE ל – DPC</u>

באופן דומה לדואליות בין DFE ל- Tomlinson Precoder, ניתן להראות כי ישנה דואליות דומה בין GDFE ל – DPC.

סכימת GDFE:

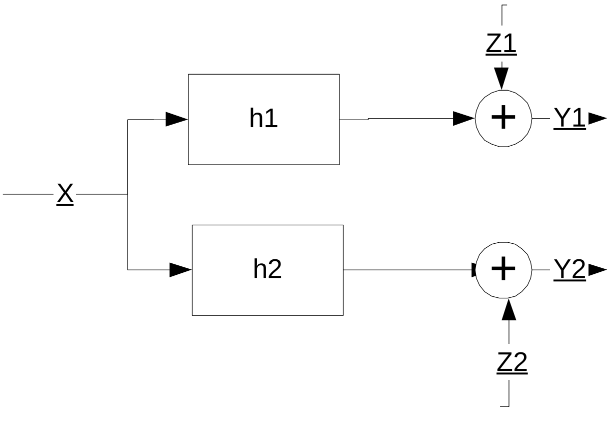


סכימת PDC הדואלית:



כאשר ע"מ שיהיה ניתן להפריד בין המשתמשים ב-BC נדרש כי FFE יהיה אלכסוני.

נניח עתה ערוץ BC בעל 2 מקלטים.



כאשר נניח ללא הגבלת הכלליות:

X – וקטור עמודה דו מימדי ממשי ($n_t=2$).

y_1,y_2 – סקלרים ממשיים ($n_{r1}=n_{r2}=1$).

$h_1=[h_{11}\ h_{12}],h_2=[h_{21}\ h_{22}]$ – וקטורי שורה דו מימדיים ממשיים.

z_1,z_2, – מ"א סקלרים ממשיים מפולגים גאוסית.

$$E\{z_1^2\} = E\{z_2^2\} = \sigma_Z^2$$
$$S_{\underline{Z}} = E\{\underline{Z}\,\underline{Z}^T\} = \sigma_Z^2 \cdot I$$
$$S_{\underline{X}} = E\{\underline{X}\,\underline{X}^T)$$
$$tr(S_{\underline{X}}) \le P$$
$$\underline{Y} = \underline{\underline{H}}X + \underline{Z} = \begin{bmatrix} \underline{h}_1 \\ \underline{h}_2 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix}$$
$$y_1 = h_{11}x_1 + h_{12}x_2 + z_1$$
$$y_2 = h_{21}x_1 + h_{22}x_2 + z_2$$

מאחר ולא ניתן להביא לצורה של degraded BC (אפילו לא statistically degraded) לא ניתן להשתמש בתחום הקיבול הידוע עבור ערוץ degraded BC אך עבור פילוג כניסה גאוסי קיים חסם עבור סכום הקצבים.

<u>מציאת סכום הקצבים:</u>

הוכחת המשפט ההפוך:

ע"פ חסם סאטו:

$$R_1 + R_2 \le \min_{\substack{S_Z \ge 0 \\ S_{Zii} = \sigma_z^2}} I(\underline{X}; y_1, y_2) = \min \frac{1}{2} \log\left(\frac{\left| \underline{\underline{H}} S_{\underline{X}} \underline{\underline{H}}^T + S_{\underline{Z}} \right|}{\left| S_{\underline{Z}} \right|} \right)$$

הוכחת השגה:

טענה: עבור פילוג כניסה גאוסי ($\underline{X}$~N(0,$S_{\underline{X}}$) הרעש הגרוע ביותר (LFN – Least Favorable Noise) מקיים:

$$S_{\underline{Z}}^{-1} - (\underline{\underline{H}} S_{\underline{X}} \underline{\underline{H}}^T + S_{\underline{Z}})^{-1} \qquad diagonal$$

הוכחה: באמצעות KKT.

טענה: עבור פילוג כניסה גאוסי (X~N(0,S_{xx}) ורעש LFN קיימת מטריצת שידור X=BU (U~N(0,I)) כך שה-FFE (ביחס לערוץ HB) בסכימת ה-PDC הינו אלכסוני.

הוכחה: אלגברית.

מסקנות:

- עבור פילוג כניסה גאוסי החסם העליון עבור סכום הקצבים מקבל מינימום עבור רעש LFN.
- במצב זה ה-FFE אלכסוני בסכימת ה-DPC ולכן ניתן להשיג את סכום הקצבים המקסימלי האפשרי (אין פגיעה בסכום הקצבים כתוצאה מהפרדת ההודעות בפענוח).
- מאחר והנ"ל נכון עבור כל $S_{\underline{X}}$ ובפרט עבור $S_{\underline{X}}$ שמביא למקסימום את סכום הקצבים.

לכן:

$$C_{SUM} = \max_{\substack{S_{XX} \\ tr(S_{XX}) \le P}} \min_{\substack{S_{ZZ} \\ S_{Zii} = \sigma_z^2 \\ S_{ZZ} \ge 0}} \frac{1}{2} \log\left(\frac{\left| \underline{\underline{H}} S_{\underline{X}} \underline{\underline{H}}^T + S_{\underline{Z}} \right|}{\left| S_{\underline{Z}} \right|} \right)$$

בבליוגרפיה:

[1] Wei Yu; Cioffi, J.M.
Sum capacity of Gaussian vector broadcast channels
Information Theory, IEEE Transactions on
Volume 50, Issue 9, Sept. 2004 Page(s): 1875 – 1892

[2] G. Caire and S. Shamai,
On the achievable throughput of a multi-antenna Gaussian broadcast channel
IEEE Trans. on Inform. Theory, Vol. 49, No. 7, pp. 1691--1706, July 2003.

[3] S. Vishwanath, N. Jindal, and A. Goldsmith,
Duality, Achievable Rates, and Sum-Rate Capacity of Gaussian MIMO Broadcast Channels
IEEE Trans. on Information Theory, Volume 49, Issue 10, pp. 2658-2668, Oct. 2003.

[4] P. Viswanath and D. Tse, IEEE
"*Sum capacity of the vector Gaussian broadcast channel and uplink-downlink duality*,"
Trans. Info Theory, pp. 1912.

[5] R. S. Cheng, S. Verdú,
"Gaussian Multiple-Access Channels with Intersymbol Interference: Capacity Region and Multiuser Water-Filling,"
IEEE Trans. on Information Theory, vol. IT-39, pp. 773-785, May 1993.

[6] W. Yu, W. Rhee, S. Boyd, and J. Cioffi,
"*Iterative water-filling for Gaussian vector multiple access channels*,"
in Proc. IEEE Int. Symp. Inf. Theory, Seattle, WA, 2001, p. 322.

הרצאה - 8

Successive Refinement and Multiple Descriptions

סוכם ע"י נדב פיין

קידוד מקור עם עיוות בשלבים (SR - Successive Refinement)

מערכת SR נראית כדלקמן (מוצג עיוות שני שלבים) –

Error! No topic specified.

במערכת זו מקודד המקור עבור משתמש איכותי (2) ועבור משתמש פחות איכותי (1). נשווה את ביצועי המערכת (מידת העיוות) למערכת ייחוס, בה הקידוד מתבצע בנפרד לשני המשתמשים:

Error! No topic specified.

במערכת הייחוס מושגת פונקצית קצב-עיוות $R(\cdot)$ במובן $R_1=R(D_1)$, $R_2=R(D_2)$, כאשר $D_2< D_1$. אם נחזור למערכת המקורית, אין זה ברור (ולרוב זה לא מתקיים), שאם $R=R(D_1)$ אזי ניתן להשיג $\Delta R=R(D_2)-R$.

הגדרה: [1] תחום קצב עיוות במערכת SR עבור מקור כלשהו –

$$R(D_1,D_2) = \text{convex closure of } \left\{(R_1,R_2);(D_1,D_2)\,\text{can be obtained with}\,(R_1,R_2)\right\}$$

הגדרה: מקור בר עידון הינו מקור שמקיים –

$$\left(R(D_1),R(D_2)\right)\in R(D_1,D_2)$$

משפט 1: מקור גאוסי עם עיוות ריבועי הוא בר-עידון.

משפט 2: במקור כלשהו עם עיוות ריבועי ניתן להתקרב עד כדי ½ ביט מפונקצית קצב-עיוות.

הוכחת 1: באופן קונסטרוקטיבי, דרך לפי המערכת הבאה –

$$\hat{\mathbf{x}}_2-\mathbf{x}=\hat{\mathbf{x}}_2-\left(\hat{\mathbf{x}}_1+\mathbf{z}\right)=\left(\hat{\mathbf{x}}_2-\hat{\mathbf{x}}_1\right)-\mathbf{z}=\hat{\mathbf{z}}-\mathbf{z}$$

יוצא שהשגיאה בקידוד העדין היא השגיאה בקידוד $\mathbf{z}$. בדחיסה (גסה) אופטימלית של $\mathbf{x}$ מתקיים – $R_1=\frac{1}{2}\log\left(\frac{\sigma_{\mathbf{x}}^2}{D_1}\right)$

בדחיסה אופטימלית של $\mathbf{z}$ מתקיים – $\Delta R\le\frac{1}{2}\log\left(\frac{D_1}{D_2}\right)$

כי השונות של **z** היא D_1, ושוויון מושג עבור **z** נורמלי. מסיכום המשווא ות מתקבל שהדחיסה העדינה אופטימלית –

$$\Delta R = \frac{1}{2}\log\left(\frac{\sigma_{\mathrm{x}}^2}{D_2}\right)\mathrm{R}+$$

□

קידוד מקור בריבוי תיאורים (Multiple Descriptions)

ניתן להגדיר בעיה כללית יותר, בעיית קידוד בריבוי תיאורים (Multiple Descriptions). כאן אין סדר בין הקידודים.

המערכת מתוארת להלן (כאן שני תיאורים) –

ניתן לחשוב על קידוד מעל רשת האינטרנט, שם כל אחד מהמצבים (קליטה של כל צירוף של תיאורים) אפשרית. אם נדרוש $D_2=\sigma_x^2$ נחזור למצב של Successive Refinement. אם נדרוש D_2 ו-D_1 קטנים מ-σ_x^2, אז ניתקל בבעיה בהשגת אופטימליות עבור D0 (במובן פונקצית קצב-עיוות) משום שההודעות (והמשערכים) יהיו קורלטיביים (וקצב 'יתבזבז').

<u>משפט [2]</u>: בהינתן חסמים על מידת עיוות D_0, D_1, ו-D_2, ניתן להשיג כל זוג קצבים מהצורה –

$$\begin{aligned} &R_1 > I(\mathbf{x};\hat{\mathbf{x}}_1) \\ &R_2 > I(\mathbf{x};\hat{\mathbf{x}}_2) \\ &R_1 + R_2 > I(\mathbf{x};\hat{\mathbf{x}}_0,\hat{\mathbf{x}}_1,\hat{\mathbf{x}}_2) + I(\hat{\mathbf{x}}_1;\hat{\mathbf{x}}_2) \end{aligned}$$

כאשר קיימת פונקצית פילוג מהצורה $p(\hat{\mathbf{x}}_0,\hat{\mathbf{x}}_1,\hat{\mathbf{x}}_2|\mathbf{x})$ עבורה מתקיימות מידות העיוות.

בתנאי השלישי מצויה הדגרדציה בביצועים במקרה של MD. עם זאת, ב-[1] מראים כיצד במקרה הנורמלי עם עיוות גבוה, ניתן להשיג את פונקצית קצב-עיוות עבור כל אחד משלושת התיאורים.

<u>משפט [2]</u>: עבור $\mathbf{x}\sim N(0,1)$ ועבור $D_1+D_2-D_0\geq 1$ ניתן להשיג כל זוג קצבים מהצורה –

$$\begin{aligned} &R_1 > \frac{1}{2}\log\left(\frac{1}{D_1}\right) \\ &R_2 > \frac{1}{2}\log\left(\frac{1}{D_2}\right) \\ &R_1 + R_2 > \frac{1}{2}\log\left(\frac{1}{D_0}\right) \end{aligned}$$

כמו כן נתון ב-[2] הפתרון למקרה של עיוות לא גבוה (שם לא מושגת פונקצית קצב-עיוות עבור D_0).

<u>קריאה נוספת:</u>

[1] – Rimoldi, "Successive refinement of information: characterization of the achievable rates", IEEE Transactions on Information Theory, VOL IT-40, No. 1, January 1994, pages 253-259

[2] – El Gamal, Cover, “Achievable Rates for Multiple Descriptions”, IEEE Transactions on Information Theory, VOL IT-28, No. 6, November 1982, pages 851-857

2008

מרצה: פרופ' רם זמיר

עורכת: מיכל שמר

הרצאה מס' 1

אופייניות וטיפוסיות, חריגות גדולות ובעיית "מעבר ספף"

סוכם ע"י רוי יוסף יבניסק

מבוא

הפוקוס המרכזי של הקורס מתמקד בבחינת תוצאות מתורת האינפורמציה עבור רשתות תקשורת. יחד עם זאת נציג שני נושאים הסוטים מהפוקוס המרכזי : תורת האינפורמציה וסטטיסטיקה , ועיוות קצב וקוונטיזציה.

מהלך השיעור

נחזור ונרחיב לגבי קבוצות אופייניות במובן החלש.

נגדיר טיפוסים, קבוצת טיפוס, וקבוצות אופייניות במובן החזק.

נדון בתורת החריגות הגדולות.

נראה כיצד ניתן להתאים את התיאוריה לבעיית "מעבר הסף".

חוק השוויון לאחרית הימים Asymptotic Equi-Partition Property (AEP)

חוק המספרים הגדולים: תזכורת **Low of Large Numbers (L.L.N)**

תהי סדרת המשתנים האקראיים הבדידים , $Z_1, Z_2, \ldots, Z_n$, מפולגים באופן בלתי תלוי ושווה פילוג , אזי מתקיים[9]:

$$\frac{1}{n}\sum_{i=1}^{n} Z_i \xrightarrow[\text{m.s.c}]{\text{a.s. \&}} E\{Z\}$$

מסקנה מחוק המספרים הגדולים

תהי סדרת המשתנים האקראיים, $X_1, X_2, \ldots, X_n$, מפולגים באופן בלתי תלוי ושווה פילוג לפי , $P(\cdot)$, אזי:

$$-\frac{1}{n}\log_2 P(X_1, X_2, \ldots, X_n) \underset{i.i.d}{=} -\frac{1}{n}\log_2 \prod_{i=1}^{n} P(X_i) =$$

$$\frac{1}{n}\sum_{i=1}^{n}\left(-\log_2 P(X_i)\right) \xrightarrow[n\to\infty]{L.L.N} E_P\left\{-\log_2 P(X_i)\right\} = H(X)$$

מתוך כך נגדיר את הקבוצה האופיינית:

$$A_{\varepsilon}^{(n)} = \left\{ x_1, x_2, \ldots, x_n : \left| -\frac{1}{n}\log_2 \Pr(x_1, x_2, \ldots, x_n) - H(X) \right| < \varepsilon \right\}$$

---

[9] להגדרה של התכנסות כמעט בוודאות, ולהתכנסות במובן ריבועי ראה נספח

תכונות:

1. מרכזת את רוב ההסתברות $\Pr\left\{A_{\varepsilon}^{(n)}\right\} > 1-\varepsilon$

2. חסם עליון על גודל הקבוצה $\left|A_{\varepsilon}^{(n)}\right| \le 2^{n(H(X)+\varepsilon)} \quad \forall n$

3. חסם תחתון על גודל הקבוצה $\left|A_{\varepsilon}^{(n)}\right| \ge (1-\varepsilon)2^{n(H(X)-\varepsilon)}$ for n sufficiently large

טיפוסים - Types

הסתברות אמפירית

תהי הסדרה, $\mathbf{x} = x_1, x_2, \dots, x_n$, נגדיר את ההסתברות האמפירית של סימבול a על ידי:

$$\frac{N(a,\mathbf{x})}{n} = \frac{\#\text{ of occurs of } a \text{ in } \mathbf{x}}{\text{length of } \mathbf{x}}$$

ניישם את חוק המספרים הגדולים על ההסתברות האמפירית:

$$\frac{N(a,\mathbf{x})}{n} = \frac{1}{n}\sum_{i=1}^{n} 1_{\{x_i=a\}} \xrightarrow[n\to\infty]{L.L.N} \Pr\{x=a\}$$

כאשר: $1_{\{x_i=a\}}$ מסמן את פונקצית האינדיקאטור.

מסקנה: מתוך חוק המספרים הגדולים נובע כי ההסתברות האמפירית שואפת , עבור n מספיק גדול, להסתברות האמיתית. בשל כך ניתן לייצר הגדרה נוספת לקבוצה אופיינית.

קבוצה אופיינית חזקה

תהי הסדרה, $\mathbf{x} = x_1, x_2, \dots, x_n$, נגדיר את הקבוצה האופיינית החזקה על ידי:

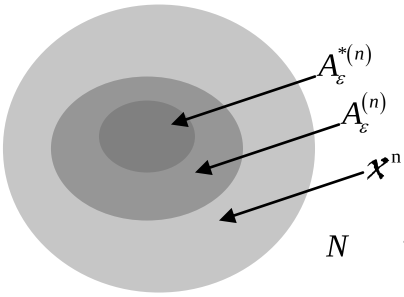
$$A_{\varepsilon}^{*(n)} = \left\{\mathbf{x} : \left|\frac{1}{n}N(a/\mathbf{x}) - \Pr(a)\right| < \varepsilon, \quad \forall a \in \mathcal{X}\right\}$$

כלומר זוהי קבוצת הסדרות שההסתברות האמפירית של כל אחד מהסימבולים מעל האלפבית , קרוב עד כדי ε להסתברות האמיתית.

היחס בין קבוצה אופיינית חזקה לחלשה

כפי שרומז השם הקבוצה האופיינית החזקה מוכלת בחלשה : $A_{\varepsilon}^{*(n)} \subset A_{\varepsilon}^{(n)}$ וזאת מכיוון שאם : $\forall x \quad \mathrm{P}(x) \approx Q(x)$ אז, בשל רציפות פונקציונאל האנטרופיה, מתקיים: $H(P) \approx H(Q)$.

הכיוון השני אינו בהכרח נכון . מקרה פרטי עבורו הכיוון השני כן מתקיים הוא המקרה של אנטרופיה בינארית. מוצג תאור גראפי הקושר בין הקבוצות.



טיפוס (ממימד n) / פילוג אמפירי של סדרה נתונה (באורך n)

תהי סדרה נתונה באורך n, מעל אלפבית $\mathcal{X}$, נגדיר את הטיפוס של הסדרה:

$$P_{\mathbf{x}} = \frac{N(a,\mathbf{x})}{n} \quad \forall a \in \mathcal{X}$$

לדוגמא עבור האלפבית : $\mathcal{X} = \{0,1,\ldots,N-1\}$, הטיפוס הינו ווקטור באורך N

המגדיר את ההסתברות האמפירית לקבלת כל אחד מהערכים האפשריים, $0,1,\ldots,N-1$:

$$P_{\mathbf{x}} = \left(\frac{N(0,\mathbf{x})}{n}, \frac{N(1,\mathbf{x})}{n}, \cdots, \frac{N(N-1,\mathbf{x})}{n}\right)$$

מרחב הטיפוסים (ממימד n)

נגדיר את אוסף ככל הטיפוסים האפשריים ממימד n: $\mathcal{P}_n$, גודל מרחב הטיפוסים ניתן לחסימה על ידי:

$$|\mathcal{P}_n| < (n+1)^{|\mathcal{X}|}$$

כלומר הוא פולינומיאלי באורך הסדרה . הבחן כי מספר הסדרות האפשריות , לעומת זאת , אקספוננציאליות באורך הסדרה.

לדוגמא עבור האלפבית $\mathcal{X} = \{0,1\}$:

$$\mathcal{P}_n = \left\{(0,1), \left(\tfrac{1}{n}, \tfrac{n-1}{n}\right), \ldots, \left(\tfrac{i}{n}, \tfrac{n-i}{n}\right), \ldots, (1,0)\right\}$$

גודל המרחב נתון על ידי: $|\mathcal{P}_n| = n+1$.

קבוצת הטיפוס

קבוצת הטיפוס ממימד כלשהו, עבור טיפוס כלשהו, מוגדרת כאוסף הסדרות שהפילוג האמפירי שלהן נתון על ידי הטיפוס:

$$T(P) = \{\mathbf{x} : P_{\mathbf{x}} = P\}, \quad P \in \mathcal{P}_n$$

גודל קבוצת הטיפוס נתונה על ידי:

$$|T(P)| = \binom{n}{nP_1 \quad nP_2 \quad \cdots \quad nP_{|\mathcal{X}|}}$$

לדוגמא עבור האלפבית $\mathcal{X} = \{0,1\}$, ו-$n=3$ קבוצת הטיפוס עבור הטיפוס, $P = \left(\tfrac{1}{3}, \tfrac{2}{3}\right)$ נתונה על ידי:

$$T(P) = \{(1,0,0), (0,1,0), (0,0,1)\}$$

וגודל קבוצת הטיפוס נתון על ידי:

$$|T(P)| = \binom{3}{3\cdot\tfrac{1}{3} \quad 3\cdot\tfrac{2}{3}} = \frac{3!}{1!2!} = 3$$

קרוב לגודל קבוצת הטיפוס

ניתן לראות כי:

$$\binom{n}{nP_1 \quad nP_2 \quad \cdots \quad nP_{|\mathcal{X}|}} \approx 2^{n\left[H(P)\pm\varepsilon\right]} \doteq 2^{nH(P)}$$

על ידי שימוש בנוסחת Sterling מתקבל חסם הבא לגודל קבוצת הטיפוס:

$$\frac{2^{nH(P)}}{(n+1)^{|\mathcal{X}|}} < \left|T(P)\right| < 2^{nH(P)}$$

ניתן להבחין כי הביטוי $(n+1)^{|\mathcal{X}|}$ הוא תת-אקספוננציאלי, כלומר הוא ניתן להצגה:

$$(n+1)^{|\mathcal{X}|} = 2^{n\left[-\frac{|\mathcal{X}|}{n}\log_2(n+1)\right]}$$

ביחס לביטוי אקספוננציאלי, נניח $2^{nH(P)}$, הוא שואף לאפס עבור n מספיק גדול.

הסתברות לסדרה מסוימת מטיפוס P המוגרלת לפי פילוג Q

תהי הסדרה $\mathbf{x} = x_1, x_2, \ldots, x_n$, סדרת המוגרלת באופן בלתי תלוי ושווה פילוג לפי הפילוג $Q(x)$, נראה כי הסתברות הסדרה תלויה בטיפוס אליו היא משתייכת בלבד:

$$Q(\mathbf{x}) = Q(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} Q(x_i) = \prod_{a\in\mathcal{X}} Q(a)^{N(a/\mathbf{x})} = \prod_{a\in\mathcal{X}} Q(a)^{nP_X} =$$

$$= 2^{n\sum_{a\in\mathcal{X}} P_X(a)\log Q(a)} = 2^{n\left[\sum_{a\in\mathcal{X}} P_X(a)\log Q(a) - \sum_{a\in\mathcal{X}} P_X(a)\log P_X(a) + \sum_{a\in\mathcal{X}} P_X(a)\log P_X(a) +\right]} = 2^{-n\left[D(P_X\|Q)+H(P_X)\right]}$$

הסתברות לסדרה כלשהי מטיפוס P המוגרלת לפי פילוג Q

אינטואיציה: הדיון הקודם עסק בהסתברותה של סדרה מסוימת השייכת לטיפוס P והוגרלה על ידי Q.
הדיון כעט יעסוק בהסתברות לקבלת סדרה כלשהי, השייכת לטיפוס P, נכנה זאת "הסיכוי לטיפוס".

$$\Pr\left\{\mathbf{x}\in T(P)\right\} = \sum_{\mathbf{x}\in T(P)} Q(\mathbf{x}) \underset{(1)}{=} \left|T(P)\right| \cdot Q(\mathbf{x}) = \left|T(P)\right| 2^{-n\left[D(P_X\|Q)+H(P_X)\right]} \underset{(2)}{\doteq} 2^{-nD(P_X\|Q)}$$

משוואה (1) נובעת מהדיון הקודם, מהמסקנה כי כל סדרה בטיפוס שוות הסתברות, שתלויה רק בטיפוס.

משוואה (2) נובעת מהחסם שהגדרנו לגודל קבוצת הטיפוס: $\left|T(P)\right| \doteq 2^{nH(P)}$

מסקנה: ההסתברות של קבוצת טיפוס היא מונוטונית לקרבה שלה לפילוג האמיתי. ככל שהטיפוס קרוב יותר, במובן הדיוורגנס, כך ההסתברות של הטיפוס תשאף לאפס לאט יותר. כמקרה קצה, קבוצת הטיפוס של הפילוג האמיתי $Q(\bullet)$ שואפת ל-1. תוצאה זו מאשררת את ההגדרה שלנו לקבוצה אופיינית במובן החזק, אוסף הטיפוסים שקרובים ל-$Q(\bullet)$.

ההסתברות להתחזות של זוג סדרות

אינטואיציה: נחבר את התוצאות שראינו עד כה לאינפורמציה ההדדית.

ידוע כי האינפורמציה ההדדית מקיימת:

$$I(X;Y)=\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}p(x,y)\log_2\frac{p(x,y)}{p(x)p(y)}=D\left(p(x,y)\|p(x)p(y)\right)$$

$$\text{Where:}\quad X,Y:p(x,y);\quad p(x)=\sum_{y\in\mathcal{Y}}p(x,y);\quad p(y)=\sum_{x\in\mathcal{X}}p(x,y)$$

נגריל זוג סדרות באופן בלתי תלוי ושווה פילוג לפי $p(x),p(y)$:

$$x_i\sim i.i.d.\ p(x);\quad y_i\sim i.i.d.\ p(y)$$

הסיכוי שהטיפוס המשותף ל- $\mathbf{x},\mathbf{y}$ שווה להסתברות המשותפת $P_{XY}(\mathbf{x},\mathbf{y})$ (למרות שהם בת"ס) הוא:

$$\Pr\left\{P_{XY}(\mathbf{x},\mathbf{y})=p(x,y)\right\}=2^{-nD\left(p(x,y)\|p(x)p(y)\right)}=2^{-nI(X;Y)}$$

כאשר $P_{XY}(\mathbf{x},\mathbf{y})$ הוא הטיפוס המשותף של $\mathbf{x},\mathbf{y}$.

ההסתברות להתחזות של זוג סדרות כאשר אחת הסדרות נתונה

התכונה הקודמת נכונה גם במקרה שבו אחת הסדרו ת נתונה, והסדרה השנייה מוגרלת כך שהיא אופיינית ביחס לפילוג השולי:

$$\Pr\left\{\mathbf{y}\text{ is strongly typical with }\mathbf{x}\text{ where }P_{\mathbf{x}}=p(\mathbf{x})\text{ w.r.t }p(\mathbf{x},\mathbf{y})\right\}=2^{-nI(X;Y)}$$

אקספוננט ספף הצלחה

תהי סידרה של 2^{nR} ניסויים בלתי תלויים כאשר הסיכוי להצלחה מוגדר על ידי 2^{-nr}. ההסתברות לקבלת הצלחה בניסוי אחד לפחות מקיימת:

$$\mathrm{P}_{success} \xrightarrow[n\to\infty]{} \begin{cases} 1 & R > r \\ 0 & R < r \end{cases}$$

<u>השלכות מוכרות של אקספוננט ספף הצלחה</u>

- השגת האינפורמציה ההדדית על ידי קוד אקראי:

יהי ספר הקוד $M = 2^{nR}, \quad CodeBook = \{\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(M)\}$ כאשר x_i מוגרל באופן בלתי תלוי ושווה פילוג לפי $p(x)$. ההסתברות ל"הצלחה", עבור קידוד ערוץ זהו למעשה כישלון, שווה:

$$P_{success} = \Pr\{\mathbf{x}(i) \text{ failed or another } \mathbf{x}(\mathrm{j}) \text{ was jointly typical with } \mathbf{y}\}$$

הסיכוי ש $\mathbf{x}(i)$ נכשל, הוא הסיכוי שה- $\mathbf{y}$ שנוצר אינו אופייני במשותף עם ה- $\mathbf{x}$ שייצר אותו, $(\mathbf{x},\mathbf{y}) \notin A_\varepsilon^{*(n)}$. הסיכוי הזה לפי הגדרת הקבוצה האופיינית שווה ל- ε.

הסיכוי להתחזות, כלומר ש- $\mathbf{x}(\mathrm{j})$ אחר שהוגרל באופן בלתי תלוי שווה פילוג לפי $p(\mathbf{x})$, והוא אופייני ביחס ל- $p(\mathbf{x},\mathbf{y})$ שווה $2^{-nI(X;Y)}$. ובסה"כ:

$$P_{success} = \varepsilon + \Pr\left\{\text{impersonating in } 2^{nR} \text{ experiments with success probability } 2^{-nI(X;Y)}\right\} =$$

$$\varepsilon + 2^{-n[I(X;Y)-R]} \xrightarrow[n\to\infty]{} \begin{cases} 1 & R > I(X;Y) \\ 0 & R < I(X;Y) \end{cases}$$

- קידוד מקור:

יהי המקור x_i המוגרל באופן בלתי תלוי ושווה פילוג לפי $p(x)$, נציע את "ערוץ המבחן":

$$p(x) \to \boxed{p(\hat{x}/x)} \to p(\hat{x})$$
$$\text{where: } E_{p(x,\hat{x})}\{d(\hat{x},x)\} < D$$

כאשר $d(\hat{x},x)$ הוא מדד העיוות.

יהי ספר הקוד $M = 2^{nR}, \quad CodeBook = \{\hat{\mathbf{x}}(1), \hat{\mathbf{x}}(2), \ldots, \hat{\mathbf{x}}(M)\}$, כאשר $\hat{x}$ מתפלג באופן בלתי תלוי ושווה פילוג לפי $p(\hat{x})$. ההסתברות ל"הצלחה" במקרה הזה, עבור קידוד המקור מילה שמצליחה להתחזות מהווה מקרה טוב עבורנו:

$$\Pr\left\{\begin{matrix} \mathbf{x} \text{ drawn by the source is not typical or} \\ \text{the } CodeBook \text{ has no word jointly typical with } \mathbf{x} \end{matrix}\right\} \xrightarrow[n\to\infty]{} \begin{cases} 1 & R < I(X;\hat{X}) \\ 0 & R > I(X;\hat{X}) \end{cases}$$

תורת החריגות הגדולות - Large Deviations

דוגמא

יהי משתנה אקראי המתפלג: $x_i \sim Bernulli\left(\frac{1}{3}\right)$

מהו הסיכוי לקבל לפחות 75 מופעים של '1' בניסוי ?

<u>חישוב מלא:</u>

$$\binom{100}{25}\left(\frac{1}{3}\right)^{75}\left(\frac{2}{3}\right)^{25}+\binom{100}{24}\left(\frac{1}{3}\right)^{76}\left(\frac{2}{3}\right)^{24}+\cdots=\sum_{k=75}^{100}\binom{100}{k}\left(\frac{1}{3}\right)^{k}\left(\frac{2}{3}\right)^{100-k}$$

<u>גישות מקורבות:</u>

משפט הגבול המרכזי:

$$\frac{1}{N}\sum_{n=1}^{N}x_i \approx N\left(\frac{1}{3},\frac{\operatorname{var}(x_i)}{n}\right)=N\left(\frac{1}{3},\frac{\frac{2}{9}}{n}\right)$$

נבחין כי ככל ש- n גדל השונות קטנה, אנו מנסים לשערך את ההסתברות של מאורע מאוד נדיר , שנופל הרבה סטיות תקן מהממוצע. ככל שאנו מתרחקים מהממוצע הקרוב הגאוסי פחות טוב. לפיכך בכדי לבחון מקרי קצה הקרוב הגאוסי לא מתאים.

<u>גישת Large Deviations:</u> $P_{(0.75,0.25)} \approx 2^{-100\cdot D\left(0.75,0.25 \| \frac{1}{3},\frac{2}{3}\right)}$

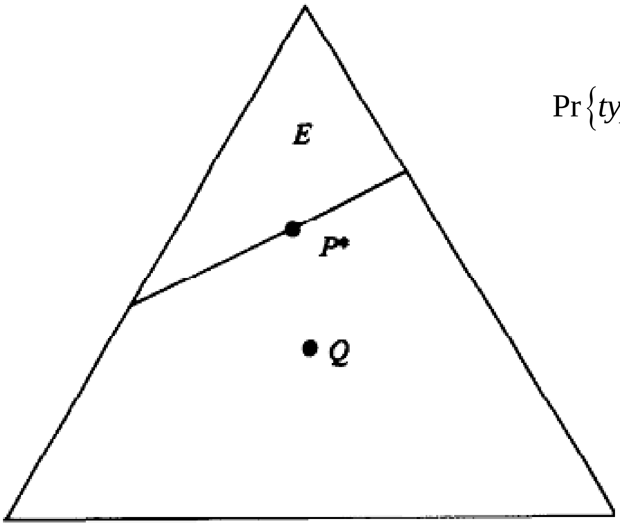
זהו גודל קל לחישוב !

משפט סאנוב

נבחין כי טיפוסים הם ווקטורים ממימד האלפבית השייכים לסימפלקס ממימד האלפבית פחות אחד . נתון תחום של פילוגים בסימפלקס, E , כאשר התחום מקיים שהוא הסגור של הפנים שלו, תחום עם נפח בכל מקום. תהי הסדרה $X_1, X_2, \ldots, X_n$ סדרת משתנים אקראיים המוגרלת באופן בלתי תלוי ושווה פילוג לפי הפילוג $Q(x) \notin E$ אזי:

$$\Pr\left\{type\left(X_1, X_2, \ldots, X_n\right)\in E\right\} \sim 2^{-nD^*} \sim 2^{-nD\left(P^* \| Q\right)}$$

כאשר $D^* = \min_{P\in E} D\left(P \| Q\right)$



איור: סימפלקס ההסתברות ומשפט סאנוב.

(מתוך Cover)

דוגמא

נחזור לדוגמא בפתיחת הנושא ונגדיר את הקבוצה $E=\left\{\left(p,1-p\right):p\geq 0.75\right\}$

עבור הגדרה זו $D^{*}=\min_{(p,1-p)\in E} D\left(p,1-p\|\tfrac{1}{3},\tfrac{2}{3}\right)=D\left(0.75,0.25\|\tfrac{1}{3},\tfrac{2}{3}\right)$ לפיכך

$$P_{(0.75,0.25)}\doteq 2^{-100\cdot D\left(0.75,0.25\|\frac{1}{3},\frac{2}{3}\right)}$$

הרחבה לכל תחום

לכל תחום בסימפלקס E מתקיים:

$$2^{-nD^{*}}\leq \Pr\left\{type\left(X_1,X_2,\ldots,X_n\right)\in E\right\}\leq\left(n+1\right)^{|\mathcal{X}|}2^{-nD^{*}}$$

<u>הוכחה</u>

חסם עליון:

$$\Pr\left\{type\left(X_1,X_2,\ldots,X_n\right)\in E\right\}=\sum_{\mathbf{x}:type(\mathbf{x})\in E}p\left(x\right)=\sum_{P\in E\cap\mathcal{P}_n}\Pr\left\{type\left(\mathbf{x}\right)=P\right\}\underset{(1)}{\leq}$$

$$\sum_{P\in E\cap\mathcal{P}_n}2^{-nD(P\|Q)}\underset{D(P\|Q)\geq D(P^{*}\|Q)}{\leq}\sum_{P\in E\cap\mathcal{P}_n}2^{-nD(P^{*}\|Q)}\underset{(2)}{\leq}\left(n+1\right)^{|\mathcal{X}|}2^{-nD(P^{*}\|Q)}=\left(n+1\right)^{|\mathcal{X}|}2^{-nD^{*}}$$

כאשר (1) הוא ההסתברות לקבוצת הטיפוס ו-(2) הוא החסם למספר הטיפוסים עבור סדרה באורך n.

חסם תחתון:

תמיד ניתן לחסום על ידי גו דל אחד מתוך הסכום , נבחר את האיבר הגדול ביותר לקבלת חסם הדוק יחסית:

$$\Pr\left\{type\left(X_1,X_2,\ldots,X_n\right)\in E\right\}=\sum_{\mathbf{x}:type(\mathbf{x})\in E}p\left(x\right)\geq 2^{-nD^{*}}=2^{-nD(P^{*}\|Q)}$$

$$\text{where }\min_{P\in E\cap\mathcal{P}^{n}}D\left(P\|Q\right)$$

דוגמא: מעבר סף

בעיית מעבר הסף מופיעה במגוון רחב של מקרים:

א. 75 אחוזי ומעלה של הצלחה בהטלה מטבע n פעמים.

ב. גלישת מונה הגעות פואסוניות:

$$N_{t_o}>N_{\max}\quad\Leftrightarrow\quad\sum_{n=1}^{N_{\max}}x_i<t_o\,,\quad\text{where } x_i\sim\text{exponential}$$

ג. שגיאה בגילוי נראות מרבית בין שתי היפותזות:

$$L.L.R.\quad:\quad\log\frac{p\left(y_1,y_2,\ldots,y_n/H_0\right)}{p\left(y_1,y_2,\ldots,y_n/H_1\right)}\underset{<}{\overset{>}{}}T$$

או עבור מודל חסר זיכרון:

$$L.L.R. \quad : \quad \sum_{i=1}^{n} \log \frac{p(y_i / H_0)}{p(y_i / H_1)} \underset{<}{>} T$$

מכיוון שבעיות חריגה מסף מופיעות בהרבה יישומים נשקיע מעט זמן בחישוב של

$D^* = \min_{P \in E} D(P \| Q)$ עבורן.

<u>הגדרת הבעיה</u>

נתון מומנט כלשהו, $m(x)$, ונשאל מהו הסיכוי להתרחשות המאורע הנדיר המוגדר על ידי:

$$\frac{1}{n} \sum_{i=1}^{n} m(x_i) \geq t$$

כאשר הסדרה $\{x_i\}_{i=1}^{n}$ מוגרלת באופן בלתי תלוי ושווה פילוג לפי $Q(x)$. בהתאמה לסאנוב נגדיר את

הקבוצה: $E = \left\{ p(x) : \sum_x p(x) m(x) \geq t \right\}$

על פי המשפט ההסתברות לחריגה נתונה על ידי

$$\Pr\{type(X_1, X_2, \ldots, X_n) \in E\} \doteq 2^{-nD^*}$$

כאשר: $D^* = \min_{p(x) \in E} \sum_x p(x) \log \frac{p(x)}{Q(x)}$

מכיוון שפונקצית הדיוורגנס קמורה וכן התחום, תת תחום של הסימפלקס, קמור, ניתן לכתוב את הביטוי ללגראנז'יאן. הפתרון האופטימאלי מתקבל עבור הלגראנז'יאן באילוץ:

$$J = \sum_x p(x) \log \frac{p(x)}{Q(x)} + \underbrace{\lambda \sum_x p(x) m(x)}_{(1)} + \underbrace{\mu \sum_x p(x)}_{(2)}$$

כאשר (1) זהו האילוץ שהקבוצה E מאלצת, בעוד (2) זהו תנאי הכרחי לפונקצית פילוג, סכום הסתברויות שווה 1, נקודה על הסימפלקס.

מתקבל:

$$p^*(x) = \frac{Q(x) e^{\lambda m(x)}}{\sum_x Q(x) e^{\lambda m(x)}}$$

כאשר את λ נבחר כך שהאילוץ מהקבוצה E מתקיים בשוויון:

$$\sum_x p(x) m(x) = t$$

הגישה הסטטיסטית

ישנן שתי אסכולות מרכזיות להתמודדות עם תורת החריגות הגדולות . שיטת הדיוורגנס איננה שיטה קלאסית בסטטיסטיקה. בסטטיסטיקה נהוג להתייחס לאי שיוויונים הבאים: מרקוב ← צ'ביצ'ב ← צ'רנוב. כיסוי נרחב לנושא זה ניתן למצוא בספר של גאלאגר. נסקור שיטה זו ונראה כי היא מביאה לפתרון זהה.

אי שוויון מרקוב

יהי Y משתנה אקראי אי שלילי בעלת תוחלת $E\{Y\}$, אזי:

$$\Pr\{Y>t\}\le\frac{E\{Y\}}{t}$$

עבור $Y=\frac{1}{n}\sum_{i=1}^{n}X_i$:

$$\Pr\{Y>t\}=\Pr\left\{\frac{1}{n}\sum_{i=1}^{n}X_i>t\right\}\le\frac{E\left\{\frac{1}{n}\sum_{i=1}^{n}X_i\right\}}{t}\underset{i.i.d.}{=}\frac{E\{X_i\}}{t}$$

לצערנו הפתרון אינו תלוי ב-n.

אי שוויון צ'ביצב

יהי Y משתנה אקראי אי שלילי בעלת תוחלת $E\{Y\}$ ושונות $\operatorname{var}(Y)$, אזי:

$$\Pr\left(\left[Y-E\{Y\}\right]^2>\Delta^2\right)\le\frac{\operatorname{var}(Y)}{\Delta^2}$$

עבור $Y=\frac{1}{n}\sum_{i=1}^{n}X_i$:

$$\Pr\left(\frac{1}{n}\sum_{i=1}^{n}X_i>\underbrace{\Delta^2+E\{X\}}_{t}\right)\underset{i.i.d}{\le}\frac{\frac{1}{n}\operatorname{var}(X)}{\left(t-E\{X\}\right)}$$

לצערנו החסם יורד ליניארית ב-n. אנו מצפים לירידה אקספוננציאלית.

אי שוויון צ'רנוב

ננסח את אי שוויון מרקוב באופן הבא:

$$\Pr\{\phi(Y)>\alpha\}\le\frac{E\{\phi(Y)\}}{\alpha}$$

אנו מתעניינים ב- Y המהווה סכום משתנים אקראיים , נתעלם מגורם הנרמול , ולכן כד אי לבחור את $\phi(Y)$ באופן הבא: $\phi(Y)=e^{sY}$

כיוון שאז:

$$E\left\{\phi(Y)\right\}=E\left\{e^{sY}\right\}=E\left\{e^{s\sum_{i=1}^{n}X_i}\right\}=E\left\{\prod_{i=1}^{n}e^{sX_i}\right\}\underset{i.i.d}{=}\prod_{i=1}^{n}E\left\{e^{sX}\right\}=\left[E\left\{e^{sX}\right\}\right]^n$$

כלומר:

$$\Pr\left\{\phi(Y)>\alpha\right\}=\Pr\left\{e^{s\sum_{i=1}^{n}X_i}>\underset{\alpha}{e^{stn}}\right\}\underset{s>0}{=}\Pr\left\{\frac{1}{n}\sum_{i=1}^{n}X_i>t\right\}\leq\left[\frac{E\left\{e^{sX}\right\}}{e^{st}}\right]^n$$

ולסיכום:

$$\Pr\left\{\frac{1}{n}\sum_{i=1}^{n}X_i>t\right\}\leq\left[\frac{E\left\{e^{sX}\right\}}{e^{st}}\right]^n\quad\forall s>0$$

זוהי משפחת חסמים פרמטרית, s , ניתן להראות כי עבור $s=s_{opt}$ מתקבל סאנוב למקרה המקביל.

השוואה בין סאנוב לצ'רנוב

חסם צ'רנוב מתאים לסדרות מ"א בדידים ורציפים כאחד. ניתן לקבל חסמים גם במקרה והסדרה מתפלגת באופן שאינו שווה פילוג, וכן במקרים בהם הגרלות תלויות.

החסם של סאנוב מאפשר הגדרה של קבוצה E דיסקרטית כללית ביותר. ובכך ניתן לפתור מספר רב של בעיות, כאשר לכל בעיה נתאים קבוצה E מתאימה. כמו כן , סאנוב מאפשר להבין את ה "פיזיקה" שמאחורי הפיתוח. למשל, סאנוב נותן השראה למשפט הגבול המותנה, המתואר בפרק הבא.

משפט הגבול המותנה - Conditional Limit Theorem

תהי E תת קבוצה סגורה וקמורה של $\mathcal{P}$ ותהי ההסתברות $Q(x)$ שאיננה שייכת לקבוצה, $Q(x) \notin E$. תהי $x_1, x_2, \ldots, x_n$ סדרת משתנים אקראיים בלתי תלויים סטטיסטית המתפלגים באופן שווה פילוג לפי $Q(x)$. יהי P^* הפילוג המגשים: $P^* = \min_{P \in E} D(P \| Q)$

אזי מתקיים:

$$\Pr\left\{x = a \mid P_{x^n} \in E\right\} \xrightarrow[n\to\infty]{\text{in probability}} P^*(a)$$

כלומר ההסתברות השולטת על קבוצת המאורעות הנדירים E, הנתונה על ידי P^*, מגדירה גם את הסתברות הסימבול בהינתן שהתרחש המאורע הנדיר.

<u>הערה:</u> גם הפילוג המשותף של קבוצה סופית של דגימות $x_1, x_2, \ldots, x_M$ כאשר M אינו עולה עם n שואף בהתניה ל- P^* $i.i.d$.

נספח: התכנסות סדרות

התכנסות אלגברית (דטרמיניסטית)

הסדרה $\{x[n]\}_n$ מתכנסת לערך x אם $\forall \varepsilon > 0$ קיים n_0 כך ש- $\forall n > n_0$ מתקיים $|x[n] - x| < \varepsilon$

ונסמן: $\lim_{n\to\infty} x[n] = x$

משמעות גיאומטרית: ניתן לצייר שרוול בעובי 2ε סביב x והחל מ- n_0 כל ה-$x[n]$ נופלים בפנים.

התכנסות סטוכאסטית:

- בכל מקום, everywhere (e), או בוודאות, sure (s) אם[10]:

$$\lim_{n\to\infty} x_n(\zeta) = x(\zeta), \quad \forall \zeta$$

אינטואיציה: כל הגרלה היא סדרה מתכנסת (בפני עצמה).

- כמעט בכל מקום, almost everywhere (ae), או כמעט בוודאות, almost sure (as) אם:

$$\Pr\left(\lim_{n\to\infty} x_n(\zeta) = x(\zeta)\right) = 1$$

נסמן: $\Pr\{x_n \to x\} = 1$

---

[10] ζ מסמן גורם אקראיות, ניתן לחשוב עליו כאינדקס של פונקציות המדגם האפשריות, x_n מסמן את האיבר ה- nי בסדרה.

▪ במובן של ממוצע ריבועים, mean square convergence (m.s. conv') אם:

$$E\left(\left[x_n(\zeta)-x(\zeta)\right]^2\right)\xrightarrow[n\to\infty]{}0$$

נסמן: $\underset{\substack{n\to\infty \\ (\lim.in.ms)}}{l.i.m}\ x_n(\zeta)\to x(\zeta)$

אינטואיציה: אוספים את הסטטיסטיקה של האיברים ה- nים, כש-n שואף לאינסוף, האנרגיה, ממוצע ריבועים, של השגיאה של ערך זה מהגבול של הסדרה שואף לאפס.

▪ בהסתברות (P), with probability p אם:

$$\Pr\left(\left|x_n(\zeta)-x(\zeta)\right|>\varepsilon\right)\xrightarrow[n\to\infty]{}0,\quad \forall\varepsilon>0$$

ניתן לדייק:

$$\lim_{n\to\infty}\left\{\Pr\left(\left|x_n(\zeta)-x(\zeta)\right|>\varepsilon\right)\right\}=0,\quad \forall\varepsilon>0$$

אינטואיציה: סדרת ההסתברויות שהמרחק בין איבר n לגבול הסדרה גדול מ- ε שואף לאפס, כש - n שואף לאינסוף.

<u>נבחין:</u>

X_n הוא משתנה אקראי המציין את האיבר ה-nי של סדרה.

$x_n(\zeta)$ גם הוא האיבר ה-nי של סדרה, אלא שהפעם העברנו את גורם האקראיות להיות ζ, הוא האינדקס של פונקצית המדגם. ההבדל הוא בכך שידיעת X_n לא חושפת את כל הסדרה, בעוד ידיעת ζ מספקת את כל פונקצית המדגם.

הרצאה מס' 2

***שימוש בסאנוב לבחינת השערות*, אקספוננט השגיאה לפענוח בערוץ רועש, ואי שיוויונים אינפורמציוניים**

סוכם ע"י רוי יוסף יבניסק

שימוש בסאנוב לבחינת השערות - Hypothesis Testing via Sanov

יישומים

בעיית המכ"ם

בהינתן האות:

$$y(t) \quad 0 \le t \le T$$

נדרשת היכולת להפריד בין שני מצבים:

$$H_1 \quad : \quad y(t) = \text{noise}$$
$$H_2 \quad : \quad y(t) = \text{noise} + \text{signal}$$

לעיתים תינתן הסתברות אפריורית $\Pr(\text{signal})$.

בעיית התקשורת הבינארית

בהינתן האות: $y(t) \quad 0 \le t \le T$

נדרשת היכולת להפריד בין שתי מילות הקוד:

$$H_1 \quad : \quad y(t) = \text{noise} + \text{codeword1}$$
$$H_2 \quad : \quad y(t) = \text{noise} + \text{codeword2}$$

שייכות לקבוצה, זמן בדיד:

בהינתן המדידה: $\mathbf{x} = [x_1, x_2, \ldots, x_n]$

וחלוקת המרחב ה-n ממדי: $\mathcal{X}^n = A \cup A^c$

נדרשת היכולת לקבוע לאיזו קבוצה המדידה שייכת:

$$H_1 \quad : \quad \mathbf{x} \in A$$
$$H_2 \quad : \quad \mathbf{x} \in A^c$$

הסתברויות שגיאה

עבור המקרה הבינארי, כלומר המקרה בו יש להפריד בין שתי היפותזות, ניתן להגדיר שני סוגי שגיאה:

$$\alpha = \Pr\{\mathbf{x} \in A / H_2 \text{ is true}\}$$
$$\beta = \Pr\{\mathbf{x} \in A^c / H_1 \text{ is true}\}$$

כאשר הראשון מתייחס לאי גילוי, ואילו השני לגילוי שווא.

קריטריוני הגילוי

בבואנו לפתור את בעיית בחינת ההשערות עלינו להגדיר מגבלות על הסתברויות השגיאה . מגבלות שונות יובילו לפתרונות שונים. נראה שלוש דוגמאות להגבלות שכיחות:

א. שגיאה אחת קריטית ואחרת פחות קריטית:

$$\begin{aligned} \alpha_n &= \alpha(n) < \varepsilon \\ \beta_n &= \beta(n) \doteq 2^{-nD} \end{aligned} \qquad \forall n$$

במקרה זה α_n היא השגיאה הפחות קריטית, השגיאה הקריטית, β_n, דועכת אקספוננציאלית עם n.

ב. זוג השגיאות קריטיות:

$$\begin{aligned} \alpha_n &= \alpha(n) \doteq 2^{-nD_1} \\ \beta_n &= \beta(n) \doteq 2^{-nD_2} \end{aligned} \qquad \forall n$$

הבחן, ניתן לקבוע את היחס בניהן על ידי קביעה מתאימה של D_1, D_2.

ג. הבעיה הבייסיאנית:

בהינתן זוג הסתברויות אפריוריות π_1, π_2, נשאף להביא למינימום את הסתברות השגיאה:

$$\overline{P}_e = \pi_1 \alpha_n + \pi_2 \beta_n \qquad \forall n$$

הלמה של ניימן ופירסון - Neyman Pearson Lemma

תנאי ההחלטה האופטימאלי, ביחס לכל אחד מקריטריוני הגילוי, הוא תמיד מהצורה:

$$\frac{\Pr(\mathbf{x}/H_1)}{\Pr(\mathbf{x}/H_2)} \underset{<}{\overset{>}{}} T$$

עבור סף מתאים, T, הנקבע לפי הקריטריון הנבחר.

פתרון לבעיית בחינת ההשערות באמצעות טיפוסים

נגדיר מודל המתאים לשיטת הטיפוסים. תהנה סט הדגימות: $x_1, x_2, x_3, \ldots$ המפולגות לפי:

$$\mathbf{x} \underset{i.i.d}{\sim} \begin{cases} p_1 & : \quad H_1 \\ p_2 & : \quad H_2 \end{cases}$$

פונקצית הפילוג המותנית בהשערה:

$$p(\mathbf{x}/H_j) = \prod_i p(x_i/H_j)$$

כלל ההחלטה הלוגריתמי של ניימן פירסון מקבל את הצורה:

$$\frac{1}{n}\sum_{i=1}^{n} \log \frac{p_1(\mathbf{x})}{p_2(\mathbf{x})} \underset{<}{\overset{>}{}} \frac{1}{n}\log T \triangleq t$$

נסמן את ההסתברות האמפירית, הטיפוס, של כל סימבול x עבור הדגימה $\mathbf{x}$ על ידי:

$$P_{\mathbf{x}}(x) \quad \forall x \in \mathcal{X}$$

ונכתוב את כלל ההחלטה במונחי הדיוורגנס:

$$\sum_{x\in\mathcal{X}} P_{\mathbf{x}}(x)\log\frac{p_1(x)}{p_2(x)} = D(P_{\mathbf{x}} \| p_2) - D(P_{\mathbf{x}} \| p_1) \gtrless t$$

אינטואיציה: נבחן לאיזה טיפוס שייכת הדגימה אותה אנו מעוניינים לסווג , נבחן את המרחק , במובן הדיוורגנס, בין שני הטיפוסים של ההיפותזות, נסווג את הדגימה בהתאם להפרש המרחקים, כאשר הסף t שקובע כיצד נסווג נקבע על פי קריטריון הגילוי.

ניתוח הסף

נגדיר את המשתנה האקראי:

$$LLR_i = \log\frac{p_1(x_i)}{p_2(x_i)} = z_i \quad i = 1,2,\dots,n$$

נשאלת השאלה, תחת היפותזה H_1 מהי ההסתברות שסכום המשתנים האקראיים Z_i, שהגדרנו לעיל יחצה סף . כלומר מאורע השגיאה , β, שקול למאורע "נדיר" של מעבר סף של ממוצע המדגם , $\frac{1}{n}\sum_{i=1}^{n} z_i$. בעיה זו מזכירה את בעית הסף.

Stein's Lemma - הלמה של סטיין

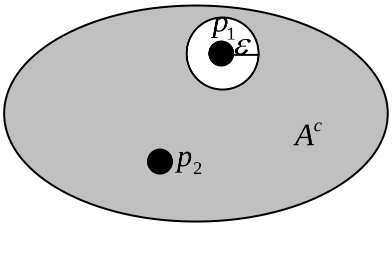
עבור קריטריון הגילוי:

$$\begin{aligned} \alpha_n &= \alpha(n) < \varepsilon \\ \beta_n &= \beta(n) \doteq 2^{-nD} \end{aligned} \quad \forall n$$

מתקבל:

$$\beta_n = \Pr\{\text{Decide } H_1 \text{ given } H_2\} \doteq 2^{-nD(p_1\|p_2)}$$

משמעות גיאומטרית:



כאשר $n\to\infty$ מתקבל $\varepsilon \to 0$, כלומר ההחלטה עבור H_1 קריטריון גילוי זה תתקבל רק כאשר הפילוג האמפירי של הדגימה יהיה במובהק דומה ל- p_1 .

תנאי ההחלטה לקריטריוני הגילוי האחרים

עבור הקריטריון:

$$\begin{aligned}\alpha_n &= \alpha(n) \doteq 2^{-nD_1} \\ \beta_n &= \beta(n) \doteq 2^{-nD_2}\end{aligned} \qquad \forall n$$

הסימטרי, כלומר $D_1 = D_2$.

וכן עבור הקריטריון הבייסיאני:

$$\overline{P}_e = \pi_1\alpha_n + \pi_2\beta_n \qquad \forall n$$

כאשר $\pi_1, \pi_2 \neq 0$ מתקבל פתרון זהה:

$$P_e^{opt} = 2^{nD^*}, \quad D^* : D\left(p_{\lambda^*} \| p_1\right) = D\left(p_{\lambda^*} \| p_2\right) \doteq D^*$$

כלומר D^* הוא המרחק המתקבל עבור פילוג p_{λ^*} המשיג מרחק שווה בין שני הפילוגים . יש להציב פילוג מהצורה:

$$p_\lambda(x) = \frac{p_1^\lambda(x)\, p_2^{1-\lambda}(x)}{\sum_{x' \in \mathcal{X}} p_1^\lambda(x')\, p_2^{1-\lambda}(x')}$$

p_{λ^*} מתקבל כפילוג המביא למרחק שווה בין שני הפילוגים.

הוכחה מפורטת מובאת בספר של Cover.

אקספוננט השגיאה לפענוח בערוץ רועש - Error Exponent

נושא זה אינו נסקר בספר של Cover, אולם ניתן לקרוא עליו בספרים הבאים:

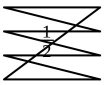
Gallager (1968), Csiszer (1981), Blahut (1989).

מוטיבציה

נתבונן בשני ערוצי מודולו 4 חסרי הזיכרון מעל האלפבית $\{0,1,2,3\}$, מהצורה הבאה:

$$Y=\left(X+N\right)\bmod 4$$

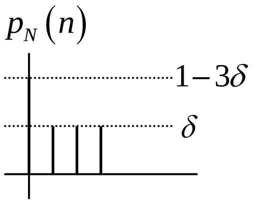
<u>ערוץ א': מכונת הכתיבה הרועשת</u>



קיבול הערוץ נתון על ידי:

$$C=\log\left|Y\right|-H\left(N\right)=\log\left(4\right)-\log\left(2\right)=1\left[bit\right]$$

<u>ערוץ ב':</u>



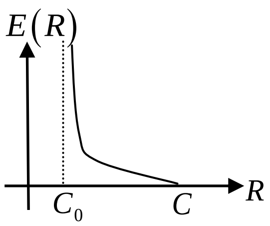
קיבול הערוץ נתון על ידי:

$$C=\log\left|Y\right|-H\left(N\right)=-\left(1-3\delta\right)\log\left(1-3\delta\right)-3\delta\log\left(\delta\right)$$

ניתן לבחור $\delta:C=1\left[bit\right]$

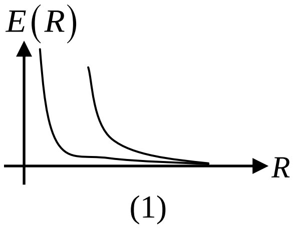
כמובן שנעדיף את ערוץ א ', וזאת מכיוון שהוא מאפשר השגה של שגיאת פענוח , $P_e=0$, עבור בלוק באורך 1. ערוץ ב' לעומתו מחייב אורך בלוק אינסופי בכדי להשיג שגיאה ששואפת לאפס.

תאור גראפי של אקספוננט השגיאה



ניתן להציג את אקספוננט השגיאה, גראפית באופן הבא:

כאשר C_0 מתאר את "קיבול אפס שגיאה ". לא בכל ערוץ ניתן להשיג "קיבול אפס שגיאה".

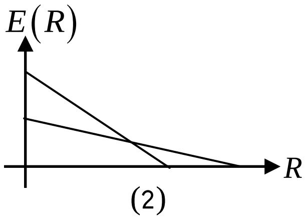


(1)

יתכנו מגוון מצבים ליחס בין ערוצים, נציג שניים:

עבור מקרה (1) ברור כי ישנו ערוץ טוב יותר . במקרה (2) ניתן לחלק את סט הקצבים לשניים. ערוץ אחד מתאים לקצבים נמוכים, ואילו השני לקצבים גבוהים.

הערה: לעיתים לאותו ערוץ פיזיקאלי ושיטות אפנון שונות ישנו ערוץ בדיד שקול שונה.



(2)

"הטעות של שנון"

במאמר משנת 1948 טוען שנון כי הסתברות השגיאה , לפענוח קוד אקראי , בהנחה שספר הקוד והערוץ אופייניים, נתון על ידי: $P_e=2^{-n\left[C-R\right]}$

כלומר שאקספוננט השגיאה ליניארי. למעשה ההנחה של שנון הייתה אופטימית, אנו יודעים כי הגרף של אקספוננט השגיאה קמור.

<u>"הוכחה"</u>

הסיכוי להתחזות מילה: $2^{-nI(X;Y)}$ נבצע $2^{nR}-1$ ניסויים. לפי תכונת "סף האקספוננט" שראינו בשיעור שעבר, נובע כי ההסתברות השגיאה היא $2^{-n[I(X;Y)-R]}$.

הכשל בהוכחה נובע מההנחה שכל המילים אופייניות וכי גם הערוץ מתנהג באופן אופייני.

הערה: שאנון כמובן הכיר ב"טעות שלו", אך היה מעוניין לפשט את הדיון.

אקספוננט השגיאה – דיון מורחב

נגדיר:

$$E(R,P,W)=\min_{V(y/x)}E(V)$$

כאשר $P(x)$ הוא פילוג הכניסה, $W(y/x)$ הוא פילוג המעבר בערוץ, ו- R הוא הקצב,

$$E(V)=D(V\|W/P)+\left[I(P,V)-R\right]^{+}$$

כאשר $X\sim P(x),Y/X\sim V(y/x)$, $I(P;V)=I(X;Y)$ וכן:

$$[S]^{+}=\begin{cases}S & S\geq 0\\ 0 & S<0\end{cases}$$

והדיוורגנס המותנה:

$$D(V\|W/P)=\sum_x P(x)\sum_y V(y/x)\log\frac{V(y/x)}{W(y/x)}$$

משפט – חסם להסתברות השגיאה

הסתברות שגיאת הפענוח חסומה על ידי:

$$P_e^{opt}\leq 2^{-nE(R,P,W)}$$

כמו כן לערוץ כלשהו $W(y/x)$ מתקיים:

$$E(R)=\max_P E(R,P,W)$$

<u>הוכחה</u>

נתייחס לספר קוד אקראי טיפוסי , להבדיל מספר קוד בלתי תלוי שווה פילוג , קרי $\mathbf{x}\sim U(T(P_{\mathbf{x}}))$.

כמפענח נבחר מפענח אוניברסאלי הממקסם אינפורמציה הדדית.

Maximum Mutual Information (MMI) מפענח מקסימום אינפורמציה הדדית

מקלט סטנדרטי לומד את הערוץ ומפענח דגימת כניסה , לפי תהליך הלימוד שעבר . מפענח מקסימום אינפורמציה הדדית בהינתן הדגימה, $\mathbf{y}$, מחפש את מילת הקוד שעבורה האינפורמציה ההדדית האמפירית מקסימאלית:

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}\in CodeBook} I\left(\mathbf{x}\wedge\mathbf{y}\right) = \arg\max_{\mathbf{x}\in CodeBook} I\left(P_X, W_{Y/X}\right)$$

כאשר P_X זהו הפילוג האמפירי לפיו נבחרות מילות הקוד , $W_{Y/X}$ זהו פילוג המעבר המושרה מהפילוג האמפירי של $\mathbf{x},\mathbf{y}$.

הבחן: משערך הנראות המרבית (ML), בו משתמש גאלאגר:

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}\in CodeBook} W\left(\mathbf{y}/\mathbf{x}\right)$$

כאשר $\mathbf{y}$ היא הדגימה שקיבלנו.

בהכללה מפענח ML טוב ממפענח MMI. במקרים הנדירים בהם הערוץ המוגרל אינו קרוב לערוץ האופייני, מפענח ה-MMI טוב יותר.

את התוצאה $E\left(R\right)=\max_{P} E\left(R,P,W\right)$ לא נוכיח.

הוכחת משפט החסם להסתברות השגיאה

כאמור יש להוכיח כי:

$$P_e^{opt} \le 2^{-nE\left(R,P,W\right)} = 2^{-n\min\limits_{V(y/x)}\left\{\underbrace{D\left(V\|W/P\right)}_{I}+\underbrace{\left[I\left(P,V\right)-R\right]^{+}}_{II}\right\}}$$

הסתברות השגיאה בפענוח MMI, למילות קוד הנבחרות אחיד מהטיפוס, $\mathbf{x}\sim U\left(T\left(P_{\mathbf{X}}\right)\right)$:

$$P_e^{MMI} = \sum_{V\in\mathcal{V}^n} \Pr\left\{\text{Channel Behaved } V\left(\mathbf{y}/\mathbf{x}\right)\right\}\cdot\Pr\left\{\begin{matrix}\text{Error in MMI Decode /}\\ \text{Channel Behaved } V\left(\mathbf{y}/\mathbf{x}\right)\end{matrix}\right\}$$

כאשר $V\left(\mathbf{y}/\mathbf{x}\right)$ מסמן כי הפילוג האמפירי הוא V.

השלמה: קבוצת הטיפוס המותנה

נגדיר את קבוצת הטיפוס המותנה:

$$T_V\left(\mathbf{x}\right)=\left\{\mathbf{y}: V_{\mathbf{y}/\mathbf{x}}=V\right\}$$

מספר הטיפוסים המותנים באורך n חסום על ידי:

$$\left|\mathcal{V}\right|^n \le \left(n+1\right)^{|\mathcal{X}||\mathcal{Y}|}$$

אם $P_{\mathbf{x}}=P$ אז גודל קבוצת הטיפוס נתונה על ידי: $\left|T_V\left(\mathbf{x}\right)\right| \doteq 2^{nH\left(V/P\right)} \doteq 2^{nH\left(\mathbf{y}/\mathbf{x}\right)}$

נחזור להוכחה:

מכיוון שפילוג הכניסה חסר זיכרון, ההסתברות לסדרת מוצא כלשהי , $\mathbf{y} \in T_V\left(\mathbf{x}\right)$, זהה. לפיכך בהינתן ערוץ אמיתי $W\left(\mathbf{y}/\mathbf{x}\right)$ ומילות כניסה מוגרלות אחיד על פני הטיפוס $P_{\mathbf{x}} = P$ והערוץ האמפירי שהתקבל הוא $V\left(\mathbf{y}/\mathbf{x}\right)$ ההסתברות ל- $\mathbf{y}$ ספציפית נתונה על ידי:

$$\Pr\left(\mathbf{y}/\mathbf{x}\right) = 2^{-n\left[D(V\|W/P)+H(V/P)\right]}$$

וההסתברות ל- $\mathbf{y}$ כלשהו מהטיפוס המותנה נתונה על ידי:

$$\Pr\left(T_V\left(\mathbf{x}\right)/\mathbf{x}\right) \approx 2^{-nD(V\|W/P)}$$

טעון זה מצדיק את הגורם I בהסתברות השגיאה.

נותר להעריך מהי השגיאה בפענוח MMI:

בהינתן ששודרה המילה $\mathbf{x}_0$ והתקבלה המילה $\mathbf{y}$ ובניהן ישנו פילוג אמפירי מותנה $V_{\mathbf{y}/\mathbf{x}_0}$, תתקבל שגיאה כאשר:

$$\exists \mathbf{x} \neq \mathbf{x}_0 : I\left(\mathbf{x} \wedge \mathbf{y}\right) > I\left(\mathbf{x}_0 \wedge \mathbf{y}\right)$$

כלומר עלינו להעריך את ההסתברות:

$$\Pr\left\{I\left(\mathbf{x} \wedge \mathbf{y}\right) > I\left(P,V\right) \text{ for some } \mathbf{x} \in CodeBook \,/\, \text{Channel Behaved } V\right\}$$

גודל זה חסום לפי ה-Union Bound על ידי:

$$\Pr\left\{I\left(\mathbf{x} \wedge \mathbf{y}\right) > I\left(\mathbf{x}_0 \wedge \mathbf{y}\right)\right\} \cdot 2^{nR} = \Pr\left\{I\left(\mathbf{x} \wedge \mathbf{y}\right) > I\left(P,V\right)\right\} \cdot 2^{nR}$$

או על ידי 1, אם הגודל הזה גדול מ-1.

נוכיח כעת כי $\Pr\left\{I\left(\mathbf{x} \wedge \mathbf{y}\right) > I\left(P,V\right)\right\} = \exp\left\{-nI\left(P,V\right)\right\}$ כאשר ההסתברות מחושבת ביחס ל - $\underline{x}$ שמתפלג אחיד על פני קבוצת הטיפוס $T(x)$. כפי שראינו בפרק על טיפוסים, הסיכוי "להתחזות" של $\underline{x}$ כאופייני במשותף (עם פילוג אמפירי $\left(V\left(\mathbf{y}/\mathbf{x}\right)\right)$ עם $\underline{y}$ היא $\exp\left\{-nI\left(P,V\right)\right\}$. בעצם, אותו סיכוי מתקיים לכל פילוג אמפירי משותף שעבורו מתקיים $I\left(\mathbf{x} \wedge \mathbf{y}\right) = I\left(P,V\right)$, ולכן הסיכוי של כלל הטיפוסים המשותפים האמפיריים (שמספרם כזכור עולה רק פולינומיאלית עם n) גם הוא $\exp\left\{-nI\left(P,V\right)\right\}$. בכך הוכחנו כי $\Pr\left\{I\left(\mathbf{x} \wedge \mathbf{y}\right) > I\left(P,V\right)\right\} = \exp\left\{-nI\left(P,V\right)\right\}$ כנדרש.

מקסימום אנטרופיה - Maximal Entropy

הספק האנטרופיה

יהי המשתנה האקראי X המתפלג $f_X(x)$ ומקיים:

$$h(X)=\tfrac{1}{2}\log\left(2\pi eP(X)\right),\quad \operatorname{var}(X)=\sigma^2,\quad E(X)=0$$

כאשר $P(X)$ שווה לשונות של המשתנה הגאוסי עם אותה אנטרופיה דיפרנציאלית, והוא מוגדר כהספק האנטרופיה.

אנטרופיה דיפרנציאלית

האנטרופיה הדיפרנציאלית מוגדרת על ידי:

$$h(X)=\int_{-\infty}^{\infty} f_X(x)\log f_X(x)dx$$

יחס בין אנטרופיה של משתנה אקראי כללי למשתנה אקראי גאוסי

<u>מקרה סקלארי:</u> נגדיר את המשתנה האקראי הגאוסי:

$$X^* \sim N\left(0,\sigma^2\right)$$

יהי משתנה אקראי X כלשהו עם שונות σ^2 אזי:

$$h\left(X^*\right)\ge h(X)\quad \forall X \text{ with } \operatorname{var}(X)=\operatorname{var}\left(X^*\right)$$

<u>מקרה וקטורי:</u> יהי הווקטור האקראי הגאוסי

$$\underline{X}^* \sim N\left(0,\operatorname{cov}(\underline{X})\right)$$

אזי:

$$h\left(\underline{X}^*\right)=\tfrac{1}{2}\log\left(2\pi e\left|\operatorname{cov}\left(\underline{X}^*\right)\right|^{\frac{1}{n}}\right)\ge h(\underline{X}),\quad \forall\underline{X} \text{ with } \operatorname{cov}(\underline{X})=\operatorname{cov}\left(\underline{X}^*\right)$$

$$\text{where } |\text{Matrix}|=abs\left(\det(\text{Matrix})\right)$$

<u>מקרה תהליכי:</u> יהי התהליך הגאוסי X^* עם פונקצית האוטוקורלציה או באופן שקול פונקצית צפיפות ההספק הספקטראלית:

$$R_K=E\left\{X_{n+K}X_n\right\},\quad S_X(f)=\sum_k R_k\exp\left\{-2\pi j\cdot f_k\right\}$$

לכל תהליך סטטציונארי מתקיים:

$$\bar{h}(X)\le\bar{h}\left(X^*\right)=\int_{-\frac{1}{2}}^{\frac{1}{2}}\tfrac{1}{2}\log\left(2\pi eS_X(f)\right)df$$

אי שוויון הספק האנטרופיה - Entropy Power Inequality (EPI)

<u>מקרה סקלארי:</u>

יהיו שני משתנים אקראיים $X \perp\!\!\!\perp Y$ מתקיים:

$$P\left(X+Y\right)\geq P\left(X\right)+P\left(Y\right) \quad \Leftrightarrow \quad 2^{2h(X+Y)}\geq 2^{2h(X)}+2^{2h(Y)}$$

שוויון מתקבל אם ורק אם המשתנים האקראיים גאוסים.

הבחן: דרך שקולה לכתוב את האי שוויון היא להגדיר את זוג המשתנים הגאוסים:

$$\tilde{X} \sim N\left(0,P\left(X\right)\right),\tilde{Y} \sim N\left(0,P\left(Y\right)\right)$$

מתקיים כי:

$$h\left(X+Y\right)\geq h\left(\tilde{X}+\tilde{Y}\right)$$

ושוב שוויון מתקבל אם ורק אם זוג המשתנים גאוסים.

אינטואיציה: אם מחברים זוג משתנים אקראיים הם הופכים להיות "יותר גאוסים".

ניתן לגזור מסקנה מעניינת (הנכונה לכל מטריצה אי-שלילית מוגדרת):

$$\left|R\right|^{\frac{1}{n}}\leq\prod_{i=1}^{n}R_{ii}\leq\tfrac{1}{n}tr\left(R\right)$$

משפט הגבול המרכזי – ניסוח שקול

אנו מכירים את הניסוח הקונבנציונאלי למשפט הגבול המרכזי:

תהי סדרת משתנים אקראיים המתפלגים באופן בלתי תלוי ושווה פילוג, לאו דווקא גאוסיים, אזי:

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}x_i \xrightarrow[n\to\infty]{} N\left(0,\sigma^2\right)$$

ניסוח אלטרנטיבי שניתן להציג בעקבות הדיון הקודם:

$$h\left(\frac{1}{\sqrt{n}}\sum_{i=1}^{n}x_i\right) \nearrow \tfrac{1}{2}\log 2\pi e\sigma^2$$

בחזרה לתכונת ה- EPI

<u>מקרה ווקטורי:</u>

$$P\left(\underline{X}+\underline{Y}\right)\geq P\left(\underline{X}\right)+P\left(\underline{Y}\right) \quad \Leftrightarrow \quad h\left(\underline{X}+\underline{Y}\right)\geq h\left(\tilde{\underline{X}}+\tilde{\underline{Y}}\right)$$

כאשר $\tilde{\underline{X}},\tilde{\underline{Y}}$ הם ווקטורים גאוס ים המפולגים באופן בלתי תלוי ושווה פילוג עם אותה אנטרופיה דיפרנציאלית כמו $\underline{X},\underline{Y}$. שוויון מתקבל אם ורק אם $\underline{X},\underline{Y}$ הם ווקטורים גאוסיים עם מטריצות קוואריאנס פרופורציוניות לאלו של $\tilde{\underline{X}},\tilde{\underline{Y}}$.

ניתן לגזור מסקנה מעניינת (הנכונה לכל זוג מטריצות אי-שלילית מוגדרות):

$$\left|R_X+R_Y\right|^{\frac{1}{n}}\geq\left|R_X\right|^{\frac{1}{n}}+\left|R_Y\right|^{\frac{1}{n}}, \quad \text{equality iff } R_X \propto R_Y$$

הקשר בין אנטרופיה לשגיאת החיזוי הליניארי

נגדיר את קצב האנטרופיה:

$$\bar{h}(X) = \lim_{n\to\infty} \tfrac{1}{n} h(x_1, x_2, \ldots, x_n) = h(x_n / x_{n-1}, x_{n-2}, \ldots, x_1) \underset{Gauss}{=}$$

$$E_{\text{past}} \left\{ \tfrac{1}{2} \log 2\pi e \operatorname{var}(x_n) / \text{past} \right\} \underset{\text{Prediction error of optimal linear estimator}}{=}$$

$$E\left\{ \tfrac{1}{2} \log 2\pi e E\left\{ \left(x_n - \sum_{i=1}^{n} a_i x_{n-i} \right)^2 \right\} \right\} = E\left\{ \tfrac{1}{2} \log 2\pi e E\left\{ e^2_{\text{Prediction}} \right\} \right\}$$

כלומר: $\bar{P}(X) = \dfrac{2^{2\bar{h}(X)}}{2\pi e} = \text{Prediction error of optimal linear estimator}$

אינפורמציית פישר וחסם קרמר ראו - חזרה

נתון משתנה אקראי המתפלג לפי משפחה של פונקציות פילוג התלויות בפרמטר θ :

$$X \sim f_X(x;\theta)$$

רוצים לשערך את θ מתוך הסדרה $X_1, X_2, \ldots, X_n$ נגדיר את האינפורמציה של פישר:

$$J(X;\theta) = E\left\{ \left(\frac{\partial}{\partial\theta} \ln f(X;\theta) \right)^2 \right\}$$

קל לראות שאם $X_1, X_2, \ldots, X_n$ מתפלגים באופן בלתי תלוי ושווה פילוג:

$$J(\underline{X};\theta) = nJ(X;\theta)$$

חסם קרמר ראו, קובע כי לכל משערך בלתי מוטה $\hat{\theta} = g(\underline{X})$ (אם קיים) מתקיים:

$$\operatorname{var}(\hat{\theta}) \geq 1 / J(\underline{X};\theta)$$

<u>למקרה הגאוסי</u>

$$X_i \sim N(\theta, \sigma^2), \quad \hat{\theta} = \tfrac{1}{n} \sum_{i=1}^{n} X_i \quad J(\underline{X};\theta) = \tfrac{n}{\sigma^2}$$

ניתן לראות כי:

$$\operatorname{var}(\hat{\theta}) = 1 / J(\underline{X};\theta)$$

<u>מקרה כללי</u>

במקרים כללים, תחת תנאים מסוימים, מתקבל שוויון אסימפטוטי:

$$n \operatorname{var}(\hat{\theta}) \xrightarrow[n\to\infty]{} 1 / J(\underline{X};\theta)$$

אינפורמצית פישר ביחס לפרמטר הזזה

הגדרת הבעיה : נניח ו- $X \sim f_X(x)$ אולם מסיבה כלשהי אנו רואים $f_X(x-\theta)$ ואנו מעוניינים לשערך את θ, אינפורמציית פישר ביחס להזזה:

$$J(X) = J\left(f_X(x-\theta);\theta\right) = \int_{-\infty}^{\infty} f_X(x)\left[\frac{\partial}{\partial x}\ln f_X(x)\right]^2 dx$$

מתקיים לכל משערך בלתי מוטה, לפי חסם קרמר-ראו:

$$\operatorname{var}\left(\hat{\theta}\right) \geq 1 \big/ J(X)$$

תכונות:

1. המקרה הקשה ביותר לשערוך פרמטר ההזזה הוא המקרה הגאוסי:

$$J\left(X^*\right) \leq J(X), \quad X^* \sim N\left(0, \operatorname{var}(X)\right)$$

2. Fischer Information Inequality (F.I.I), אם $X \perp\!\!\!\perp Y$ אזי:

$$\frac{1}{J(X+Y)} \geq \frac{1}{J(X)} + \frac{1}{J(Y)}$$

3. DeBruijn Identitiy, הנגזרת של האנטרופיה ביחס לפרטורבציה גאוסית:

$$\frac{\partial}{\partial t} h\left(X + \sqrt{t}Z\right) = \frac{1}{2} J(X), \quad Z \sim N(0,1) \perp\!\!\!\perp X$$

אי שוויון ברון מינקובסקי

תהינה A, B קבוצות של נקודות ב- $\mathbb{R}^n$, ונגדיר:

$$A+B \triangleq \{x+y : x\in A, y\in B\}$$

אזי:

$$Volume(A+B) \geq Volume\left(\tilde{A}\right) + Volume\left(\tilde{B}\right)$$

כאשר $\tilde{A}, \tilde{B}$ כדורים עם אותו הנפח כמו A, B .

אינטואיציה: אם נחבר שני גופים שאינם כדורים, הסכום יהפוך ל"יותר" כדורי.

האנטרופיה של ראני

$$h_r(X) \triangleq \begin{cases} \frac{1}{1-r}\log\int f^r(x)\,dx & 0 < r < \infty, r \neq 1 \\ -\int f(x)\log f(x)\,dx & r = 1 \\ \log\left|\operatorname{support}\left(f(x)\right)\right| & r = 0 \end{cases}$$

עבור $r=0$ מתקבל מדד לנפח , עבור $r=1$ מתקבלת אינפורמציית שנון . קיים אי שוויון כללי , לאנטרופיית ראני שנותן כמקרה פרטי את מינקוסקי ואת ה-EPI.

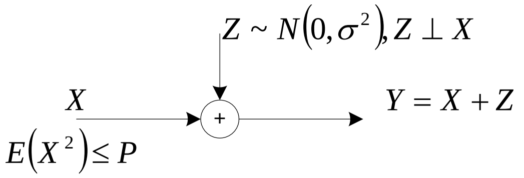
הרצאה מס' 3

קוונטיזציה, סריגים ותורת האינפורמציה

סוכם ע"י: יובל לומניץ, תום הראל

המגבלה של פילוג אחיד

פילוג מבוא בערוץ גאוסי



הקיבול מושג ע"י פילוג כניסה גאוסי $X^* \sim N(0,P)$.

$$C = I(X^*;X^*+Z) = h(X^*+Z) - h(Z) = \tfrac{1}{2}\log\left(1+\frac{P}{\sigma^2}\right)$$

נניח שנרצה במקום פילוג זה להשתמש בפילוג אחיד $X \sim Unif\left[-\frac{\Delta}{2},\frac{\Delta}{2}\right]$. רוב שיטות השידור המקובלות מקרבות פילוג אחיד (לדוגמא M-QAM). כדי להשיג את אילוץ ההספק נקבע $EX^2 = \frac{\Delta^2}{12} = P$. הקצב שנשיג חסום ע"י

$$I(X;X+Z) = h(X+Z) - h(Z)$$

וההפסד הוא

$$C - I(X;X+Z) = h(X^*+Z) - h(Z) - \left(h(X+Z) - h(Z)\right) =$$

$$= h(X^*+Z) - h(X+Z) \underset{\sigma^2 << D}{\approx} h(X^*) - h(X) = \tfrac{1}{2}\log(2\pi eP) - \log(\Delta) =$$

$$= \tfrac{1}{2}\log(2\pi eP) - \tfrac{1}{2}\log(12P) = \tfrac{1}{2}\log\left(\frac{2\pi e}{12}\right) \approx 0.254bit$$

ההפסד נקרא "shaping loss". לחילופין ניתן להגדיר את ההפסד במונחי הספק: כמה נצטרך להעלות את ההספק במקרה היוניפורמי לקבלת אותו קצב:

$$\tfrac{1}{2}\log(2\pi eP) = \tfrac{1}{2}\log(12P')$$

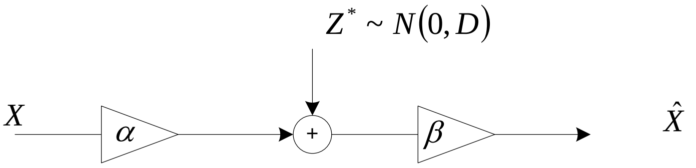
$$P'/P = \frac{2\pi e}{12} \approx 10^{1.5/10} = 1.5dB$$

"רעש" אחיד לעומת גאוסי בבעיית Rate-distortion

פונקציית rate-distortion:

$$R(D) = \min_{\hat{X}:E\left(X-\hat{X}\right)^2 \le D} \left(I\left(X;\hat{X}\right)\right)$$

הערוץ המגשים את ה-Rate-distortion במקרה ש-X הוא גאוסי $X \sim N(0,\sigma^2)$ הוא ערוץ ה-AWGN הבא:

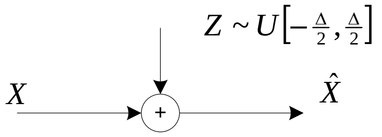


עם $\alpha = \beta = \sqrt{1-\frac{D}{\sigma^2}}$, ומתקבל:

$$I(X;\hat{X}) = \tfrac{1}{2}\log\left(\frac{\sigma^2}{D}\right) = R(D)$$

עבור $D \ll \sigma^2$ מתקבל $\alpha=\beta\approx 1$.

לעומת זאת ערוץ בר מימוש בקירוב ע"י קונטייזר פשוט הוא כזה שבו שגיאת הקונטיזציה היא מ"א אחיד:



עבור ערוץ זה:

$$I(X;\hat{X}) = h(X+Z) - h(Z) \underset{s^2 \ll D}{\approx} h(X) - h(Z)$$

ההבדל בין המקרים הוא ב-h(Z) ולכן ההפרש שנקבל:

$$I(X;\hat{X}) - R(D) \approx h(Z^*) - h(Z) = \tfrac{1}{2}\log(2\pi e D) - \log(\Delta) =$$

$$= \tfrac{1}{2}\log\left(\frac{2\pi e}{12}\right) \approx 0.254 bit$$

שקילות בין רעש גאוסי iid לפילוג אחיד על כדור ממימד גבוה

<u>כיוון א':</u>

אם $X=X_1,X_2\ldots X_N$ וקטור iid גאוסי $N(0,\sigma^2)^n$, אזי

$$f_{\underline{X}}(\underline{x}) \xrightarrow[n\to\infty]{} Unif\left(Ball_n\left(\underline{0},\sqrt{n\cdot\sigma^2}\right)\right)$$

כאשר

$$Ball_n(\underline{x}_0, r) \equiv \left\{\underline{x} : \left\|\underline{x}-\underline{x}_0\right\| \le r\right\}$$

וההתכנסות היא במובן מקורב (הערה: זה אינו ביטוי מדויק כי n מופיע גם בצד ימין, ראה הגדרה מדוייקת יותר להלן)

<u>כיוון ב':</u>

עבור וקטור אקראי $\underline{U}$ מפולג בפילוג אחיד על פני כדור:

$$\underline{U} \sim Unif\left(Ball_n(\underline{0},R)\right),$$

$$R = \sqrt{n\sigma^2}$$

הפילוג של כל קבוצת דגימות $U_1,\ldots U_k$ שואף לפילוג גאוסי iid $N(0,\sigma^2)^k$ כאשר $n\to\infty$.

הוכחה מקורבת של א':

פונקצית הפילוג היא:

$$f_{\underline{X}}(\underline{x}) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left(-\frac{\|\underline{x}\|^2}{2\sigma^2}\right)$$

ולכן הפילוג איזוטרופי (קוים שווי פילוג יוצרים מעטפות כדוריות).

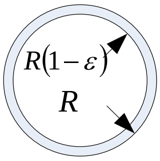
לפי החוק החלש של המספרים הגדולים

$$\frac{1}{n}\|\underline{X}\|^2 = \frac{1}{n}\sum_{i=1}^{n} X_i^{\,2} \xrightarrow[n\to\infty]{} \sigma^2$$

כאשר ההתכנסות היא בהסתברות ובמובן ריבועי, לכן ניתן לומר כי

$$\|\underline{X}\|^2 \approx n\sigma^2$$

כלומר $\underline{x}$ נמצא בקירוב על פני קליפה כדורית ברדיוס $R = \sqrt{n\sigma^2}$. עתה נראה שפילוג על כדור ופילוג על קליפת הכדור הם קרובים מהבחינה שההסתברות והנפח של איזור פנימי בכדור שמרוחק ε מהקליפה שואפת ל-0. ידוע שנפח כדור ברדיוס R מסדר n נתון ע"י $V_n(R)=V_n{\cdot}R^n$. אם נסתכל על חלק פנימי של הכדור שהוא כדור ברדיוס $R(1\text{-}\varepsilon)$ (הכדור פחות קליפה בעובי ε), אז היחס בין הנפחים יהיה:



$$\frac{V_n((1-\varepsilon)R)}{V_n(R)} = \frac{V_n\cdot((1-\varepsilon)R)^n}{V_n\cdot R^n} = (1-\varepsilon)^n \xrightarrow[n\to\infty]{} 0$$

כלומר רוב נפח הכדור מתרכז בקליפה ועבור n גדול ניתן לומר שכל נפח הכדור הוא בקליפה. לכן הפילוג האחיד על הכדור והפילוג האחיד על הקליפה נבדלים זה מזה בתחום שנפחו היחסי וההסתברות שלו (תחת הפילוג האחיד) שואפים ל-0.

<u>הערה:</u> ביטוי מדוייק יותר לשקילות שהראנו בא' הוא

$$\tfrac{1}{n}D\left(Unif\left(Ball_n\left(\underline{0},\sqrt{n\cdot\sigma^2}\right)\right)\middle\|\, f_{\underline{X}}(\underline{x})\right) \xrightarrow[n\to\infty]{} 0$$

כלומר ה-Divergence המנורמל בין פילוג אחיד על פני הכדור לבין פילוג הדגימות הגאוסיות שואף ל-0. ניתן להראות טענה זו ע"י חישוב ה-Divergence הנ"ל כפונקציה של המומנט השני המנורמל על פני הכדור G_n^* (ראה הגדרה דומה עבור סריגים בהמשך). מתקבל $D(..\|..) = \frac{1}{2}\log\left(2\pi e G_n^*\right)$, וכיון ש: $G_n^* \underset{n\to\infty}{\to} \frac{1}{2\pi e}$ אז $D \underset{n\to\infty}{\to} 0$.

קוונטיזציה

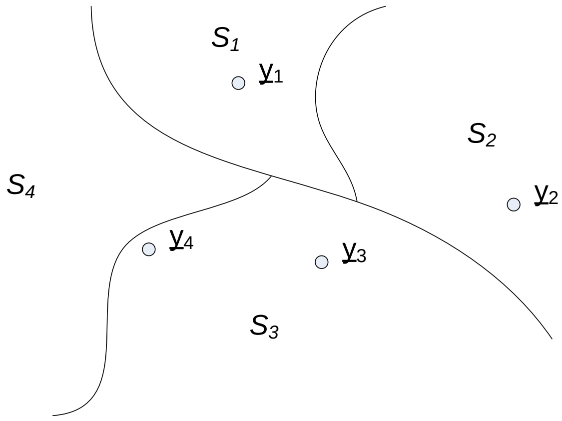
נדבר על המקרה הוקטורי ועל קוונטיזציה סקלרית כמקרה פרטי/מנוון.

הגדרת קוונטייזר וקטורי

קוונטייזר כללי וקטורי n מימדי (V.Q Vector Quantizer) מוגדר ע"י אוסף של N אזורי החלטה $\{S_i\}_{i=1}^{N}$ זרים $S_i \cap S_j = \phi$ המכסים את כל המרחב $\dot{\bigcup}_{i=1..N} S_i = \Re^n$ ($\dot{\bigcup}$ מסמן איחוד זר), ו-N מילות קוד $\{\underline{y}_i\}_{i=1}^{N}$. נגדיר את הקונטייזר כ:

$$Q(\underline{x}) = \underline{y}_i \ \text{ if } \ \underline{x} \in S_i$$

Q נקרא קוונטיזר וקטורי ביחס לחלוקה $\{S_i\}_{i=1}^{N}$ ומילות הקוד $\{\underline{y}_i\}_{i=1}^{N}$.



תנאי לויד (Lloyd)

בהינתן מדד עוות הפרשי $d(\underline{x},\underline{y})=d(\underline{x}-\underline{y})$, ופילוג מקור $f_{\underline{X}}(x)$ (לא בהכרח רציף), אזי שני התנאים הבאים הם תנאים הכרחיים לקוונטייזר של N מילות קוד בעל עוות ממוצע מינימלי, ז"א קוונטייזר המביא למינימום את $E(d(\underline{X},Q(\underline{X})))$ על פני $\{S_i,\underline{y}_i\}_{i=1}^{N}$.

1. בהינתן מילות הקוד $\underline{y}_1\ldots\underline{y}_N$, החלוקה צריכה לקיים את תנאי ה-Nearest-Neighbor:

$$\forall j\neq i: d(\underline{x},\underline{y}_i)<d(\underline{x},\underline{y}_j)\Rightarrow \underline{x}\in S_i$$

2. בהינתן חלוקה $\{S_i\}_{i=1}^{N}$ של המרחב, מילות הקוד הן מרכזי הכובד של תחומי החלוקה:

$$\underline{y}_i=\arg\min_{\underline{y}}\left(E\left(d(\underline{X},\underline{y})\mid \underline{X}\in S_i\right)\right)$$

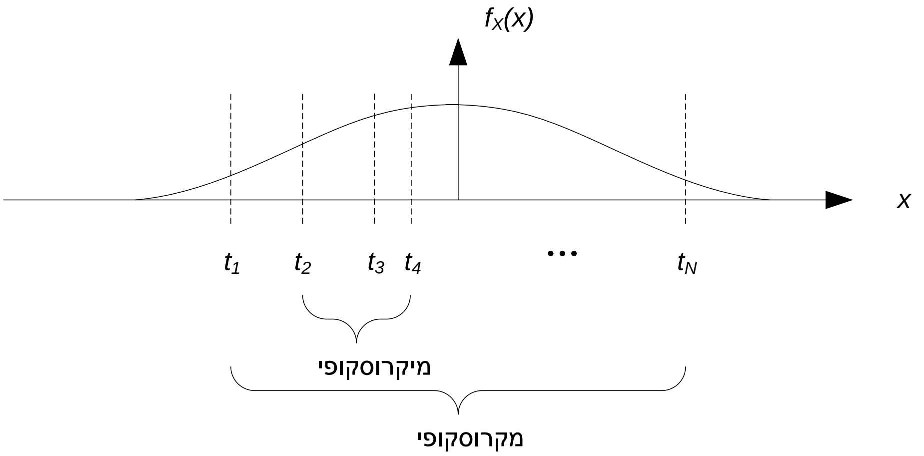
בפרט עבור מדד עוות ריבועי $d(\underline{x},\underline{y})=\|\underline{x}-\underline{y}\|^2$, מתקיים:

$$\underline{y}_i=\arg\min_{\underline{y}}\left(E\left(\|\underline{x}-\underline{y}\|^2\mid \underline{X}\in S_i\right)\right)=E(\underline{X}\mid \underline{X}\in S_i)$$

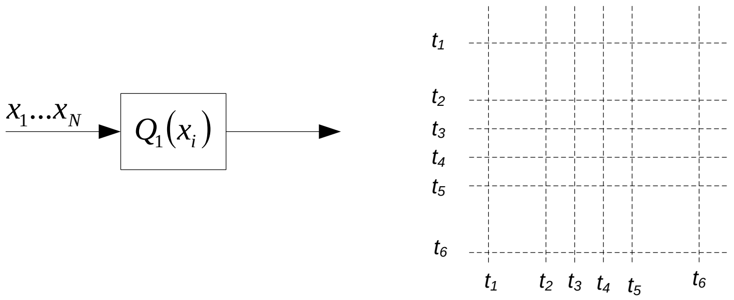
מתוך תנאי לויד ניתן ליצור אלגוריתם איטרטיבי למציאת קוונטייזר שהוא לפחות אופטימלי מקומית (מינימום מקומי), ע"י אתחול במילות קוד שרירותיות, הפעלת (1) כדי למצוא את אזורי ההחלטה, הפעלת (2) כדי למצוא מילות קוד חדשות וכו'. כיון ש-S_i מגדירות את המקודד, ו-$\underline{y}_i$ את המפענח, ניתן להסתכל על (1) כאופטימיזציה של המקודד, ועל (2) כאופטימיזציה של המפענח. בתנאים מסוימים של קמירות על הפילוג יש מינימום יחידי והאלגוריתם האיטרטיבי מתכנס אליו.

למה קוונטיזציה וקטורית?

קוונטיזציה סקלרית מוגדרת פשוט ע"י אוסף של ספים: $S_i = [t_{i-1}, t_i)$:



אם נפעיל קוונטייזר חד מימדי על ווקטור באורך n נקבל מכפלה קרטזית של אזורי ההחלטה ונקודות הקוד



שלוש סיבות לשימוש בקוונטיזציה ווקטורית:

1. **הרווח הגרעיני (Granular Gain)** – סידור יעיל יותר של מילות הקוד ברמה המיקרוסקופית: יחס טוב יותר בין הנפח המכוסה ע"י כל מילה למרחק/עוות.
2. **רווח העיצוב (Shaping Advantage)** – התכנסות הפילוג לקבוצה אופיינית, מקטין את הנפח שהקוונטייזר צריך לכסות (/בצורה יעילה).
3. **התייחסות לזיכרון במקור** (תלות בין דגימות מקטינה את האנטרופיה של הוקטור ואת הנפח שצריך לכסות)

סיבות (2) ו-(3) מתייחסות למבנה <u>המקרוסקופי</u> ז"א צורת התחום המכוסה בצורה יעילה ע"י הקוונטייזר, ו-(1) מתייחסת למבנה <u>המיקרוסקופי</u>, ז"א לחלוקה הפנימית של התחום.

קוונטיזציה ברזולוציה גבוהה (High Resolution Quantization)

קוונטיזציה ברזולוציה גבוהה מתייחסת לגבול של עוות נמוך ותאים צפופים. ההנחה היא שבתוך תא קוונטיזציה, הפילוג הוא בקירוב אחיד, במובן שהוריאציה של צפיפות הפילוג ביחס לפילוג עצמו היא קטנה בכל תא באזור הגרעיני.

ניתן לקשור את המושג של וריאציה ביחס לפילוג ל-Fisher Information (נגזרת של log הפילוג).

נגדיר פונקציית צפיפות פיזור מילות הקוד $\lambda(\underline{x})$, מנורמלת ל-1: $\int_{\Re^n} \lambda(\underline{x})d\underline{x} = 1$, ומתקיים שמספר מילות הקוד בתחום S במרחב הוא בקירוב $N\int_S \lambda(\underline{x})d\underline{x}$.

מההנחות נובע כי:

1. $f(\underline{X} \mid \underline{X} \in S_i) \sim Unif(S_i)$
2. $p_i \equiv \Pr(\underline{X} \in S_i) = \int_{S_i} f_{\underline{X}}(\underline{x})d\underline{x} \approx f_{\underline{X}}(\underline{y}_i)\cdot \underbrace{\int_{S_i} d\underline{x}}_{Volume} \equiv f_{\underline{X}}(\underline{y}_i)\cdot V_i$
3. $D_i \equiv E(d(\underline{X},\underline{y}) \mid \underline{X} \in S_i) \approx G(S_i - \underline{y}_i)\cdot V_i^{2/n}$

כאשר הגדרנו V_i כנפח התא ה-i. ההנחה האחרונה מתקיימת כאשר מדד העיוות הוא ריבועי, ו-$G(S)$ (עבור קבוצה $S \subset \Re^n$ כלשהי, במקרה שלנו תא הקוונטיזציה) מוגדר כיחס בין המומנט השני של פילוג אחיד על S מחולק במימד, לבין הנפח של S בחזקת $2/n$ (הנרמול בנפח הוא כדי לקבל גודל חסר יחידות שאינו רגיש לכווץ)

$$G(S) \equiv \frac{1}{n}\frac{\frac{1}{V}\int_S \|\underline{x}\|^2 d\underline{x}}{V^{2/n}} = \frac{1}{n}\frac{\int_S \|\underline{x}\|^2 d\underline{x}}{V^{1+2/n}} = \frac{1}{n}\frac{\int_S \|\underline{x}\|^2 d\underline{x}}{\left(\int_S d\underline{x}\right)^{1+2/n}}$$

אם נניח שכל תאי הקוונטיזציה הם בעלי אותה צורה עד כדי מתיחה וסיבוב סביב הנקודה y_i, אזי G הוא קבוע $G(S_i - \underline{y}_i) = G$. נפח תאי הקוונטיזציה באזור כלשהו V_0 סביב הנקודה $\underline{x}$ נתון בקירוב ע"י חלוקת נפח האזור למספר התאים:

$$V(\underline{x}) \approx \frac{\int_{V_0} d\underline{x}}{N\int_{V_0} \lambda(\underline{x})d\underline{x}} \xrightarrow[Vol(V_0)\to 0]{} \frac{1}{N\lambda(\underline{x})}$$

לכן העיוות הממוצע הוא בקירוב:

$$D \equiv E(d(\underline{X},Q(\underline{X}))) = \sum_{i=1}^{N} p_i D_i \approx \sum_{i=1}^{N} f_{\underline{X}}(\underline{y}_i)\cdot V_i \cdot G(S)\cdot V_i^{2/n} \approx$$

$$\approx \int_{\Re^n} f_{\underline{X}}(\underline{x})\cdot V(\underline{x})^{1+2/n}\cdot G(S)d\underline{x} = G(S)\cdot \int_{\Re^n} \frac{f_{\underline{X}}(\underline{x})}{(N\lambda(\underline{x}))^{1+2/n}}d\underline{x}$$

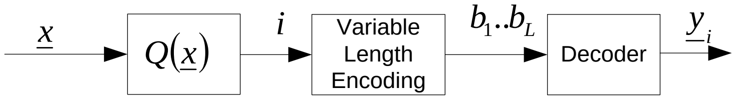
זוהי נוסחת Bennett. לאחר אופטימיזציה של λ מקבלים:

$$\lambda^{opt}(\underline{x}) \propto \left(f_{\underline{X}}(\underline{x})\right)^{\frac{n}{n+2}}$$
$$D^{opt} = G(S)\cdot \left\| f_{\underline{X}} \right\|_{\frac{n}{n+2}} \cdot 2^{-2R}$$
$$Where$$
$$R \equiv \tfrac{1}{n}\log(N)$$
$$\left\| f \right\|_{\alpha} \equiv \left[\int_{\Re^n} f^{\alpha}(\underline{x})d\underline{x}\right]^{\frac{1}{\alpha}}$$

<u>הערה</u>: עבור $\alpha<1$, $\left\| f \right\|_{\alpha}$ אינה נורמה.

קוונטיזציה עם קידוד אנטרופיה (Entropy Constrained Quantization)

עד כה הנחנו שה"מחיר" של כל מילת קוד הוא קבוע או במילים אחרות שהמגבלה היא על כמות מילות הקוד. בקידוד אנטרופיה נניח שניתן לבצע קידוד באורך משתנה:



אורך המילה הממוצע בקידוד משתנה באורך בלוק גדול הוא בקירוב האנטרופיה של i (או של $\underline{y}_i$), לכן הקצב (כמות סיביות לסימבול מקור) יהיה:

$$R = \tfrac{1}{n}E(L_i) \approx \tfrac{1}{n}H(Q(\underline{X}))$$

והעיוות יהיה כמו קודם:

$$D \equiv E(d(\underline{X}, Q(\underline{X})))$$

המטרה היא להשיג מינימום עוות D תחת אילוץ על הקצב R או להיפך (מינימום קצב תחת אילוץ על העיוות).

$$H(Q(\underline{X})) = -\sum_{i=1}^{N} p_i \log(p_i) \approx .. \approx h(\underline{X}) - \int_{\Re^n} f_{\underline{X}}(\underline{x})\log\left(\frac{1}{N\lambda(\underline{x})}\right)d\underline{x}$$

לאחר מינימיזציה של λ תחת אילוץ על העיוות (אותה נוסחא כמו קודם) מתקבל:

$$R^{opt} = \tfrac{1}{n}H(Q^{opt}) \approx \tfrac{1}{n}h(\underline{X}) - \tfrac{1}{2}\log\left(\frac{D}{G(S)}\right)$$

והפילוג λ^{opt} המתקבל בגבול $n \to \infty, N \to \infty$ הוא פילוג אחיד על כל המרחב. הסיבה היא שבניגוד למקרה הקודם המחיר של מילות קוד שההסתברות לקבל אותן היא נמוכה, הוא נמוך יחסית, ולכן אין חשיבות לריכוז מילות הקוד בתחום שבו האות נמצא בסבירות גבוהה.

קישור לתורת קצב עוות:

$$\underbrace{\frac{1}{n}\log N}_{\substack{\text{Rate without}\\ \text{Entropy Quantization}}} \geq \underbrace{\frac{1}{n}H(Q(\underline{X}))}_{\substack{\frac{1}{n}h(\underline{X})-\frac{1}{2}\log\left(\frac{D}{G(S)}\right)\\ \text{Rate with Entropy Quantization}}} \geq \underbrace{R_{SLB}(D)}_{\substack{\frac{1}{n}h(\underline{X})-\frac{1}{2}\log(2\pi eD)\\ \text{Shannon Lower bound}\\ \text{on rate-distortion function}\\ R_{SLB}(D)\approx R(D)\\ \text{When } D<<\sigma^2}} \leq \underbrace{R(D)}_{\substack{\text{Rate distortion}\\ \text{function}}}$$

אי-השוויון מתקבל ע"י תיאוריית קצב עוות (לא ניתן להשיג קצב נמוך יותר מ-$R(D)$ ולכן גם לא מ-R_{SLB}). אם נציב את הנוסחאות באי שוויון נקבל $G(S)\geq\frac{1}{2\pi e}$. $G(S)$ שואף לערך זה (מלמעלה) במקרה של כדור n מימדי, ולא ניתן לקבל $G(S)$ נמוך יותר.

מפרק זה ניתן להסיק מוטיבציה שתוביל אותנו לסריגים: למצא חלוקה של המרחב (או איזור במרחב) אחידה, עפ"י צורה S שיש לה מומנט שני מנורמל קטן ככל האפשר $G(S)$.

סריגים - קודים ליניאריים טובים במרחב האוקלידי

סריג Λ במרחב האוקלידי $\Re^n$ הוא אוסף ליניארי דיסקרטי של נקודות:

$$\Lambda=\left\{G\cdot\underline{i}:\underline{i}\in Z^n\right\}$$

כאשר $G_{[n\times n]}$ נקראת המטריצה היוצרת של הסריג. נסמן את העמודות של G (וקטורי הבסיס) ב- g_i:

$$G=\left(g_1\vdots g_2\vdots\cdots\vdots g_n\right)$$

$$G\cdot\underline{i}=\sum_{j=1}^{n}i_j g_j$$

תכונת הליניאריות:

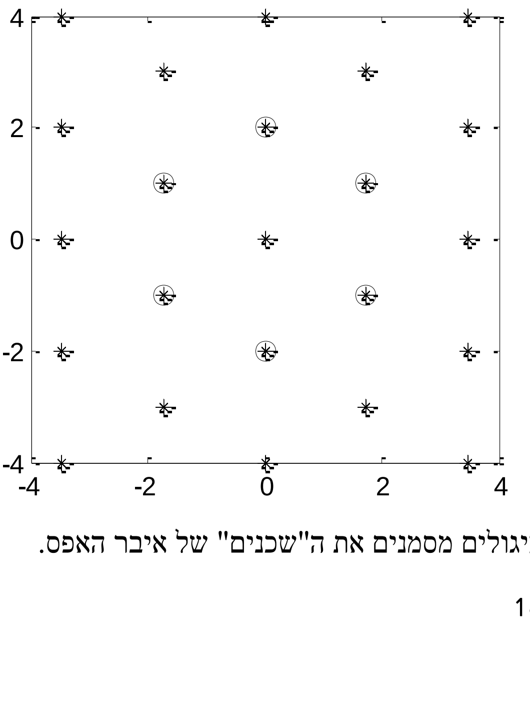
$$l_i,l_j\in\Lambda\Rightarrow l_i+l_j\in\Lambda$$

__דוגמאות:__

n=1: $\Lambda=\{0,\pm\Delta,\pm2\Delta,...\}$

n=2: הסריג היחיד "המעניין" הוא הסריג המשושה:

$$G=\begin{pmatrix}0&\sqrt{3}\\2&1\end{pmatrix}$$



העיגולים מסמנים את ה"שכנים" של איבר האפס.

ייצוגים שקולים לסריג: $G' = T \cdot G$ כאשר T מטריצת שלמים ו- $|T|=1$.

חלוקה סריגית: חלוקה של המרחב כאיחוד זר של תאים המתקבלים ע"י הזזה של תא הראשית בוקטורים l_i.

$$\Re^n = \dot{\bigcup} S_i$$

$$S_i = S_0 + l_i$$

S_0 (או V_0) נקרא "תא הראשית".

דוגמא: המקבילון של $g_1, \ldots, g_n$:

$$\left\{ \sum_{i=1}^{n} \alpha_i g_i : 0 \le \alpha_i \le 1 \right\} = G \cdot \begin{pmatrix} Unit \\ Cube \end{pmatrix} = G \cdot [0,1]^n$$

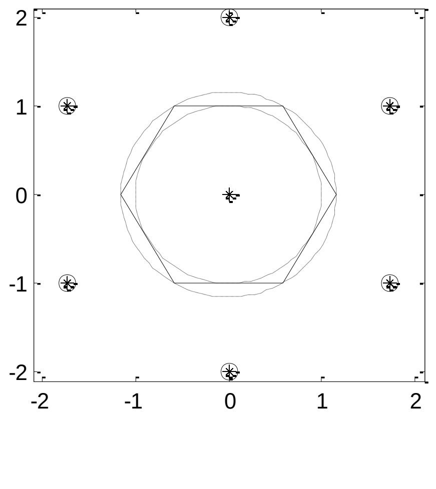
חלוקת וורונוי (Voronoi Partition): חלוקה סריגית לפי "השכן הקרוב ביותר" ביחס למדד הפרשי נתון (למשל מרחק אוקלידי).

עבור הסריג המשושה, תא וורונוי הוא משושה.

נפח התא אינווריאנטי לכלל החלוקה (כי בתוך נפח גדול מספר התאים שווה בקירוב למספר הנקודות, ולא תלוי בחלוקה), ולכן שווה לנפח המקבילון $\left|\det(G)\right|$.

תכונות של החלוקה:

- מומנט שני: $\sigma^2(\Lambda) = \frac{1}{nV} \int_{\underline{x} \in V_0} \|\underline{x}\|^2 \, d\underline{x}$
- רדיוס חוסם
- רדיוס חסום



<u>טיב של הסריג</u>

1. טיב לכיסוי (Covering):
הרדיוס החוסם של V_0 – רדיוס הכיסוי:

$$R_{\text{covering}} = \arg\min_R \left\{ R : \bigcup_i Ball\left(l_i, R\right) = \Re^n \right\}$$

עובי הכיסוי, $\theta\left(1\leq\right)$, מוגדר כנפח הכדור החוסם חלקי נפח תא וורונוי.

2. טיב לאריזה (Packing):

הרדיוס החסום:

$$R_{packing} = \arg\max_R \left\{ R : Ball\left(0, R\right) \bigcap Ball\left(l_i, R\right) = \phi, \forall l_i \in \Lambda \setminus 0 \right\}$$

צפיפות האריזה, $\Delta\left(1\geq\right)$, מוגדרת כנפח הכדור החסום חלקי נפח תא וורונוי.

3. טיב לקוונטיזציה (תחת מדד עיוות ריבועי):

מומנט שני מנורמל:

$$G\left(\Lambda\right) = \frac{\sigma^2\left(\Lambda\right)}{V^{2/n}} = \frac{1}{n} \cdot \frac{\int_{V_0} \left\|\underline{x}\right\|^2 d\underline{x}}{\left(\int_{V_0} d\underline{x}\right)^{1+\frac{2}{n}}}$$

- זה גודל חסר מימדים.
- העיוות הממוצע (תחת הנחת קוונטיזציה ברזולוציה גבוהה H.R.Q):

$$D_{MSE} = \sigma^2\left(\Lambda\right) = G\left(\Lambda\right) \cdot V^{\frac{2}{n}}$$

- אי-שוויון איזופרימטרי: מבין כל הצורות בעלות נפח נתון, לכדור יש מינימום מומנט שני:

$$G\left(\Lambda\right) > G_n^* = G\left(Ball\left(0, R\right)\right)$$

- נגדיר: $G_n = \min_{\Lambda\in\Re^n} G\left(\Lambda\right)$. מתקיים:

$$G_1=\frac{1}{12}$$
$$G_2=G\left(hexagon\right)=\frac{5}{36\sqrt{3}}$$
$$G_n,G_n^*\underset{n\to\infty}{\rightarrow}\frac{1}{2\pi e}$$

4. טיב לקידוד ערוץ גאוסי לבן:

נניח ספר קוד המורכב ממילים $l_i\in\Lambda$ (נתעלם מאילוץ ההספק), וערוץ AWGN:

$$Y=X+Z$$
$$Z\sim \mathrm{N}\left(0,\sigma^2\right)$$
$$X\in\Lambda$$

מפענח סבירות מרבית:

$$\underline{\hat{x}}_{M.L}=\arg\max_{\underline{x}\in\Lambda} p\left(\underline{y}\,|\,\underline{x}\right)=\arg\min_{l_i}\left\|\underline{y}-l_i\right\|=Q\left(y\right)$$

נגדיר:

$$\mu\left(\Lambda,P_e\right)\equiv\left.\frac{V^{\frac{2}{n}}}{\sigma^2}\right|_{\Pr\left\{Z\notin V_0\right\}=P_e}$$

ברור ש: $\mu\left(\Lambda,P_e\right)\underset{P_e\to 0}{\rightarrow}\infty$.

נגדיר כעת:

$$\mu_n\left(P_e\right)\equiv\inf_{\Lambda}\mu\left(\Lambda,P_e\right)$$

עבור כל $0<P_e<1$ מתקיים:

$$\mu_n\left(P_e\right)>\mu_n^*\left(P_e\right)$$
$$\mu_n\left(P_e\right),\mu_n^*\left(P_e\right)\underset{n\to\infty}{\rightarrow}2\pi e$$

כאשר μ_n^* הוא אותה הגדרה עבור צורת כדור.

הרצאה מס' 4

קידוד מקור עם עיוות לבעיות רשת

סוכם ע״י מיכל שמר

מבוא

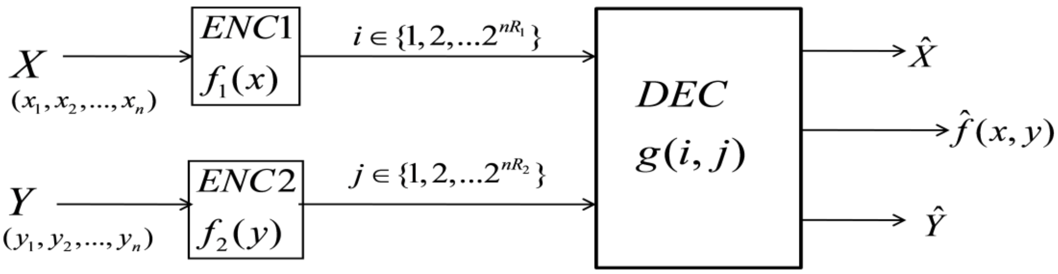
- דחיסה מבוזרת: דחיסה מכמה מקודדים
- דחיסה בתנאי אי-וודאות: מקור אחד למספר משתמשים
- מתקיימת דואליות בין הבעיות הבאות:

$$\text{Wyner Ziv} \Leftrightarrow \text{Gelfand Pinsker}$$

$$\text{Multi Terminal Source Coding} \Leftrightarrow \text{BCC}$$

דחיסה מבוזרת של מקורות עם עיוות

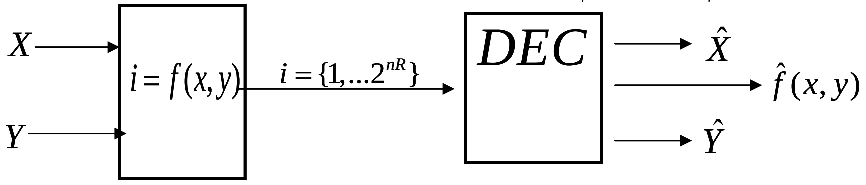
<u>סכימת המערכת:</u>
(שני מקורות או יותר מקודדים בנפרד)



- מניחים כי המקורות תלויים
- מטרת המפענח לחשב את $\hat{x}$, $\hat{y}$ או פונקציה שלהם.

<u>השאלה הנשאלת:</u> כיצד ניתן לנצל את הקורלציה בין המקורות במקודד?

תרחיש הייחוס: P2P - מקודד אחד מקבל את כל המידע ומשדר זרם של ביטים.



מדד העיוות: ניתן להגדיר מס' אילוצי העיוות כדלקמן: $d_i(X,Y;\hat{X},\hat{Y},\hat{f}_i(X,Y)) \quad i=1,\dots,k$

<u>דוגמאות פשוטות:</u>

- שיחזור עם עיוות של שני מקורות בינאריים תחת מדד המינג:

$$\frac{1}{n}Ed_H\left(\underline{x},\underline{\hat{x}}\right)\le D_x$$

$$\frac{1}{n}Ed_H\left(\underline{y},\underline{\hat{y}}\right)\le D_y$$

- אות ממשי תחת מדד עיוות ריבועי:

$$\frac{1}{n}E\|x-\hat{x}\|^2 \le D_x$$

$$\frac{1}{n}E\|y-\underline{\hat{y}}\|^2 \le D_y$$

<u>המטרה</u>: הגדרת תחום בר-השגה עבור פונקצית הקצב עיוות:

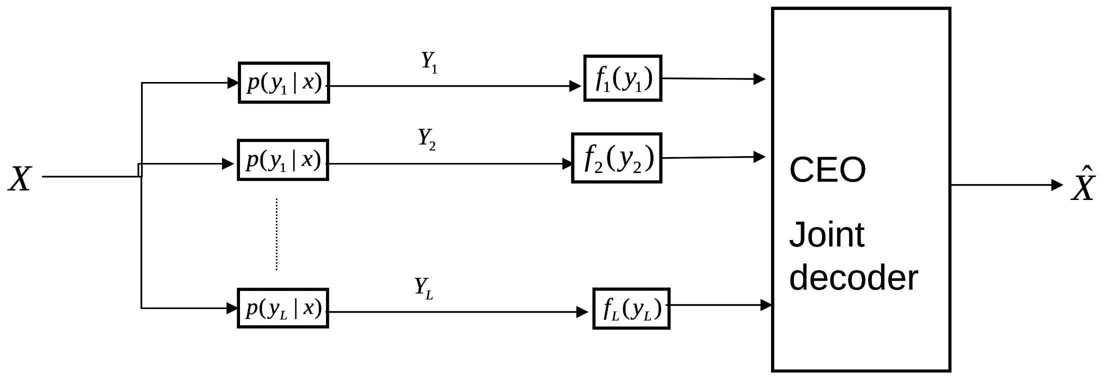
$$R=\left\{(R_1,R_2): \text{constraints } D_1...D_k \text{ hold}\right\}$$

עד כה, אין פיתרון לבעיה הכללית.

מקרים פרטיים של דחיסה מבוזרת עם עיוות:

- בעיית ה- CEO.
- דחיסה מרחוק: Remote/Noisy/Indirect Source Coding
- בעיית Two Help One – Korner Marton

בעיית הדיווח למנכ"ל – ה- CEO

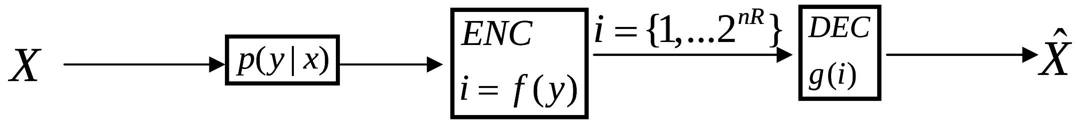


Y_i - מדידות רועשות של מקור חבוי X

המקרה המקובל ("המעניין") הינו ערוץ גאוסי תחת מדד עיוות ריבועי: $Y_i = X + N_i$

הבעיה נכללת בתחום של הסקה סטטיסטית תחת אילוצי תקשורת.

גרסת P2P של ה- CEO : Remote/Noisy/Indirect Source Coding



בעיית Dobrushin – Tsybakov

את בעיית הקידוד הלא ישירה אנו מתרגמים לבעיית קידוד מקור ישירה, אך עם מדד עיוות חדש.

$$R \equiv R_{x \text{ via } y}(d,D)$$

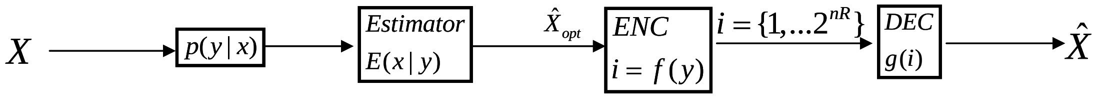
$$R \equiv R_{x \text{ via } y}(d,D) = R_Y(d_{\text{eff}},D)$$

$$d_{\text{eff}}(y,\hat{x}) \equiv E\left\{d(X,\hat{x}) \mid Y=y\right\}$$

קישור הבעיה לבעיית BT (Berger-Tung)[11]: ניתן להוסיף את העברת אות המקור X בקצב אפס, בעוד מדד העיוות יתייחס רק למקור ולא למדידות.

בעיית Wolf-Ziv (1970)

תחת מדד עיוות ריבועי, ניתן לפתור את בעיית BT (תתואר בהמשך) באופן הבא:



ומתקבל: $R_{x \text{ via } y}(MSE, D) = R_{\hat{X}_{opt}}(MSE, D)$

תחת מדד עיוות ריבועי , מתקיים עיקרון הפרדה (שיערוך וקידוד). לפיכך, ניתן ראשית לחשב את משערך ה- MMSE של X מתוך Y, ואח"כ לבצע קידוד:

$$D \geq D_{\min} = Var(x \mid y)$$

בכל בעיה מהצורה: $D \geq D_{\min} = \min_{g(\bullet)} E(x, g(y))$ נקבל כי שוויון יושג רק כאשר $R \to \infty$.

בפיתרון של Wolf-Ziv חבוי עיקרון האורתוגונאליות:

$$e_1 = X - \hat{X}^{opt}(y) \quad \perp \hat{X}^{opt}$$
$$e_2 = \hat{X}^{opt}(y) - \hat{X} \quad \perp \hat{X}$$

הביטוי הראשון מתייחס לשגיאת השערוך, ואילו השני לשגיאת הקוונטייזר/הדוחס.
מערכת קוונטיזציה אופטימאלית מקיימת ששגיאת הקוונטיזציה ניצבת לכל פונקציה של הכניסות.
כלל מרכז הכובד : נקודת השחזור = נקוות התוחלת המותנית ($\longleftarrow$ שגיאת הדוחס ניצבת למוצא הקוונטייזר).

$$e_1 \perp e_2 \Rightarrow E(e_1 + e_2)^2 = E(e_1)^2 + E(e_2)^2$$

תחום הקצבים של Berger-Tung (1978)

הערה: זוהי הכללה של בעיית WZ לבעיות Multi-Terminal והיא חסרת converse, למעט במקרה הגאוסי תחת מדד עיוות ריבועי.

ניתן להשיג עיוותים D_1, D_2 (באופן כללי עד D_k) בקידוד X ו- Y אם קיימים מ"א U,V כך שמתקיים: $U \leftrightarrow X \leftrightarrow Y \leftrightarrow V$ (long Markov chain):

$$\begin{cases} R_1 \geq I(X;U \mid V) \\ R_2 \geq I(Y;V \mid U) \\ R_1 + R_2 \geq I(X,Y \mid U,V) \end{cases}$$

---

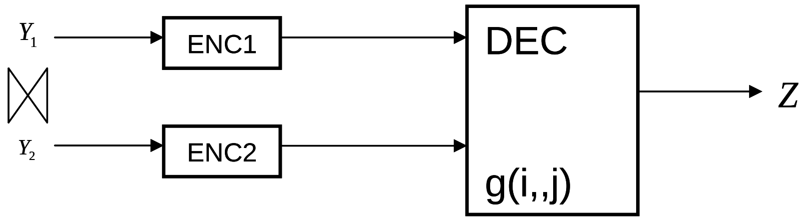
[11] הבעיה תתואר בהמשך

וכן פונקציות $g_1(u)$, $g_2(u)$ כך שמתקיים:

$$\begin{cases} Ed_1(X, g_1(U)) \le D_1 \\ Ed_2(Y, g_2(V)) \le D_2 \end{cases}$$

תחום BT הינו בר השגה לכל מדד עיוות , אך הינו הדוק רק במקרה של מא"ג תחת מדד עיוות ריבועי. כמו כן, זהו תחום הדוק עבור בעיית ה – CEO הגאוסית תחת מדד עיוות ריבועי.
כיצד מתאימים את תחום הקצבים של BT לבעיית ה – CEO הגאוסית? נתייחס אל X כאל אחד המקורות בבעיה, אך נקצה לו קצב אפס. מדד העיוות לעומת זאת, יתייחס רק לעיוות על X, וירשה עיוות בלתי מוגבל על Y_i.

Two Help One (Korner-Marton 1979)



התלות בין המקורות נובעת מערוץ BSC, כלומר $P_r(Y_1 \ne Y_2) = p$.

מדד העיוות הינו: $d(Z, Y_1, Y_2; \hat{Z}) = d_H(Z; \hat{Z})$

הקידוד הינו מבוזר ומתקיים: $Z \equiv Y_1 \oplus Y_2$.

פיתרון Berger-Tung:

$$R_1 + R_2 \ge H(Y_1, Y_2) \underset{\text{chain rule}}{=} 1 + H_B(p)$$

$\Leftarrow$ גישת ה- single letter נכשלת.
במידה ולדוחסים הייתה ניתנת האפשרות לשיתוף פעולה , הם היו מחשבים את $Z \equiv Y_1 \oplus Y_2$ ישירות, ואז ניתן היה לדחוס לפי $H_B(p)$.

Korner-Marton הראו שניתן לדחוס לפי:

$$R_1 = R_2 = H_B(p)$$
$$\Rightarrow R_{sum} = 2H_B(p)$$

<u>*הוכחת ה – Converse*</u>

Y_2 ידוע למפענח, נחשב חסם תחתון עבור הקצב הנדרש לדחיסת Y_1:

$$R_1 \ge H(Y_1 | Y_2) = H_B(p)$$
$$R_2 \ge H(Y_2 | Y_1) = H_B(p)$$

למעשה, אנו מעוניינים ב"דחיסת הרעש":

ENC1: *syndrome*(Y_1)=HY_1
ENC2: *syndrome*(Y_2)=HY_2

<u>הערה</u>: העברת הסינדרום שקולה להעברת הסדרה Y_1 מודולו ספר קוד בינארי ליניארי, כאשר H מטריצת בדיקת הזוגיות.

המפענח ניעזר בליניאריות של הקוד:

$$\text{DEC:}\ \hat{Z} = f(syndrome1 \oplus syndrome2) = f\left(H(y_1 \oplus y_2)\right) = f\left(HZ\right)$$

אם H היא מטריצת בדיקת זוגיות של קוד טוב לערוץ BSC(p), אזי נוכל לשחזר את Z מתוך HZ בהסתברות גבוהה $\Leftarrow \hat{Z} = Z$.

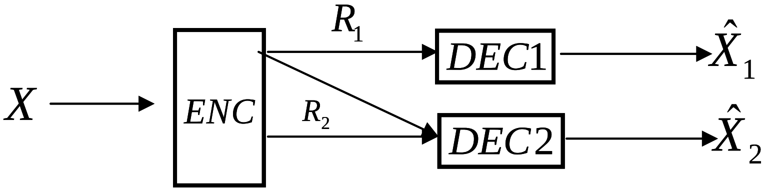
<u>מסקנה</u>: תחום BT אינו אופטימאלי באופן כללי.

אילו בעיות כדאי לפתור בעזרת BT? כאשר בבעיה טמון מקור חבוי (לדוגמא: בעיית ה - CEO), ואז מתקיים כי המדידות בלתי תלויות בהינתן המקור. במקרים אלו, פיתרון האות הבודדת יתקבל כאופטימאלי.

דחיסה בתנאי אי-ודאות

גורמי אי-ודאות:
- תעבורה ברשת (קיבול).
- תקינות של נתיבים.
- מדד העיוות.

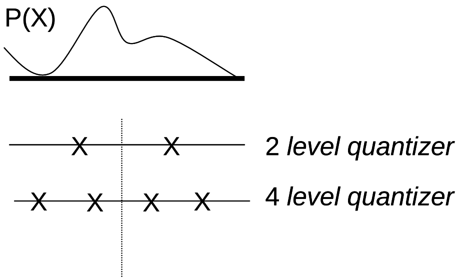
שני תרחישי יסוד:
1. עידון הדרגתי (Successive Refinement)



2. ריבוי תיאורים (Multiple Description).

Successive Refinement

דוגמא:



מיקום נקודת הייצוג יקבע לפי תנאי לויד, כלומר נקודת מרכז הכובד.
באופן כללי, קווטייזר ארבע רמות אינו עידון של קוונטייזר שתי רמות.

<u>מסקנה</u>: שימוש בתכונת ה- SR טומן בחובו הפסד.

נשאל שתי שאלות:

1. מהם הקצבים $R_1, \Delta R$ והעיוותים D_1, D_2 ברי ההשגה?
2. האם קיים Perfect Successive Refinement (PSR)?

<u>תוצאות:</u>

1. Rimoldi(1994)

זוג עיוותים D_1, D_2 הוא בר השגה בתחום SR אם"ם קיימים זוג מ"א כך ש:

$$\begin{cases} R_1 \ge I(X;\hat{X}_1) & Ed_1(X,\hat{X}_1) \le D_1 \\ R_1 + \Delta R \ge I(X;\hat{X}_1,\hat{X}_2) & Ed_2(X,\hat{X}_2) \le D_2 \end{cases}$$

2. Equitz & Cover (1991)

ניתן להשיג PSR אם"ם ניתן לכתוב את המ"א $\hat{X}_1$, $\hat{X}_2$ המגשימים את פונקצית קצב העיוות בעיוותים D_1, D_2 כשרשרת מרקוב: $X \leftrightarrow \hat{X}_2^* \leftrightarrow \hat{X}_1^*$.

כלומר:

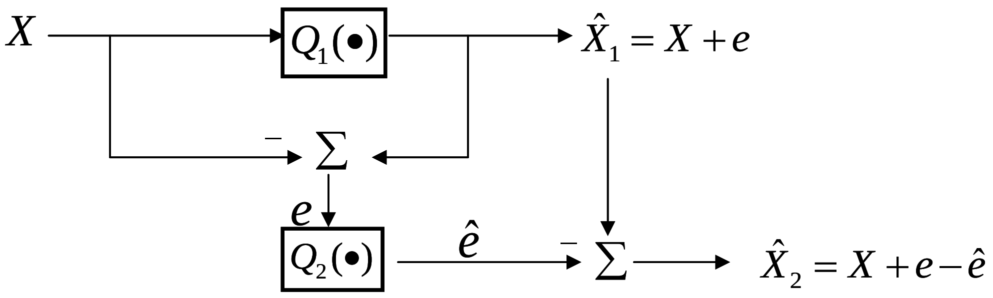
קיים $p^*(X_1 \mid X)$ כך ש: $I(X,X_1^*) = R(D_1)$

קיים $p^*(X_2 \mid X)$ כך ש: $I(X,X_2^*) = R(D_2)$

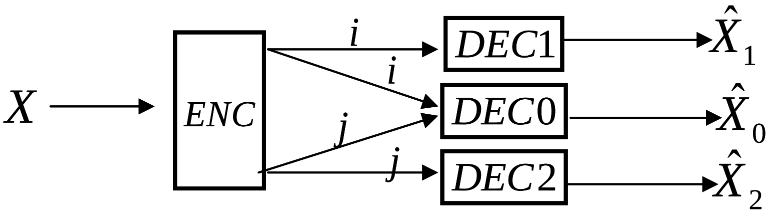
קיים פילוג היפותטי $p(X_2 \mid X_1)$ כך שמתקיים: $p^*(X_1 \mid X) = p^*(X_2 \mid X)p(X_1 \mid X_2)$

המקרה הרציף היחיד בו מתקיים התנאי: פילוג גאוסי תחת מדד עיוות ריבועי.

3. Successive Quantization (Multi-Stage)



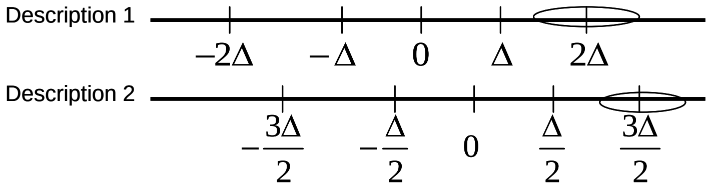
דחיסת מקור עם ריבוי תיאורים (Multiple Description)



"סיפור המעשה": משלוח ידיעה באינטרנט/ערוץ: אם כל הודעה תגיע בנפרד, נרצה לקבל תיאור גס, אם שתי ההודעות תגענה יחדיו, נרצה לקבל תיאור עדין יותר.

<u>דוגמא 1</u>: Staggered Quantizers

נתבונן בקוונטייזר סקלרי עם גודל צעד Δ:



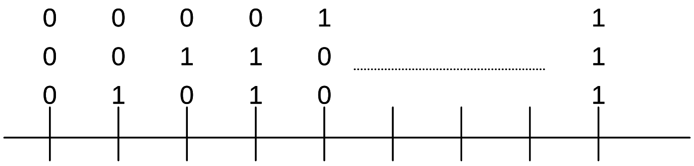
שקלול שני התיאורים מצמצם את תחום אי-הוודאות לגבי ערך המשתנה לכדי $\frac{\Delta}{2}$.

קוונטיזר אופטימאלי למא"ג מקיים: $D=\sigma_X^2\,2^{-2R}$

ההפסד במימוש בעזרת קווניטזר סקלרי: $D\cong\sigma_X^2\,2^{-2R}\,\frac{2\pi e}{12}$ (תחת הנחת רזולוציה גבוהה - HR)

$$\Rightarrow D_0\cong\frac{1}{4}\sigma_X^2\,2^{-2R}\,\frac{2\pi e}{12}>>\sigma_X^2\,2^{-4R}\,\frac{2\pi e}{12}=D_0^{opt}$$

<u>דוגמא 2</u>: LSB[12]-MSB



התיאור הראשון יורכב מ- MSB ואילו התיאור השני יורכב מה- LSB.

$$D_0\cong\sigma_X^2\,2^{-2R_{sum}}\left(\frac{2\pi e}{12}\right)$$

$$D_1\cong\sigma_X^2\,2^{-2R_1}\left(\frac{2\pi e}{12}\right)$$

[12] LSB\MSB – Least\Most Significant Bit

<u>המטרה</u>: מציאת תחום הקיום של "החמישיות" $\left(R_1, R_2, D_1, D_2, D_0\right)$ ברות ההשגה (בגבול בו אורך הבלוק הולך לאינסוף).

התחום של El-Gamal & Cover (1982)

(קצבים ברי-השגה – Inner Bounds)

הערה: הוכיחו direct ולא converse , אופטימאלי רק במקרה הגאוסי.

ניתן להשיג חמישייה אם קיימים מ"א $\hat{X}_0, \hat{X}_1, \hat{X}_2$ כך שיתקיים:

$$\begin{cases} R_1 \ge I(X;\hat{X}_1) \\ R_2 \ge I(X;\hat{X}_2) \\ R_1 + R_2 \ge I(X;X_0,X_1,X_2) + I(X_1;X_2) \end{cases}$$

תחת אילוצי העיוות הבאים:

$$Ed(X;\hat{X}_0) \le D_0$$
$$Ed(X;\hat{X}_1) \le D_1$$
$$Ed(X;\hat{X}_2) \le D_2$$

נניח כי אילוץ העיוות הינו דטרמיניסטי ("קשה"):

$$X_0 \triangleq g_0(x) \;;\; X_1 \triangleq g_1(x) \;;\; X_2 \triangleq g_2(x)$$

$$\Rightarrow \begin{cases} R_1 \ge H(g_1(x)) = H(x_1) \\ R_2 \ge H(g_2(x)) = H(x_2) \\ R_1 + R_2 \ge H(X_0,X_1,X_2) + I(X_1;X_2) = \\ = H(X_1,X_2) + H(X_0 \mid X_1,X_2) + I(X_1;X_2) = \\ = H(X_1) + H(X_2) + H(X_0 \mid X_1,X_2) \end{cases}$$

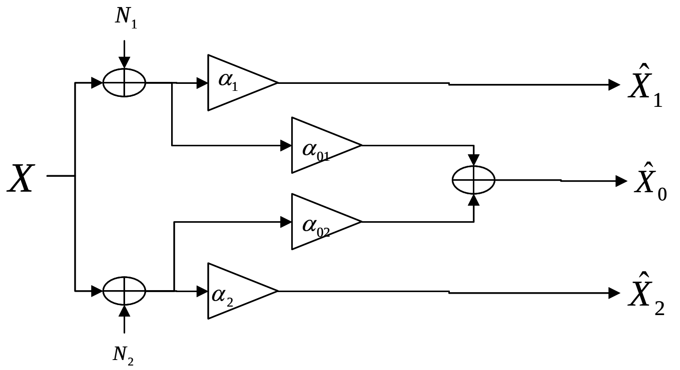
המקרה הגאוסי הריבועי:

(Quadratic Gaussian)

$$D_i = E(x - x_i)^2$$
$$X \sim N\left(0, \sigma_X^2\right) \quad i.i.d$$

Ozarow(1980) הוכיח משפט הפוך ביחס לפיתרון EG&C עבור המקרה הנ"ל. ההוכחה מסתמכת על עיקרון ה- EPI.

Ozarow's Test Channel



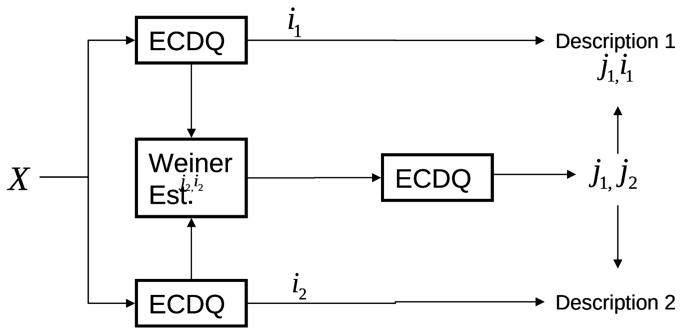
α_1 - שיערוך וינר של X מתוך X+N.

$$\Rightarrow D_1 = \frac{\sigma_X^2}{\sigma_X^2 + \sigma_{N_1}^2}$$

$$\begin{cases} R_1 = I(X;X_1) = \frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\sigma_{N_1}^2}\right) \\ R_2 = I(X;X_2) = \frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\sigma_{N_2}^2}\right) \\ R_1 + R_2 = I(X;X_2) + I(X;X_1) + I(N_1;N_2) \end{cases}$$

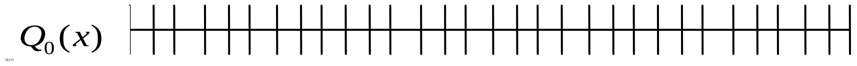
<u>שיטות קוונטיזציה:</u>

1. יעל פרנק דיין (2000):



2. Index Assignment – Vaishampayan(1993)

השיטה מתחילה מתיאור מרכזי , ומחלקת אותו ע"פ אינדקסים לשני תיאורים נפרדים בהתאם לטבלה הבאה:



1	3	6				
2	5	8	9			
4	7	10	12	14		
	11	13	15			
		16				

האינדקסים המפורטים בתוך הטבלה הם האינדקסים של הקוונטייזר המרכזי . התיאורים הנפרדים יבנו ע"פ מס' העמודה ומס' השורה של האינדקס המרכזי.

האינדקס j - פענוח עמודות.
האינדקס i - פענוח שורות.

עבור מס' אינדקסים כולל קבוע:

- רצועה צרה גוררת מס' רב של שורות/עמודות
- רצועה רחבה גוררת מס' רב של שורות/עמודות, היינו קצב נמוך.

חיסרון השיטה:

- קושי בהרחבת השיטה למקרה הוקטורי.
- מטבעה סימטרית, ועל כן אין באפשרותה לתת מענה למקרה הלא-סימטרי.
- אין אפשרות לקחת סטנדרטים קיימים (וידאו, קול וכו') וליישמה בהם.

הרצאה מס' 5

ערוץ ההפצה

סוכם ע"י אמיר רובין

A broadcast channel Overview may be found in the 2004 Lecture notes by Zak Levi.

Marton bounds for the broadcast channel

Inner bound for the achievable rates – 1st version of 2:

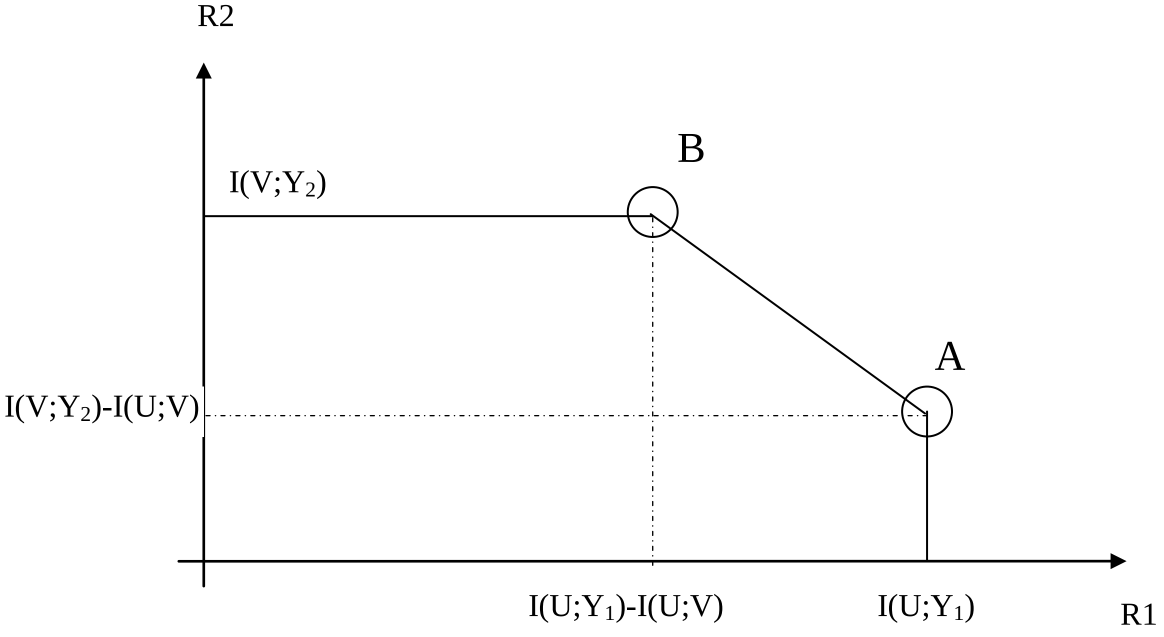
For every BCC the achievable rate region meets the following:

$$C^*_{Bcc} = \left\{ (R_1, R_2): \begin{array}{l} R_1 \le I(U;Y_1) \\ R_2 \le I(V;Y_2) \\ R_1 + R_2 \le I(U;Y_1) + I(V;Y_2) - I(U;V) \end{array} \right\}$$

$$\{U, V : (U,V) \leftrightarrow X \leftrightarrow (Y_1, Y_2)\}$$

<u>A coding/decoding system for given (U,V,X)</u>
For given U,V and X the region looks as shown in figure 7.

Figure 15



The way to obtain the corner point A: $(I(U;Y_1), I(V;Y_2)-I(U;V))$ is as follows:

Building code books:

a. Randomize 2^{nR1} words as u that are iid with distribution of P(U).
b. Randomize $2^{nR2'}$ words as v that are iid with distribution of P(V).
c. Random binning: Distribute the v words randomly and uniformly between 2^{nR2} cells (where $R_2<R_2'$).
d. Share the code books and cells distribution with the coder and decoder.

Transmission given w_1=i and w2=j

a. Select the u word with index i from the U coed book.
b. Search in the j cell the word v that is jointly typical with u (considering P(U,V))
c. Marton's solution can be expressed by: $x=\varphi(u,v)$
d. Transmission would be of $x_i=\varphi(u_i,v_i)$ where i=1,…n

Reception:

a. Given y_1 receiver 1 finds u in the code book that is jointly typical with that y_1. This provides w_1.
b. Given y_2 receiver 2 finds u in the code book of w_1 that is jointly typical with that y_2. This provides w_1. Than receiver 2 finds v in the code book of w_2 that is jointly typical with it and with u in the cell fit for derived w_2.

The Gelfand – Pinsker capacity may be viewed as:

$$C_{Bcc}^{Marton} \geq \left\{ (R_1, R_2): \begin{array}{l} R_1 \leq I(U;Y_1) \\ R_2 \leq I(V;Y_2) \\ R1 + R2 \leq I(U;Y_1) + I(V;Y_2) - I(U;V) \end{array} \right\}$$

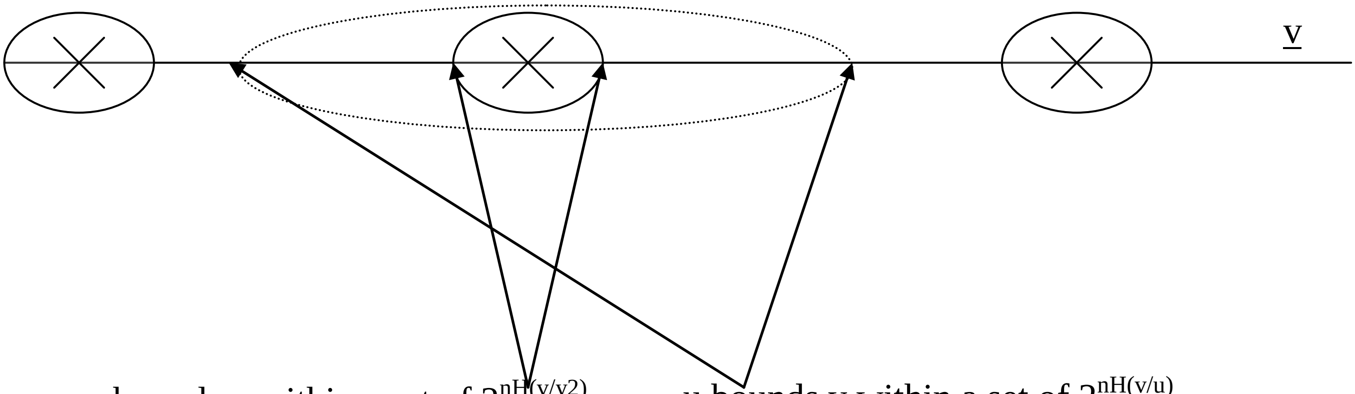
$$\{U,V : (U,V) \leftrightarrow X \leftrightarrow (Y_1, Y_2)\}$$

$$V \equiv "S"$$

$$C^{GP} = I(U;Y) - I(U;S)$$

<u>Error events analysis:</u>

a. According to the AEP, with probability 1-ε for sufficiently large n: (u, v, x, y1, y2) are jointly typical with respect to the true distributions.
b. Coding error: There's no v that is jointly typical with u in the j cell. For combating this we need: $R_2'>I(U;V)+R_2$ (I).
c. Decoding error in the 1st receiver (point A in figure 7 above):
   - $R_1<I(U;Y_1)$
d. Decoding error in the 2nd receiver:
   - For combating cases of 2 jointly typical v with y2 and with u we require that: $R_2'<I(V;Y_2)$ (II)
   - For combating cases of impersonation and as derived from (I) and (II), we require that: $R_2<I(V;Y_2)-I(U;V)$



$\underline{y}_2$ bounds $\underline{v}$ within a set of $2^{nH(\underline{v}/\underline{y}2)}$ $\underline{u}$ bounds $\underline{v}$ within a set of $2^{nH(\underline{v}/\underline{u})}$

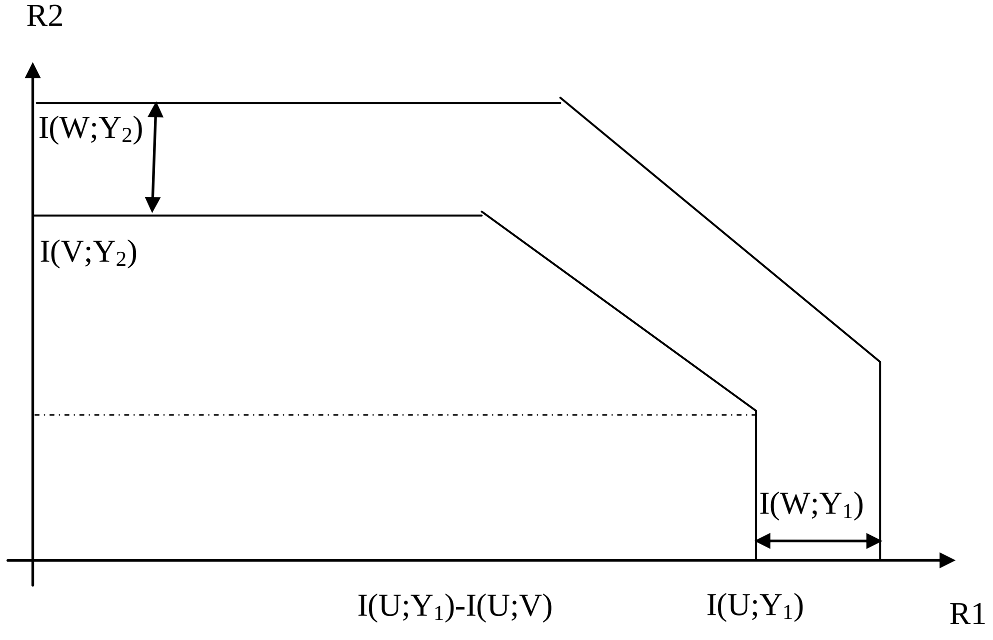
Inner bound for the achievable rates –2nd version and a generalization of 1st:

For every BCC the achievable rate region meets the following:

$$C_{Bcc}^{marton}(W,U,V) \geq \left\{ (R_1, R_2): \begin{array}{l} R_1 \leq I(W,U;Y_1) \\ R_2 \leq I(W,V;Y_2) \\ R1+R2 \leq \min(I(W;Y_1), I(W;Y_2)) + \\ I(U;Y1/W) + I(V;Y2/W) - I(U;V/W) \end{array} \right\}$$

$$C^{marton} = CloseConvexhull(C_{BCC}^{marton})$$

$$\{W,U,V : (W,U,V) \leftrightarrow X \leftrightarrow (Y_1, Y_2)\}$$



The special case of degraded channel

X ⬄Y_1⬄Y_2

Let V= ϕ an empty set

Marton's U=X

Marton's W=U

Therefore, according to the bounds from the previous paragraph:

$$C_{Bcc}^{marton}(W,U,V) \geq \left\{ (R_1, R_2): \begin{array}{l} R_1 \leq I(U,X;Y_1) \\ R_2 \leq I(U;Y_2) \\ R1 + R2 \leq I(U;Y_2) + I(X;Y1/U) \end{array} \right\}$$

$$C^{marton} = CloseConvexhull(C_{BCC}^{marton})$$

We can define:

R_2=R_0

$\Delta R1 = R_1 - R_0$

The derived C^{marton} is:

C^{marton}:

$R_0 <= I(U;Y_2)$

$\Delta R1 <= I(X;Y_1/U)$

For Gaussian BC:

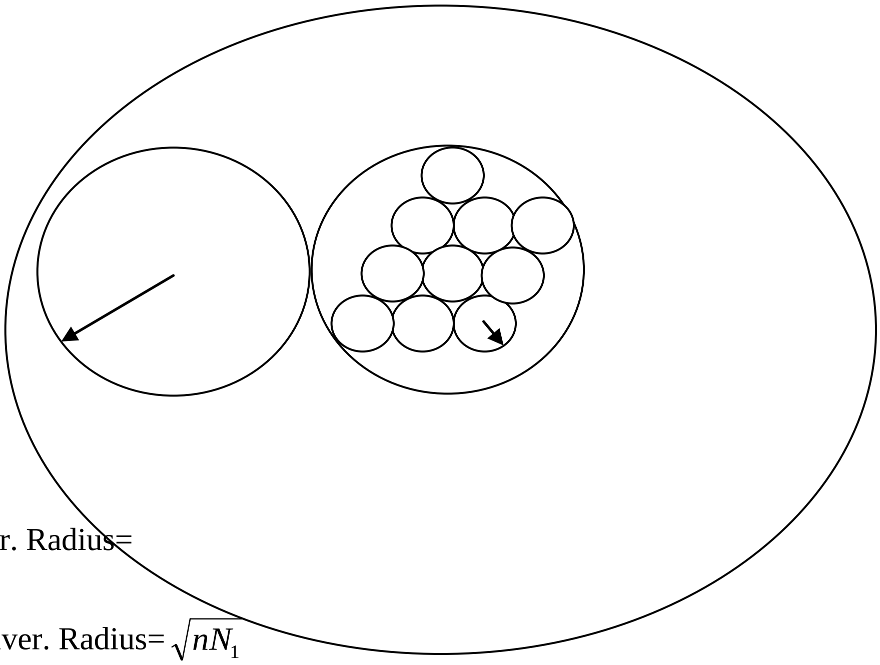
Y_1=X+Z_1

Y_2=X+Z_2=Y1+Z_2'

The capacity region:

U~N(0,αP), V~N(0,(1-α)P)

(R_1,R_2)=$(\frac{1}{2}\log_2(1+\frac{(1-\alpha)P}{N1}), \frac{1}{2}\log_2(1+\frac{\alpha P}{(1-\alpha)P+N2})$



Larger circle represents words for the bad receiver. Radius= $\sqrt{n((1-\alpha)P+N_2)}$

Smaller circle represents words for the good receiver. Radius= $\sqrt{nN_1}$

All code words are with same power P.

Capacity outer bound for the general BC

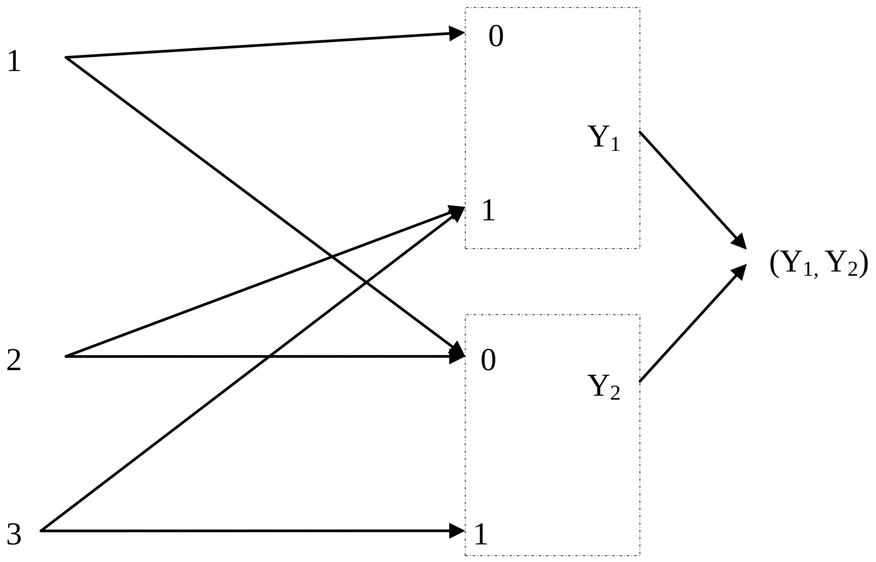
$$C_{Operative}(V) \le \left\{ (R_1, R_2) : \begin{array}{l} R_1 \le I(X;Y_1) \\ R_2 \le I(X;Y_2) \\ R1 + R2 \le \\ I(V;Y2) + I(X;Y1/V) \end{array} \right\}$$

$$\{V : V \leftrightarrow X \leftrightarrow (Y_1, Y_2)\}$$

Where V is side information that is known only to the decoder.

Marton's inner and outer bounds coincide in the following cases:

1. Degraded BC
2. Deterministic BC. This channel is of the type:
   $Y_1=f_1(X)$, $Y_2=f_2(X)$, $H(Yi/X)=0$
   for 2 deterministic functions f_1 and f_2. For example: Blackwell channel:



Pinsker-Marton theorem:
Capacity region of a deterministic channel:

$$\left\{ (R_1, R_2) : \begin{array}{l} R_1 \le H(Y_1) \\ R_2 \le H(Y_2) \\ R1 + R2 \le H(Y_1, Y_2) \end{array} \right\}$$

Over all channel inputs X.

2010

מרצה: פרופ׳ רם זמיר
מתרגל: אנטולי חינה

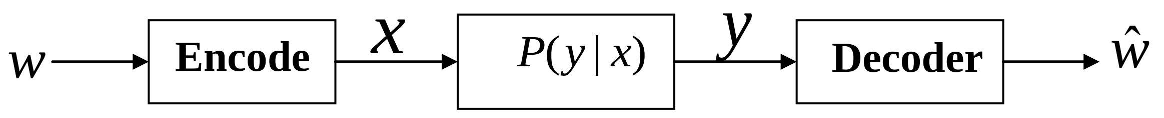
הרצאה מס' 1

מבוא

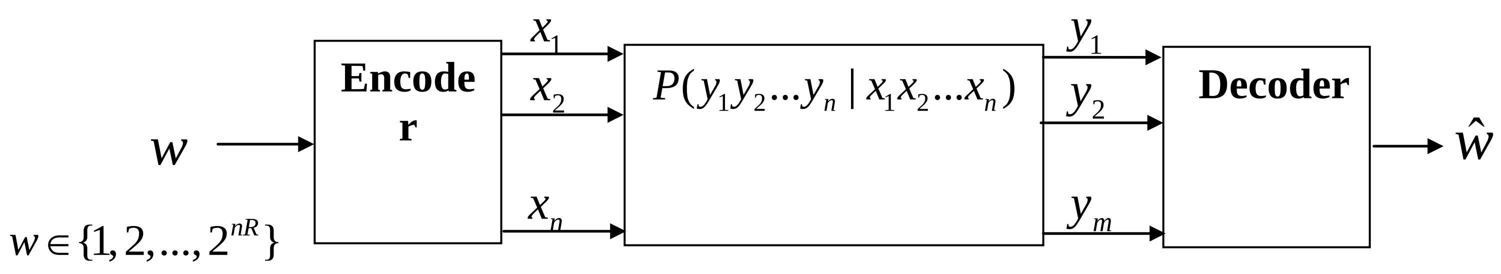
סיכם עמית שטראוס

Multi user channel – ערוץ מרובה משתנים

בבעיית ה – point to point (p2p) ראינו את בעיות הייחוס הללו:

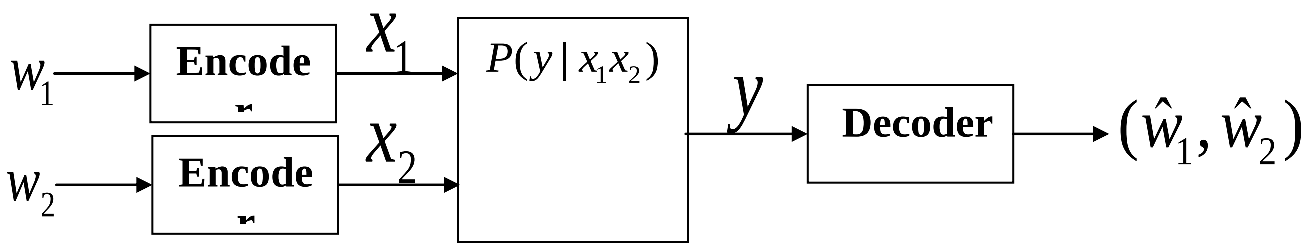


או בבעיית ה-p2p MIMO:

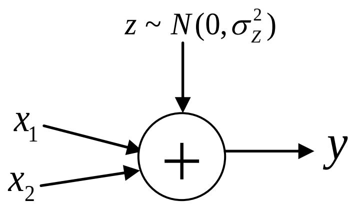


M.A.C. - Multiple Access Channel ערוץ מרובה משדרים

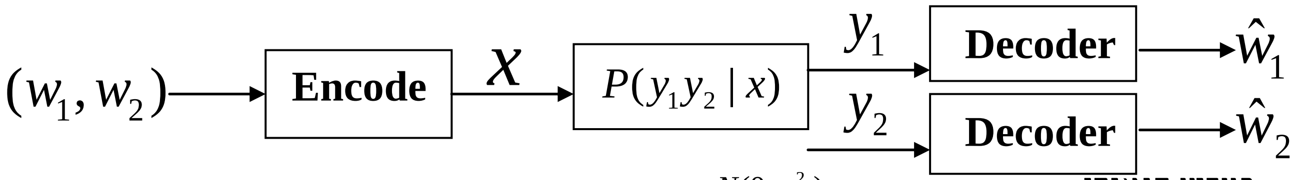
[Shannon 1961, Ahlswede 1970,Liao 1971]



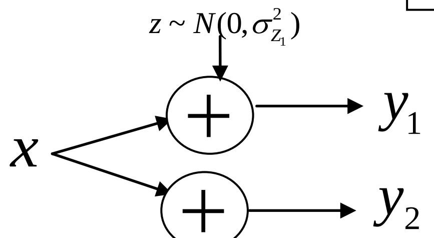
בעיית ה- MAC בערוץ הגאוסי:



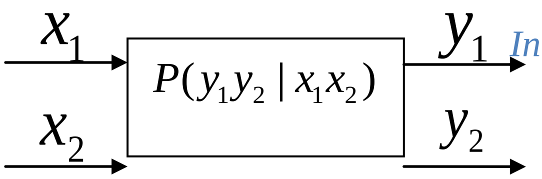
BroadCast Channel- ערוץ מרובה מקלטים/ערוץ הפצה



בערוץ הגאוסי:

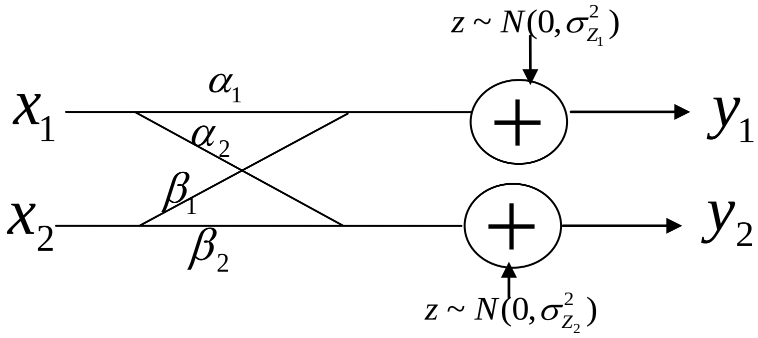


Interference Channel *ערוץ הפרעה*

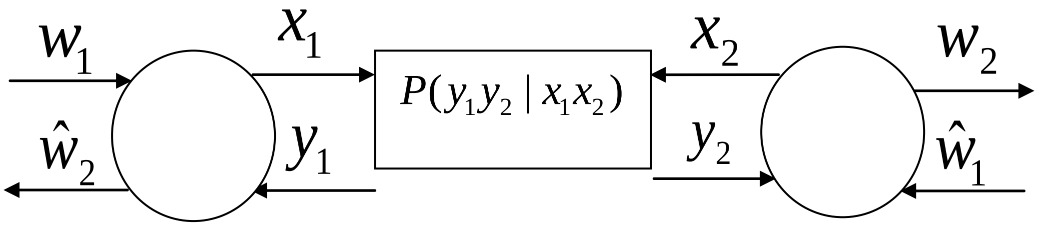


הכניסות הם מבוזרות – העיבוד בשידור/קליטה נעשה במקומות שונים.

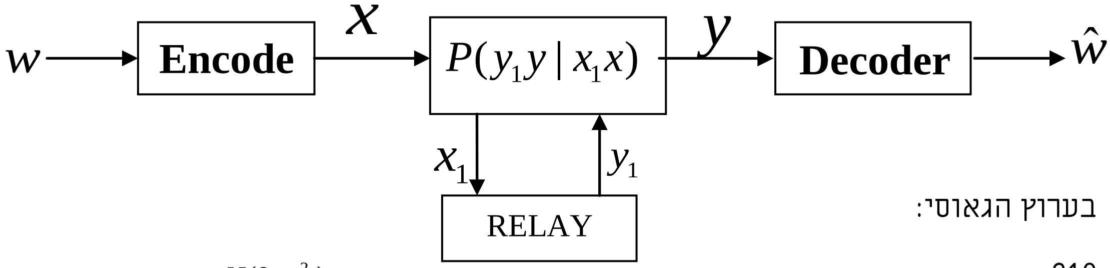
בערוץ הגאוסי:



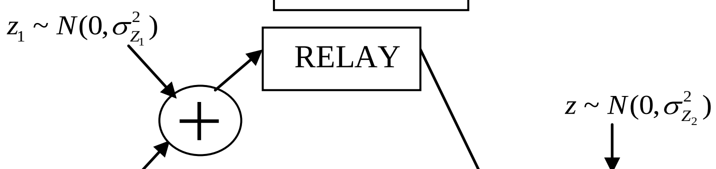
Two-way Channel *ערוץ דו כיווני/תקשורת אינטראקטיבית*



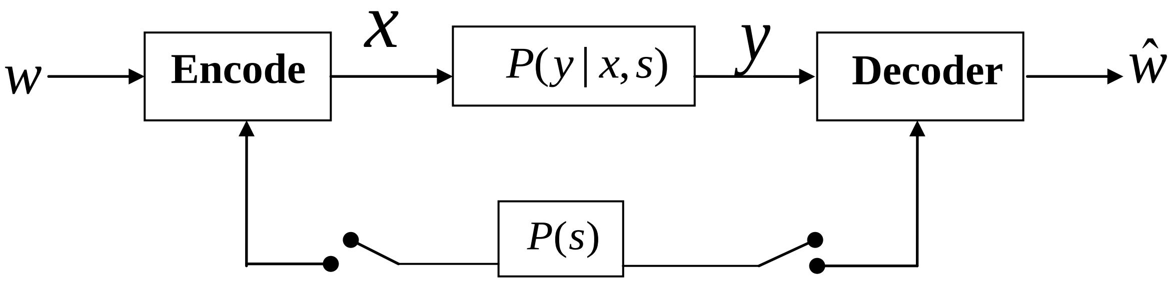
Relay *בעיית ממסר*



בערוץ הגאוסי:



Side Information   ערוץ עם מצב ידוע

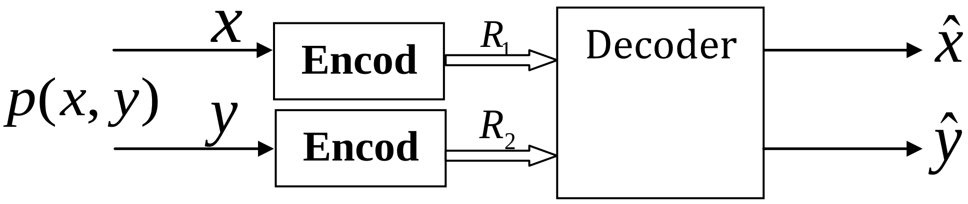


המצב S יכול להיות ידוע למקודד למפענח לשניהם או לאף אחד מהם.

Multi-User sources

D.S.C.   מקורות קורלטיביים/ מבוזרים

[Slepian-Wolf 1973]



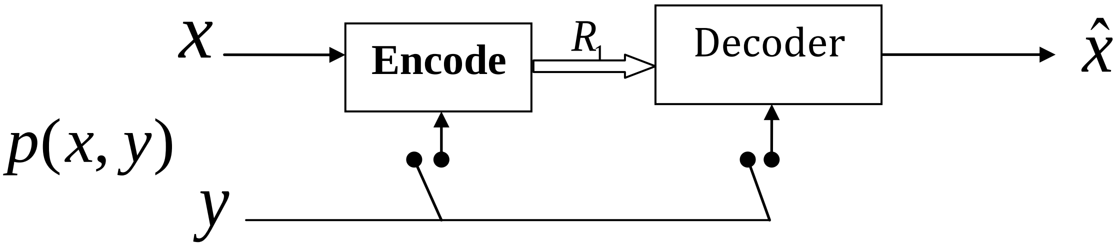
[כאשר ⟹ מסמל ערוץ דיגיטלי ללא רעש.]

Lossless if $x = \hat{x}$

Lossy if $d(x, \hat{x})$

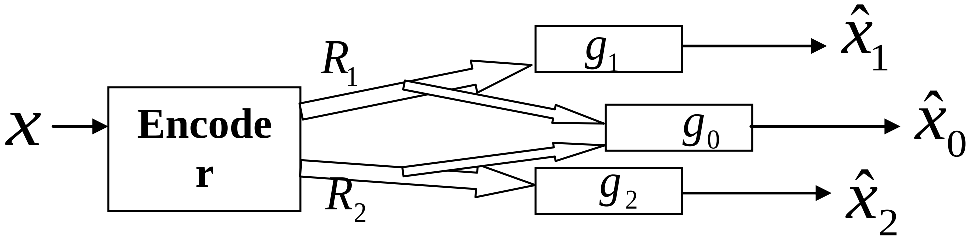
S.I. קידוד מקור עם אינפורמציית צד

[Wyner -Ziv 1976]



קידוד מקור עם ריבוי תיאורים M.D

[El Gamal 1962]



מקודדים את x ואז x מתפצל:

אם מגיע רק $\hat{x}_1$ או $\hat{x}_2$ רוצים רמת שיחזור מסוימת.

אם שניהם מגיעים רוצים רמת שיחזור $\hat{x}_0$

סוגי מיון הבעיות:

- היסטורי
- דילוגים – כמה "קפיצות" האות עובר עד שהוא מגיע ליעד
- שיטות ניתוח אינפורמציוניות
  - סטנדרטי
  - משתנה עזר
  - Random Binnig
  - קודים ליניארים / סריגים

מה יש בבעיות רשת שאין ב p2p:

1. הפרעות הדדיות.
2. שיתוף פעולה (ממסר helper).
3. משוב.
4. אינפורמציה $\neq$ חומר [ב-p2p אינפורמציה היא כמו צינור בבעיות רשת אין זה כך ניתן לדוגמא לשכפל].
5. אין את עקרון ההפרדה!

בבעיית p2p של קיבול עם אילוץ הספק P ראינו כי $C=\frac{1}{2}\log(1+SNR)$, כאשר $SNR=\frac{P}{\sigma_z^2}$. הקיבול מושג כאשר $\underline{X}(i)_j \sim N(0,P)$ ($j=1,2,\ldots,n$) הפתרון הוא ע"י קוד אקראי i.i.d. כאשר יש n תהליכים אקראיים.

כאשר n גדול ניתן לתאר את מילות הקוד יושבות על שפה של כדור n-מימדי

רדיוס הכדור של מילות הקוד x: $\sqrt{nP}$.

רדיוס כדורי הרעש z: $\sqrt{n\sigma_Z^2}$.

רדיוס של y: $\sqrt{n(\sigma_Z^2+P)}$.

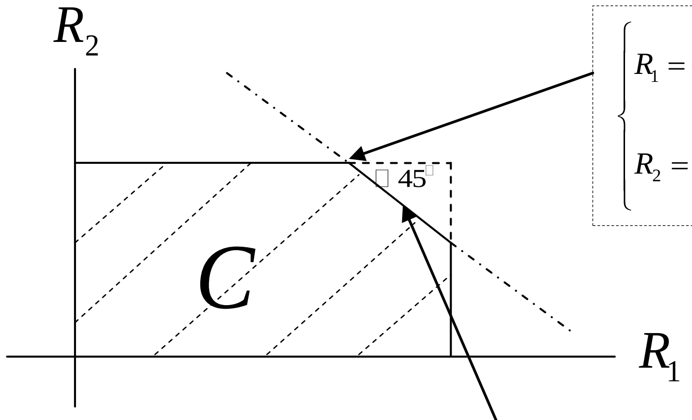
בהינתן y מחפשים את ה-x-ים האופייניים עם y, ולפי ה-AEP, ההסתברות שהיא מילת הקוד ששודרה שואפת ל-1, והסיכוי שמילת קוד אחרת (התחזות) נמצאת גם בכדור שואפת ל-0, בתנאי שהקצב קטן מהקיבול.

בעיית ה MAC עבור M=2:

בבעיה זו יש שני ,משתמשים שכל משתמש משדר בקצב אחר, ולכן כאן קיים **תחום קיבול** (לעומת גודל סקלרי ב- p2p).
תחום הקיבול:

במקרה הכללי   במקרה הגאוסי

$$C=\left\{(R_1,R_2):\begin{array}{c}R_1\le I(x_1;y\mid x_2),\\ R_2\le I(x_2;y\mid x_1),\\ R_1+R_2\le I(x_1,x_2;y\mid x_2)\end{array}\right\}=\left\{(R_1,R_2):\begin{array}{r}R_1\le\frac{1}{2}\log\left(1+{P_1}/{\sigma_Z^2}\right),\\ R_1\le\frac{1}{2}\log\left(1+{P_2}/{\sigma_Z^2}\right),\\ R_1\le\frac{1}{2}\log\left(1+\frac{P_1+P_2}{\sigma_Z^2}\right)\end{array}\right\}$$

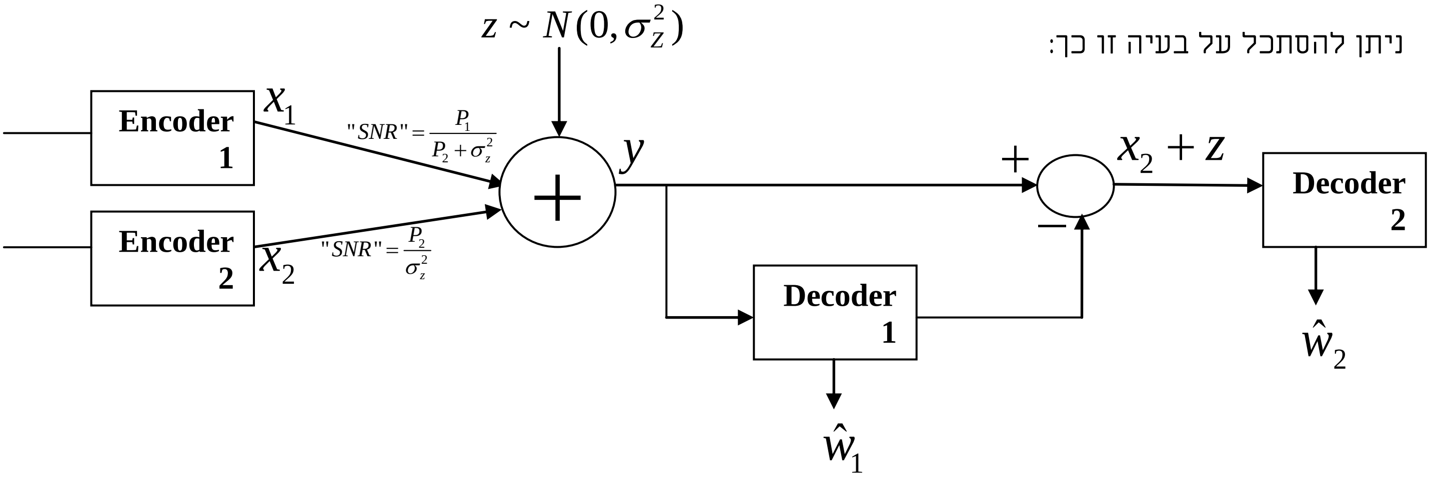


$$\left\{\begin{array}{l}R_1=\frac{1}{2}\log\left(1+\frac{P_1}{P_2+\sigma_Z^2}\right)\\ R_2=\frac{1}{2}\log\left(1+\frac{P_2}{\sigma_Z^2}\right)\end{array}\right\}\Rightarrow R_1+R_2=\frac{1}{2}\log\left(1+\frac{P_1+P_2}{\sigma_Z^2}\right)$$

כל הנקודות על הקו מקיימות

פרשנות הנדסית:
user2 הוא רעש עבור user1

ניתן להסתכל על בעיה זו כך:



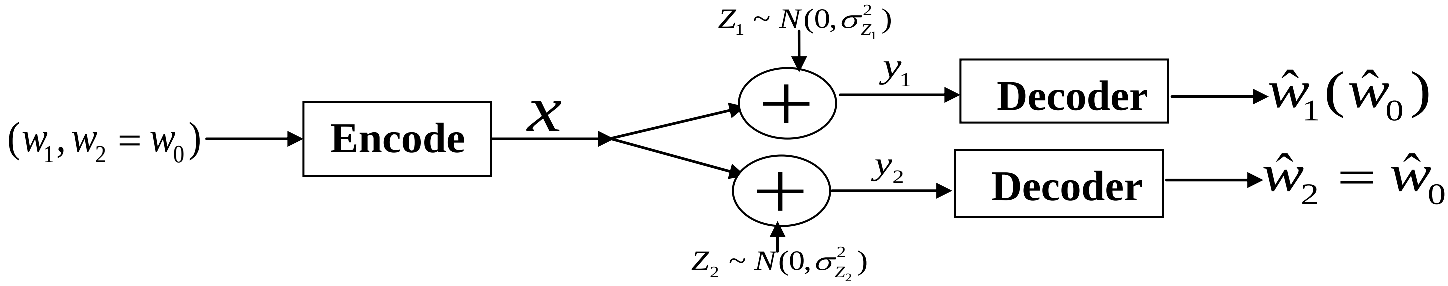
עבור המקרה $P_1 = P_2 = P$ נקבל $R_1 + R_2 \le \frac{1}{2}\log\left(1+\frac{2P}{\sigma_Z^2}\right)$

ואילו בבעיית הייחוס של ה-p2p: $C = \max_{p(x_1,x_2)} I(x_1,x_2;y)$ עם אילוץ הספק P.

כלומר במקרה זה נקבל: $P_1 = P_2 = P \Rightarrow \max(\mathrm{var}(x_1+x_2)) = 4P$

וא"כ $R_1 + R_2 \le \frac{1}{2}\log\left(1+\frac{4P}{\sigma_Z^2}\right)$, קרי ב- 3db יותר בעקבות שיתוף הפעולה בין המקודדים ("coherence gain")

בעיית Gaussian B.C.C



(אות השידור X הוא סופרפוזיציה של שני ספרי קוד גאוסים.)

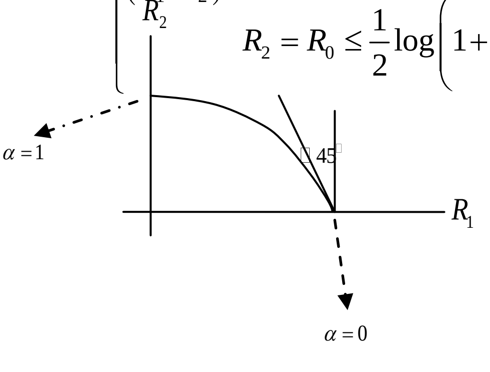
אם הרעשים $\sigma_{z_1}^2 = \sigma_{z_2}^2$ אז הבעיה שקולה לבעיית p2p. כאשר הרעשים שונים נרצה להעביר יותר אינפורמציה ל-user עם הרעש היותר נמוך, כי כל הודעה שמיועדת למשתמש "הגרוע" ניתן לפענח אצל המשתמש "הטוב".

$$C = \left\{ (R_1,R_2): \begin{array}{l} R_1 \le \frac{1}{2}\log\left(1+\frac{(1-\alpha)P}{\sigma_{Z_1}^2}\right) \\ R_2 = R_0 \le \frac{1}{2}\log\left(1+\frac{\alpha P}{(1-\alpha)P+\sigma_{Z_2}^2}\right) \end{array} \right\}$$

$0 \le \alpha \le 1$

$\alpha = 0$ משדרים רק ל- $user_1$

$\alpha = 1$ משדרים רק ל- $user_2$



הרצאה מס' 2

טיפוסים, אופייניות, "חריגות גדולות" ואקספוננט שגיאב

סוכם ע"י נבות בליק

חוק המספרים הגדולים (L.L.N.)

תהי $\{z_i\}$ סדרה של מ"א i.i.d. בעלי תוחלת $E\{z\}$, אזי

$$\frac{1}{n}\sum_{i=1}^{n} z_i \xrightarrow[n\to\infty]{} E\{z\}$$

כאשר ההתכנסות היא במובן m.s. (החוק החלש) וגם במובן a.s. (החוק החזק). כל אחד ממובני ההתכנסות הללו גורר גם התכנסות בהסתברות (p).

כמקרה פרטי, ניתן לראות:

$$-\frac{1}{n}\log p(X_1,...,X_n) = -\frac{1}{n}\log\prod_{i=1}^{n} p(X_i) =$$

$$= -\frac{1}{n}\sum_{i=1}^{n}\log p(X_i) \xrightarrow[n\to\infty]{} E\{-\log p(X)\} \triangleq H(X) = -\sum_{k\in\mathcal{X}} p_k \log p_k$$

נגדיר פונקצית אינדיקטור של המאורע $\{X_i = a\}$:

$$z_i = \text{indicator}\{X_i = a\} = 1_{\{X_i=a\}} = \begin{cases} 1, & X_i = a \\ 0, & \text{otherwise} \end{cases}$$

מכאן נוכל לקבל את הפילוג האמפירי של X:

$$\frac{1}{n}\sum_{i=1}^{n} z_i = \text{emirical dist.} \triangleq \frac{1}{n}N(a\,|\,\underline{x})$$

מחוק המספרים הגדולים נובע, שהגודל הנ"ל שואף לפילוג של X:

$$\frac{1}{n}N(a\,|\,\underline{x}) \xrightarrow[n\to\infty]{LLN} p_X(a)$$

אופייניות

הגדרה – קבוצה אופיינית במובן החלש:

$$A_{\varepsilon}^{(n)} = \left\{\underline{x} : \left| -\frac{1}{n}P(\underline{x}) - H(X) \right| < \varepsilon \right\}$$

הגדרה – קבוצה אופיינית במובן החזק:

$$A_{\varepsilon'}^{(n)*} = \left\{\underline{x} : \left| \frac{N(a\,|\,\underline{x})}{n} - P_X(a) \right| < \varepsilon' \qquad \forall a\in\mathcal{X} \right\}$$

הערות:

(1) נשים לב כי

$$-\frac{1}{n}\log p(\underline{x}) = -\frac{1}{n}\sum_{i=1}^{n}\log p(x_i) = -\sum_{a\in\mathcal{X}}\log p_X(a)\cdot\frac{N(a\,|\,\underline{x})}{n}$$

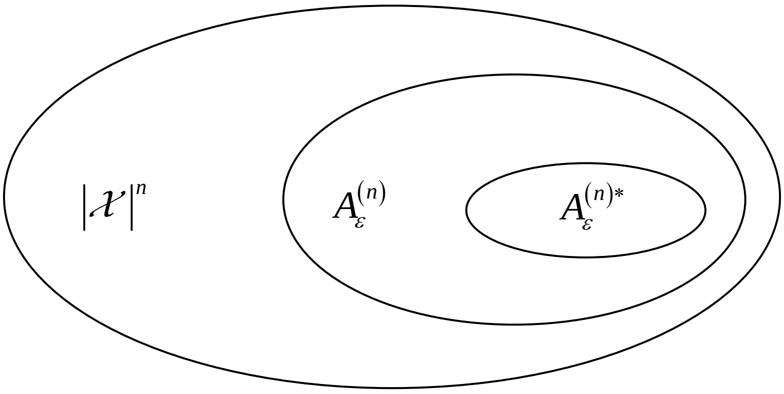
ולכן אם $\underline{x}$ מתפלג בקירוב לפי $p_X(x)$ אזי הוא בהכרח שייך לקבוצה אופיינית חלשה. מכאן נסיק כי אופייניות חזקה גוררת אופייניות חלשה.

(2) אופייניות חלשה לא בהכרח גוררת אופייניות חזקה.

(3) במקרה הבינארי עם אילוץ $0\le p\le 1/2$, יש שקילות בין שני סוגי האופייניות.

לדוגמא, עבור מקור טרנארי:

$$\mathcal{X}=\{0,1,2\} \qquad ; \qquad |\mathcal{X}^n| = |\mathcal{X}|^n = 3^n$$



A.E.P. – 'חוק השוויון באחרית הימים'

סימונים:
- $\doteq$ מציין שוויון עד לסדר ראשון באקספוננט.
- $A\backslash B$ מציין את חיסור הקבוצה B מהקבוצה A.

תכונות של הקבוצה האופיינית:

(1) $\Pr\left\{A_\varepsilon^{(n)}\right\}\xrightarrow[n\to\infty]{}1$.

(2) הסתברות כל סדרה בקבוצה $\doteq 2^{-nH}$.

(3) גודל הקבוצה $\doteq 2^{nH}$.

(1), (2) ו-(3) נכונים לשני סוגי האופייניות. לכן:

$$\Pr\left\{A_\varepsilon^{(n)}\setminus A_\varepsilon^{(n)*}\right\}\xrightarrow[n\to\infty]{}0$$

טיפוסים

באיזו הסתברות יתקבלו סדרות עם פילוג אמפירי P ממקור עם פילוג Q?

1. *טיפוס (type) של סדרה:*

$$P_{\underline{x}}=\begin{bmatrix}\frac{N(1|\underline{x})}{n} & \frac{N(2|\underline{x})}{n} & \dots & \frac{N(K|\underline{x})}{n}\end{bmatrix}^T$$

$$P_{\underline{x}}(k)=\frac{N(k|\underline{x})}{n}$$

2. *מרחב הטיפוסים (להבדיל ממרחב הפילוגים):*

$$|P_n|\le(n+1)^{|\mathcal{X}|-1}$$

לדוגמא, א"ב בינארי:

$$P_n=\left\{(0,1),\left(\frac{1}{n},\frac{n-1}{n}\right),...,\left(\frac{n-1}{n},\frac{1}{n}\right),(1,0)\right\}$$

3. *קבוצת הטיפוס:*

$$T_P=\{\underline{x}:\ \text{type}(\underline{x})=P\}$$

במקרה הבינארי:

$$|T_P|=\binom{n}{np}$$

במקרה הכללי:

$$|T_P|=\begin{pmatrix} & n & \\ np_1 & np_2 & \dots & np_K\end{pmatrix}\square\frac{n!}{(np_1)!(np_2)!\cdots(np_K)!}$$

<u>*דוגמא*</u>:

$\mathcal{X}=\{0,1\}$; $n=3$

$$P=\begin{bmatrix}\frac{1}{3} & \frac{2}{3}\end{bmatrix}$$

$T_P=\{(1,0,0),(0,1,0),(0,0,1)\}$; $|T_P|=\frac{3!}{2!1!}=3$

4. *קירוב סטירלינג לגודל קבוצת הטיפוס*

$$|T_P|\square 2^{nH(\underline{P})}$$

קירוב עדין יותר נותן:

$$\frac{1}{(n+1)^{|\mathcal{X}|}}2^{nH(\underline{P})}<|T_P|<2^{nH(\underline{P})}$$

5. ***הסתברות לסדרה מסוימת מטיפוס P ממקור עם פילוג Q:***

$$P_{\underline{x}} = P$$

$$\Pr\left\{\underline{X} = \underline{x}\right\} = Q\left(\underline{x}\right) \overset{\text{i.i.d.}}{=} \prod_{i=1}^{n} Q\left(x_i\right) = \prod_{a\in\mathcal{X}} Q\left(a\right)^{N(a|\underline{x})} = \prod_{a\in\mathcal{X}} Q\left(a\right)^{nP(a)} = 2^{n\sum_{a\in\mathcal{X}} P(a)\log Q(a)} =$$

$$= 2^{n\left[\sum_{a\in\mathcal{X}} P(a)\log P(a) - \sum_{a\in\mathcal{X}} P(a)\log\frac{P(a)}{Q(a)}\right]} = 2^{-n\left[D(P\|Q)+H(P)\right]}$$

הערה: קיבלנו שלכל הסדרות מקבוצת הטיפוס יש את אותה ההסתברות להתרחש.

6. ***ההסתברות שתתקבל סדרה כלשהי מקבוצת הטיפוס P ממקור עם פילוג Q:***

$$\Pr\left\{\underline{x}\in T_P\right\} = Q^n\left(T_p\right) = \sum_{\underline{x}\in T_P} Q^n\left(\underline{x}\right)$$

ראינו בסעיף הקודם כי $Q^n\left(\underline{x}\right) \equiv 2^{-n\left[D(P\|Q)+H(P)\right]}$ לכל $\underline{x}\in T_P$, וכן בסעיף 4 קיבלנו $\left|T_P\right| \doteq 2^{nH(\underline{P})}$. לכן:

$$\Pr\left\{\underline{x}\in T_P\right\} = \sum_{\underline{x}\in T_P} Q^n\left(\underline{x}\right) \doteq \left|T_P\right|\cdot 2^{-n\left[D(P\|Q)+H(P)\right]} \doteq 2^{nH(\underline{P})}\cdot 2^{-n\left[D(P\|Q)+H(P)\right]} = 2^{-nD(P\|Q)}$$

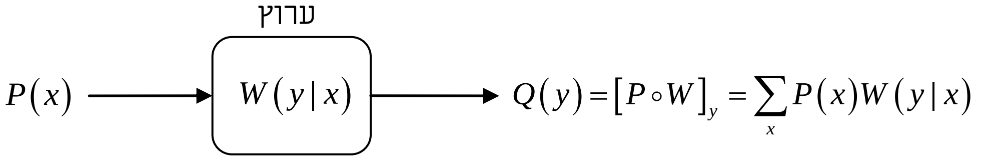
משמעות ה-divergence: אקספוננט הסיכוי לסדרה מטיפוס P "שאיננו אופייני" ביחס לפילוג המייצר Q.

7. ***הקשר בין אינפורמציה הדדית ל-divergence:***

סימונים:

- $P\circ W$ מציין את הפילוג המשותף של P,W.
- $P\times W$ מציין את הפילוג הבת"ס של P,W

$$I\left(X;Y\right) \equiv I\left(P,W\right) = \sum_x P\left(x\right)\sum_y W\left(y|x\right)\log\frac{W\left(y|x\right)}{Q\left(y\right)}$$



רואים כי למעשה $I\left(P,W\right) = D\left(P\circ W \| P\times W\right)$.

אינפורמציה הדדית היא אקספוננט הסיכוי שזוג $\underline{X},\underline{Y}$ בת"ס, עם הסתברויות שוליות P,Q בהתאמה יהיו שייכים לקבוצת הטיפוס $T_{P\circ W}$ (כלומר "התחזות": $\underline{X},\underline{Y}$ ייראו כאילו הם תלויים).

8. *טיפוסיות מותנית (טיפוס דרך ערוץ)*

- *טיפוס מותנה:* $V_{\underline{y}|\underline{x}}$ (מטריצה $|\mathcal{X}|\cdot|\mathcal{Y}|$).
- *קבוצת טיפוס מותנית:* $T_V\left(\underline{x}\right)$ = אוסף כל הסדרות $\underline{y}$ שנותנות אותו טיפוס מותנה V ביחס ל-$\underline{x}$.

אם $\underline{x}$ הוא מטיפוס P , אזי:

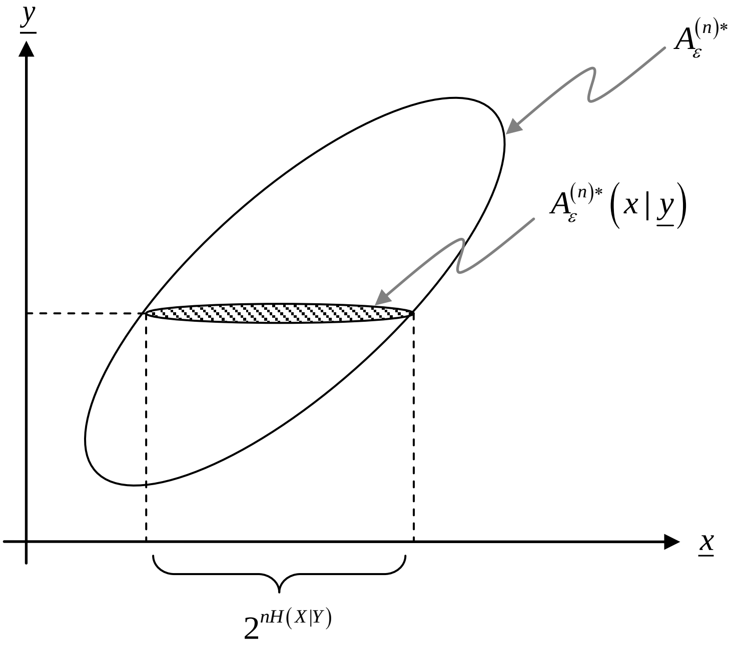
$$\left|T_V\left(\underline{x}\right)\right| = 2^{nH(V|P)}$$

$$H\left(V|P\right) \triangleq -\sum_x P\left(x\right)\sum_y V\left(y|x\right)\log V\left(y|x\right)$$

9. *הסיכוי שערוץ $W\left(y|x\right)$ יתנהג כאילו הוא ערוץ $V\left(y|x\right)$ ביחס לכניסה $\underline{x}$ מטיפוס P:*

$$W^n\left(V|P\right) = 2^{-nD\left(V\|W|P\right)}$$

$$D\left(V\|W|P\right) \triangleq \sum_x P\left(x\right)\sum_y V\left(y|x\right)\log\frac{V\left(y|x\right)}{W\left(y|x\right)}$$



10. *'אקספוננט סף הצלחה*

מבצעים 2^{nR} ניסויים בת"ס עם סיכוי הצלחה 2^{-nr} בכל ניסוי. אזי:

$$\Pr\left\{\text{at least one success}\right\}\xrightarrow[n\to\infty]{}\begin{cases}0, & R<r \quad (\text{I})\\ 1, & R>r \quad (\text{II})\end{cases}$$

מקרה (I) נכון גם אם הניסויים תלויים.

נקשר תוצאה זו לשתי בעיות חשובות בתורת האינפורמציה:

- ***קיבול ערוץ:*** נגדיר "success" = מילת קוד מתחרה מתוך ספר הקוד התחזתה לאופיינית. במקרה זה, R הוא קצב השידור בערוץ, ו- $r=I(P,W)$ כאשר P הוא פילוג הכניסה ו- W הוא פילוג המעבר בערוץ. קיבלנו במקרה זה כי אם $R<I(P,W)$, ההסתברות להתחזות שואפת ל-0 ולכן ניתן לשדר עם הסתברות שגיאה קטנה כרצוננו.
- ***פונקצית קצב עיוות:*** נגדיר "success" = נמצאה מילת קוד המקיימת את תנאי העיוות. במקרה זה, R הוא קצב הקידוד, ו- $r=I(X;\hat{X})$ כאשר X הוא המקור ו- $\hat{X}$ הוא מוצא המפענח. ראינו כי אם $R>I(X;\hat{X})$, ההסתברות שעבור מילת מקור תמצא מילה המקיימת את תנאי העיוות שואפת ל-1, ולכן ניתן לקודד ולפענח תחת אילוץ העיוות הנתון.

חריגות גדולות (large deviations)

דוגמא:
נתון מקור ברנולי כך ש-

$$P(1)\triangleq \Pr\{X_i=1\}=\frac{1}{3}$$

מה הסיכוי שמתוך 100 ניסויים יתקבלו לפחות 75 אחדים?

✓ דרך 1 – חישוב ישיר:

$$\Pr\{N_1\geq 75\}=\sum_{k=75}^{100}\binom{100}{k}\left(\frac{1}{3}\right)^k\left(\frac{2}{3}\right)^{100-k}$$

✓ דרך 2 – שימוש במשפט הגבול המרכזי:

$$\Pr\{N_1\geq 75\}=\Pr\left\{\sum_{i=1}^{100}X_i>75\right\}=\Pr\left\{\underbrace{\frac{1}{100}\sum_{i=1}^{100}X_i}_{\sim N\left(\frac{1}{3},\frac{2/9}{n}\right)}>0.75\right\}$$

✓ דרך 3 – משפט סאנוב.

משפט סאנוב
יהא E תחום סגור בעל נפח של פילוגים על $\mathcal{X}$. נניח שהסדרה $x_1,\ldots,x_n$ מתפלגת i.i.d. לפי $Q(x)$, כאשר $Q\notin E$. אזי:
$$\Pr\{\text{type}(x_1,\ldots,x_n)\in E\}\underset{n\to\infty}{\doteq}2^{-nD(P^*\|Q)}$$
כאשר:
$$P^*=\arg\min_{P\in E}D(P\|Q)\triangleq D(E\|Q)$$

הערות:

(1) בדוגמא שלנו $Q=\text{Bernulli}(1/3)$ ו- E הוא אוסף הפילוגים עם $P(1)\geq 0.75$.

(2) גם ללא התנאי ש- E סגור בעל נפח מתקיים חסם עליון:

$$\Pr\left\{P_{\underline{x}} \in E\right\} \le (n+1)^{|\mathcal{X}|} \cdot 2^{-nD\left(P^* \| Q\right)}$$

(3) דוגמא לתחום סגור בעל נפח הוא תחום קמור סגור.

(4) כללית, אנו דורשים ש- E יקיים את התנאי: "E is the closure of its interior".

<u>הוכחת החסם העליון</u>

$$\Pr\left\{\text{type}(x_1,...,x_n) \in E\right\} = \sum_{P\in E}\Pr\left\{\text{type}(x_1,...,x_n) = P\right\} \overset{(1)}{=} \sum_{P\in E\bigcap P_n}\Pr\left\{\text{type}(x_1,...,x_n) = P\right\} =$$

$$\overset{(2)}{\doteq} \sum_{P\in E\bigcap P_n} 2^{-nD(P\|Q)} \overset{(3)}{\le} \sum_{P\in E\bigcap P_n} 2^{-nD\left(P^*\|Q\right)} \overset{(4)}{\le} \sum_{P\in P_n} 2^{-nD\left(P^*\|Q\right)} = |P_n| \cdot 2^{-nD\left(P^*\|Q\right)} \overset{(5)}{\le} (n+1)^{|\mathcal{X}|} \cdot 2^{-nD\left(P^*\|Q\right)}$$

הצדקות למעברים:

(1) E מכיל גם נקודות שאינן שייכות לקבוצת הטיפוסים P_n, אך בנקודות אלה ההסתברות מתאפסת ולכן ניתן להשמיט אותן מהסכימה ולסכום על תת-הקבוצה $E\bigcap P_n$ בלבד.

(2) לפי ההוכחה בעמוד 218.

(3) לפי הגדרת P^*.

(4) מוסיפים איברים אי-שליליים לסכום.

(5) לפי החסם על גודל של מרחב הטיפוסים (עמוד 217).

סאנוב ביחס למעבר סף (threshold crossing) וקישור לחסם צ'רנוף

<u>דוגמאות למעבר סף:</u>

(1) הצלחות בתהליך ברנולי.

(2) גלישה של מונה פואסוני.

(3) גילוי סבירות מירבית או בייסיאני בבחינת השערות:

$$\text{L.L.R. = log likelihood ratio = } \log\frac{P(y_1,...,y_n\,|\,H_0)}{P(y_1,...,y_n\,|\,H_1)} = \sum_{i=1}^{n}\log\frac{P(y_i\,|\,H_0)}{P(y_i\,|\,H_1)} \underset{\text{decide } H_1}{\overset{\text{decide } H_0}{\gtrless}} T$$

<u>ייצוג הבעייה במונחי סאנוב:</u>

נרשום את מאורע מעבר הסף ע"י מומנט אמפירי:

$$\frac{1}{n}\sum_{i=1}^{n} m(x_i) \ge t$$

המומנט האמפירי שקול למומנט של הטיפוס, לכן נבחר את הקבוצה E להיות

$$E = \left\{P : \sum_{x\in\mathcal{X}} P(x)m(x) \ge t\right\}$$

כאשר התנאי $Q \notin E$ שקול ל-

$$\sum_{x} Q(x)m(x) < t$$

לפי משפט סאנוב, ההסתברות למעבר הסף נתונה ע"י:

$$\Pr\left\{\frac{1}{n}\sum_{i=1}^{n}m(x_i)\geq t\right\}=\Pr\left\{\text{type}(x_1,...,x_n)\in E\right\}\underset{n\to\infty}{\approx}2^{-nD\left(P^*\|Q\right)}$$

כאשר

$$P^*=\arg\min_{P\in E}D(P\|Q)=\arg\min_{\left\{P:\sum_x P(x)m(x)\geq t\right\}}\sum P(x)\log\frac{P(x)}{Q(x)}$$

ניתן לפתור את בעית המינימיזציה תחת אילוץ ע"י גזירת הלגרנז'יאן:

$$J(P)=D(P\|Q)-\lambda\sum_x P(x)m(x)+\mu\sum_x P(x) \qquad , \qquad \lambda>0$$

כאשר האיבר הימני נובע מהאילוץ:

$$\sum_x P(x)=1$$

הערה: נשים לב שהצבת $P=Q$ אמנם תאפס את האיבר $D(P\|Q)$, אבל האיבר השני יהיה שווה ל-

$$-\lambda\sum_x Q(x)m(x)>-\lambda t$$

בעוד שאנו מחפשים P המקיימת את האילוץ, כלומר:

$$-\lambda\sum_x P(x)m(x)\leq-\lambda t$$

כלומר, בחירת P עם מומנט $m(\cdot)$ יותר גבוה אמנם "תקלקל" את האיבר הראשון, אך תקטין את השני.

צורת הפתרון:

$$P_\lambda^*(x)=K\cdot Q(x)e^{-\lambda m(x)}$$

כאשר K הוא קבוע נרמול כך ש-$P_\lambda^*(\cdot)$ היא פונקצית הסתברות:

$$K\triangleq\frac{1}{\sum_{x'}Q(x')e^{-\lambda m(x')}}$$

וכן λ נבחר כך שהאילוץ מתקיים בשוויון:

$$\sum_x P_\lambda^*(x)m(x)=t$$

ניתן לראות כי קיבלנו פילוג מוטה של Q. עבור בחירה זו של $P_\lambda^*(\cdot)$, המשקל באקספוננט יהיה:

$$D\left(P_\lambda^*\|Q\right)=\sum_x K\cdot Q(x)e^{-\lambda m(x)}\log\frac{K\cdot Q(x)e^{-\lambda m(x)}}{Q(x)}=\sum_x K\cdot Q(x)e^{-\lambda m(x)}\left(\log K-\lambda m(x)\right)=$$

$$=\log K-\lambda\cdot\sum_x K\cdot Q(x)e^{-\lambda m(x)}\cdot m(x)=\log K-\lambda\cdot\begin{bmatrix}m\text{-th moment of the}\\ \text{tilted distribution}\end{bmatrix}$$

קישור סאנוב לחסמים קלאסיים

(1) *חסם מרקוב* – אם Y מ"א אי שלילי אזי:

$$\Pr\left\{Y>t\right\}\le\frac{E\left\{Y\right\}}{t}$$

בפרט, אם $Y=\frac{1}{n}\sum_{i=1}^{n}Z_i$ כאשר $\left\{Z_i\right\}$ מ"א i.i.d. בעלי תוחלת $E\left\{Z\right\}$ נקבל:

$$\Pr\left\{\frac{1}{n}\sum_{i=1}^{n}Z_i>t\right\}\le\frac{E\left\{Z\right\}}{t}$$

← קיבלנו חסם שאינו תלוי ב-n. החסם הזה לא טוב – אנחנו הרי רוצים חסם אקספוננציאלי ב-n, כמו בסאנוב.

(2) *חסם צ'בישב* (מתוך מרקוב):

$$\Pr\left\{\left|Y-\bar{Y}\right|>\Delta\right\}=\Pr\left\{\left(Y-\bar{Y}\right)^2>\Delta^2\right\}\le\frac{\operatorname{var}\left(Y\right)}{\Delta^2}$$

$$\Rightarrow\Pr\left\{Y>\bar{Y}+\Delta\right\}\le\frac{\operatorname{var}\left(Y\right)}{\Delta^2}$$

בפרט, אם נגדיר את Y כמו קודם וכן $t\,\Box\,\Delta+E\left\{Z\right\}$, נקבל:

$$\Pr\left\{\frac{1}{n}\sum_{i=1}^{n}Z_i>t\right\}\le\frac{\operatorname{var}\left(Z\right)}{n\left(t-\bar{Y}\right)^2}$$

← קיבלנו חסם יורד לפי $1/n$. החסם הזה עדיין לא מספיק טוב, משום שהירידה לא אקספוננציאלית ב-n.

(3) *חסם צ'רנוף* (צ'בישב מוכלל):

$$\Pr\left\{\phi\left(Y\right)>\alpha\right\}<\frac{E\left\{\phi\left(Y\right)\right\}}{\alpha}$$

עבור Y שהוא סכום איברים בת"ס, כדאי לבחור:

$$\phi\left(Y\right)=\exp\left(sY\right),\qquad s>0$$

ואז:

$$\Pr\left\{\sum_{i=1}^{n}Z_i>nt\right\}=\Pr\left\{\exp\left(s\sum_{i=1}^{n}Z_i\right)>\exp\left(snt\right)\right\}\overset{\text{Markov}}{\le}\frac{E\left\{\exp\left(s\sum_{i=1}^{n}Z_i\right)\right\}}{\left(e^{st}\right)^n}=$$

$$=\frac{E\left\{\prod_{i=1}^{n}e^{sZ_i}\right\}}{\left(e^{st}\right)^n}\overset{\text{i.i.d.}}{=}\frac{\prod_{i=1}^{n}E\left\{e^{sZ_i}\right\}}{\left(e^{st}\right)^n}\overset{\text{i.i.d.}}{=}\frac{\left(E\left\{e^{sZ}\right\}\right)^n}{\left(e^{st}\right)^n}=\left(\frac{E\left\{e^{sZ}\right\}}{e^{st}}\right)^n,\qquad\forall s>0$$

← קיבלנו חסם אקספוננציאלי ב-n, כפי שרצינו.

אם $Y=\sum_{i=1}^{n} m\left(X_i\right)$, אז נגדיר $Z_i=m\left(X_i\right)$ ואז נרשום $E\left\{e^{s\cdot m(X)}\right\}$ במקום $E\left\{e^{sZ}\right\}$

ונקבל:

$$\Pr\left\{\frac{1}{n}\sum_{i=1}^{n} m\left(X_i\right)>t\right\}\le e^{-nD}$$

כאשר:

$$D=\min_s\left\{st-\log\sum_x Q\left(x\right)e^{s\cdot m(x)}\right\}$$

טענה (להוכחה בתרגיל בית): חסם צ'רנוף האופטימלי (מינימום לפי s) מתלכד עם חסם סאנוב.

יתרונות צ'רנוף

- לא מוגבל לא"ב סופי.
- מאפשר ניתוח גם אם המשתנים בת"ס אך לא i.i.d.
- מאפשר טיפול בתהליכים עם זיכרון.

יתרונות סאנוב

- נותן הבנה של ה"פיזיקה" של הבעיה.
- כללי יותר.
- ברור התנאי לשוויון בחסם.
- משפט גבול מותנה (יילמד בהרצאה הבאה).

הרצאה מס' 3

"חריגות גדולות" ומשפט סאנוב - המשך

סוכם ע"י אייל חיטרון

Large Deviation Theory ומשפט סאנוב – המשך מההרצאה הקודמת

1. תזכורת: משפט סאנוב Sanov

המשתנים האקראיים $X_1,\cdots,X_n$ מתפלגים i.i.d עם התפלגות $Q(x)$ מעל א"ב סופי X , E היא קבוצת התפלגויות מעל X שמוכלת בסגור של הפנים שלה, ובנוסף נניח שמתקיים $Q \notin E$.

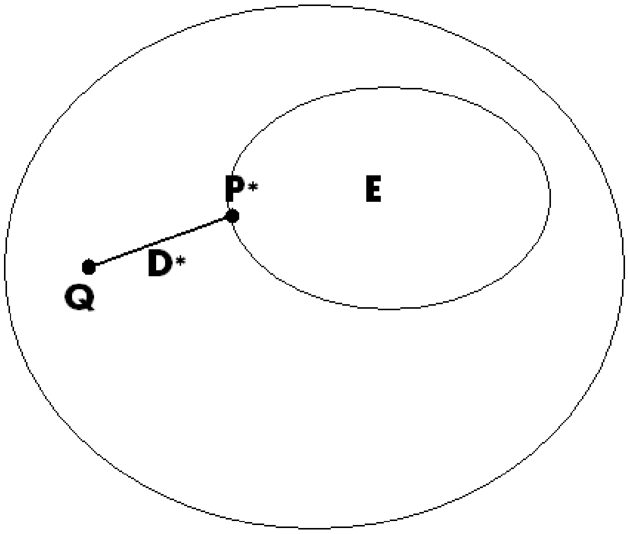
אזי, ההסתברות שהטיפוס של הוקטור $X_1,\cdots,X_n$ יהיה שייך לקבוצה E הינה:

$$P(P_X \in E) \doteq 2^{-nD*}$$

כאשר D* הוא ה"מרחק" המינימלי בין Q לבין התפלגות כלשהי ב E:

$$D* = \inf_{P \in E} D(P \| Q) = D(P* \| Q)$$

P* היא ההתפלגות שמשיגה את המרחק המינימלי D*, בהנחה שהתפלגות זו הינה יחידה.



אינטואיטיבית, $2^{-nD(P*\|Q)}$ הינו הסיכוי ל"התחזות", כלומר הסיכוי שסדרה שהוגרלה באופן i.i.d לפי התפלגות Q "תיראה כמו" סדרה שהוגרלה לפי התפלגות P*.

2. משפט הגבול המותנה: Conditional Limit Theorem

משפט זה מספר לנו כיצד "נראה" מאורע ה"התחזות": אם ההתפלגות P* יחידה, אזי <u>בהינתן</u> המאורע ה"נדיר" $P_X \in E$ הוקטור X מתפלג, בקירוב, באופן <u>אחיד</u> בתוך קבוצת הטיפוס T_{P*}.

ניסוח יותר מדוייק: בהינתן המאורע $P_X \in E$ כל רכיב של הוקטור X מתפלג, בגבול כאשר $n \to \infty$, לפי ההתפלגות P*:

$$\lim_{n\to\infty} P(X_i = a \mid P_X \in E) = P^*(a)$$

יתרה מזאת, אם נתבונן ב k רכיבים שונים מתוך הוקטור X, אזי בהינתן המאורע $P_X \in E$ הם מתפלגים בקירוב i.i.d לפי ההתפלגות *P:

$$\lim_{n\to\infty} P(X_{i_1} = a_1, \cdots, X_{i_k} = a_k \mid P_X \in E) = \prod_{j=1}^{k} P^*(a_{i_j})$$

3. דוגמאות לשימוש ב Large Deviation Theory

1. ***מעבר סף:***

יהיו $X_1, \cdots X_n$ מפולגים i.i.d לפי התפלגות $P(X)$, ותהא $m(\cdot)$ "פונקציית מומנט" של X (למשל, מומנט ריבועי). מאורע "מעבר הסף" מוגדר ע"י $\left\{ \frac{1}{n} \sum_{i=1}^{n} m(X_i) \geq t \right\}$, כאשר מתקיים $E(m(X)) < t$. כלומר, מעבר סף מתרחש כאשר התוחלת האמפירית של $m(X)$ עוברת את הסף t, שהינו גדול יותר מהתוחלת האמיתית של $m(X)$.

במקרה זה הקבוצה E מוגדרת ע"י:

$$E = \left\{ P : \sum_a P(a) m(a) \geq t \right\}$$

כלומר זהו אוסף כל הפילוגים כך שהתוחלת של m(X) היא לפחות t.

2. ***בחינת השערות Hypothesis Testing***

במקרה זה נתונות שתי השערות לגבי ההתפלגות של Xi: $P_0(x)$ או $P_1(x)$, שתיהן i.i.d.

ההחלטה בין שתי ההשערות מתבצעת על פי ה log-likelihood ratio test:

$$\sum_{i=1}^{n} \log \frac{P_0(X_i)}{P_1(X_i)} \underset{H_1}{\overset{H_0}{\gtrless}} t$$

המקרה ה"מאוזן" הוא כאשר t הוא קבוע (לא תלוי ב n).
במקרה הלא מאוזן, מתקיים $t \to \infty$ (בדרך כלל מחליטים "1") או $t \to -\infty$ (בדרך כלל מחליטים "0").

- במקרה שבו $t \to -\infty$, מקבלים:

$$P(1 \mid H_0) \doteq 2^{-nD(P_1 \| P_0)}$$

- במקרה המאוזן מקבלים

$$P(1 \mid H_0) \doteq P(0 \mid H_1) \doteq 2^{-nD^*}$$

כאשר *D הינו מרחק קולבאק-לייבלר (הדיברגנס) של נקודת ה"אמצע" בין P_0 ו P_1 מכל אחד מהקצוות:

$$D^* = D(P^* \| P_0) = D(P^* \| P_1)$$

ניתן להראות שנקודת ה"אמצע" P^* היא מהצורה:

$$P^*(a) = K \cdot P_1(a)^{\lambda} \cdot P_0(a)^{1-\lambda}$$

כאשר הפרמטר λ נבחר כך שיתקיים $D(P^* \| P_0) = D(P^* \| P_1)$.

3. גילוי ML בין שתי מילות קוד

זהו מקרה פרטי של בחינת השערות: נניח ש x(1),x(2) הן שתי מילות קוד, אשר מוגרלות i.i.d לפי פילוג P(x). Y הינו המוצא של ערוץ חסר זיכרון p(y|x), כאשר בכניסה משודרת אחת מבין שתי המילים x(1),x(2).
מבחן ה log-likelihood ratio הוא כעת:

$$\sum_{i=1}^{n} \log \frac{P(Y \mid X(2)_i)}{P(Y \mid X(1)_i)} \underset{1}{\overset{2}{\gtrless}} 0$$

אם נגדיר $Z_i = \log \frac{P(Y \mid X(2)_i)}{P(Y \mid X(1)_i)}$, אז נקבל שהסתברות השגיאה חסומה מלמעלה ע"י:

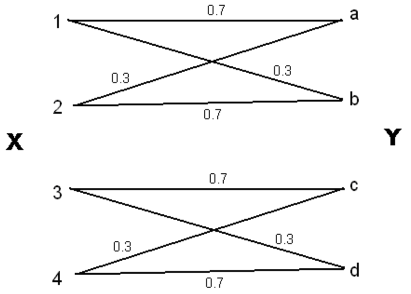
$$P(2 \mid 1) \le \min_{s \ge 0} \left(E\left(e^{sZ_i}\right) \right)^n \underset{s=\frac{1}{2}}{=} \left(\sum_y \sum_x P(x) \sqrt{P(y \mid x)} \right)^n$$

ב. אקספוננט שגיאה במונחי דיברגנס

1. למה אקספוננט שגיאה?

ראשית ננסה להבין למה אקספוננט שגיאה הוא בכלל מעניין.
נתבונן, למשל, בשני הערוצים הבאים, מא"ב בגודל 4 לא"ב בגודל 4:

ערוץ א':



ערוץ ב':

Y=(X+Z) mod 4

P(Z=0)=0.9

P(Z=1)=0.08

P(Z=2)=0.01

P(Z=3)=0.01

באיזה ערוץ נעדיף להשתמש?
לכאורה, ערוץ ב' עדיף כי הקיבול שלו גדול יותר:

$$C_1 = H(\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{4}) - H(Y \mid X) \approx 1.119 bit$$

$$C_2 = H(\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{4}) - H(Y \mid X) \approx 1.439 bit$$

אולם, אם אנחנו מעוניינים לשדר בקצב נמוך יותר מאשר $C_0 = 1bit$, בערוץ א' ניתן לעשות זאת ללא שגיאה כלל (למשל, אם משדרים רק 1 ו 3), ולעומת זאת בערוץ ב' תמיד מקבלים הסתברות שגיאה שונה מאפס. (הגודל C_0 נקרא zero-error capacity של הערוץ).
כלומר, קיבול הערוץ אינו הגודל המעניין היחיד המאפיין את הערוץ! באופן כללי, אפשר לשאול מהי הסתברות השגיאה P_e כפונקציה של הקצב R ושל גודל הבלוק n. בדרך כלל

נתעניין בהתנהגות האקספוננציאלית של P_e כפונקציה של n כאשר הקצב נשאר קבוע, כלומר הגודל המעניין הוא אקספוננט השגיאה:

$$E(R) = -\lim_{n\to\infty} \frac{1}{n} P_e$$

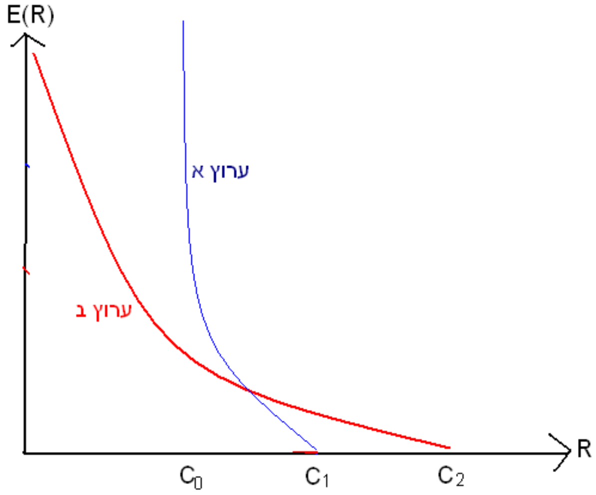
או במילים אחרות:

$$P_e \doteq 2^{-nE(R)}$$

בדרך כלל מתייחסים ל P_e^{opt} , שהיא הסתברות השגיאה של הקוד האופטימלי באורך n לערוץ הנתון $p(y|x)$:

$P_e^{opt} = \min P_e$, when min is over all codes of length n and rate R.

אם נצייר את E(R) עבור שני הערוצים שבדוגמה, נקבל התנהגות כזו:



כלומר, בתחום קצבים מסויים נעדיף את ערוץ א', ובתחום קצבים אחר נעדיף את ערוץ ב'.

2. חסמים אקספוננציאלים עבור הסתברות השגיאה בין 2 מילות קוד בערוץ BSC

א. מילות קוד אקראיות:

$$\overline{P_e} \le \left[2\left(\tfrac{1}{2}\sqrt{\varepsilon}+\tfrac{1}{2}\sqrt{1-\varepsilon}\right)^2\right]^n$$

(הסיבה לכך שלא מקבלים 0 עבור $\varepsilon = 0$ היא שקיים סיכוי של 2^{-n} ששתי מילות הקוד שנבחרו הינן זהות).

ב. מילות קוד משלימות (כלומר, שונות זו מזו בכל אחד מהביטים):

$$\overline{P_e} \le 2^{-nD(0.5,0.5\|\varepsilon,1-\varepsilon)} = 2^{-n\cdot\left(-\frac{1}{2}\log(\varepsilon)-\frac{1}{2}\log(1-\varepsilon)-1\right)} = \left[2\sqrt{\varepsilon(1-\varepsilon)}\right]^n$$

ג. מילות קוד "אורתוגונליות" (כלומר, שונות זו מזו בדיוק בחצי מהביטים):

$$\overline{P_e} \le \left[2\sqrt{\varepsilon(1-\varepsilon)}\right]^{n/2} = \left[\sqrt{2\sqrt{\varepsilon(1-\varepsilon)}}\right]^n$$

3. ה"טעות" של שאנון [1948]

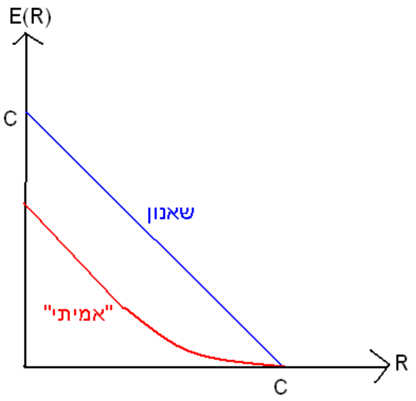
כדי להוכיח שניתן להתקרב כרצוננו לקיבול הערוץ, שאנון הזניח את המקרים בהם הערוץ או ספר הקוד מתנהגים בצורה לא טיפוסית. במקרה זה, אם ספר הקוד מכיל 2^{nR} מילים שהוגרלו באופן i.i.d, אזי לפי ה union bound ניתן לחסום את הסתברות השגיאה ע"י:

$$P_e \le 2^{nR}2^{-nC} = 2^{-n(C-R)}$$

ולכן אם R<C אז ניתן להשיג $P_e \to 0$ כאשר $n \to \infty$.

הזנחת המאורעות הלא-טיפוסיים היא אמנם מוצדקת לצורך הוכחת משפט הקיבול, כי לפי ה AEP הסתברותם של מאורעות אלה שואפת לאפס. אולם, הביטוי שמקבלים לקצב שבו הסתברות השגיאה שואפת לאפס, $2^{-n(C-R)}$, הינו אופטימי מדי.

באופן כללי, אם נגדיר אקספוננט שגיאה ע"י $E(R) = -\lim_{n\to\infty}\frac{1}{n}P_e^{opt}$, אז נקבל את התמונה הבאה:



הגרף הכחול מתאר את החסם ה"שגוי" של שאנון, ואילו הגרף האדום הוא אקספוננט השגיאה האמיתי של קוד אקראי.

4. חישוב אקספוננט השגיאה באמצעות שיטת הטיפוסים

גישת הניתוח:

באופן כללי הניתוח יהיה דומה לניתוח random coding של שאנון, עם מספר שינויים, אשר נועדו להתגבר על הבעיה של חוסר האופייניות:

א. כדי להתגבר על חוסר-אופייניות של מילות הקוד: במקום להגריל את מילות הקוד באופן i.i.d, אנחנו נגריל את מילות הקוד באופן אחיד על פני קבוצת הטיפוס Tp, כלומר:

$$P(\underline{x}_i = \underline{x}) = \begin{cases} 1/|T_P| & \text{if } x \in T_P \\ 0 & \text{otherwise} \end{cases}$$

כאשר מילות הקוד השונות מוגרלות באופן בלתי-תלוי.

באופן זה נימנע משגיאה שנגרמת בגלל ספר קוד שהוגרל "רע". קוד כזה נקרא constant decomposition code.

ב. כדי להתגבר על חוסר-אופייניות של הערוץ: במקום להשתמש במפענח ML (maximum likelihood), אשר הינו המפענח האופטימלי כאשר סטטיסטיקת הערוץ ידועה, אנחנו נשתמש במפענח MMI (maximum mutual information). היתרון במפענח זה הוא שהוא מפענח אוניברסאלי, כלומר, אינו מסתמך על הסטטיסטיקה של הערוץ, ולכן הוא יכול לפעול טוב יותר כאשר הערוץ מתנהג בצורה

"לא אופיינית". לשם דוגמה, נתבונן בערוץ BSC עם פרמטר $\varepsilon < \frac{1}{2}$, ונניח שהערוץ "הפך" יותר מחצי מהביטים. במקרה זה, מפענח ML כנראה לא יבחר את מילת הקוד הנכונה!

ניגש לניתוח עצמו:

1. הגרלת ספר הקוד: יהי P טיפוס של סדרות באורך n מא"ב X. נגריל ספר קוד אקראי עם $M = 2^{nR}$ מילים באורך n, כולן מטיפוס P: $x_1,\dots x_M \in T_P$.

2. הגדרת מפענח MMI: בהינתן מוצא הערוץ y, נחליט שמילת הקוד הנכונה היא x_i אם לכל $j \neq i$ מתקיים:

$$I(x_i \wedge y) > I(x_j \wedge y)$$

כאשר I(x^y) היא האינפורמציה האמפירית בין x ל y:

$$I(x^\wedge y) = \sum_{a\in X}\sum_{b\in Y} \frac{n(a,b|x,y)}{n} \cdot \log \frac{\frac{n(a,b|x,y)}{n}}{\frac{n(a|x)}{n}\cdot\frac{n(b|y)}{n}}$$

כאשר $n(a|x)$ הוא מספר הפעמים שהאות a הופיעה בוקטור x, $n(b|y)$ הוא מספר הפעמים שהאות b הופיעה בוקטור y, ו $n(a,b|x,y)$ הוא מספר הפעמים ש (a,b) הופיע בזוג הסדרות (x,y).

במילים אחרות, אם נסמן ב V את הטיפוס המותנה של y בהינתן x_i , וב 'V את הטיפוס המותנה של y בהינתן x_j , אזי נעדיף את x_j על פני x_i אם מתקיים $I(P;V) \le I(P;V')$, כאשר $I(P;V)$ היא האינפורמציה הדדית של ערוץ עם פילוג כניסה P(x) ופילוג מעבר V(y|x).

5. חישוב חסם עליון על הסתברות השגיאה:

טענה: הסתברות השגיאה הממוצעת של הקוד הנ"ל, עם מפענח MMI, חסומה מלמעלה (עד כדי מקדם פולינומיאלי ב n) ע"י:

$$P_e \le 2^{-n\cdot\min_V\left(D(V\|W|P)+[I(P,V)-R]^+\right)} = 2^{-nE_r(R,P,W)}$$

כאשר:

$$E_r(R,P,W) \equiv \min_V\left(D(V\|W|P)+[I(P,V)-R]^+\right)$$

חסם זה נקרא Random Coding Exponent Function של ערוץ W עם התפלגות כניסה P.

הוכחה:

נניח בה"כ שנשלחה המילה x_0 , ונסמן ב W(y|x) את התפלגות המעבר האמיתית של הערוץ.

בשונה מהניתוח של שאנון, במקום להניח שהערוץ התנהג בצורה טיפוסית (כלומר שהטיפוס המותנה של y בהינתן x הוא W), אנחנו נחשב את הסתברות השגיאה בהינתן שהערוץ התנהג "כמו" V, ונסכום על פני כל האפשרויות של V תוך שימוש בנוסחת ההסתברות השלמה (כאשר למזלנו הסכום מכיל רק מספר פולינומיאלי של איברים):

$$Pe = \sum_V P(y\in T_V(x_0)\,|\,x=x_0)P(error\,|\,x=x_0, y\in T_V(x_0)) \quad (*)$$

כאשר:

א. $P(y\in T_V(x_0)\,|\,x=x_0)$ היא ההסתברות שהערוץ W התנהג "כמו" הערוץ V

ב. $P(error\,|\,x=x_0, y\in T_V(x_0))$ היא ההסתברות שהמפענח טעה בהינתן שהערוץ התנהג "כמו" V.

את שני האיברים הנ"ל ניתן לחסום באמצעות ה union bound ושיטת הטיפוסים:

א. חישוב ההסתברות שהערוץ התנהג כמו V

כיוון שהכניסה לערוץ היא x0, שהיא סדרה מטיפוס P, הסיכוי שהערוץ W "יתחזה" לערוץ V הוא:

$$P(y\in T_V(x_0)\,|\,x=x_0) \quad = \quad |T_V(x_0)|\cdot\prod_a\prod_b W(b\,|\,a)^{n(a|x_0)V(b|a)}$$

$$=|T_V(x_0)|\cdot\prod_a\prod_b W(b\,|\,a)^{nP(a)V(b|a)}$$

$$\doteq 2^{nH(V|P)}\cdot\prod_a\prod_b 2^{nP(a)V(b|a)\log W(b|a)}$$

$$=2^{n\left[-\sum_a\sum_b P(a)V(b|a)\log V(b|a)+\sum_a\sum_b P(a)V(b|a)\log W(b|a)\right]}$$

$$=2^{n\left[-\sum_a\sum_b P(a)V(b|a)\log\frac{V(b|a)}{W(b|a)}\right]}$$

$$=2^{-nD(V\|W|P)}$$

ב. חישוב ההסתברות שהמפענח טעה בהינתן שהערוץ התנהג כמו V

את ההסתברות הזו נחסום תוך שימוש ב union bound:

$$P(error\,|\,x=x_0,y\in T_V(x_0))\le 2^{nR}\cdot P(\hat{x}=x_1\,|\,x=x_0,y\in T_V(x_0))$$

לפי הגדרת מפענח MMI, שגיאה מסוג זה יכולה להתרחש רק כאשר האינפורמציה ההדדית האמפירית בין y ל x1 גדולה יותר מאשר זו בין y ל x0:

$$P(error\,|\,x=x_0,y\in T_V(x_0))\le 2^{nR}\cdot P(I(y\wedge x_1)\ge I(y\wedge x_0)\,|\,x=x_0,y\in T_V(x_0))$$

כיוון ש x1 הינה מילת קוד שנבחרה באופן יוניפורמי מתוך קבוצת הטיפוס T_P, באופן בלתי תלוי ב x0 וב y, ההסתברות לכך היא:

$$P\big(I(y\wedge x_1)\ge I(y\wedge x_0)\,|\,x=x_0,y\in T_V(x_0)\big)=\frac{\left|\{x_1\,|\,x_1\in T_P,I(y\wedge x_1)>I(y\wedge x_0)\}\right|}{|T_P|}$$

$$=\frac{\left|\{x_1\,|\,x_1\in T_P,I(y\wedge x_1)>I(P;V)\}\right|}{|T_P|}$$

כדי לחשב את גודל הקבוצה במונה, נניח שה"ערוץ" מ x1 ל y התנהג כמו $\tilde{V}$, ונסכום על פני כל האפשרויות של $\tilde{V}$ (שמספרן הוא, שוב, פולינומיאלי). כמו כן נסמן ב V^{-1} את הערוץ ה"הפוך" מ y ל x0, ב $\tilde{V}^{-1}$ את הערוץ ה"הפוך" מ y ל x1, וב Q את הטיפוס של y:

$$
\begin{aligned}
&P\left(I(y\wedge x_1) \geq I(y\wedge x_0) \mid y \in T_V(x_0)\right) \\
&= \sum_{\tilde{V}} \frac{\left|\left\{x_1 \mid x_1 \in T_P, y \in T_{\tilde{V}}(x_1), I(y\wedge x_1) > I(P;V)\right\}\right|}{\left|T_P\right|} \\
&= \sum_{\tilde{V}} \frac{\left|\left\{x_1 \mid x_1 \in T_P, y \in T_{\tilde{V}}(x_1), I(P;\tilde{V}) > I(P;V)\right\}\right|}{\left|T_P\right|} \\
&= \sum_{\tilde{V}:I(P;\tilde{V})>I(P;V)} \frac{\left|\left\{x_1 \mid x_1 \in T_P, y \in T_{\tilde{V}}(x_1)\right\}\right|}{\left|T_P\right|} = \sum_{\tilde{V}:I(P;\tilde{V})>I(P;V)} \frac{\left|T_{\tilde{V}^{-1}}(y)\right|}{\left|T_P\right|}
\end{aligned}
$$

כעת נשתמש במשפטים שלמדנו בשיעור שעבר כדי לחשב את גדלי קבוצות הטיפוס במונה ובמכנה:

$$P(I(y\wedge x_1)\geq I(y\wedge x_0)\mid y\in T_V(x_0)$$

$$\doteq \sum_{\tilde{V}:I(P;\tilde{V})>I(P;V)} \frac{2^{nH(\tilde{V}^{-1}|Q)}}{2^{nH(P)}} = \sum_{\tilde{V}:I(P;\tilde{V})>I(P;V)} 2^{-n\left(H(P)-H(\tilde{V}^{-1}|Q)\right)}$$

$$= \sum_{\tilde{V}:I(P;\tilde{V})>I(P;V)} 2^{-nI(P;\tilde{V})} \leq \sum_{\tilde{V}:I(P;\tilde{V})>I(P;V)} 2^{-nI(P;V)} \doteq 2^{-nI(P;V)}$$

בסך הכל קיבלנו שההסתברות לטעות במפענח MMI, בהינתן שהערוץ מ x0 ל y התנהג כמו V, חסומה מלמעלה ע"י:

$$P(error\mid x=x_0, y\in T_V(x_0))\leq 2^{nR}\cdot 2^{-nI(P;V)} = 2^{-n[I(P;V)-R]}$$

אולם, מתקיים גם החסם הטריויאלי $P(error\mid x=x_0, y\in T_V(x_0))\leq 1$, ולכן ניתן לכתוב:

$$P(error\mid x=x_0, y\in T_V(x_0))\leq 2^{-n[I(P;V)-R]^+}$$

כאשר:

$$x^+ \equiv \begin{cases} x & x>0 \\ 0 & x\leq 0 \end{cases}$$

ג. ועכשיו הכל ביחד

נציב את א' ואת ב' בנוסחה (*) ונקבל:

$$Pe=\sum_V P(y\in T_V(x_0)\mid x=x_0)P(error\mid x=x_0, y\in T_V(x_0))$$

$$\leq \sum_V 2^{-nD(V\|W|P)}\cdot 2^{-n[I(P,V)-R]^+} = \sum_V 2^{-n\left(D(V\|W|P)+[I(P,V)-R]^+\right)}$$

כיוון שהסכום הוא על פני מספר פולינומיאלי של טיפוסים, עד כדי מקדם פולינומיאלי מתקיים החסם העליון:

$$P_e\leq 2^{-n\cdot\min_V\left(D(V\|W|P)+[I(P,V)-R]^+\right)} = 2^{-nE_r(R,P,W)}$$

כאשר:

$$E_r(R,P,W)\equiv\min_V\left(D(V\|W\mid P)+[I(P,V)-R]^+\right)$$

מש"ל.

6. שתי הערות לסיום – ללא הוכחות

<u>א.</u> המקסימום של $E_r(R,P,W)$ על פני כל פילוגי הכניסה P (לאו דווקא טיפוסים!), <u>מתלכד</u> עם פונקצית האקספוננט של גלגר (reliability function). בפרט, זהו חסם עליון הדוק כאשר הקצב הוא מעל הקצב הקריטי.

<u>ב.</u> הגודל $E_{SP}(R,P,W)\equiv\min_{V:I(P;V)<R} D(V\|W\mid P)$ נקרא sphere packing bound, והוא למעשה חסם תחתון על אקספוננט השגיאה עבור <u>כל</u> בחירה של ספר הקוד, כאשר P הינו הטיפוס המשותף של כל מילות הקוד [Csizar & Korner, p. 166]. שני החסמים הנ"ל מתלכדים כאשר הקצב הינו מעל הקצב הקריטי.

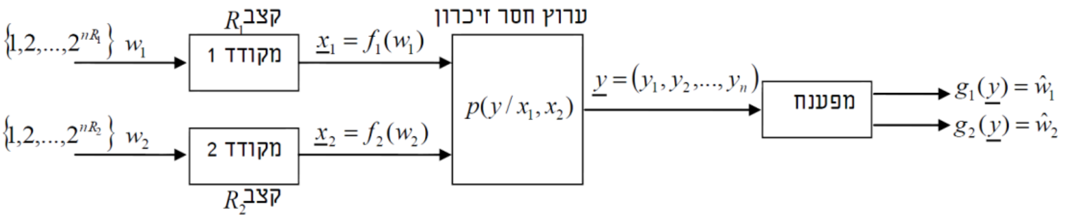
הרצאה מס' 4

(Multiple Access Channel - MAC) ערוץ מרובה משדרים

סוכם ע"י אור אורדנטליך

מודל

מודל הערוץ נתון ע"י הסכימה הבאה:



מגדירים מאורע שגיאה לפי:

$$P_e \overset{\Delta}{=} \{\hat{w}_1 \neq w_1 \cup \hat{w}_2 \neq w_2\}$$

נגדיר את תחום הקיבול האופרטיבי להיות:

$$C^{oper} = closure\{(R_1, R_2)\, that\ are\ achivable\}$$

(R_1, R_2) are achievable if exist encoders $f_1(\cdot), f_2(\cdot)$ and decoders $g_1(\cdot), g_2(\cdot)$ s.t

$P_e \to 0$

הערה : ה"סגור" (closure) שקול לסופרימום בבעיית הקיבול point to point הרגילה – הקיבול מוגדר בתור הסופרימום על פני כל הקצבים ברי ההשגה.

MISO point to point – תרחיש ייחוס

ברור שבעזרת מערכת בה שתי הכניסות לערוץ $\underline{x}_1, \underline{x}_2$ נוצרו ע"י מקודד משותף ניתן להשיג ביצועים טובים יותר (או לפחות זהים) מאלו של מקודדים מבוזרים. לכן תרחיש הייחוס, לביצועי מערכת בערוץ ה-MAC יהיה הערוץ הבא:

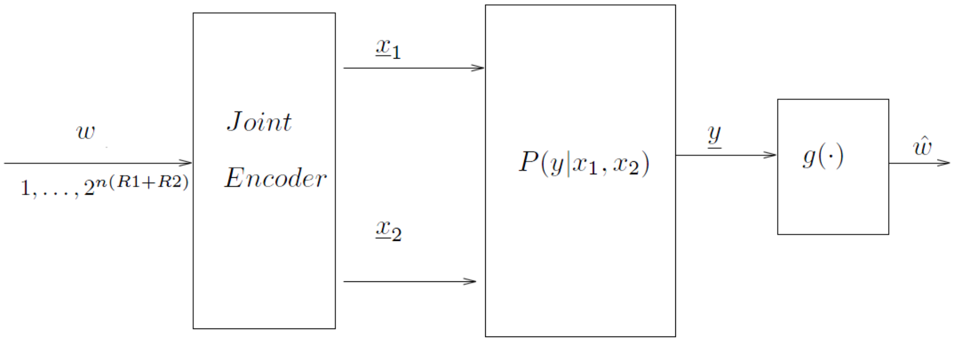


Figure 1: MISO channel - reference scenario.

דוגמאות:

נתחיל את הדיון בערוצי MAC בשתי דוגמאות לערוצים ללא רעש:

<u>דוגמא 1: כופל בינארי</u>

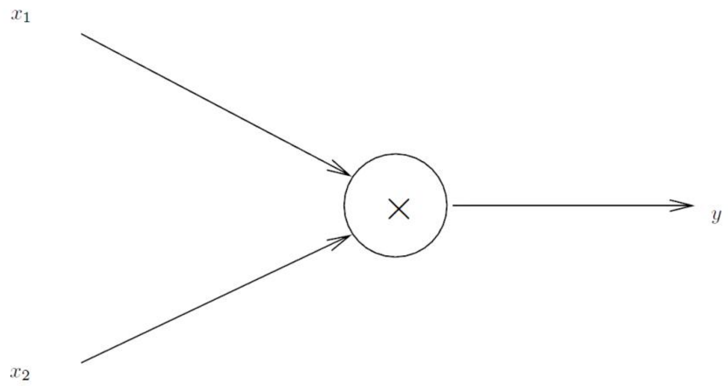


Figure 2: Binary Multiplier.

בערוץ זה $y = x_1 \cdot x_2$. מתקיים:

$$C_1 = \max\{R_1 \in C\} = \max_{p(x_1),x_2} I(x_1; y \mid X_2 = x_2)$$

המקסימיזציה מתבצעת על כל הערכים ש-x_2 יכול לקבל. בוחרים את x_2 כך שהערוץ מ-x_1 ל-y יהיה הכי נוח. בערוץ זה ברור שהבחירה $x_2 = 1$ אופטימאלית, ומתקבל ערוץ "נקי" בין x_1 ל-y ולכן $C_1 = 1 \frac{bit}{channeluse}$.

את C_2 מחשבים באותה צורה בדיוק.

במערכת מסונכרנת (כל המשתמשים יחד עם המקלט מסונכרנים), אם $(R_1, R_2) \in C$ וגם $(R_1', R_2') \in C$, אזי $\alpha(R_1, R_2) + (1-\alpha)(R_1', R_2') \in C$. ההוכחה לכך היא ע"י time sharing.

לא ניתן להשיג $R_1 + R_2 > 1 \frac{bit}{channeluse}$ מכיוון שלערוץ מוצא בינארי (מערכת הייחוס שלנו לא יכולה להשיג קצב טוב יותר ע"י joint encoding).

נפתח חסמים על ביצועי המערכת:

1) חסם <u>עליון</u> טריוויאלי מתקבל ע"י מערכת ה-MISO:

$$R_1 + R_2 \le C(\text{Joint Encoding}) = \max_{p(x_1,x_2)} I(x_1, x_2)$$

2) בחסם (1) הרשינו כל פילוג כניסה משותף $p(x_1, x_2)$, אבל מכיוון שבערוץ ה-MAC ביטי האינפורמציה של x_1, x_2 בלתי תלויים, ניתן לקבל חסם <u>עליון</u> אופטימי פחות, אך ריאלי יותר ע"י:

$$R_1 + R_2 \le \max_{p(x_1)p(x_2)} I(x_1, x_2; y) = C_{12}$$

ההוכחה מתקבלת מאי שוויון פאנו, ואז ירידה מביטוי multi-letter לביטוי single-letter, אך לא תובא כאן. בנוסף החסם בר השגה כפי שנראה בהוכחת משפט קיבול ה-MAC.

באופן כללי בבעיית ה-MAC נקבל:

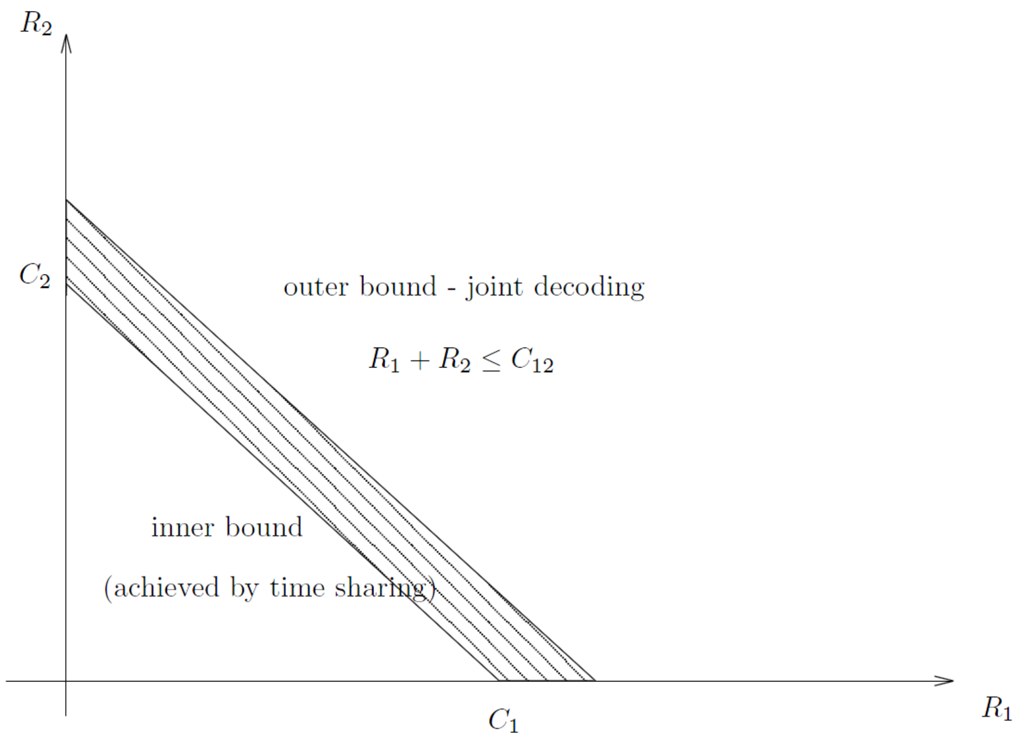


Figure 3: Bounds on achievable rate regions.

במקרה של הכופל הבינארי $C_1 = C_2 = C_{12}$, כלומר החסם החיצון שווה לחסם הפנימי מתוך שיקולים בסיסיים.

דוגמא 2: ערוץ בינארי חיבורי

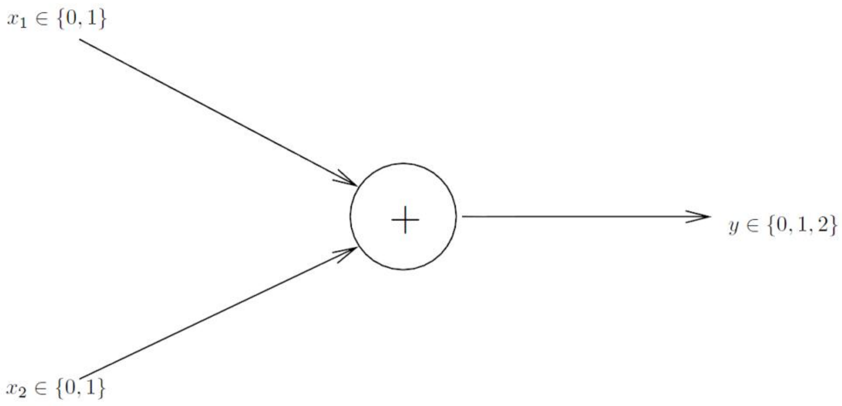


Figure 4: Binary Erasure MAC.

כל אחת מכניסות הערוץ בינארית, אבל הסכום שמבצע הערוץ הוא סכום רגיל (לא modulo2):

עבור $x_2 = 0$ או $x_2 = 1$ כל עוד הוא קבוע לכל אורך השידור ניתן להשיג

$C_1 = 1\frac{bit}{channeluse}$.

באותה צורה ניתן להשיג $C_2 = 1\frac{bit}{channeluse}$.

$$C_{12} = \max_{p(x_1)p(x_2)} I(x_1,x_2;y) = \max_{p(x_1)p(x_2)} I(x_1,x_2;x_1+x_2)$$

עבור פילוג כניסה כלשהוא (ו-Joint Encoding):

$$\max_{p(x_1,x_2)} I(x_1,x_2;y) = \log|Y| = \log(3) = 1.58\frac{bit}{channeluse}$$

מושג ע"י כל פילוג כניסה $p(x_1,x_2)$ עבורו Y מתפלג אחיד על $\{0,1,2\}$, למשל:

$$p(x_1,x_2) = \begin{cases} 1/3 & x_1=0, x_2=0 \\ 1/6 & x_1=1, x_2=0 \\ 1/6 & x_1=0, x_2=1 \\ 1/3 & x_1=1, x_2=1 \end{cases}$$

ניתן לחשב את C_{12} ולקבל $C_{12}=1.5\frac{bit}{channeluse}$. נראה כיצד ניתן להשיג נקודה ספציפית על C_{12} - הנקודה $R_1=1, R_2=0.5 \Rightarrow R_1+R_2=1.5$.

את x_1 נשדר לא מקודד (אחרת לא ניתן להשיג $R_1=1$) עם פילוג ברנולי $\frac{1}{2}$. אם נגדיר את המוצא $y=1$ בתור מחיקה (E), הערוץ השקול שרואה משתמש 2 הוא BEC עם $P(E)=\frac{1}{2}$:

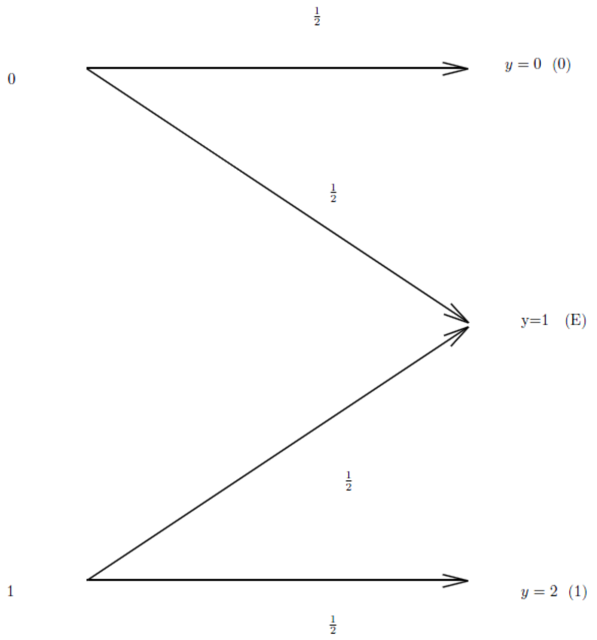


Figure 5: Equivalent BEC.

(כלומר אם $y=0$ יודעים שמשתמש 2 שידר 0, אם $y=2$ יודעים שמשתמש 2 שידר 1, ואם $y=1$ לא יודעים)

משתמש 2 ישדר לכן עם קוד המיועד לערוץ BEC עם $P(E)=\frac{1}{2}$. הקיבול של ערוץ כזה הוא:

$$C_{BEC}=1-\varepsilon=1-\frac{1}{2}=\frac{1}{2}\frac{bit}{channeluse}$$

ולכן משתמש 2 יכול לשדר בקצב $R_2=\frac{1}{2}$ (הקוד יאפשר לפענח את $\underline{x}_2$ כל עוד התנהגות הערוץ היא אופיינית ביחס ל-BEC של 50% מחיקות – כלומר כל עוד היו בקירוב $n/2$ מחיקות).

המפענח בשלב ראשון יפענח את $\underline{x}_2$, בעזרת הקוד, ואחר כך יפחית את $\underline{x}_2$ מ- $\underline{y}$ לקבלת $\underline{x}_1$. עקום הקצבים ברי ההשגה יראה כך:

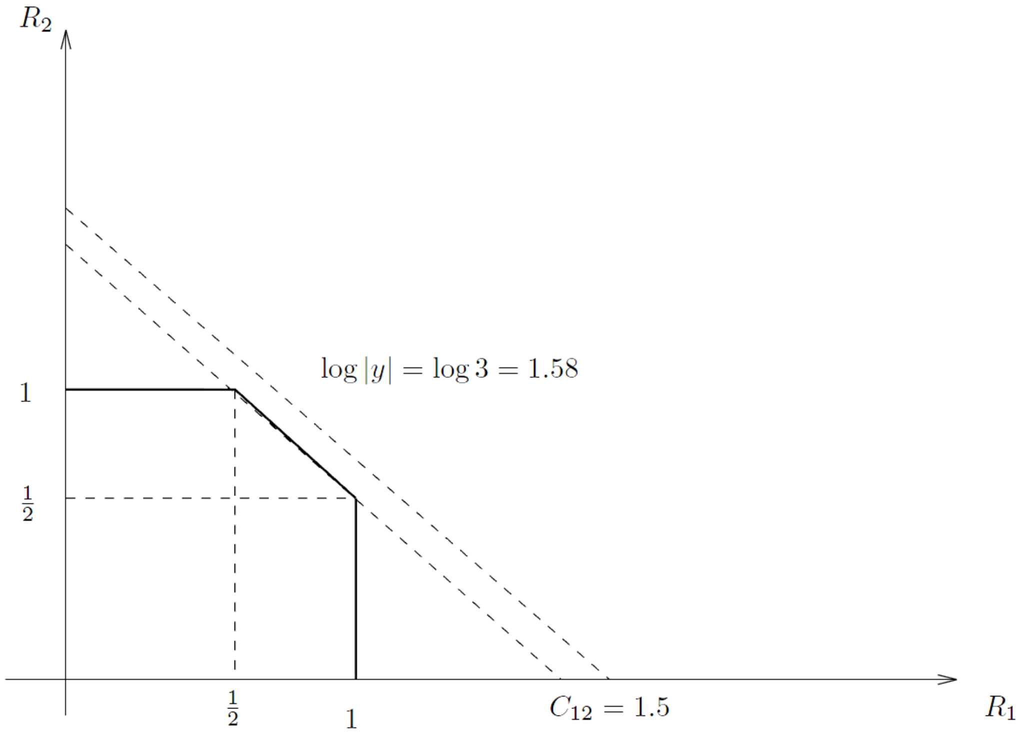


Figure 6: Achievable rate regions for Binary Erasure MAC.

משפט – פתרון ווקטורי (Multi-letter solution) – Van Der Meulen 1971

יהא C_n מוגדר בתור אוסף הקצבים (R_1, R_2) שמקיימים:

$$R_1 \le \frac{1}{n} I(\underline{x}_1;\underline{y}) \quad , \quad R_2 \le \frac{1}{n} I(\underline{x}_2;\underline{y})$$

(ביחס לווקטורים n-מימדיים) עבור פילוג כלשהוא $p(\underline{x}_1)p(\underline{x}_2)$. אזי:

$$C_{MAC} = \bigcup_{n\ge1} C_n \underset{(a)}{=} \lim_{n\to\infty} C_n$$

(את מעבר (a) אפשר להראות)

<u>הוכחת צד ישר:</u>

יהא $N = m \cdot n$ (כפולה שלמה של n). נגריל 2^{NR_1} מילות קוד לפי $p(\underline{x}_1)$ (מתייחסים לכל n סימבולים של המקור $\underline{x}_1$ בתור סופר סימבול, ובונים ספר קוד לסופר סימבולים האלו iid בת"ס מווקטור לווקטור:

$$\underbrace{\underbrace{\underline{x}_1^0}_{\text{n symbols of } x_1}\ \underbrace{\underline{x}_1^1}_{\text{n symbols of } x_1}\ ,\dots,\ \underbrace{\underline{x}_1^N}_{\text{n symbols of } x_1}}_{\text{N super symbols}}$$

וכנ"ל עבור משתמש 2.

משפט הקיבול לבעיית ה- point to point מראה שניתן לפענח את $\underline{x}_1$ ואת $\underline{x}_2$ מתוך $\underline{y}$ בתנאי שמתקיים:

$$R_1 \le I(\underline{x}_1;\underline{y}) \quad , \quad R_2 \le I(\underline{x}_2;\underline{y})$$

הוכחת צד הפוך (converse):

$$nR_1 \le H(\underline{x}_1) = H(\underline{x}_1) - H(\underline{x}_1 \mid \underline{y}) + H(\underline{x}_1 \mid \underline{y}) = I(\underline{x}_1;\underline{y}) + H(\underline{x}_1 \mid \underline{y})$$

לפי אי שוויון Fano:

$$H(\underline{x}_1 \mid \underline{y}) \le H(P_e) + P_e \log |\underline{x}_1|$$

כאשר

$$P_e = p(\underline{x}_1(\underline{y}) \ne \underline{x}_1)$$

מכיוון ש- $\log|\underline{x}_1| = n\log|x_1|$, נקבל:

$$nR_1 \le I(\underline{x}_1;\underline{y}) + nP_e \log|x_1| = I(\underline{x}_1;\underline{y}) + \varepsilon' n$$

לכן אם $P_e \to 0$ חייב להתקיים:

$$nR_1 \le \frac{1}{n} I(\underline{x}_1;\underline{y})$$

<u>יתרון של הגישה הווקטורית:</u> הוכחה פשוטה משיקולים בסיסיים של בעיית point to point.

<u>חסרונות:</u>

1) הפיתרון לא שימושי - האופטימיזציה נותרה רב ממדית במימד הולך לאינסוף.

2) קיימים מספר ייצוגים שונים לצורת הפתרון:

מהוכחת הצד ההפוך של המשפט מתקבל שלכל מערכת עם $P_e \to 0$ מתקיים:

$$nR_1 \le H(\underline{x}_1) - H(\underline{x}_1 \mid \underline{y}, \underline{x}_2) + \varepsilon' n = I(\underline{x}_1;\underline{y},\underline{x}_2) = I(\underline{x}_1;\underline{y} \mid \underline{x}_2)$$

(המעברים נכונים מכיוון ש- $\underline{x}_1, \underline{x}_2$ בת"ס)

אבל את המקסימיזציה עושים על $I(\underline{x}_1;\underline{y})$ לפי $p(\underline{x}_1)$

משפט קיבול MAC (Ahlswede 1970):

תחום הקיבול האינפורמציוני $C^{\inf}$ הוא הסגור של הקמור של:

$$(R_1,R_2):\begin{cases} R_1 < I(x_1;y|x_2) \\ R_2 < I(x_2;y|x_1) \\ R_1+R_2 < I(x_1,x_2;y) \end{cases}$$

עבור איזשהו פילוג מכפלה $p(x_1)\cdot p(x_2)$.

($p(x_1,x_2,y)=p(x_1)\cdot p(x_2)p(y|x_1,x_2) \Leftarrow$)

מתקיים:

$$C^{oper}=C^{\inf}$$

הערה: אם יש אילוץ כניסה (למשל אילוץ הספק) המקסימיזציה מתייחסת גם אליו.

הוכחת צד ישר:

- משתמשים בקודים אקראיים iid ע"פ $p(x_1),p(x_2)$:

$$\mathcal{C}_1=\{\underline{x}_1(i)\}_{i=1}^{M1}, \mathcal{C}_2=\{\underline{x}_2(j)\}_{j=1}^{M2}$$

בגודל $2^{nR_1}, 2^{nR_2}$, אשר ידועים למקודדים ולפענחים.

- השידור הוא מיפוי אחד לאחד מ- $w_i=j$ ל- $\underline{x}_i(j)$ עבור $i=1,2$ ו- $1\le j\le 2^{nR_i}$
- פעולת המפענח היא על בסיס אופייניות:

$A_\varepsilon^{(n)}(x_1,x_2,y)$ - אוסף השלשות $(\underline{x}_1,\underline{x}_2,\underline{y})$ של ווקטורים n ממדיים שאופייניים במשותף ביחס לפילוג $p(x_1,x_2,y)$.

בהינתן $\underline{y}$ נחפש זוג :

$$\underline{x}_1(i)\in\mathcal{C}_1,\ \underline{x}_2(j)\in\mathcal{C}_2$$

שאופייני איתו במשותף. אם מצאנו אחד ורק אחד כזה, אז $\hat{w}_1=i,\hat{w}_2=j$. אם לא - נכריז שגיאה.

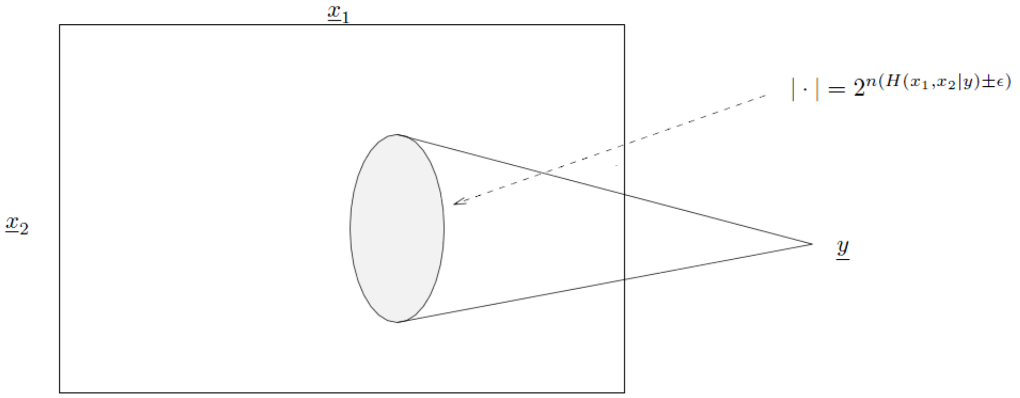


Figure 7: Schematic description of joint typical sequences $(\underline{x}_1,\underline{x}_2)$, with a given typical $\underline{y}$.

ניתוח מאורעות שגיאה:

נגדיר את המאורע:

$$E_{ij}=(\underline{x}_1(i),\underline{x}_2(j),\underline{y})\in A_\varepsilon^{(n)}$$

עקב הסימטריה בהגרלת ספרי הקוד ניתן להתרכז במקרה ששודרו ההודעות הראשונות:

$\underline{x}_1 = \underline{x}_1(1)$

$\underline{x}_2 = \underline{x}_2(1)$

לפענוח תקין נדרש: $E_{11} \bigcap_{j\neq 1} E_{1j}{}^c \bigcap_{i\neq 1} E_{i1}{}^c \bigcap_{i,j\neq 1} E_{ij}{}^c$. לפיכך הסתברות השגיאה תהיה:

$$\overline{P}_e = \Pr\left\{ E_{11}{}^c \bigcup_{j=1}^{M_2} E_{1j} \bigcup_{i=1}^{M_1} E_{i1} \bigcup_{i,j=2}^{M_1,M_2} E_{ij} \right\} \underset{UnionBound}{\leq}$$

$$\leq \Pr\{E_{11}{}^c\} + (M_2-1)\Pr\{E_{1j}\} + (M_1-1)\Pr\{E_{i1}\} + (M_1-1)(M_2-1)\Pr\{E_{ij}\}$$

כאשר הסימון $\overline{P}_e$ מתייחס למיצוע על פני כל ספרי הקוד.

$$1)\ \Pr\{E_{11}{}^c\} \leq \varepsilon$$

$$2)\ \Pr\{E_{ij}\} \leq 2^{-n[I(x_1,x_2;y)-3\varepsilon]}$$

$$3)\ \Pr\{E_{i1}\} \leq 2^{-n[I(x_1;y,x_2)-3\varepsilon]}$$

$$4)\ \Pr\{E_{1j}\} \leq 2^{-n[I(x_2;y,x_1)-3\varepsilon]}$$

(1) נובע מתוך ה-AEP.

(2) הוא מאורע התחזות של $(\underline{x}_1, \underline{x}_2)$ בת"ס עם $\underline{y}$, לזוג אופייני איתו במשותף.

(3) הוא מאורע התחזות של $\underline{x}_1(i)$ שלא שודר לאופייני עם $(\underline{x}_2(1), \underline{y})$

(4) הוא מאורע התחזות של $\underline{x}_2(j)$ שלא שודר לאופייני עם $(\underline{x}_1(1), \underline{y})$

$$\overline{P}_e \leq \varepsilon + 2^{n(R_1+R_2)} 2^{-nI(x_1,x_2;y)} + 2^{n(R_1)} 2^{-nI(x_1;y,x_2)} + 2^{n(R_2)} 2^{-nI(x_2;y,x_1)}$$

נשים לב שמהעובדה ש-$I(x_1, x_2) = 0$ בצירוף עם כלל השרשרת נובע:

$I(x_1; y, x_2) = I(x_1, y \mid x_2)$

$I(x_2; y, x_1) = I(x_2, y \mid x_1)$

ולכן עבור (R_1, R_2) שמקיימים את תנאי המשפט

$$\overline{P}_e \leq \varepsilon + o(1) \xrightarrow{n\to\infty} \varepsilon$$

- כמו בבעיית ה-point to point ניתן להראות שקיים לפחות זוג אחד $(\mathcal{C}_1, \mathcal{C}_2)$ שעבורו P_e (ממוצע על מילות הקוד) הוא לפחות טוב כמו $\overline{P}_e$ (ממוצע על מילות וספרי הקוד).
- בניגוד לבעיית ה-point to point לא ניתן לטעון שאפשר לדלל את הקוד הקרטזי $(\mathcal{C}_1 \times \mathcal{C}_2)$

  בכדי להבטיח ש- $p_{e,\max} \to 0$
- הבדל בין ספרי קוד בקידוד משותף ובקידוד מבוזר:

  בקידוד משותף נקבל $(\underline{x}_1, \underline{x}_2)$ בזוגות נפרדים:

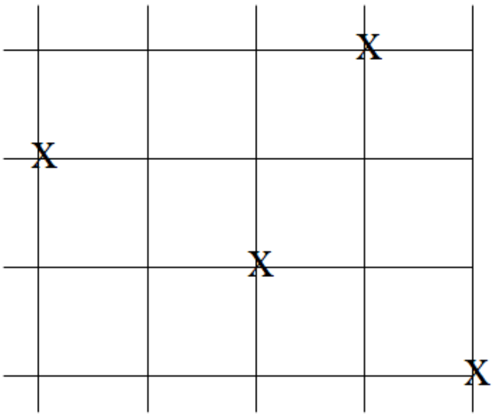


Figure 8: Schematic representation of joint codes $\mathcal{C}_1, \mathcal{C}_2$.

בקידוד מבוזר נקבל מכפלה של ספרי הקוד:

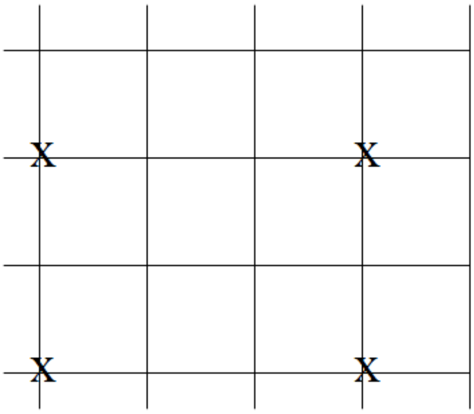


Figure 9: Schematic representation of distributed codes $\mathcal{C}_1 \times \mathcal{C}_2$.

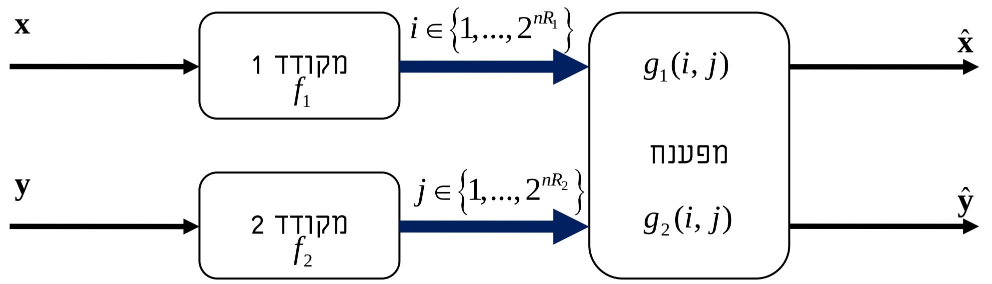
הרצאה מס' 5

קידוד מבוזר של מקורות קורלטיביים – בעיית Slepain-Wolf

סוכם ע״י רן זמיר

תאור הבעיה

נתונה מערכת עם שני מקורות קורלטיביים $\mathbf{x},\mathbf{y}$ בעלי פילוג משותף $p(\mathbf{x},\mathbf{y})$. כל מקור מקודד בנפרד ומשודר בקצבים R_1,R_2 בהתאמה. המפענח הוא משותף והוא משחזר את $\hat{\mathbf{x}},\hat{\mathbf{y}}$.



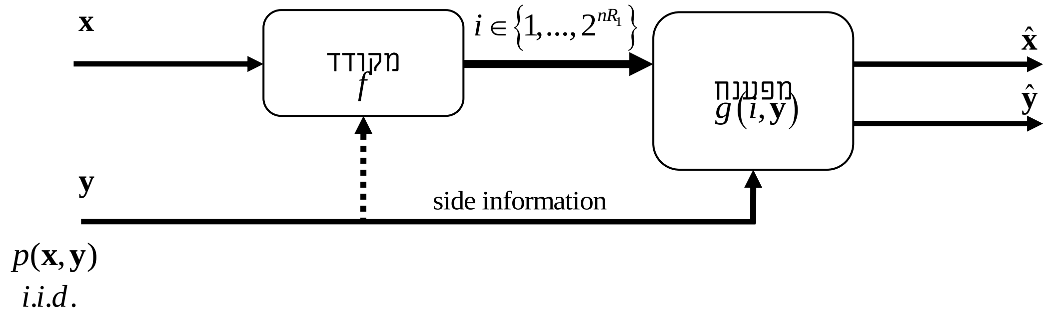
$p(\mathbf{x},\mathbf{y})$
i.i.d.

$$P_e = \Pr\{(\hat{\mathbf{x}},\hat{\mathbf{y}}) \neq (\mathbf{x},\mathbf{y})\}$$

זוג קצבים (R_1,R_2) הוא בר-השגה אם קיימת סדרת מערכות קידוד $(f_{1n}, f_{2n}, g_{1n}, g_{2n})$ בקצבים (R_1,R_2) שמשיגים $P_e \xrightarrow[n\to\infty]{} 0$.

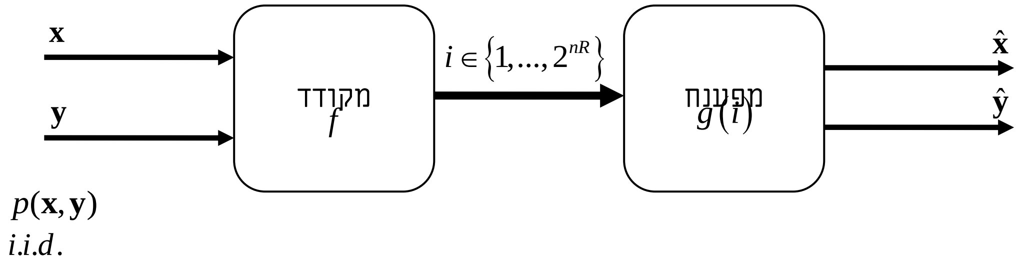
בהתאם, נגדיר את $\square^{oper}$ - תחום הקצבים ברי ההשגה (האופרטיבי).

מקרה פרטי – קידוד מקור עם אינפורמצית צד (לא מקודדת)

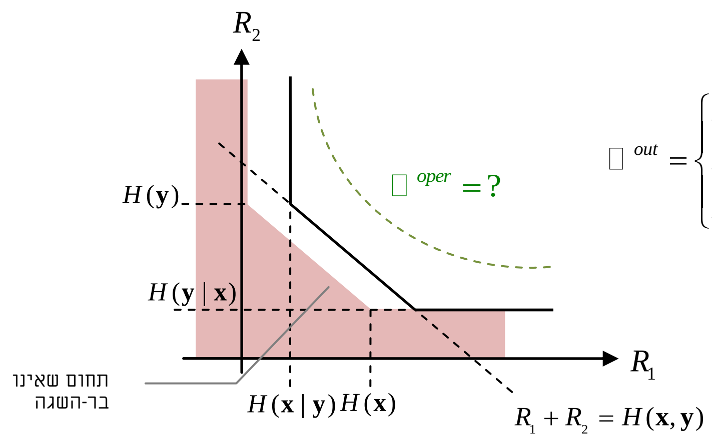


$\mathbf{y}$ ניתן לקידוד מלא והעברה למפענח בקצב $R_2 \geq H(\mathbf{y})$ ללא אי-ודאות.

תרחיש הייחוס: קידוד משותף של זוג מקורות



חסם חיצון לתחום הקצבים:



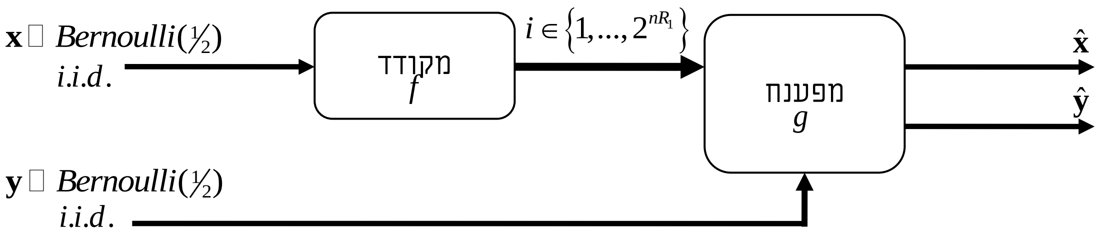
$$\mathcal{R}^{out} = \begin{cases} R_1 + R_2 \ge H(\mathbf{x},\mathbf{y}) & \text{(i)} \\ R_1 \ge H(\mathbf{x}|\mathbf{y}) & \text{(ii)} \\ R_2 \ge H(\mathbf{y}|\mathbf{x}) & \text{(iii)} \end{cases}$$

כאשר החסם החיצון נובע:
(i) מתרחיש הייחוס.
(ii) מהמקרה הפרטי.
(iii) כנ"ל.

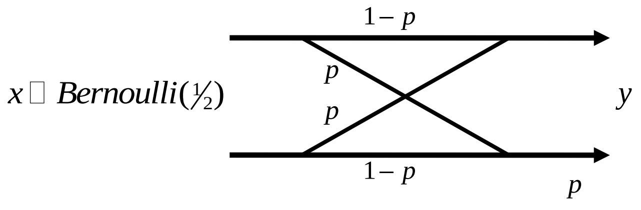
משפט Slepian-Wolf

$\mathcal{R}^{out} = \mathcal{R}$ כלומר אין הפסד על קידוד מבוזר מבחינת סכום הקצבים.

דוגמה 1 – מקור בינארי סימטרי כפול (DSBS)



כאשר הקשר בין x ל- y נתון ע"י ערוץ BSC:



$$p(x,y) = \underbrace{p(x)}_{Ber(1/2)} \underbrace{p(y|x)}_{BSC(p)}$$

- כיצד ניתן להשיג את נקודת הפינה $(R_1,R_2) = (H(x|y), H(y))$?

<u>נתבונן תחילה בבעיית קידוד ערוץ BSC:</u>
ניתן לתאר את הקשר בין $\mathbf{x}$ ל-$\mathbf{y}$ גם כך: $\mathbf{y} = \mathbf{x} \oplus \mathbf{z}$ (*)
כאשר $z \sim Bernoulli(p)$, x,z בת"ס ו- $\oplus$ מציין חיבור מודולו 2.

פתרון לבעית קידוד הערוץ נתון ע״י קוד בינארי לינארי שמשיג קיבול בערוץ BSC(p):

$$\mathcal{C}=\left\{\mathbf{x}\in(0,1)^n:\mathbf{x}=\mathbf{Gu},\forall\mathbf{u}\in(0,1)^k\right\}$$

$\mathbf{G}_{n\times k}$ היא המטריצה היוצרת של קוד הבלוק הלינארי - כל מילת קוד **x** (באורך n) היא תוצר של מכפלת מילת מידע **u** (באורך k) ב-**G**. היתירות שמוספת למילת הקוד היא באורך n-k ביטים.

$\mathbf{H}_{(n-k)\times n}$ היא מטריצת בדיקת הזוגיות של הקוד. והיא מקיימת את התכונה שמכפלת כל מילת קוד בה נותנת את וקטור האפס.

מגדירים סינדרום של וקטור $\mathbf{y}_{n\times 1}$: $\quad \mathbf{s}_{(n-k)\times 1}=\mathbf{Hy}$

מהגדרה זו, ומהגדרת **H** נובע שהסינדרום של כל מילת קוד חוקית הוא אפס.

קוסט (או הזזה בינארית) של הקוד היא אוסף כל הוקטורים עם סינדרום נתון $\mathbf{s}_i$. כלומר

$$S_i=\left\{\mathbf{x}\in(0,1)^n:\mathbf{Hx}=\mathbf{s}_i\right\}$$

אם הקוד ״משיג״ קיבול אזי:

$$(**)\quad \frac{k}{n}\to Capacity=1-H_B(p)$$

וכן קיימת פונקצית פענוח $f(\cdot)$:

$$\hat{\mathbf{z}}=f(\mathbf{Hy})=f(\mathbf{H}(\mathbf{x}\oplus\mathbf{z}))=f\Big(\underbrace{\mathbf{Hx}}_{=\mathbf{0}}\oplus\mathbf{Hz}\Big)=f(\mathbf{Hz})\underset{w.h.p.}{=}\mathbf{z}$$

$$\hat{\mathbf{x}}=\mathbf{y}\oplus\hat{\mathbf{z}}\underset{w.h.p.}{=}\mathbf{y}\oplus\mathbf{z}=\mathbf{x}$$

<u>כעת נחזור למערכת קידוד SW למקור DSBS:</u>

y מועבר למפענח בקצב $R_2=H(y)$.

המקודד משדר את הסינדרום של **x**: $\mathbf{s}=\mathbf{Hx}$ כלומר n-k ביטים.

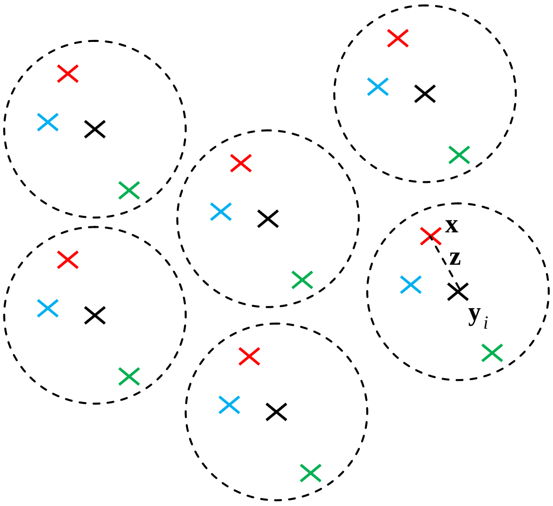
$$R_1=\frac{n-k}{n}=1-\frac{k}{n}\underset{(**)}{=}H_B(p)=H(\mathbf{x}\,|\,\mathbf{y})$$

המפענח מחשב ראשית את y ללא שגיאה (מהנחת התרחיש).

ולאחר מכן מחשב את $\hat{\mathbf{x}}$:

$$\hat{\mathbf{z}}=f(\mathbf{s}\oplus\mathbf{Hy})=f(\mathbf{Hx}\oplus\mathbf{Hy})=f(\mathbf{H}(\mathbf{x}\oplus\mathbf{y}))=f(\mathbf{Hz})\underset{w.h.p.}{=}\mathbf{z}$$

$$\Rightarrow\hat{\mathbf{x}}=\mathbf{y}\oplus\hat{\mathbf{z}}\underset{w.h.p.}{=}\mathbf{y}\oplus\mathbf{z}=\mathbf{x}$$



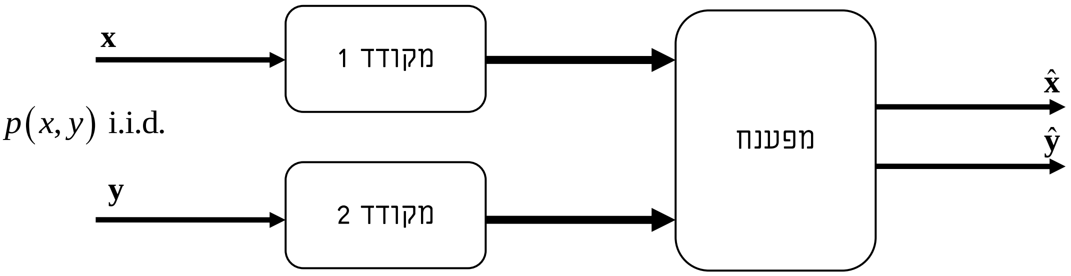
נקודות בעלות אותו צבע שייכות לאותו קוסט (בעלות אותו סינדרום).

$$\mathbf{x}=\mathbf{y}_i\oplus\mathbf{z}$$
$$\mathbf{z}=\mathbf{Hx}$$

במקרה של קידוד הערוץ, נסתכל על ערוץ ה- BSC ההפוך (שמטעמי סימטריה זהה לערוץ הישר), **y** ייצג את מילות הקוד החוקיות, והמילה המתקבלת לאחר הערוץ **x** נופלת בכדור המינג ברדיוס np מסביב לוקטור ה-**y** (ההסתברות ש-**x** יפול מחוץ לכדור קטנה מ- ε קטן כרצוננו). מכיוון שהקוד משיג קיבול, מובטח שניתן לשייך את כל ה-**x**-ים בתוך הכדור לוקטור ה-**y** שנשלח.

בחזרה לדוגמה שלנו, הקשר בין **x** ו-**y** הנתון ב-(*), גורם לכך שהוקטור **x** נמצא בהסתברות גבוהה בתוך כדור המינג ברדיוס np מסביב לוקטור ה-**y** . ולכן, אם למפענח ידוע הוקטור **y**, מספיק למקודד לשלוח את וקטור ה"רעש" **z** שהוא ההיסט של הוקטור **x** ממרכז הכדור (ההיסט מוגדר חד-חד-ערכית ע"י הסינדרום של **x**, כלומר $\mathbf{z} = f(\mathbf{s}) = f(\mathbf{Hx})$), ומכיוון שאנו יודעים ש-**x** נמצא בתוך כדור ההמינג מסביב ל-**y** בהסתברות גבוהה והקוד לעיל משיג קיבול, אזי וקטור ה"רעש" מספיק על מנת לאפשר פענוח תקין של **x**.

דוגמה 2



כאשר $p(x,y)$ נתון ע"י:

x\y	0	1
0	1/3	1/3
1	0	1/3

המקודד יכול לחסוך בביטים אף על פי שאינפורמצית הצד אינה ידועה לו.

$$H(x) = H(y) = H_B(1/3) \approx 0.9bit$$

$$H(x,y) = \log_2 3 \approx 1.58bit$$

אם מקודדים בצורה נאיבית מבודדת: $R_1 + R_2 \approx 2 \times 0.9 = 1.8bit$

קידוד מערכת ע"פ SW מאפשר להתקרב כרצוננו ל- 1.58bit .

הוכחת משפט SW (המקרה הכללי)

1. המשפט ההפוך הוא טריוויאלי (משיקולי קידוד בתרחיש "קל" יותר).
2. המשפט הישר - הוכחה ע"י Random Binning (חלוקה אקראית לתאים) [גישה לא קונסטרוקטיבית להוכחת המשפט].

בניית הקוד

נחלק את כל אחד מ- $\mathbf{x} \in \mathcal{X}^n$ ל- 2^{nR_1} תאים בפילוג אחיד ובת"ס $\Pr\{\mathbf{x} \in bin\} = 2^{-nR_1}$.

נחלק את כל אחד מ- $\mathbf{y} \in \mathcal{Y}^n$ ל- 2^{nR_2} תאים בפילוג אחיד ובת"ס $\Pr\{\mathbf{y} \in bin\} = 2^{-nR_2}$
.

מיידעים את המקודדים והמפענח על החלוקה (ספר הקוד) שנבחרה.

נשים לב שבניית ספר הקוד אינה תלויה ב- $p(\mathbf{x},\mathbf{y})$.

קידוד

כל מקודד מדווח את אינדקס התא אליו משתייך הוקטור שהוא רואה.

<u>דוגמה פשוטה למקרה שאין אינפורמציית-צד</u>

(*) נקודד מקור (ללא אינפורמצית צד) ע"י חלוקת כל הוקטורים **x** ל- 2^{nR} תאים (בפילוג אחיד) ונשדר את אינדקס התא של כל מילת מקור שמתקבלת.

ישנם $\left|A_\varepsilon^{(n)}\right| \doteq 2^{nH(\mathbf{x})}$ וקטורים בקבוצה האופיינית.

מה הסיכוי ששני **x**-ים ששייכים לקבוצה האופיינית יפלו לאותו תא?

נניח ש-x אופייני מסויים נפל לתא i, מה הסיכוי ש-x אופייני נוסף יפול גם כן בתא i?

זה שקול ל- $2^{nH(x)}-1$ ניסויים עם סיכוי הצלחה 2^{-nR}. ההסתברות שלפחות אחד ה-x-ים האופייניים יפול לתא ה-i היא:

$$\Pr\begin{Bmatrix} any \\ "success" \end{Bmatrix} \xrightarrow{n\to\infty} \begin{cases} 0, & H(\mathbf{x})<R \\ 1, & H(\mathbf{x})>R \end{cases}$$

פענוח

מתוך זוג אינדקסים (i,j) שהוא מקבל, המפענח יחפש בזוג התאים (i,j) זוג וקטורים (**x**,**y**) השייכים לקבוצה האופיינית במשותף.

נגדיר את הקבוצה האופיינית המשותפת החלשה:

$$A_\varepsilon^{(n)}(\mathbf{x},\mathbf{y}) \doteq \left\{ (\mathbf{x},\mathbf{y}) : \begin{array}{l} \left|\frac{1}{n}\log p(\mathbf{x},\mathbf{y}) - H(\mathbf{x},\mathbf{y})\right| < \varepsilon \\ \left|\frac{1}{n}\log p(\mathbf{x}) - H(\mathbf{x})\right| < \varepsilon \\ \left|\frac{1}{n}\log p(\mathbf{y}) - H(\mathbf{y})\right| < \varepsilon \end{array} \right\}$$

ננתח את מאורעות השגיאה:

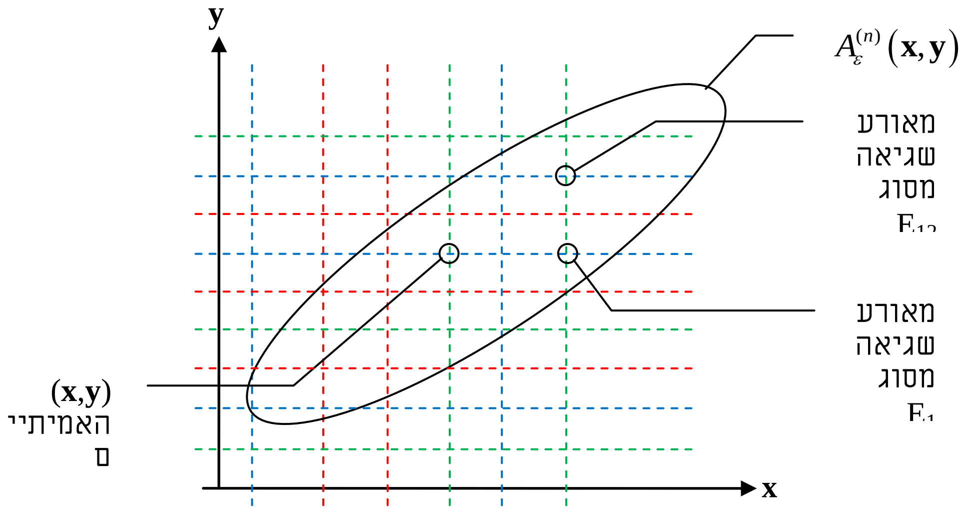
נגדיר:

E_0 – הזוג (**x**,**y**) האמיתי אינו אופייני במשותף. כלומר $(\mathbf{x},\mathbf{y}) \notin A_\varepsilon^{(n)}(\mathbf{x},\mathbf{y})$.

E_{12} – זוג אחר (**x'**,**y'**) אופייני במשותף "נפל" לאותו זוג תאים כמו (**x**,**y**).

E_1 – **x'** אחר אופייני במשותף עם **y** נפל לאותו תא כמו **x**.

E_2 – **y'** אחר אופייני במשותף עם **x** נפל לאותו תא כמו **y**.



הצבעים מייצגים את מספר התא אליו נפלה מילת המקור.

הסתברות השגיאה:

$$P_e=\Pr\{E_0\cup E_{12}\cup E_1\cup E_2\}\underset{\substack{Union\\Bound}}{\le}\Pr\{E_0\}+\Pr\{E_{12}\}+\Pr\{E_1\}+\Pr\{E_2\}$$

עבור n מספיק גדול $\Pr\{E_0\}<\varepsilon$ ע"פ ה-JAEP.

$$\Pr\{E_{12}\}\le\sum_{\substack{(\mathbf{x}',\mathbf{y}')\in A_\varepsilon^{(n)}\\(\mathbf{x}',\mathbf{y}')\neq(\mathbf{x},\mathbf{y})}}2^{-n(R_1+R_2)}\underset{(*)}{\approx}\left(2^{nH(x,y)}-1\right)\cdot2^{-n(R_1+R_2)}\xrightarrow[n\to\infty]{\text{if }H(x,y)<R_1+R_2}0$$

נשים לב שהתכונה $2^{nH(\mathbf{x}|\mathbf{y})}\approx\left|A_\varepsilon^{(n)}(\mathbf{x}|\mathbf{y})\right|$ נכונה רק עבור **y** אופייני במובן החזק

(התכונה מתקיימת גם לאפייניות חלשה בממוצע לפי $p(\mathbf{y})$).

נניח פענוח לפי אופייניות חזקה. ולכן קיימים (בקירוב) $2^{nH(\mathbf{x}|\mathbf{y})}$ **x**-ים אחרים שאופייניים במשותף עם **y**. הסיכוי שאחד ה-x-ים יפול לתא מסויים:

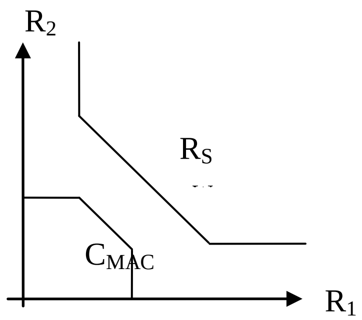
$$2^{nH(\mathbf{x}|\mathbf{y})}\cdot2^{-nR_1}\xrightarrow[n\to\infty]{\text{if }R_1>H(\mathbf{x}|\mathbf{y})}0$$

זהה ל-(iii).

ולכן אם מתקיים $\begin{cases}R_1+R_2>H(\mathbf{x},\mathbf{y})\\R_1>H(\mathbf{x}|\mathbf{y})\\R_2>H(\mathbf{y}|\mathbf{x})\end{cases}$ אזי $P_e\xrightarrow[n\to\infty]{}0$.

הערות:

1) המקודד הוא אוניברסלי (לא תלוי בפילוג המקורות), המפענח תלוי בפילוג המקורות.
2) לא קיימת "גרסת האפמן" (כלומר קידוד באורך משתנה עם אפס שגיאה ממש) לבעיית SW.
3) קידוד משותף MAC-SW:
מתברר שאין עיקרון הפרדה לבעיה זו ויתכן מצב שבו אין חיתוך בין תחום קצבי SW האפשריים לתחום C_{MAC}. למשל,



אבל קיימת דרך "ללא הפרדה" שמאפשרת: $\Pr\left\{\left(\hat{\mathbf{s}}_1,\hat{\mathbf{s}}_2\right)\neq\left(\mathbf{s}_1,\mathbf{s}_2\right)\right\}\xrightarrow{n\to\infty}0$.

למשל, מקור כפול המתפלג ע"פ:

$s_1 \backslash s_2$	0	1
0	1/3	1/3
1	0	1/3

וערוץ MAC מסוג binary adder: $y=x_1+x_2$

מתקיים: $C_{MAC}\cap R_{SW}=\varnothing$ אבל ניתן להעביר ללא קידוד (ע"י שידור המקור ישירות לערוץ) בהסתברות שגיאה אפס.

היות והמקרה $y=s_1+s_2=1$ אומר בוודאות ש- $s_1=0,\ s_2=1$ אזי אין אי-ודאות במקלט לגבי $\left(s_1,s_2\right)$!

נשים לב ש- $R_{SW}\geq H\left(X,Y\right)=\log(3)\approx 1.58\text{ bit}$ בעוד ש- $C_{MAC}=1.5\text{ bit}$ ולכן $C_{MAC}\cap R_{SW}=\varnothing$.

הרצאה מס' 6

סריגים

סוכם ע"י ניר אדמתי

הגדרה

סריג במרחב $\Re^n$ היא קבוצה מדידה (אינסוף בר-מניה) של נקודות הסגורה תחת שיקוף וחיבור.

סימון: $\Lambda = \{\underline{\lambda_i}\}$ (= סריג), כאשר $\{\underline{\lambda_i}\}$ הן נקודות הסריג.

שיקוף: $\underline{\lambda}\epsilon\Lambda \rightarrow -\underline{\lambda}\epsilon\Lambda$

חיבור: $\underline{\lambda}, \underline{\lambda}'\epsilon\Lambda \rightarrow \underline{\lambda} + \underline{\lambda}'\epsilon\Lambda$

מסקנה: $\underline{\lambda_0} = \underline{0}\epsilon\Lambda$

מכאן גם נובע כי $\underline{\lambda}, \underline{\lambda}'\epsilon\Lambda \rightarrow k_1\underline{\lambda} + k_2\underline{\lambda}'\epsilon\Lambda$ עבור k_1, k_2 שלמים כלשהם.
הגדרה שקולה דרך מטריצה יוצרת (אוסף וקטורי בסיס):

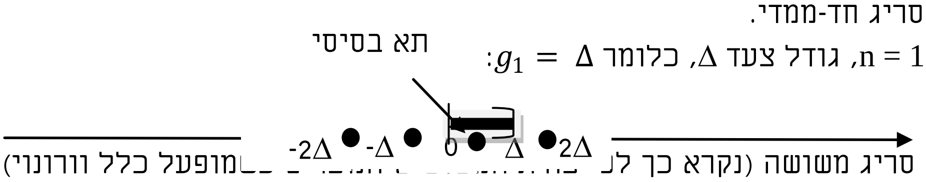
$$\Lambda = \{G\underline{i} \mid \underline{i}\epsilon\mathbb{Z}^n\} = \left\{\sum_{m=1}^{n} i_m \underline{g_m} \mid \underline{i} = [i_1, \dots, i_n]^T \epsilon\mathbb{Z}^n\right\}$$

כאשר $\{\underline{g_m}\}$ הן עמודות המטריצה G.

$G = I$ הוא מקרה פרטי: $\Lambda = \mathbb{Z}^n$ (integer lattice).

דוגמאות:

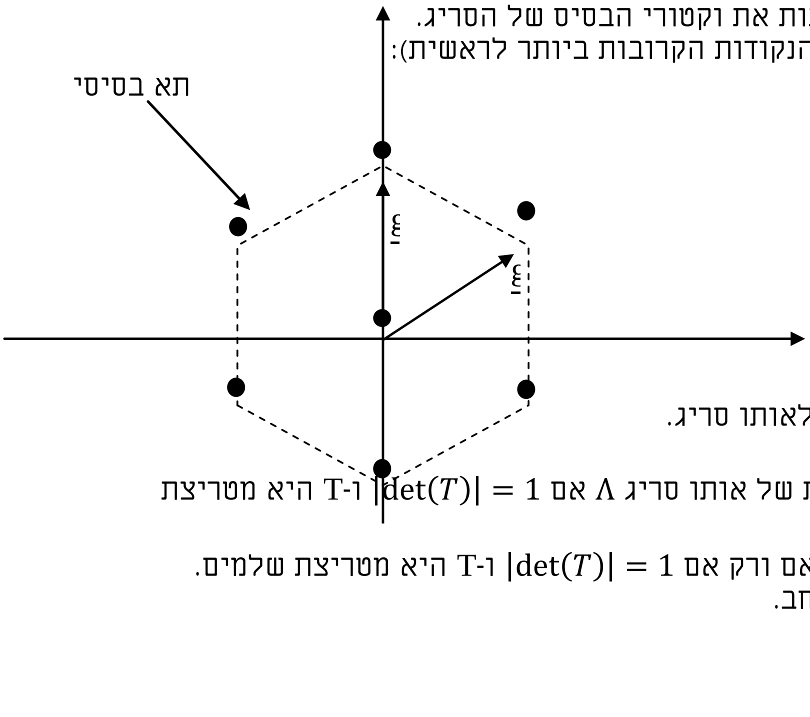
1. סריג חד-ממדי.
$n = 1$, גודל צעד Δ, כלומר $g_1 = \Delta$:



2. סריג משושה (נקרא כך ל[illegible] מופעל כלל וורונוי)
$n = 2$.

$$G = \begin{pmatrix} 0 & \sqrt{3} \\ 2 & 1 \end{pmatrix}$$

עמודות המטריצה G מציינות את וקטורי הבסיס של הסריג.
נתבונן בחלק מהסריג (רק הנקודות הקרובות ביותר לראשית):



הערה:

- יתכנו אינסוף בסיסים לאותו סריג.

כלל: $G' = GT$ היא מטריצה יוצרת של אותו סריג Λ אם $|\det(T)| = 1$ ו-T היא מטריצת שלמים.

במילים אחרות, $\Lambda(GT) = \Lambda(G)$ אם ורק אם $|\det(T)| = 1$ ו-T היא מטריצת שלמים.
סריג בעצם משרה חלוקה של המרחב.

חלוקה סריגית:

חלוקה של המרחב לתאים p_i כך ש- $p_i = p_0 + \underline{\lambda_i}$, כאשר p_0 הוא תא בסיסי השייך לנקודת האפס של הסריג ו-$\underline{\lambda_i}$ היא נקודת סריג.

נשים לב כי החיבור במשוואה של p_i הוא סכום מינקובסקי בין קבוצות המוגדר באופן הבא:
$A + B = \{a + b \mid a\epsilon A, b\epsilon B\}$

החלוקה היא במובן שמתקיים: $\bigcup p_i = \Re^n$ ו- $p_i \cap p_j = \emptyset$ עבור i≠j.
כלומר, זהו כיסוי זר של המרחב.

<u>דוגמה 1:</u>

חלוקה למקבילונים: $p_0 = \left\{\alpha_1 \underline{g_1} + \cdots + \alpha_n \underline{g_n} \,\middle|\, 0 \le \alpha_i < 1 \ \forall i = 1, \dots, n\right\}$

p_0 הוא מקבילון ראשי שנוצר על ידי n וקטורים $\{\underline{g_m}\}$ שהן עמודות המטריצה G.

לכל חלוקה של סריג נתון מתקיים: $vol(p_i) = |\det(G)| \stackrel{\text{def}}{=} \det(\Lambda)$ עבור i כלשהו ("נפח הסריג" או "דטרמיננט הסריג").

ניתן להיווכח כי $vol(p_0) = |\det(G)|$

במקרה של חלוקה למקבילונים ניתן להוכיח לפי:

1. (קוביה סטנדרטית) G = מקבילון, כאשר קוביה סטנדרטית היא מעל $[0,1)^n$, ואז ניקח יעקוביאן.
2. דרך גרם שמידט.
3. $G = QR$ כאשר Q היא מטריצה אורתונורמלית(יוניטרית) ו-R מטריצה משולשית. אז $|\det(G)| = |\det(R)|$.

האם יתכן שהנפח של התא הבסיסי יהיה תלוי בייצוג של הסריג (דרך G)?

מתקיים ש-$|\det(G)|$ הוא גודל אינווריאנטי למטריצה היוצרת G של Λ, ומסמנים: $|\det(G)| = \det(\Lambda)$.

נביא שתי הוכחות:

הוכחה 1: הוכחה עבור חלוקה כללית (למשל חלוקת וורונוי שמוגדרת בהמשך)

ניקח קוביה גדולה שמכילה N נקודות סריג עם נפח תא סריג p_i שווה בקירוב ל- $\frac{\text{נפח קוביה}}{N}$ ללא תלות באיך נוצר התא.

השוויון הוא בקירוב כיוון שיתכנו זליגות של תאי קצה מהקוביה, אך עם הגדלת מספר התאים (N) הזליגות זניחות ביחס.

<u>דוגמה 2:</u> "חלוקת וורונוי"
(ניתנת להגדרה לכל מידת מרחק 'נורמה')

$$p_0 = \left\{\underline{x} \middle| \|\underline{x}\| \le \left\|\underline{x} - \underline{\lambda_i}\right\| \ \forall i \ne 0\right\}$$

$$p_i = \left\{\underline{x} \middle| \left\|\underline{x} - \underline{\lambda_i}\right\| \le \left\|\underline{x} - \underline{\lambda_j}\right\| \ \forall j \ne i\right\}$$

ν_i הוא תא וורונוי אם הוא כולל את כל הנקודות ב- $\Re^n$ הקרובות ל-$\underline{\lambda_i}\epsilon\Lambda$ יותר מלכל נקודת סריג $\underline{\lambda_j}\epsilon\Lambda$ אחרת.

<u>סימון תא וורונוי בסיסי:</u> $p_0 = \nu_0$

הוכחה 2: "הוכחה אלגנטית"

יהיו p_0' ו- p_0'' חלוקות סריגיות של המרחב כפי שהוגדר ב"חלוקה סריגית", כלומר מתקיים:

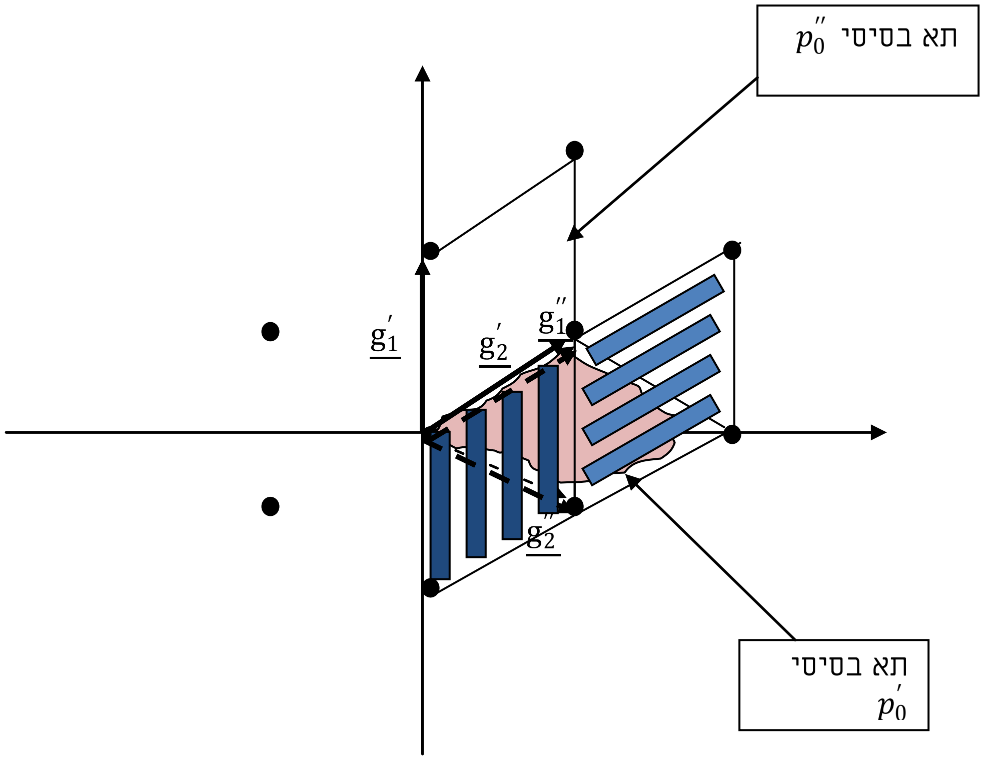
$$\Re^n = \dot{\bigcup_i} p_i' = \dot{\bigcup_i} p_i''$$

כאשר המרחב הוא n-ממדי והנקודה מעל סימן האיחוד מזכירה לנו שהחלוקה היא זרה.

כפי שראינו מתקיים $p_i = p_0 + \underline{\lambda_i}$, כאשר p_0 הוא תא בסיסי השייך לנקודת האפס של הסריג ו-$\underline{\lambda_i}$ היא נקודת סריג.
מתקיים:

$$p_0^{'} = \dot{\bigcup_i}\left(p_0^{'} \bigcap p_i^{''}\right) = \dot{\bigcup_i}\left(p_0^{'} \bigcap \left(p_0^{''} + \underline{\lambda_i}\right)\right)$$

כאשר השוויון הראשון (שמוכר מהסתברות ומקומבינטוריקה) נובע מאיחוד זר של תאי סריג רלוונטיים (ביחס לחיתוך) עם תא הסריג הבסיסי $p_0^{'}$. הסבר גרפי לשוויון הראשון עבור $\Re^2$ וחלק מנקודות הסריג:



וקטורי הבסיס של החלוקה $p_0^{'}$ הם $\underline{g}_1^{'} = \binom{\sqrt{3}}{1}$, $\underline{g}_2^{'} = \binom{\sqrt{3}}{-1}$, ווקטורי הבסיס של החלוקה $p_0^{''}$ הם $\underline{g}_1^{''} = \binom{0}{2}$, $\underline{g}_2^{''} = \binom{\sqrt{3}}{1}$.
השוויון השני נובע מההצבה $p_i^{''} = p_0^{''} + \underline{\lambda_i}$.
באותו אופן ומאותם השיקולים מתקיים:

$$p_0^{''} = \dot{\bigcup_i}\left(p_i^{'} \bigcap p_0^{''}\right) = \dot{\bigcup_i}\left(\left(p_0^{'} + \underline{\lambda_i}\right) \bigcap p_0^{''}\right)$$

תחת לקיחת נפח (vol) מתקיים:

$$\mathrm{vol}\left\{\dot{\bigcup_i}\left(p_0^{'} \bigcap \left(p_0^{''} + \underline{\lambda_i}\right)\right)\right\} = vol\left\{\dot{\bigcup_i}\left(\left(p_0^{'} - \underline{\lambda_i}\right) \bigcap p_0^{''}\right)\right\}$$

מכאן שמתקיים: $\mathrm{vol}\{p_0^{'}\} = vol\{p_0^{''}\}$
כיוון שהחלוקות הן כלשהן ברור ש"נפח הסריג" (כפי שהוגדר) אינו תלוי בחלוקה.

הערה: כמובן שהסריג נשאר זהה ורק החלוקות שלו שונות, לכן אותן נקודות סריג $\underline{\lambda_i}$ מופיעות בנוסחאות.

<u>הערה:</u>
שייכות נקודות שפה היא כל עוד מתקיים כלל החלוקה שהוגדר בחלוקה הסריגית.

<u>הגדרה:</u>
יהי $\underline{u} \sim Unif(p_0)$
$\underline{u}$ נקרא dither.

סימון: $V = \det(\Lambda)$

<u>הגדרה: מדד טיב לקוונטיזציה</u>
אם נשתמש בחלוקת וורונוי ($\mathrm{p}_0 = \nu_0$), אז:

$$\sigma_\Lambda^2 \overset{\text{def}}{=} Second\ Moment\ of\ the\ lattice\ \overset{\text{def}}{=} \frac{1}{n} E\{\|\underline{u}\|^2\}$$

$$\mathrm{G}(\Lambda) \overset{\text{def}}{=} \mathrm{NSM} = Normalized\ Second\ Moment\ of\ the\ lattice \overset{\text{def}}{=} \frac{\sigma_\Lambda^2}{\mathrm{V}^{\frac{2}{n}}}$$

נשים לב כי $\mathrm{G}(\Lambda)$ הינו אינווריאנטי למתיחה/כיווץ של Λ.

בסריג חד-ממדי: $\mathrm{G}(\Lambda) = \frac{1}{12}$

בסריג משושה: $\mathrm{G}(\Lambda) < \frac{1}{12}$

נגדיר: $G_n \overset{\text{def}}{=} \min_{\Lambda \epsilon\, \Re^n} \mathrm{G}(\Lambda)$

תמיד מתקיים: $G_n \geq G_n(\mathrm{Ball})$
זהו אי-השוויון האיזו-פרמיטרי: לכדור יש את המומנט השני הקטן ביותר מבין כל הגופים ה-n ממדיים עם נפח נתון.

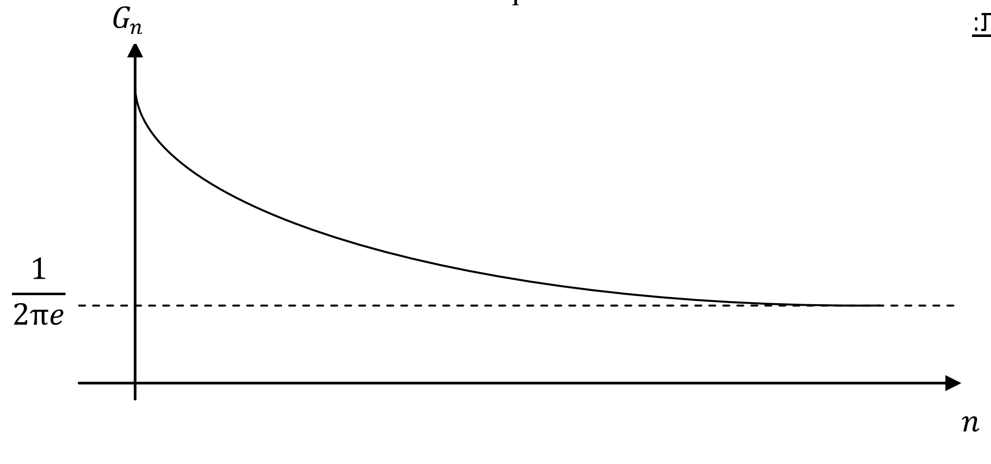
נסמן: $G_n^* = G(Ball) = \frac{\sigma^2(Ball)}{V^{\frac{2}{n}}}$

כשהכוונה ב-$\sigma^2(Ball)$ היא קח פילוג אחיד על פני כדור וחשב מומנט שני לממד.

תוצאה אסימפטוטית: $\lim_{n\to\infty} G_n = \lim_{n\to\infty} G_n(\mathrm{Ball}) = \frac{1}{2\pi e}$

ההוכחה מובאת במאמר: "On lattice quantization noise"

<u>גרפית:</u>



<u>הגדרה: מדד טיב לאפנון/קידוד ערוץ</u>

$$P_e(\Lambda, \sigma_\Lambda^2) \overset{\text{def}}{=} P_r(\underline{z} \notin \nu_0) \quad when \quad \underline{z} \sim N(\underline{0}, \sigma_z^2 I)\ \ \mathrm{AWGN}$$

$$\mu(\Lambda, P_e) = VNR = Volumn\ to\ Noise\ Ratio \overset{\text{def}}{=} \frac{V^{\frac{2}{n}}}{\sigma_z^2}$$

כאשר σ_z^2 נבחר כך שיתקיים $P_e(\Lambda, \sigma_z^2) = P_e$.

<u>הערה:</u>

$P_e\left(\Lambda,\sigma_z^2\right)$ מייצג את הסתברות שגיאת פענוח ML אם משתמשים בסריג Λ כקונסטלציה לשידור, וגודל הקונסטלציה מאוד גדול יחסית לגודל התאים. אז $P_e\left(\Lambda,\sigma_z^2\right)$ הוא הסיכוי שהרעש יוציא אותנו מהתא.

תוצאה אסימפטוטית: $\lim_{P_e\to 0}\mu\left(\Lambda,p\right) = \infty$

מסקנה: יש למתוח (ממש) את הסריג כדי להשיג הסתברות שגיאה קטנה.

עבור סריג Λ סקלרי מתקיים: $\mu\left(\Lambda,p\right) = func(Q_{func})$, כאשר $Q_{func}(x) \stackrel{\text{def}}{=} \int_x^{\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx$

עבור ממדים גבוהים יותר יש להשתמש בפילוג ψ^2 מסדר n.

נוכל להגדיר: $\mu_n(P_e) \stackrel{\text{def}}{=} \min_{\Lambda\epsilon\,\Re^n}\mu\left(\Lambda,P_e\right)$

תמיד מתקיים: $\mu_n\left(\Lambda,P_e\right) \geq \mu_n(n\ dimension\ ball\ with\ the\ same\ P_e)$

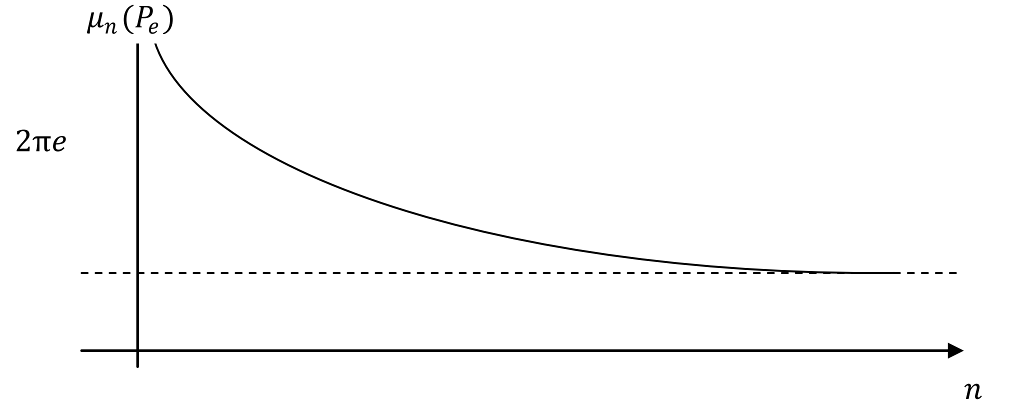
נסמן: $\mu_n^*(P_e) = \mu_n(n\ dimension\ ball\ with\ the\ same\ P_e) = \frac{V^{\frac{2}{n}}}{\sigma_z^2}$

וכמו בהגדרה σ_z^2 היא השונות של רעש נורמלי לבן כך שמתקיים $P_e = P_e(Ball,\sigma^2)$.

הסדרות $\mu_n(P_e)$ ו-$\mu_n^*(P_e)$ יורדת עם n ומתכנסות ל-$2\pi e$ לכל $0 < P_e < 1$.

ההוכחה מובאת במאמר של פולטירה ובמאמר של פורנו-שרוט-צאנט.

<u>גרפית:</u>



- כדור טוב יותר מכל תא סריגי באותו הנפח במובן של מומנט שני מנורמל (G) ויחס נפח לרעש (μ) - כדור חוסם מלמטה את $G(\Lambda)$ ואת $\mu\left(\Lambda,P_e\right)$.
- הסתברות השגיאה של כדור טובה יותר.

<u>קוונטייזר (Λ,p)</u>

$$Q_\Lambda\left(\underline{x}\right) = \underline{\lambda_i} \qquad if \quad \underline{x}\epsilon p_i$$

<u>עבור חלוקת וורונוי:</u>

$$Q_\Lambda\left(\underline{x}\right) = \underline{\lambda_i} \qquad if \quad \left\|\underline{x} - \underline{\lambda_i}\right\| \leq \left\|\underline{x} - \underline{\lambda_j}\right\| \ \forall j \neq i$$

אם החלוקה היא חלוקת וורונוי אז כלל השיוך הוא השכן הקרוב ביותר.

<u>שגיאת הקוונטיזציה מוגדרת</u> $Q_\Lambda\left(\underline{x}\right) - \underline{x}$

אם $\underline{x}$ הוא וקטור אקראי שמתפלג אחיד על תחום גדול במרחב (או פונקציית צפיפות הפילוג "חלקה" ורזולוציית הקוונטיזציה גדולה), אז שגיאת הקוונטיזציה מתפלגת אחיד על פני תא בסיסי.

<u>קוונטייזר עם "dither מתחסר"</u>

$$\hat{\underline{x}} = Q_\Lambda\left(\underline{x} + \underline{u}\right) - \underline{u}$$

<u>הערה:</u>

$Q_\Lambda(\underline{x} + \underline{u}) - \underline{u}$ שקול להזזת מערכת התאים ב-$\underline{u}$.

<u>**מודולו סריג**</u>

$$\underline{x}\ mod\ \Lambda = \underline{x} - Q_\Lambda(\underline{x}) = minus\ quantization\ error$$

(הכללת מושג המודולו לוקטורים)

<u>**שגיאת קוונטיזציה עם dither**</u>

$$\hat{\underline{x}} - \underline{x} = Q_\Lambda(\underline{x} + \underline{u}) - \underline{u} - \underline{x} = -(\underline{x} + \underline{u})\ mod\ \Lambda$$

משפט:

אם $\underline{u} \sim Unif(p_0)$ אז $\forall \underline{x} \rightarrow (\underline{x} + \underline{u})\ mod\ \Lambda \sim Unif(p_0)$

כלומר שגיאת הקוונטיזציה אחידה בתא וורונוי בסיסי ובת"ס במקור.

<u>Generalized Dither</u>

מותר להשתמש בכל $\underline{u}$ שמקיים $\underline{u}\ mod\ \Lambda \sim unif(p_0)$.

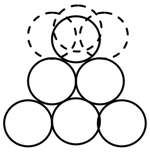
<u>**אריזה וכיסוי של כדורים שמרכזם על סריג (*Sphere packing and covering*)**</u>

1. בעיית האריזה

<u>**סריג *Face Cubic Centered (FCC)***</u>

זו אריזה סריגית אופטימלית במרחב $\mathfrak{R}^3$.

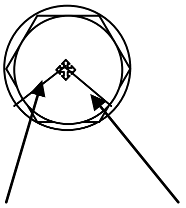
ציור להמחשה ממבט על:



כאשר ——— מציין שכבה ראשונה ו- - - - מציין שכבה שניה, והשכבות הן אחת על השניה (מסודרות כך שמרכז כל כדור באזורי החורים של השכבות מעל/מתחת).

סריג ה-FCC הוא הפתרון האופטימלי של בעיית האריזה במרחב התלת-ממדי: הבאת כמות הכדורים למקסימום בנפח נתון.

גרפית:



נגדיר r_{eff} לפי: $vol(Ball(r_{\text{eff}})) = \det(\Lambda)$.

ברור שמתקיים $r_{pack} \leq r_{\text{eff}} \leq r_{cov}$

נשים לב כי לפי הגדרה כל כדור מציין תא וורונוי.

<u>יעילות האריזה:</u>

נרצה ש-r_{eff} יהיה כמה שיותר קרוב ל-r_{pack}.

$$\rho_{pack} \stackrel{\text{def}}{=} \frac{r_{pack}}{r_{\text{eff}}} < 1$$

ושוויון (לאחד) אם n=1.

פתרון הבעיה $\max_{\Lambda \epsilon \mathfrak{R}^n} \rho_{pack}(\Lambda)$ נותן את הסריג עם האריזה האופטימלית.

<u>צפיפות האריזה:</u>

$$\rho_{pack}^{n} = \frac{\text{נפח מנוצל על ידי כדורים}}{\text{גודל האיזור בו אורזים}} \lim_{\text{גודל האיזור בו אורזים}\to\infty} \stackrel{\text{def}}{=} \text{צפיפות האריזה}$$

2. בעיית הכיסוי

עבור סריג $\boldsymbol{\Lambda}$ נתון מגדירים את רדיוס הכיסויי:

$$\text{רדיוס חוסם של תא וורונוי} = r_{cov} = \max_{\underline{x}\in\Re^n}(\min_{\underline{\lambda}\in\Lambda}\|\underline{x}-\underline{\lambda}\|) = \max_{\underline{x}\in\Re^n}\|\underline{x}-\underline{\lambda}\|$$

$$(\rho_{cov}(\Lambda))^{\mathrm{n}} \stackrel{\text{def}}{=} \left(\frac{r_{cov}}{r_{\text{eff}}}\right)^n = \frac{\text{סך הכל נפח כדורים}}{\text{נפח אזור מכוסה}} \lim_{\text{אזור}\to\infty} = \text{עובי הכיסוי}$$

פתרון הבעיה $\min_{\Lambda}\rho_{cov}(\Lambda)$ נותן את בעיית הכיסוי.

עבור n=3, הפתרון האופטימלי הוא Body Centered Cubic Lattice (BCC Lattice).

<u>מדוע כדאי לדבר על כדורים?</u>

בתורת האינפורמציה 1 ראינו שרעש גאוסי לבן שואף עם הממד לכדור (*AEP*).

הקשר בין כדור לגאוסי לבן:

$$AEP: \underline{z}\sim N(\underline{0},\sigma^2 I), AWGN \quad then \quad A_{\varepsilon}^{(n)}(z) = Ball(\underline{0},\sqrt{n\sigma^2})$$

<u>מסקנות:</u>

1. $$\left|A_{\varepsilon}^{(n)}\right| = 2^{nh(z)} = 2^{n\frac{1}{2}\log(2\pi e\sigma^2)} = (2\pi e\sigma^2)^{\frac{n}{2}}$$

$$|Ball(\underline{0},r)| = v_n r^n = v_n(n\sigma^2)^{\frac{n}{2}}$$

כאשר $r = \sqrt{n\sigma^2}$ ו-v_n הוא נפח כדור יחידה בממד n.

מכאן $v_n\sim\left(\frac{2\pi e}{n}\right)^{\frac{\mathrm{n}}{2}}$ עבור n מספיק גדול.

2. $P_e(Ball,\sigma^2) \stackrel{\text{def}}{=} P_r(\underline{z}\notin Ball(\underline{0},\sqrt{nt})) \to \begin{cases}0 & ,t>\sigma^2\\ 1 & ,t<\sigma^2\end{cases}$ עם $n\to\infty$.

קשר בין:

- אפנון ↔ אריזה
- קוונטיזציה ↔ כיסוי

$$G_n^* \leq^{(1)} G(\Lambda) \leq^{(3)} G_n^*\rho_{cov}^2$$

$$\mu_n^*(P_e) \leq^{(2)} \mu(\Lambda,P_e) \leq^{(4)} \frac{\mu_n^*(P_e)}{\rho_{pack}^2}$$

(1) מכל הגופים עם נפח נתון, לכדור מומנט שני מינימלי.

(2) מכל הגופים עם נפח נתון, ההסתברות $P_e(\text{גוף},\sigma^2)$ היא המינימלית עבור כדור (תואם לגאוסיאן במובן של התרחקות מהראשית).

(3) המומנט השני של הכדור המכיל את תא הסריג גדול מהמומנט השני של הכדור המוכל. מומנט שני של כדור החוסם תא סריגי גדול יותר ממומנט שני של תא וורונוי.

(4) לכדור חסום יש הסתברות שגיאה גרועה יותר מתא וורונוי.

Minkowski – Hanwha Theorem (סוף המאה ה-19)

קיימת סדרת סריגים Λ_n כך ש- $\rho_{pack}\,(\Lambda_n) > \frac{1}{2}$.

אחרים הראו כי ... $\lim_{n\to\infty} \sup\ \ \rho_{pack}\,(\Lambda_n) < 0.6$, כלומר לא ניתן להגיע ל-1.

אולם למרות התוצאה ה"שלילית" הזו ידוע שקיימת סדרת סריגים שמקיימת $\lim_{n\to\infty} \frac{\mu(\Lambda_n, P_e)}{\mu_n^*(P_e)} = 1$.

<u>הערה:</u>

דומה לפער בין "חסם המינג" ל"חסם גילברט-וארשאמוב" בקודים לינארים במרחב הבינארי.

רוג'רס (60's)

קיימת סדרת סריגים Λ_n כך ש- $\lim_{n\to\infty} \rho_{cov}\,(\Lambda_n) = 1$.

עבור סדרה זו מתקיים: $\lim_{n\to\infty} \frac{G(\Lambda_n)}{G_n^*} = 1$ וכן מתקיים: $\lim_{n\to\infty} G_n^* = \frac{1}{2\pi e}$

ולכן במובן כיסוי/קוונטיזציה תאי סריגים "טובים" אכן שואפים לכדורים.

הרצאה מס' 7

שימוש בסריגים לקידוד – קודי Voronoi

סוכם ע"י אדם משיח

מוטיבציה

המטרה היא להשיג קיבול ערוץ (קידוד ערוץ) או פונקצית קצב- עיוות (קידוד מקור) ע"י שימוש בסריגים. בעיה בשימוש בסריג לצורך קידוד מקור /ערוץ היא שהסריג הוא אינסופי מעצם הגדרתו. לא ניתן להשתמש בסריג אינסופי בקידוד ערוץ בגלל מגבלת ההספק, ואילו בקידוד מקור בגלל שנדרש כמות אינסופית של ביטים לייצוג כל נקודת סריג. כדי להימנע מבעיה זו נתחום את ספר הקוד הסריגי בתוך אזור מסוים במרחב. נעשה זאת ע"י שימוש בתא בסיסי של סריג דליל יותר.

סריגים מקוננים

נאמר ששני סריגים Λ_1 ו Λ_2 מקוננים אם מתקיים $\Lambda_2 \subset \Lambda_1$.

כלומר אם: $\underline{x} \in \Lambda_2 \Rightarrow \underline{x} \in \Lambda_1$

Λ_1 נקרא *הסריג העדין* ו Λ_2 נקרא *הסריג הגס*.

אם Λ_1 בעל מטריצה יוצרת G_1 ו Λ_2 בעל מטריצה יוצרת G_2 אזי קיימת מטריצה J עם רכיבים שלמים ובעלת $\det(J) > 1$ כך ש: $G_1 = G_2 \cdot J$.

אם ניתן לכתוב $J = kU$, כאשר U מטריצת יוניטרית ו k מספר שלם, אזי Λ_2 זהה ל Λ_1 עד כדי שינוי גודל (scaling) וסיבוב. מקרה פרטי זה נקרא *"Self Similar"*.

נגדיר את ספר הקוד של קוד ורונוי המתאים לסריגים Λ_1 ו Λ_2 ע"י:

$$VoronoiCodebook = \Lambda_1 \cap \nu_{0,2} = \Lambda_1 \bmod \Lambda_2 \square \left\{ \underline{x} \bmod \Lambda_2 : \underline{x} \in \Lambda_1 \right\}$$

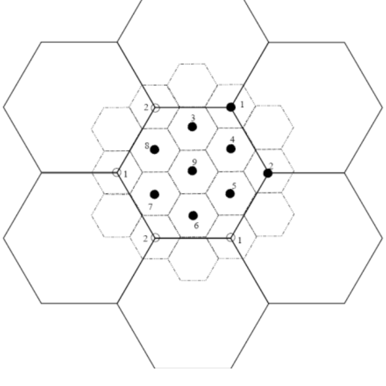
כאשר $\nu_{0,2}$ הוא תא ורונוי הבסיסי (מתאים ל $\underline{x} = \underline{0}$) של Λ_2.

גודל הקוד פשוט נתון ע"י מספר וקטורי הסריג העדין Λ_1 הנכנסים בתא אחד של הסריג הגס Λ_2:

$$\left|VoronoiCodebook\right| = \frac{V_2}{V_1} = \frac{\left|\det(G_2)\right|}{\left|\det(G_1)\right|} = \left|\det(J)\right|$$

וקצב הקוד נתון ע"י: $R = \frac{1}{n}\log_2\left(\left|VoronoiCodebook\right|\right) = \frac{1}{n}\log_2\left(\left|\det(J)\right|\right)$

יחס הקינון (Nesting Ratio) מוגדר ע"י: $\sqrt[n]{\left|\det(J)\right|}$.



איור 6: דוגמא לסריגים מקוננים

Dithered Voronoi Codebook

מחברים לכל וקטורי הקוד וקטור $\underline{u}$ (dither), כאשר החיבור הוא מודולו הסריג Λ_2 :

$$DitheredVoronoiCodebook = \left(\Lambda_1 + \underline{u}\right) \bmod \Lambda_2 = \left\{\left(\underline{x}+\underline{u}\right) \bmod \Lambda_2 : \underline{x} \in \Lambda_1\right\}$$

בגלל פעולת המודולו קל לראות שגודל ספר הקוד לא השתנה, כלומר:

$$\left|DitheredVoronoiCodebook\right| = \left|\det\left(\mathrm{J}\right)\right| \ , \ \forall \underline{u}$$

השגת קיבול ערוץ AWGN ע"י קוד וורונוי

נתבונן בערוץ AWGN: $\underline{y} = \underline{x} + \underline{z}$, כאשר $Z \sim \mathrm{N}\left(0, N\right)$. נניח מגבלת הספק P.

ספר קוד: Dithered Voronoi Codebook עם מילות הקוד $\left(\lambda_i + \underline{u}\right)_{\lambda_i \in \Lambda_1} \bmod \Lambda_2$, כאשר הdither מפולג באופן אחיד על תא וורונוי הבסיסי: $\underline{u} \sim Unif\left(\upsilon_{0,2}\right)$. כלומר המשדר משדר:

$$\underline{x} = \left(\lambda_i + \underline{u}\right)_{\lambda_i \in \Lambda_1} \bmod \Lambda_2$$

כלל החלטה: מתבסס על בחירת נקודת הסריג העדין הקרובה ביותר (לאחר חיסור הdither) והטלתה לתוך תא וורונוי הבסיסי של הסריג הגס:

$$\hat{\underline{\lambda}}_i = Q_{\Lambda_1}\left(\underline{y} - \underline{u}\right) \bmod \Lambda_2$$

זה שקול להטלת הנקודה המתקבלת (לאחר חיסור הdither) לתוך תא וורונוי הבסיסי של הסריג הגס ורק לאחר מכן לקרב לנקודת הקוד הקרובה ביותר:

$$\tilde{y} = \left(\underline{y} - \underline{u}\right) \bmod \Lambda_2$$

$$\hat{\underline{\lambda}}_i = Q_{\Lambda_1}\left(\underline{\tilde{y}}\right) \bmod \Lambda_2$$

יש לשים לב שהdither ידוע גם במקודד וגם במפענח (*Common Randomness*).

הספק השידור: הספק השידור הממוצע זהה לכל $\underline{\lambda} \in \Lambda_1$ ותלוי רק בתכונות של Λ_2 :

$$\frac{1}{n}\mathrm{E}\left\|\underline{x}\right\|^2 = \frac{1}{n}\mathrm{E}\left\|\left(\underline{\lambda} + \underline{u}\right) \bmod \Lambda_2\right\|^2 = \frac{1}{n}\mathrm{E}\left\|\underline{u}\right\|^2 = \sigma^2_{\Lambda_2}$$

לכן אם נבחר סריג גס Λ_2 כך ש $\sigma^2_{\Lambda_2} = P$, אז מגבלת ההספק תתקיים בשוויון.

הסתברות שגיאה: מכיוון שהחלטה מבוססת על בחירת נקודת הסריג העדין הקרובה ביותר לוקטור הנקלט, מאורע השגיאה הוא: $\underline{y} \bmod \Lambda_2 \notin \left(\underline{u} + \upsilon_{i,1}\right) \bmod \Lambda_2$, כאשר $\upsilon_{i,1}$ הוא תא וורונוי של λ_i המתאים למילת הקוד ששודרה. לכן הסתברות השגיאה הינה:

$$P_e = \Pr\left\{\left(\underline{x} + \underline{z}\right) \bmod \Lambda_2 \notin \left(\underline{u} + \upsilon_{i,1}\right) \bmod \Lambda_2\right\} = \Pr\left\{\left(\lambda_i + \underline{u} + \underline{z}\right) \bmod \Lambda_2 \notin \left(\underline{u} + \upsilon_{i,1}\right) \bmod \Lambda_2\right\}$$

מאורע זה שקול למאורע: $\left(\lambda_i + \underline{u} + \underline{z}\right) \notin \left(\underline{u} + \upsilon_{i,1}\right) + \Lambda_2$

וע"י העברת אגפים נקבל:

$\underline{z} \notin \left(\upsilon_{i,1} - \lambda_i\right) + \Lambda_2$ מכיוון ש $\upsilon_{i,1} - \lambda_i = \upsilon_{0,1}$ נקבל: $P_e = \Pr\left\{\underline{z} \bmod \Lambda_2 \notin \upsilon_{0,1}\right\}$

ניתן להראות זאת גם ע"י שימוש בפענוח בשני שלבים שהוצג קודם. בשלב הראשון המקלט מחסר את הdither ומטיל את הנקודה המתקבלת לתוך תא וורונוי הבסיסי של הסריג הגס:

$$\tilde{y} = \left(\underline{y}-\underline{u}\right)\bmod \Lambda_2 = \left(\underline{x}+\underline{z}-\underline{u}\right)\bmod \Lambda_2 = \left(\left(\lambda_i+\underline{u}\right)\bmod \Lambda_2+\underline{z}-\underline{u}\right)\bmod \Lambda_2 \overset{(a)}{=}$$
$$= \left(\lambda_i+\underline{u}+\underline{z}-\underline{u}\right)\bmod \Lambda_2 = \left(\lambda_i+\underline{z}\right)\bmod \Lambda_2$$

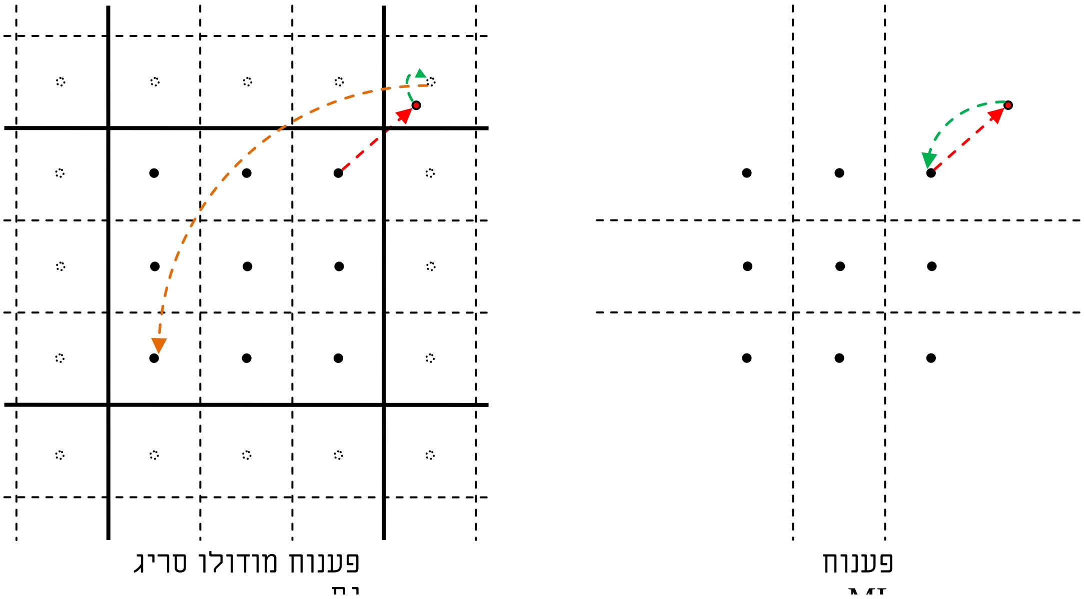
כאשר ב (a) השתמשנו בחוק הפילוג לפעולת המודולו :

$$\left(\underline{a}\bmod \Lambda+\underline{b}\right)\bmod \Lambda = \left(\underline{a}+\underline{b}\right)\bmod \Lambda$$

כלומר קיבלנו "ערוץ שקול" ממילות הקוד λ_i של השריג העדין אל $\tilde{y}$, שהוא ערוץ AWGN עם פעולת מודולו. המקלט מחליט על מילת הקוד ששודרה מתוך מוצא הערוץ השקול ע"י $\underline{\hat{\lambda}}_i = Q_{\Lambda_1}\left(\underline{\tilde{y}}\right)\bmod \Lambda_2$. לכן, סיכוי הטעות בערוץ זה הוא:

$$P_e = \Pr\left\{\underline{z}\bmod \Lambda_2 \notin \upsilon_{o,1}\right\}\ ,\ \forall \underline{u},\underline{\lambda}_i$$

<u>הערה</u>: בניגוד לפענוח ML, בשיטת הפענוח שתוארה למעלה שגיאת הפענוח זהה לכל הסימבולים ששודרו. בפענוח ML לסימבולים בקצות הקונסטלציה תהיה הסתברות שגיאה נמוכה יותר מכיוון שיש להם פחות שכנים . מסיבה זו גם ברור שפענוח מודולו הסריג הגס פחות טוב מפענוח ML. דוגמא פשוטה למצב בו פענוח ML טוב משמעותית מפענוח מודולו סריג גס ניתן לראות ב איור 7. החץ האדום מתאר את הרעש שגורם לכך שהמקלט מקבל קלט השונה מהסימבול ששודר . החץ הירוק מתאר את פעולת הפענוח בכל אחד מהמקרים (ללא המודולו), והחץ הכתום מתאר את פעולת המודולו.



איור 7: הדגמת ההבדל בין פענוח ML לפענוח מודולו סריג גס

קצב הקוד:

$$Rate=\frac{1}{n}\log\left(\left|CodeBook\right|\right)=\frac{1}{n}\log\left(\frac{V_2}{V_1}\right)=\frac{1}{n}\log\left(\frac{V_2}{V_1}\right)=\frac{1}{2}\log\left(\frac{V_2^{2/n}}{V_1^{2/n}}\right)$$

ועל ידי הצבת $G(\Lambda_2)=\frac{\sigma^2_{\Lambda_2}}{V_2^{2/n}}$, $\mu(\Lambda_1,p_e)=\frac{V_1^{2/n}}{N}$, $\sigma^2_{\Lambda_2}=P$ נקבל:

$$Rate=\underbrace{\frac{1}{2}\log\left(\frac{P}{N}\right)}_{C_{AWGN}\ \text{at high SNR}}-\underbrace{\frac{1}{2}\log\left(G(\Lambda_2)\cdot\mu(\Lambda_1,p_e)\right)}_{\text{Capacity Loss}}$$

האיבר הראשון שווה (בקירוב) לקיבול הערוץ ב SNR גבוה ($P>>N$). לכן ב SNR גבוה האיבר השני מתאר את ההפסד ביחס לקיבול, שנובע מהמימד הסופי של הסריגים.

הסריג העדין צריך להיות טוב לאפנון. כלומר, כזה שעבור הסתברות שגיאה מסויימת יהיה בעל נפח מינימלי (יגדיל את הקצב), שקול ל $\mu(\Lambda_1,p_e)$ מינימאלי. ידוע ש $2\pi e\le\mu(\Lambda_1,p_e)$ ושקיימת סדרת סריגים עם מימד הולך וגדל כך ש:

$$\mu(\Lambda_1,p_e)\xrightarrow{n\to\infty}2\pi e$$

הסריג הגס צריך להיות טוב לקוונטיזציה. כלומר, כזה שעבור מומנט שני נתון יהיה בעל נפח מקסימלי (יגדיל את הקצב), השקול למומנט שני מנורמל מינימלי. ידוע ש $\frac{1}{2\pi e}\le G(\Lambda_2)$ וקיימת סדרת סריגים עם מימד הולך וגדל כך ש:

$$G(\Lambda_2)\xrightarrow{n\to\infty}\frac{1}{2\pi e}$$

עבור בחירה כזו של הסריגים Λ_1 וΛ_2 ההפסד שואף לאפס, ונקבל:

$$Rate\xrightarrow{n\to\infty}\frac{1}{2}\log\left(\frac{P}{N}\right).$$

דוגמא:

עבור Λ_1 שהוא סריג טוב לאפנון ואילו Λ_2 סריג קובי (למשל קונסטלציית QAM ב2 מימדים או PAM במימד אחד) נקבל הפסד קיבול גדול מאפס:

$$loss=\frac{1}{2}\log\left(G(\Lambda_2)\cdot\mu(\Lambda_1,p_e)\right)=\frac{1}{2}\log\left(\frac{1}{12}\cdot 2\pi e\right)\cong 0.254bit$$

ההפסד הזה נובע מshaping של ספר הקוד. מכאן, הרווח הנובע מבחירת Λ_2 טוב לקוונטיזציה נקרא shaping gain.

השגת הקיבול בSNR כללי

הקצב שהתקבל על-ידי הסכמה שתוארה מקודם היה נמוך מהקיבול גם עבור הפסד שואף לאפס (בחירת סדרת סריגים אופטימלית):

$$Rate = \frac{1}{2}\log\left(\frac{P}{N}\right) - \frac{1}{2}\log\left(G\left(\Lambda_2\right)\cdot\mu\left(\Lambda_1, p_e\right)\right) \leq \frac{1}{2}\log\left(\frac{P}{N}\right) < \frac{1}{2}\log\left(1+\frac{P}{N}\right) = C_{AWGN}$$

אולם, עבור יחס אות לרעש גבוה ($P >> N$) מתקיים $\frac{1}{2}\log\left(\frac{P}{N}\right) \cong \frac{1}{2}\log\left(1+\frac{P}{N}\right)$

והקיבול מושג בקירוב עבור בחירה טובה (אסימפטוטית) של הסריגים, כפי שתואר קודם.

הסיבה העקרונית להפסד ב SNR כללי נובעת משיטת הפענוח הלא אופטימאלית . עבור רעש מספיק חזק המוציא את הווקטור הנקלט מחוץ לאזור וורונוי הבסיסי של הסריג הגס, הפענוח שתואר קודם שונה משמעותית מפענוח ה ML (האופטימאלי במובן מינימום הסתברות שגיאה). זאת מכיוון שספר הקוד חסום באזור וורונוי הבסיסי של הסריג הגס , ולכן פענוח ML מקרב את הוקטור שהתקבל לזה הקרוב ביותר בתוך אזור זה , אולם פעולת המודולו שבפענוח למעלה יוצרת מצב בו יכול להיבחר וקטור רחוק בהרבה . מכיוון שאנחנו מתעניינים רק במאורע שגיאה (ולא בגודל העיוות הנוצר במאורע כזה), ההבדל בהסתברות השגיאה בין שני המפענחים קיים רק עבור סימבולי הקצה . עבור סימבולים אלו הסתברות השגיאה של מפענח הML קטנה יותר, כפי שתואר קודם. בSNR גבוה (ולכן קצב גבוה) תא שריג גס מכיל הרבה מאוד תאים של שריג עדין ולכן התרומה של סימבולי הקצה להסתברות השגיאה זניחה . אולם, עבור SNR נמוך הסימבולים האלו מהווים חלק לא מבוטל מספר הקוד ולכן נצפה לירידה בקצב האפשרי בשימוש בסכמה הפשוטה המוצגת למעלה. כדי למנוע מצב זה , אפשר "לנרמל" את האות הנקלט כך שסיכוי היציאה מחוץ לתא וורונוי הבסיסי יהיה קטן . פעולה זו מתבצעת ע"י סינון ווינר של האות ששודר מתוך האות שנקלט.

תזכורת: סינון וינר (עבור מ"א סקלרים)

רוצים לשערך את X מתוך $Y = X + Z$ כאשר הפילוג שלהם נתון. עבור משתנים גאוסים במשותף משערך הMMSE זהה למשערך הליניארי האופטימאלי ונתון ע"י (עבור תוחלות 0):

$\hat{X}^{MMSE} = \alpha Y$ כאשר הקבוע α נבחר כך ששגיאת השערוך הריבועית הממוצעת מינימלית.

$\alpha_{wiener} = \frac{\sigma_X^2}{\sigma_X^2 + \sigma_Z^2}$ ואז השגיאה היא: $MMSE = \frac{\sigma_X^2\sigma_Z^2}{\sigma_X^2 + \sigma_Z^2} = \frac{1}{\frac{1}{\sigma_X^2} + \frac{1}{\sigma_Z^2}}$

קל לראות ש $MMSE \leq \sigma_Z^2$ מתכונות הממוצע ההרמוני, ובנוסף שעבור $SNR = \frac{\sigma_X^2}{\sigma_Z^2} \to \infty$

התאמת הסכמה לSNR כללי

ספר הקוד לא משתנה, אלא רק המקלט.

מקלט: במקום להשתמש בווקטור $\underline{y}$ הנקלט, המקלט משתמש בשערוך של $\underline{x}$ מתוך $\underline{y}$:

$$\underline{\tilde{y}} = \left(\underline{\hat{x}} - \underline{u}\right) \bmod \Lambda_2 = \left(\alpha \underline{y} - \underline{u}\right) \bmod \Lambda_2$$

וכלל ההחלטה הוא (כמו קודם): $\hat{\underline{\lambda}}_i = Q_{\Lambda_1}\left(\underline{\tilde{y}}\right) \bmod \Lambda_2$

למה: הערוץ השקול בין $\underline{\lambda}_i$ לבין $\underline{\tilde{y}}$ הוא: $\underline{\tilde{y}} = \left(\underline{\lambda}_i + \underline{Z}_{eff}\right) \bmod \Lambda_2$ כאשר הרעש האפקטיבי נתון ע"י:

$\underline{Z}_{eff} = \left((\alpha-1)\underline{x} + \alpha \underline{z}\right) \bmod \Lambda_2$ והוא בת"ס ב $\underline{\lambda}_i$.

הוכחה:

$$\underline{\tilde{y}} = \left[\alpha \underline{y} - \underline{u}\right] \bmod \Lambda_2 = \left[\alpha\left(\underline{x} + \underline{z}\right) - \underline{u}\right] \bmod \Lambda_2 = \left[\alpha \underline{x} + \alpha \underline{z} - \underline{u}\right] \bmod \Lambda_2 =$$

$$= \left[\underline{x} - \underline{u} + \left(\alpha - 1\right)\underline{x} + \alpha \underline{z}\right] \bmod \Lambda_2 = \left[\left(\lambda_i + \underline{u}\right) \bmod \Lambda_2 - \underline{u} + \left(\alpha - 1\right)\underline{x} + \alpha \underline{z}\right] \bmod \Lambda_2 =$$

$$= \left[\lambda_i + \underline{u} - \underline{u} + \left(\alpha - 1\right)\underline{x} + \alpha \underline{z}\right] \bmod \Lambda_2 = \left[\lambda_i + \underbrace{\left(\alpha - 1\right)\underline{x} + \alpha \underline{z}}_{Z_{eff}}\right] \bmod \Lambda_2$$

מכיוון ש $\underline{u} \sim Unif\left(\upsilon_{0,2}\right)$ אזי $\underline{x} \sim Unif\left(\upsilon_{0,2}\right)$ לכל λ_i ולכן $\underline{x}$ בת"ס ב λ_i. בנוסף $\underline{z}$ בת"ס ב λ_i, ולכן $\underline{Z}_{eff}$ בת"ס ב λ_i.

***הערה:** במימד סופי הרעש האפקטיבי $\underline{Z}_{eff}$ איננו גאוסי (כי $\underline{x}$ לא גאוסי) אולם כאשר המימד שואף לאינסוף $\underline{x}$ שואף לו"א גאוסי (במובן דיברגנס), ולכן גם $\underline{Z}_{eff}$ שואף להיות גאוסי. לכן בגבול נקבל ערוץ אפקטיבי AWGN עם רעש $\underline{Z}_{eff}$. יש לציין שהרעש האפקטיבי איננו חסר זיכרון, מכיוון שרכיבי $\underline{x}$ תלויים לכל בחירה של Λ_2 שאיננו ריבועי. עבור שריג חד-מימדי הרעש האפקטיבי ח"ז, וגם בגבול כאשר המימד שואף לאינסוף רכיבי $\underline{x}$ שואפים להיות מפולגים גאוסית iid, ולכן $\underline{Z}_{eff}$ שואף להיות ח"ז.*

עבור $\alpha = \alpha_{wiener}$ מתקבל:

$$Var\left(\underline{Z}_{eff}\right) = \frac{P \cdot N}{P + N} < P, N$$

קצב: אם נציב את וריאנס הרעש האפקטיבי במקום וריאנס הרעש האמיתי בפיתוח לקצב נקבל:

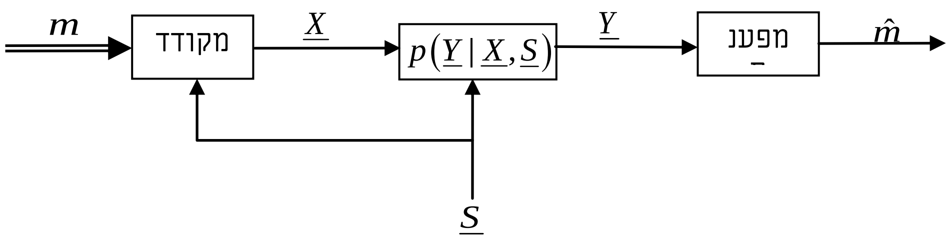
$$Rate = \underbrace{\frac{1}{2}\log\left(1 + \frac{P}{N}\right)}_{C_{AWGN}} - \underbrace{\frac{1}{2}\log\left(G\left(\Lambda_2\right) \cdot \mu\left(\Lambda_1, p_e\right)\right)}_{\text{Capacity Loss}}$$

כעת עבור בחירת סדרת סריגים מתאימה נקבל $Rate \xrightarrow{n \to \infty} C_{AWGN}$.

הערה חשובה: *כדי להראות שאכן השגנו את הקיבול , יש גם להראות שסדרת המקודדים הנ"ל (סדרת הסריגים) משיגה שגיאה הולכת ל 0 ולא רק קצב ששואף לקיבול . אולם, יש לשים לב שהבנייה למעלה נכונה לכל הסתברות שגיאה קטנה כרצוננו . לכל Pe נתון, אפשר למצוא סדרת סריגים* $\left\{\Lambda_1^{(n)},\Lambda_2^{(n)}\right\}_{n=1}^{\infty}$ *כך ש* $Rate \xrightarrow{n\to\infty} C_{AWGN}$. *לכן, ניתן למצוא סדרת סריגים כך שגם* $Rate \xrightarrow{n\to\infty} C_{AWGN}$ *וגם* $Pe \xrightarrow{n\to\infty} 0$.

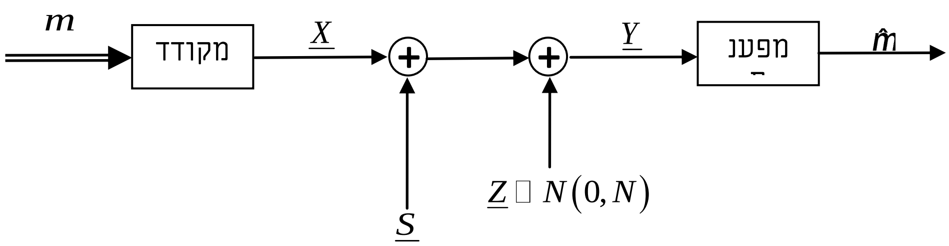
ערוץ עם אינפורמצית צד – המקרה הגאוסי

הבעייה הכללית של ערוץ עם אינפורמציית צד הידועה במקלט:



איור 8: ערוץ עם אינפורמציית צד הידועה במקלט.

במקרה הגאוסי הסכמה מכונה "Dirty Paper Channel":



איור 9: Dirty Paper Channel.

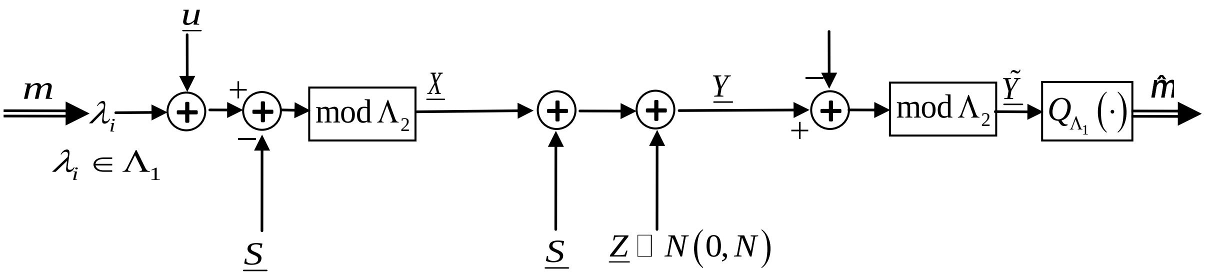
אם לא הייתה מגבלת הספק כניסה לערוץ , המשדר היה יכול פשוט לשדר $\underline{X}=\underline{x}_i-\underline{S}$, כאשר $\underline{x}_i$ היא מילת קוד מתוך ספר קוד טוב לערוץ AWGN. אולם, יתכן שחיסור זה יצור מצב בו $\frac{1}{n}\mathrm{E}\left\{\left\|\underline{X}\right\|^2\right\}>P$, מה שמפר את מגבל הספק הכניסה. הפתרון לבעיה זו הוא, בדומה לערוץ AWGN "רגיל", פעולת מודולו שמונעת שידור הספק ממוצע גדול מידי . למעשה, נראה שאין שום בזבוז הספק על קיזוז ההפרעה.

פתרון ע"י קוד וורונוי

כמו בהשגת הקיבול של ערוץ AWGN ללא הפרעה, סכמת הקידוד והפענוח מתבססת על שני סריגים מקוננים $\Lambda_2\subset\Lambda_1$. כמו קודם, Λ_1 צריך להיות טוב לאפנון ואילו Λ_1 צריך להיות טוב לקוונטיזציה.

ראשית נניח SNR גבוה ונתבונן בסכמת השידור הבאה:

$\underline{u}$



איור 10: סכמת הקידוד/פענוח לערוץ Dirty Paper Channel עבור SNR גבוה.

כמו קודם , גם כאן יש לבחור את הסריג הגס כך ש $\sigma_{\Lambda_2}^2 = P$ על מנת שתתקיים מגבלת ההספק.

בכניסה לקוונטייזר (מבצע את ההחלטה) במקלט מתקבל:

$$\tilde{\underline{Y}} = (\underline{Y} - \underline{u}) \bmod \Lambda_2 = (\underline{X} + \underline{S} + \underline{Z} - \underline{u}) \bmod \Lambda_2 = \left((\underline{\lambda}_i + \underline{u} - \underline{S}) \bmod \Lambda_2 + \underline{S} + \underline{Z} - \underline{u} \right) \bmod \Lambda_2 =$$

$$\overset{(a)}{=} \left(\underline{\lambda}_i + \cancel{\underline{u}} - \cancel{\underline{S}} + \cancel{\underline{S}} + \underline{Z} - \cancel{\underline{u}} \right) \bmod \Lambda_2 = (\underline{\lambda}_i + \underline{Z}) \bmod \Lambda_2$$

כאשר ב(a) השתמשנו בחוק הפילוג לפעולת המודולו.

כלומר, קיבלנו ערוץ שקול:

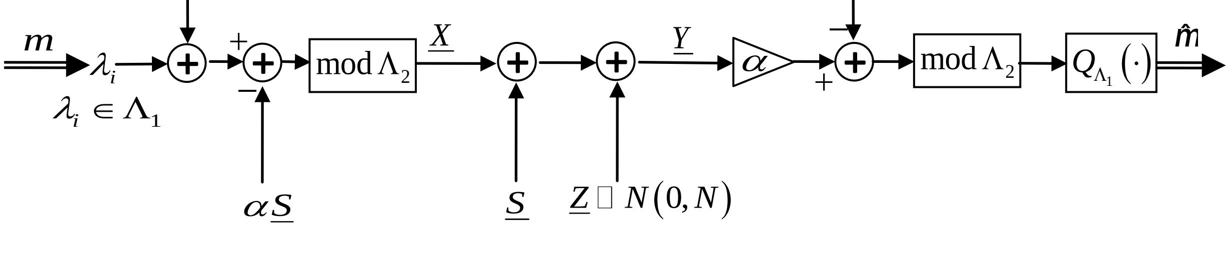
$$\tilde{\underline{Y}} = (\underline{\lambda}_i + \underline{Z}) \bmod \Lambda_2$$

גם בערוץ AWGN ללא הפרעה מתקבל בדיוק אותו קשר בין $\underline{\lambda}_i$ לבין $\tilde{\underline{Y}}$ (ע"י שימוש בחוק הפילוג כמו כאן), ולכן שני הערוצים האלו יתנו אותם ביצועים עבור סכמת הקידוד הנ"ל, כאשר משתמשים באותם סריגים. לכן, כמו קודם עבור SNR גבוה נקבל:

$$Rate = \underbrace{\frac{1}{2}\log\left(\frac{P}{N}\right)}_{C_{AWGN}\ \text{at high SNR}} - \underbrace{\frac{1}{2}\log\left(G(\Lambda_2)\cdot\mu(\Lambda_1, p_e)\right)}_{\text{Capacity Loss}}$$

התאמת הסכמה לSNR כללי

עבור SNR כללי סכמת הקידוד והפענוח נראית באופן הבא:



איור 11: סכמת הקידוד/פענוח לערוץ Dirty Paper Channel עבור SNR כללי.

האות המשודר הוא: $\underline{X} = (\underline{\lambda}_i + \underline{u} - \alpha\underline{S}) \bmod \Lambda_2$

בכניסה לקוונטייזר (מבצע את ההחלטה) במקלט מתקבל:

$$\tilde{\underline{Y}} = \left(\alpha\underline{Y} - \underline{u}\right)\bmod\Lambda_2 = \left(\alpha\left(\underline{X}+\underline{S}+\underline{Z}\right)-\underline{u}\right)\bmod\Lambda_2 = \left(\left(\alpha-1\right)\underline{X}+\underline{X}+\alpha\underline{S}+\alpha\underline{Z}-\underline{u}\right)\bmod\Lambda_2 =$$
$$= \left(\left(\alpha-1\right)\underline{X}+\left(\underline{\lambda}_i+\underline{u}-\alpha\underline{S}\right)\bmod\Lambda_2+\alpha\underline{S}+\alpha\underline{Z}-\underline{u}\right)\bmod\Lambda_2 =$$
$$= \left(\left(\alpha-1\right)\underline{X}+\underline{\lambda}_i+\underline{u}-\alpha\underline{S}+\alpha\underline{S}+\alpha\underline{Z}-\underline{u}\right)\bmod\Lambda_2 = \left(\underline{\lambda}_i+\left(\alpha-1\right)\underline{X}+\alpha\underline{Z}\right)\bmod\Lambda_2$$

אם נגדיר את הרעש האפקטיבי להיות $\underline{Z}_{eff} = \left((\alpha-1)\underline{X}+\alpha\underline{Z}\right)\bmod\Lambda_2$ אז הערוץ השקול הוא:

$$\tilde{\underline{Y}} = \left(\underline{\lambda}_i+\underline{Z}_{eff}\right)\bmod\Lambda_2$$

כאשר מכיוון ש $\underline{u} \sim Unif\left(\upsilon_{0,2}\right)$ ובגלל פעולת המודולו במשדר נקבל שגם $\underline{X} \sim Unif\left(\upsilon_{0,2}\right)$.

מכאן, ש $\underline{\lambda}_i$ בת"ס ב $\underline{Z}_{eff}$, וגם אסימפטוטית $\underline{Z}_{eff}$ שואף להיות גאוסי . עבור $\alpha = \alpha_{wiener}$

נקבל $Var\left(\underline{Z}_{eff}\right) = \frac{P\cdot N}{P+N} < P, N$, ולכן בסה"כ גם בSNR כללי קיבלנו ערוץ שקול זהה לזה שהתקבל עבור ערוץ AWGN. מכאן, שהקצב של הסכמה הנ"ל הוא:

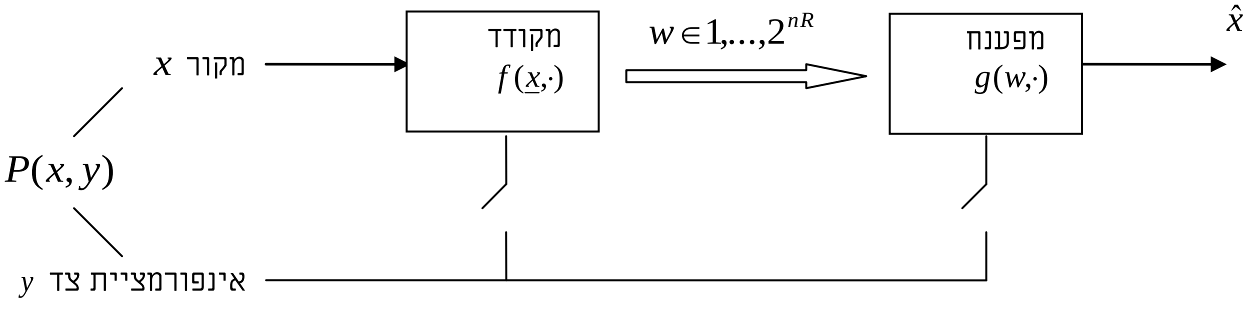
$$Rate = \underbrace{\frac{1}{2}\log\left(1+\frac{P}{N}\right)}_{C_{AWGN}} - \underbrace{\frac{1}{2}\log\left(G\left(\Lambda_2\right)\cdot\mu\left(\Lambda_1, p_e\right)\right)}_{\text{Capacity Loss}}$$

וקצב זה מושג לכל הסתברות שגיאה קטנה כרצוננו (כפי שהוסבר קודם).

הרצאה מס' 8

קידוד מקור עם אינפורמציית צד

סוכם ע"י רונן דר



מדד עיוות

1. $d(x,\hat{x})$ - למשל $(x-\hat{x})^2$.
2. $d(x,\hat{x},y)$ - למשל $y\cdot(x-\hat{x})^2$.

במקרה ש-y ידוע אך ורק במפענח אזי:

הזוג (R,D) הינו בר השגה אם קיימת מערכת $w=f(x)$, $\hat{x}=g(w,y)$ כך שמתקיים $\frac{1}{n}E\sum_{i=1}^{n}d(x_i,\hat{x}_i,y_i)\le D$. הקצב R המינימאלי שהוא בר השגה עם עיוות D.

מצבי מתגים אפשריים

1. A, B פתוחים

$$R_{NO-SI}(D)=R_x(D)=\min_{\begin{cases}P(\hat{x}|x)\\ Ed(x,\hat{x})\le D\end{cases}} I(x;\hat{x})$$

2. A, B סגורים

$$R_{SI@Both}(D)=R_{x|y}(D)=\min_{\begin{cases}P(\hat{x}|x,y)\\ Ed(x,\hat{x},y)\le D\end{cases}} I(x;\hat{x}\mid y)\equiv\sum_{y}P(Y=y)\cdot I(x;\hat{x}\mid y)$$

3. A סגור, B פתוח

פונקצית קצב העיוות אינה תלויה ב- y

$$R_{SI@Enc}(D) = \min_{\begin{cases} P(\hat{x}|x,y) \\ Ed(x,\hat{x})\le D \end{cases}} I(x,y;\hat{x}) = \min_{\begin{cases} P(\hat{x}|x,y) \\ Ed(x,\hat{x})\le D \end{cases}} I(x;\hat{x}) = R_{NO_SI}(D)$$

* ניתן להוכיח גם עבור קוונטייזר ממימד סופי.

פונקצית קצב העיוות תלויה ב- y:

$$R_{SI@Enc}(D) = \min_{\begin{cases} P(\hat{x}|x,y) \\ Ed(x,\hat{x},y)\le D \end{cases}} I(x,y;\hat{x})$$

4. A פתוח, B סגור (Wyner-Ziv 1976)

$$R_{SI@Dec}(D) = \min_{\begin{cases} y\leftrightarrow x\leftrightarrow u \\ P(u|x) \\ Ed(x,\underbrace{g(u,y)}_{\hat{x}})\le D \end{cases}} \min_{u} \min_{g(\cdot)} I(x;u\mid y) \equiv I(x;u) - I(y;u) \equiv H(u\mid y) - H(u\mid x)$$

- x,y,u שלשה מרקובית:

$$y \leftrightarrow x \leftrightarrow u$$
$$P(y,x,u) = P(y)\cdot P(x\mid y)\cdot P(u\mid x)$$

- u משתנה עזר שלא קיים בבעיה המקורית:

$$|u| \le |\chi| + 1$$

דוגמא למקרה 3 עם מדד עיוות התלוי באינפורמציית הצד

$x \sim unif(0,1,\ldots,q-1)$, y בינארי Bernoulli(p) ובת"ס ב-x.

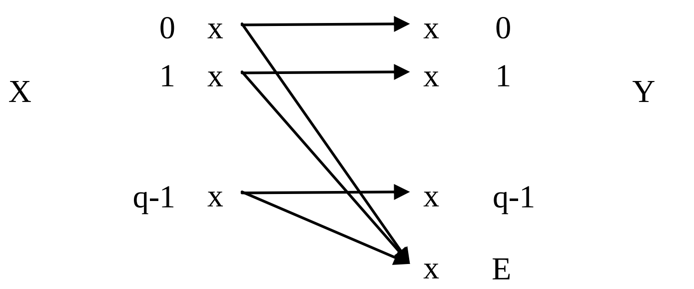
$$d(x,\hat{x},y) = \begin{cases} 1, x\ne\hat{x}, y=1 \\ 0, x=\hat{x}, y=1 \\ 0, y=0 \end{cases}$$

ו. פורמלית:

$$R_{SI@Enc}(D=0) = \min_{\begin{cases} P(\hat{x}|x,y) \\ Ed(x,\hat{x},y)=0 \end{cases}} I(x,y;\hat{x})$$

נציין כי ביטוי זה קשה לחישוב.

ז. ע״י שימוש בקוד לתיקון שגיאות:



- ״קוד C לתיקון e מחיקות מתוך n״ – אם לכל מילת קוד ולכל תבנית (pattern) של e מחיקות קיימת מילת קוד אחת ויחידה שמתלכדת עם $n-e$ הסימבולים שלא נמחקו.
  תיקון מחיקות $\Leftrightarrow$ אינטרפולציה של אות מוגבל סרט מתוך ״מספיק דגימות״:
- ברור שגודל הקוד חסום ע״י $|C| \le q^{n-e}$.
- נשים לב שאם אי-השיוויון חזק, אזי לא כל צירוף של $n-e$ סימבולים ש״עברו בשלום״ הוא אפשרי.
- ״קוד מושלם״ (MDS – Maximum Distance Separable) אם $|C| = q^{n-e}$, כלומר לכל צירוף של $n-e$ סימבולים לא מחוקים יש מילת קוד יחידה שמשלימה אותם.
- אם הקוד C ליניארי אזי כל קוסט שלו הוא קוד מושלם לתיקון e מחיקות.

מקודד מקבל:

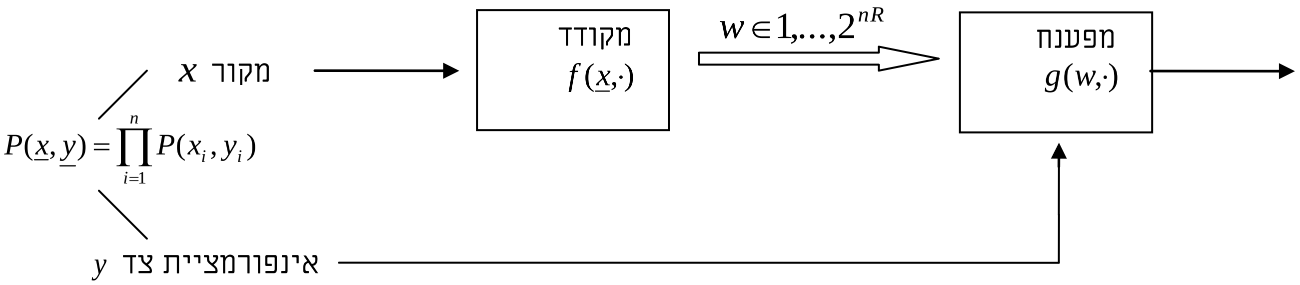
$$\underline{x} = x_1, x_2, \ldots, x_n$$

$$\underline{y} = 1,1,0,1,0,\ldots,1$$, 0- don't care

המקודד מוחק את e הנקודות שבהן y=0, מוצא מילת קוד שתואמת ל- $n-e$ הסימבולים הנותרים ומשדר אינדקס שמגדיר את מילת הקוד (משדר $n-e$ סימבולים היות ואנו מניחים קוד מושלם). נקבל:

$$R_{SI@Enc}(D) = R_{SI@Both}(D) = \frac{1}{n}(n-e)\log(q)$$

בעיית Wyner-Ziv – קידוד מקור עם עיוות עם אינפורמציית צד במפענח



משפט WZ

$$R^{WZ}_{X|Y}(D)=\min_{\substack{u \\ \left\{\begin{array}{l} u\leftrightarrow x\leftrightarrow y \\ Ed(x,\varphi(u,y))\le D\end{array}\right.}}\min_{\varphi} I(x;u\mid y)=I(x;u)-I(u;y)=H(u\mid y)-H(u\mid x)$$

*

$$I(x;u\mid y)=H(u\mid y)-H(u\mid x,y)=$$
$$=(H(u)-H(u\mid x))-(H(u)-H(u\mid y))=I(x;u)-I(u;y)$$

כאשר בשוויון השני השתמשנו בעובדה ש- u,x,y שלשה מרקובית.

* עבור מדד עיוות תלוי SI - $Ed(x,\varphi(u,y),y)\le D$.

לפני שנוכיח את משפט WZ (ביטוי "אות בודדת") ניתן משפט קידוד ווקטורי:

$$n\cdot R_n(D)=\min_{\substack{w=f(\underline{x}) \\ \left\{\frac{1}{n}E\sum_{i=1}^{n}d(x_i,g_i(\underline{y},w))\le D\right.}}\min_{g(\cdot)} I(\underline{x};w)\cong\min_{w=f(\underline{x})}\min_{g(\cdot)} I(\underline{x};w\mid\underline{y})$$

$$\Downarrow$$

$$R_{x|y}{}^{WZ}(D)=\inf_{n}\ R_n(D)$$

מדוע נכון?

$$n\cdot R=\log(|w|)\overset{(a)}{\ge}H(\underline{w})\overset{(b)}{\ge}I(\underline{x};w)\overset{(c)}{\ge}I(\underline{x};w\mid\underline{y})$$

(a) שיוויון כאשר w מתפלג אחיד על $1,\dots,2^{nR}$.

(b) שיוויון כאשר w=f(x) , פונקציה דטרמיניסטית של $\underline{x}$.

(c) אינפורמציה הדדית קמורה. שיוויון כאשר $\underline{y}$ בת"ס ב-w (אף פעם לא מתקיים בדיוק, אך מתורת Slepian wolf ידוע כי ניתן להתקרב לשוויון כאשר מימד הקוד שואף לאינסוף).

הוכחת החלק ההפוך

נשים לב ש- $w,\underline{x},\underline{y}$ שרשרת מרקובית וכן נגדיר $u_i \equiv (w, y_1^{i-1}, y_{i+1}^{n})$. נשים לב כי מתקיים:

$$P(y_i, x_i, u_i) = P(y_i, x_i, w, y_1^{i-1}, y_{i+1}^{i-1}) = P(y_i, x_i)\cdot P(w, y_1^{i-1}, y_{i+1}^{i-1} \mid y_i, x_i) =$$
$$= P(y_i, x_i)\cdot P(w, y_1^{i-1}, y_{i+1}^{i-1} \mid x_i) = P(y_i, x_i)\cdot P(u_i \mid x_i)$$

כלומר, $u_i \leftrightarrow x_i \leftrightarrow y_i$ שרשרת מרקובית.
נבחן את קצב קידוד המקור:

$$n\cdot R \overset{(a)}{\ge} I(\underline{x};w\mid \underline{y}) \overset{(b)}{=} \sum_{i=1}^{n} I(x_i;w\mid \underline{y},x_1^{i-1}) \overset{(c)}{=} \sum_{i=1}^{n} H(x_i\mid \underline{y},x_1^{i-1}) - H(x_i\mid \underline{y},x_1^{i-1},w) \overset{(d)}{=}$$
$$\overset{(d)}{=} \sum_{i=1}^{n} H(x_i\mid y_i) - H(x_i\mid \underline{y},x_1^{i-1},w) \overset{(e)}{\ge} \sum_{i=1}^{n} H(x_i\mid y_i) - H(x_i\mid \underline{y},w) \overset{(f)}{=}$$
$$\overset{(f)}{=} \sum_{i=1}^{n} H(x_i\mid y_i) - H(x_i\mid u_i,y_i) = \sum_{i=1}^{n} I(x_i;u_i\mid y_i) \overset{(g)}{\ge}$$
$$\overset{(g)}{\ge} n\cdot \frac{1}{n}\sum_{i=1}^{n} R_{x|y}^{WZ}(D_i) \overset{(h)}{\ge} n\cdot R_{x|y}^{WZ}\Big(\frac{1}{n}\sum_{i=1}^{n} D_i\Big) \overset{(i)}{\ge} n\cdot R_{x|y}^{WZ}(D)$$

(a) ראינו בעמוד הקודם.
(b) כלל השרשרת.
(c) פירוק אינפורמציה הדדית להפרש אנטרופיה.
(d) $P(\underline{x},\underline{y})$ חסר זיכרון.
(e) התניה מקטינה אנטרופיה.
(f) $u_i \equiv (w, y_1^{i-1}, y_{i+1}^{n})$.
(g) $R_{x|y}^{WZ}$ מוגדרת כמינימום על פני כל הזוגות $g(\cdot),u$.
נגדיר $D_i \equiv \mathrm{E}d(x_i,\hat{x}_i)$ כאשר $\hat{x}_i = g(w,\underline{y}) \equiv g(u_i,y_i)$.
(h) אי-שיוויון יאנסן (פונקצית WZ קמורה).
(i) תנאי העיוות הכולל - $\frac{1}{n}\sum_{i=1}^{n} D_i \le D$.

הוכחת המשפט הישר

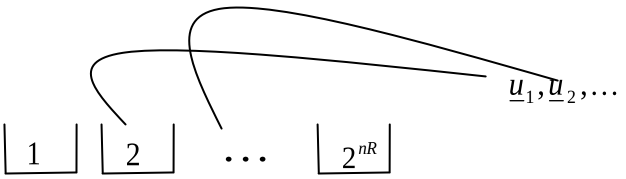
בניית קוד אקראי עם "random binning".

1) בניית קוד (offline):

1.1. נבחר פילוג $P(u|x)$ ונניח קשר מרקובי $u \leftrightarrow x \leftrightarrow y$. נבחר פונקצית שיחזור $\hat{x} = g(u,y)$.

1.2. נגריל מתוך $P(\underline{u}) \sim iid$ 2^{nR1} מילות קוד "וירטואליות" $\underline{u}$ כך ש-$R_1 > I(x;u)$. C_1 ספר הקוד.

1.3. נפזר את 2^{nR1} ה-$\underline{u}$-ים בספר הקוד C_1 בין 2^{nR} תאים בהסתברות אחידה ונדאג ש-$R_1 < R + I(y;u)$.



נשים לב שאם $R > I(x;u) - I(y;u)$ אזי ניתן למצוא R_1 שמקיים: $I(y;u) + R > R_1 > I(x;u)$.

1.4. נעביר את תחולת התאים לידיעת המקודד והמפענח.

* הערה: מהגדרת פונקצית WZ – אם $D \equiv \mathrm{E}d(x, g(u,y))$ אזי $I(x;u) - I(u;y) \geq R^{WZ}_{x|y}(D)$.

2) קידוד:

2.1. בהינתן ווקטור המקור $\underline{x}$, בחר $\varepsilon > 0$ ומצא $\underline{u} \in C_1$ שאופייני במשותף עם $\underline{x}$ לפי $P(u|x)$ (כלומר, $(\underline{x},\underline{u}) \in A^{(n)}_{\varepsilon}(x,u)$).

2.2. שדר את האינדקס j של התא שמכיל את $\underline{u}$. אם לא מצאנו נכריז שגיאת קידוד.

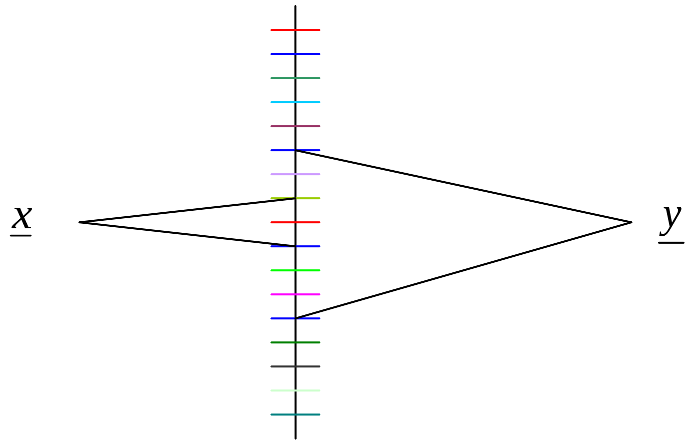
3) פיענוח:

בהינתן אינפורמציית הצד $\underline{y}$ ו-j, מצא בתא ה-j וקטור $\underline{\hat{u}}$ שאופייני במשותף עם $\underline{y}$ לפי $P(y,u)$ - $(\underline{y},\underline{\hat{u}}) \in A^{(n)}_{\varepsilon}(y,u)$. נשים לב כי $P(y,u) = \sum_x P(u|x) \cdot P(y|x) \cdot P(x)$.

אם לא מצאנו $\underline{u}$ יחיד נכריז שגיאת פיענוח.

אם הצלחנו אזי השיחזור יהיה - $\hat{x}_i = g(\hat{u}_i, y_i)$ $\forall i = 1,\ldots,n$.

$\underline{u} \in C_1$-ים



צבע – מספר תא של $\underline{u}$ בספר הקוד.

תחום במשולש – כל ה-$\underline{u}$-ים שאופייניים במשותף עם $\underline{x}$ או $\underline{y}$.

גודל התחום של $\underline{y}$ - $2^{nH(u|y)}$.

גודל התחום של $\underline{x}$ - $2^{nH(u|x)}$.

אם אין $\underline{u}$ צבוע בתחום של $\underline{x}$ - שגיאת קידוד.

אם $\underline{u}$ האמיתי אינו בתחום של $\underline{y}$ - שגיאת פיענוח מסוג I.

אם קיימים שניים או יותר $\underline{u}$ מאותו צבע בתחום של $\underline{y}$ - שגיאת פיענוח מסוג II.

4) ניתוח מאורעות השגיאה:

- שגיאת קידוד – לא נמצא $\underline{u}$ אופייני עם $\underline{x}$.
  הסיכוי שמילת קוד אחת תהיה אופיינית עם $\underline{x}$ ("סיכוי התחזות") - $\Pr \doteq 2^{-nI(x;u)}$.
  $R_1 > I(x;u) \Leftarrow$ עפ"י אכספוננט ספ הצלחה, תהיה התחזות בהסתברות שואפת לאחד (כאשר n שואף לאינסוף).
- שגיאת פיענוח I - $\underline{u}$ האמיתי איננו אופייני עם $\underline{y}$.

Markov Lemmma

אם $(\underline{x},\underline{y}) \in A_\varepsilon^{(n)*}(x,y)$ (אופייניות חזקה) ואם הסדרה $\underline{z}$ נוצרת מתוך $\underline{y}$ דרך ערוץ חסר זיכרון $P(y|z)$ אזי $(\underline{x},\underline{z}) \in A_\varepsilon^{(n)*}(x,z)$ בהסתברות גבוהה כאשר $x \leftrightarrow y \leftrightarrow z$ שרשרת מרקוב.

$\underline{u}$ אופייני עם $\underline{x}$ וכן מתקיים $u \leftrightarrow x \leftrightarrow y$ ולכן לפי Markov Lemma, הסיכוי $\underline{u}$ האמיתי איננו אופייני עם $\underline{y}$ קטן מ-ε.

- שגיאת פיענוח II – קיים יותר מ-$\underline{u}$ אחד בתא j שאופייני במשותף עם $\underline{y}$.
  הסיכוי לשגיאה זו שקול להתחזות ביחס ל-$P(y,u)$:
  הסיכוי ש-$\underline{u}$ מוגרל "יתחזה" - $\Pr \doteq 2^{-nI(u;y)}$
  הסיכוי ש-$\underline{u}$ מוגרל ייפול בתא j - $\Pr = 2^{-nR}$.
  $\Leftarrow$ סה"כ הסיכוי ש-$\underline{u}$ מוגרל יהיה גם בתא j וגם אופייני עם $\underline{y}$ הוא - $\Pr = 2^{-n(I(u;y)+R)}$.

$R_1 < R + I(u;y)$ ולכן לפי אכספוננט ספ הצלחה, הסיכוי ש- $\underline{u}$ כלשהוא מתוך $(2^{nR_1}-1)$ האחרים יגרום לשגיאה, שואף לאפס (כאשר n שואף לאינסוף).

5) בדיקת קיום תנאי העיוות:

אם $\underline{u}$ אופייני עם $\underline{x}$ במובן החזק $\Leftarrow$ $\frac{1}{n}\sum_{i=1}^{n} d(x_i, g(u_i, y_i)) = \mathrm{E}d(x, g(u,y)) \pm \varepsilon$.

***הערה**: כל האופייניות המצוינות הינן אופייניות חזקות.

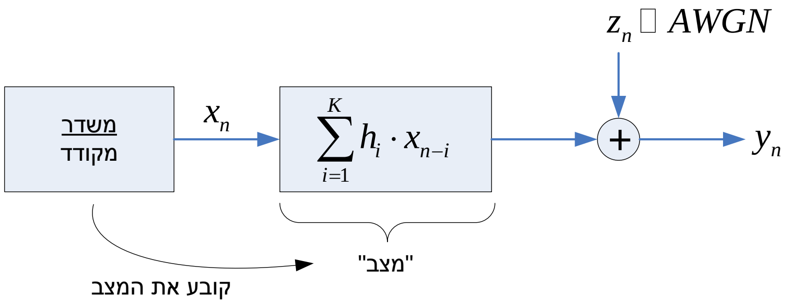
הרצאה מס' 9

ערוצים תלויי מצב עם אינפורמציית צד

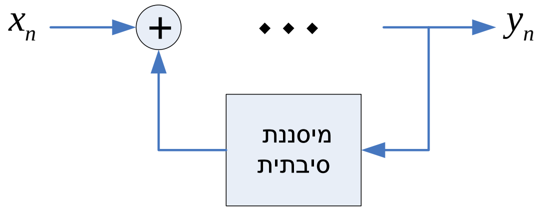
סוכם ע"י נועם טל

דוגמאות

0. <u>ערוץ</u>: (לא נדון במקרים אלו – מצבים לא מן הטבע, כלומר מצב הערוץ **תלוי סטטיסטית בהודעה המשודרת**)
   - ערוץ עם מצב תלוי כניסה (FIR):



   - ערוץ עם מצב תלוי מוצא (IIR):



1. <u>כתיבה על נייר מלוכלך</u>: (Writing on Dirty Paper - WDP)

$$Y = X + S + Z, \qquad Z \sim AWGN$$

המצב S (הפרעה) ידוע למקודד.

משתנים רציפים ← אילוץ כניסה – למשל $E\left[X^2\right] \le P$

Z בת"ס בזוג (X,S) (מניחים תמיד כזו אי-תלות).

תוצאות ב- WDP:

$$C_{SI@Enc} = C_{SI@Dec} = C_{SI@Both} = \frac{1}{2}\log\left(1 + \frac{P}{N}\right)$$

2. <u>ערוץ עם דעיכות</u>: (Fading Channel)

$$Y = S \cdot X + Z$$

S – הגבר משתנה בזמן - "דעיכה":
- slow fading - סדרת דעיכות קבועה לאורך בלוק (אורך הקוד) משתנה מבלוק לבלוק.
- fast fading - סדרת דעיכות משתנה מסימבול לסימבול.

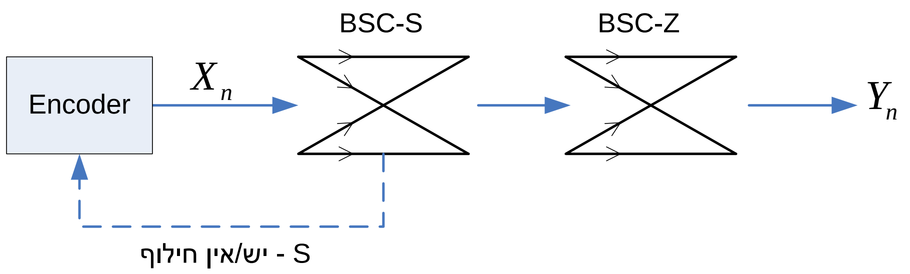
המשתנים רציפים.

3. <u>ערוץ אימפולסיבי</u>:

$$Y = X + S \cdot Z$$

S - קובע אם הרעש חזק או חלש. הרבה פעמים בינארי (רעש חזק/חלש).
<u>הערה</u>: אם S ידוע למקלט אז ערוץ דעיכות וערוץ אימפולסיבי הם שקולים (בהנחה שלא מחלקים ב- 0).

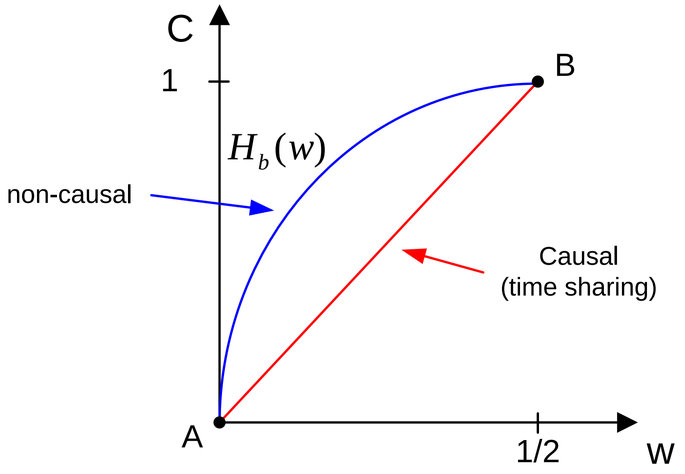
4. <u>WDP בינארי</u>:



$$Y_n = X_n \oplus S_n \oplus Z_n$$

תחת אילוץ כניסה ("הספק"): $\frac{1}{n} \cdot w_H(\underline{X}) \leq w$

תוצאות ל- WDP בינארי:
במקרה בו הערוץ השני לא קיים: $Z_n \equiv 0$ ו- $S_n \sim Bernoulli(1/2)$
הקיבול כתלות במגבלת ההספק נראה כך:



A - אין שידור אינפורמציה
B - S ידוע ואילוץ ה"הספק" מאפשר להפוך ביט השידור כאשר S=1.
יש הבדל בין המקרה הסיבתי בו רק המצב הנוכחי ידוע (והעבר), לבין המקרה הלא סיבתי בו יודעים גם את המצבים העתידיים.

5. <u>זיכרון עם תאים דפוקים</u>: (Memory with Defective Cells)

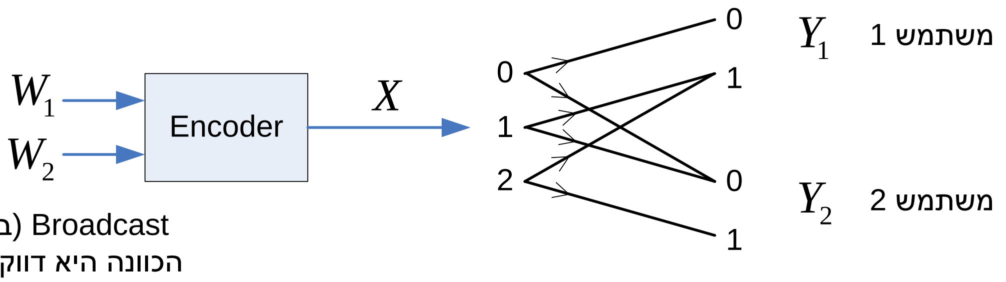
$$Y=\begin{cases} X, & S=\text{"}Normal\text{"} \\ 0, & S=\text{"}stuck@0\text{"} \\ 1, & S=\text{"}stuck@1\text{"} \end{cases}$$

מקודד יודע לכתוב ולקרוא ← כלומר יכול לסרוק את הזיכרון ולזהות תאים דפוקים.
מפענח יודע רק לקרוא ← כלומר מפענח לא יודע אילו תאים דפוקים.
אם שניהם היו יודעים אילו תאים דפוקים אז הקיבול במקרה הבינארי הוא:

$$C_{SI@Both}=\frac{\text{מס' תאים תקינים}}{\text{סה"כ גודל הזיכרון}}$$

ניתן להראות כי: $C_{SI@Enc}=C_{SI@Both}$

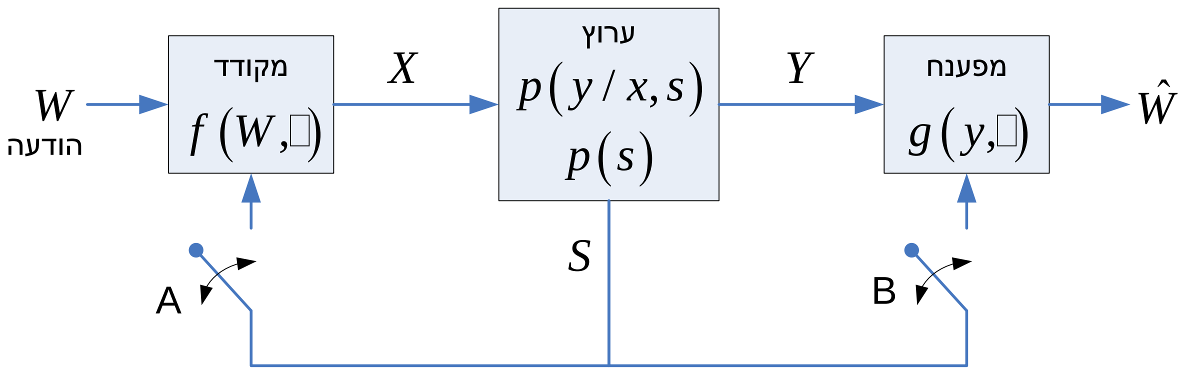
6. <u>ערוץ Blackwell</u>: (סוג של ערוץ הפצה B.C.C)



Broadcast (במקרה זה הכוונה היא דווקא להודעות פרטיות לכל משתמש)

ניתן לשדר למשל למשתמש 1 בקצב של $1_{bit/symbol}$.
שידור לשמתמש 1 מהווה "מצב" עבור משתמש 2 שידוע למשדר: X=0 ← stuck@0.

הגדרה פורמלית של המודל



כאשר W ו- S הם בת"ס.
(המצב S נובע מן הערוץ)

<u>SI@Tx</u>:
א. אינפורמציית צד ידועה באופן "לא סיבתי": [Gelfand, Pinsker 1980]
(זיכרונות [Koznitsov, Tsibokov 70's]
דפוקים)

$$x_i = f_i\left(W, S_1^n\right), \qquad i = 1, 2, \ldots n$$

ב. אינפורמציית צד ידועה סיבתית: [Shannon 1958]

$$x_i = f_i\left(W, S_1^i\right), \qquad i = 1, 2, \ldots n$$

אינפורמציית צד בשני הצדדים לעומת במקלט בלבד

$$C_{SI@Both}=\max_{p(x/s)} I\left(x;y/s\right)\equiv \max_{p(x/s)}\sum_{s'} p(s')\cdot I\left(x;y/s=s'\right)$$

$$C_{SI@Rx}=\max_{p(x)} I\left(x;y,s\right)=\max_{p(x)} I\left(x;s\right)+I\left(x;y/s\right)=\max_{p(x)} I\left(x;y/s\right)$$

כאשר השיוויון האחרון נובע מכך ש- S ו- X בת"ס.

יתקיים שיוויון $C_{SI@Both}=C_{SI@Rx}$ אם ורק אם הפילוג המגשים $p^*\left(x/s=s'\right)$ אינו תלוי במצב s' (למשל בערוץ DMC סימטרי ובהנחה שאין אילוץ בכניסה, p^* אחיד ללא תלות ברעש).

האם זיכרון במצב משפיע על קיבול $C_{SI@Rx}$ או $C_{SI@Both}$?

<u>הנחה</u>: בהינתן סדרת המצבים הערוץ הוא i.i.d, כלומר הערוץ חסר זיכרון באופן מותנה:

$$p\left(\underline{y}/\underline{x},\underline{s}\right)=\prod_{i=1}^{n} p\left(y_i/x_i,s_i\right)$$

או באופן שקול: $p\left(\underline{s},\underline{x},\underline{y}\right)=p\left(\underline{s}\right)\cdot p\left(\underline{x}\right)\cdot\prod_{i=1}^{n} p\left(y_i/x_i,s_i\right)$ (נתרכז

כרגע במקרה של $C_{SI@Rx}$, כלומר $p\left(\underline{x},\underline{s}\right)=p\left(\underline{s}\right)\cdot p\left(\underline{x}/\underline{s}\right)=p\left(\underline{s}\right)\cdot p\left(\underline{x}\right)$)

קיבול $C_{SI@Rx}$ עבור מצבים עם זיכרון (ערוץ חסר זיכרון באופן מותנה)

א. <u>קיבול</u>:

$$C_{SI@Rx}^{(n)}=\max_{p(\underline{X})}\frac{1}{n}\cdot I\left(\underline{X};\underline{Y}/\underline{S}\right)\underset{(a)}{=}\max_{p(\underline{X})}\frac{1}{n}\sum_{\underline{s}} p\left(\underline{s}\right)\cdot I\left(\underline{X};\underline{Y}/\underline{S}=\underline{s}\right)$$

$$\underset{(b)}{\le}\max_{p(\underline{X})}\frac{1}{n}\sum_{\underline{s}} p\left(\underline{s}\right)\cdot\sum_{i=1}^{n} I\left(X_i;Y_i/S_i=s_i\right)\underset{(c)}{=}\frac{1}{n}\sum_{\underline{s}} p\left(\underline{s}\right)\cdot\sum_{i=1}^{n} C_{s_i}\underset{(d)}{=}\sum_{s} p\left(s\right)\cdot C_s$$

(a) מהגדרת אינפורמציה הדדית מותנית.
(b) פירוק להפרש אנטרופיות:

$$H\left(\underline{Y}/\underline{S}=\underline{s}\right)-H\left(\underline{Y}/\underline{S}=\underline{s},\underline{X}\right)\le\sum H\left(Y_i/S_i=s_i\right)-\sum H\left(Y_i/S_i=s_i,X_i\right)$$

(c) הכנסת max לסכום הפנימי.
(d) החלפת סדר סכומים – למשל עבור i=1 (זהה לשאר ובסוף n מצטמצם):

$$\frac{1}{n}\sum_{\underline{s}} p\left(\underline{s}\right)\cdot C_{s_1} = \frac{1}{n}\sum_{s_1}\sum_{s_2}\ldots\sum_{s_n} p\left(s_1\right)\cdot p\left(s_2^n / s_1\right)\cdot C_{s_1} =$$

$$\frac{1}{n}\sum_{s_1} p\left(s_1\right)\cdot C_{s_1}\sum_{s_2}\ldots\sum_{s_n} p\left(s_2^n / s_1\right) = \frac{1}{n}\sum_{s_1} p\left(s_1\right)\cdot C_{s_1}$$

<u>מסקנה</u>: היות ו- (b) מושג בשיוויון ע"י פילוג מבוא חסר זיכרון: $p\left(\underline{x}\right)=\prod_{i=1}^{n} p\left(x_i\right)$, זיכרון במצבים איננו משפיע על הקיבול

<u>אינטואיציה</u>: בד"כ חשוב למקלט רק אם מצב הערוץ "רע" כרגע או "טוב" כרגע ולא חשובה ההיסטוריה (עבור בלוק ארוך אופייניות מבטיחה שאחוז המצבים הרעים/טובים יהיה בהתאם להסתברות **השולית** של המצב).

ב. <u>אקספוננט שגיאה</u>:

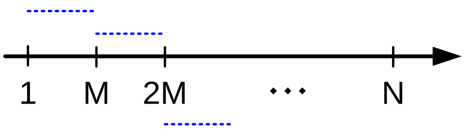
$$E\left(R\right)=\max_{p(x)}\max_{0\le\rho\le1}\left[E_0\left(\rho, p\left(x\right), p\left(y,s/x\right)\right)-\rho R\right]$$

כאשר הסתברות השגיאה מקיימת: $P_e \le e^{-N\cdot E(R)}$

בהנחה שאין למצבים זיכרון:

$$E_0\left(\rho\right)=-\log\left[\sum_s p\left(s\right)\sum_y\left(\sum_x p\left(x\right)\cdot p\left(y/x,s\right)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right]$$

נניח זיכרון-בלוק: המצב קבוע על פני M סימבולים ואז משתנה באופן בת"ס:



← לכל בלוק, האקספוננט מותנה במצב $s=s_0$ שקול:

$$M\cdot\left[E_0\left(\rho, p\left(x\right), p\left(y/x,s_0\right)\right)-\rho R\right]$$

← על פי הפיתוח הקודם:

$$E\left(R\right)=-\frac{1}{M}\log\left[\sum_{s_0} p\left(s_0\right)\cdot e^{-M\cdot E_0\left(\rho, p(x), p(y/x,s_0)\right)}\right]-\rho R$$

ניתן לראות שנוצרת כאן הדגשה של האקספוננט בערוצים רעים, וההדגשה משמעותית יותר כשרחוקים מהקיבול. $\left(\frac{1}{t}\log\left[\sum_i e^{\pm t\cdot x_i}\right]\xrightarrow{t\to\infty}\begin{cases}\max(x_i) & +\\ \min(x_i) & -\end{cases}\right)$

כלומר, כאשר M גדול אזי רחוק מהקיבול $\left(\rho \to 0\right)$ נוצרת הדגשת יתר של המצבים בהם האקספוננט נמוך: $\lim_{M\to\infty} E\left(R\right)=\min_s E\left(R, p\left(y/x,s\right)\right)$

<u>מסקנה</u>: יש השפעה של זיכרון במצבים על אקספוננט השגיאה

משפט קידוד לערוץ עם מצב ידוע לא סיבתית במשדר

$\underline{X} = f\left(W,\underline{S}\right)$ (תלות לא סיבתית)

$P_e = \Pr\left(\hat{W} \neq W\right) \quad \hat{W} = g\left(\underline{Y}\right)$

$C_{SI@Rx}$ = מקסימום על קצבים ברי השגה שמאפשרים $P_e \xrightarrow{n\to\infty} 0$)

<u>גלפנד פינסקר (1983) GP</u>:

$$C_{SI@Tx} = \max_{\substack{p(x,u/s) \\ u\leftrightarrow(x,s)\leftrightarrow y}} \left[I\left(u;y\right) - I\left(u;s\right)\right] =$$

$$\underset{\substack{\text{assuming} \\ \text{finite} \\ \text{alphabet}}}{=} \max_{\substack{p(x,u/s) \\ u\leftrightarrow(x,s)\leftrightarrow y}} \left[H\left(u/s\right) - H\left(u;y\right)\right]$$

כאשר מספיק לחפש u עם אלפבית בגודל: $|U| \le |X| + |S|$

<u>הערות</u>:

1. משתנה העזר u לא שייך לבעיה המקורית (אבל ניתן לחסום את גודל הא"ב שלו – אחרת אולי היתה בעיה לבצע מקסימיזציה אם תחום החיפוש אינו סופי).
2. מספיק לבצע מקסימיזציה על p(u/s) ו- x שתלוי דטרמיניסטית ב- u וב- s; כלומר קיימת פונקציית מיפוי $\varphi\left(u,s\right)$ כך ש: $p\left(x/u,s\right) = \begin{cases} 1 & x = \varphi\left(u,s\right) \\ 0 & o.w \end{cases}$
3. אולי arg(G.P)<0, כלומר עבור בחירת u לא טובה (u תלוי חזק מדי ב- s) ההפרש יכול להיות שלילי. אבל המקסימום תמיד יהיה אי-שלילי (אפשר להניח שתמיד ניקח ערכים חיוביים).
4. קיבול עם SI סיבתי: (Shannon 1958)

$$x = \varphi\left(\cdot,s\right), \quad \varphi: S \to X, \ |\varphi| = |X|^{|S|}$$

$$C_{SI@Tx}^{causal} = \max_{\varphi} \max_{\substack{p(u) \\ x=\varphi(u,s)}} \left[I\left(u;y\right)\right]$$

הקיבול הנ"ל שקול לקיבול GP עם אילוץ ש- u ו- s בת"ס.

הוכחת המשפט הישר

- נניח שבחרנו p(u/s) ו- $x = \varphi\left(u,s\right)$ (וש- arg(GP)>0). ניבנה קוד אקראי (random binning).
- <u>בנייה</u> (Offline)
  - ➢ נגריל קוד מורחב $C = \left\{\underline{u}\right\}$ בגודל 2^{nR_1} באופן i.i.d לפי p(u):

$\left(p\left(u\right) = \sum_s p\left(s\right)\cdot p\left(u/s\right)\right)$ נבחר (נראה בהמשך למה) $R_1 < I\left(u;y\right)$

  - ➢ נפזר את הוקטורים $\underline{u}$ בין 2^{nR} תאים באופן אחיד.

➢ ההודעה = תא.

- <u>מקודד</u>:

בהינתן W=i, אינפורמציית צד $\underline{s}$ ו- $\varepsilon > 0$:

➢ מצא סדרה $\underline{\tilde{u}}$ בתא i אופיינית (חזקה) במשותף עם $\underline{s}$ $\leftarrow \left(\underline{\tilde{u}}, \underline{s}\right) \in A_\varepsilon^{(n)*}\left(u, s\right)$

➢ נשדר $x_i = \varphi\left(\tilde{u}_i, s_i\right)$ $\quad i = 1, 2, \ldots, n$

➢ <u>שגיאה</u>: I. אם לא מצאנו $\underline{\tilde{u}}$ אופייני במשותף (חזק) עם $\underline{s}$ (מותר למצוא יותר מאחד!)

- <u>מפענח</u>: $g\left(\underline{y}\right)$

➢ מחפש בקוד המורחב C וקטור $\underline{\hat{u}}$ שאופייני במשותף עם $\underline{y}$. ההודעה $\hat{W}$ תהיה מספר התא אליו שייך $\underline{\hat{u}}$.

➢ <u>שגיאות</u>:

II. $\underline{y}$ לא אופיני עם אף $\underline{u}$ (ספציפית, לא אופייני עם $\underline{\tilde{u}}$ האמיתי)

III. יותר מ- $\underline{u}$ אופייני אחד (נהיה פסימיים למרות שנצדק אם שניהם באותו תא)

- <u>ניתוח מאורעות שגיאה</u>:

I. הסיכוי ש- $\underline{u}$ אקראי יהיה אופייני במשותף (חזק) עם $\underline{s}$ $\doteq 2^{-nI(u;s))}$

הסיכוי ש- $\underline{u}$ אקראי ייפול לתא i: $\doteq 2^{-nR}$

$\leftarrow \Pr\left(I\right) = 2^{-n\left[I(u;s)+R\right]} \leftarrow$ על פי אקספוננט סף הצלחה אם

$R_1 > I\left(u;s\right) + R$ אזי נמצא בתא i, $\underline{\tilde{u}}$ אופייני בהסתברות גבוהה.

II. הסיכוי ש- $\underline{\tilde{u}}$ האמיתי לא אופייני עם $\underline{y}$:

על פי Markov Lemma (מעבר דרך מתווך):

$$\left(\underline{\tilde{u}}, \underline{s}\right) \in A_\varepsilon^{(n)*} \longrightarrow \boxed{p\left(\underline{y} / \underline{x}, \underline{s}\right)} \longrightarrow \underline{y}$$

מתווך

אם $\left(\underline{\tilde{u}}, \underline{s}\right)$ אופייניים חזק אזי $\left(\underline{\tilde{u}}, \underline{s}, \underline{x}, \underline{y}\right)$ אופייניים ביחס לפילוג המרקובי המותנה.

$\leftarrow \Pr\left(II\right) < \varepsilon$

III. הסיכוי ש- $\underline{u}$ לא אמיתי יהיה אופייני עם $\underline{y}$ $\doteq 2^{-nI(u;y)}$ ("התחזות").

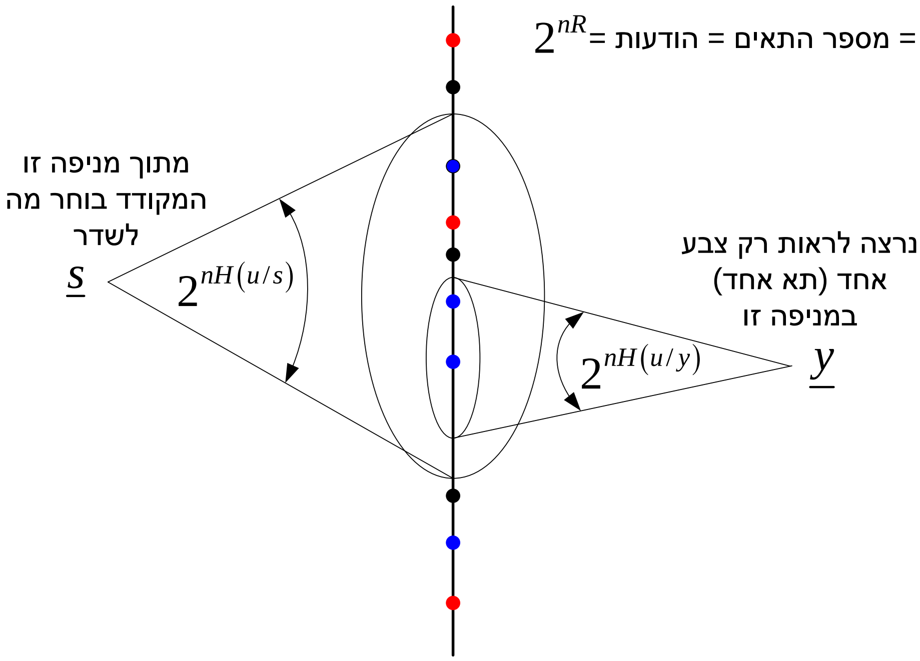
$\leftarrow$ אם $R_1 < I\left(u;y\right)$ אזי הסיכוי להתחזות שואף ל- 0.

I+II+III. אם $R < I\left(u;y\right) - I\left(u;s\right)$ אזי ניתן למצוא R_1 שמקיים:

$$I\left(u;s\right) + R < R_1 < I\left(u;y\right)$$

כך שכל מאורעות השגיאה הם בהסתברות שואפת ל- 0.

<u>הסבר גרפי להוכחה:</u>



<u>דוגמא</u>: פתרון לבעיית קוסטה (DPC)

$$y = x + s + z \qquad E\left[x^2\right] \le P,\quad z \sim N(0, N)$$

לפי פתרון GP: $u = \alpha \cdot s + \tilde{x}$

כאשר $\tilde{x}$ בת"ס ב- s ו-

$$x = \varphi(u, s) = u - \alpha \cdot s$$

$$\alpha = \frac{P}{P+N} = \alpha_{wiener} = \frac{SNR}{1+SNR}$$

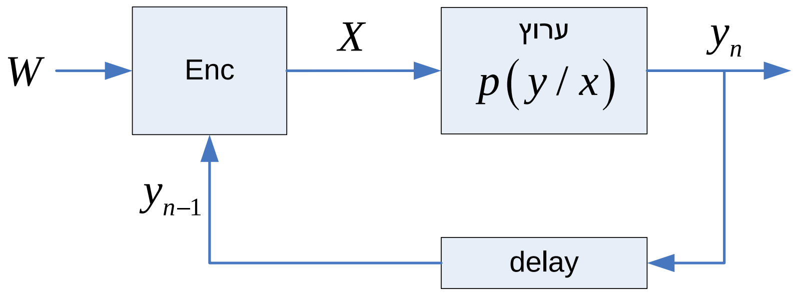
קישור לסריגים

תאים שקולים לסריג גס ← קוד מקור טוב (בעיית כיסוי).

אוסף מילות הקוד $\{\underline{u}\}$ שקול לסריג עדין ← קוד ערוץ טוב (בעיית אריזה).

קישור של בעיית SI@Tx הסיבתית לערוץ עם משוב

<u>משוב:</u>

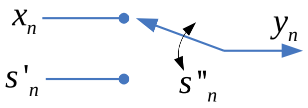


<u>הבדלים:</u> 1. ב- GP, S ו- W בת"ס, לעומת משוב - W תלוי ב- y_{n-1} .

2. ידיעת המצב לפני שידור מאפשרת השפעה על התנהגות הערוץ ברגע הנוכחי, בעוד שמשוב מאפשר (לפעמים) לתקן בדיעבד.

זיכרון עם תאים תקולים (Memory with Defective Cells)

נגדיר את המצב באופן הבא: $s=(s',s'')$ כאשר s" מסמל אם התא תקוע או לא ו- s' מייצג את הערך שנמצא בתא התקוע, כלומר:



$$y=\begin{cases} x, & s''=0\ (normal) \\ s', & s''=1\ (stuck) \end{cases}$$

הסיכוי לתא מקולקל = Pr(s"=1) = p

<u>פיתרון GP:</u>

$$u=y=\tilde{x}\cdot(1-s'')+s'\cdot s''$$

$$\tilde{x}\sim Unif(X)$$

$$x=\tilde{x}$$

בדיקת לגיטימיות של u: (קיום תנאי המרקוביות)

$u\leftrightarrow(x,s)\leftrightarrow y$ מתקיים היות והערוץ דטרמיניסטי בהינתן המצב:

$y=func(x,s)=func(x,s',s'')$ והקצב המתקבל:

$$I(u;y)-I(u;s)=H(u/s)-\underbrace{H(u/y)}_{0}=H(u/s',s'')=$$

$$=(1-p)\cdot\log|X|=C_{SI@Both}$$

פיתרון "מעשי" ע"י שימוש בקוד מושלם (MDS) לתיקון מחיקות

תזכורת: MDS יודע לתקן e מחיקות ← לכל תבנית (pattern) של n-e סימבולים לא מחוקים ישנה השלמה **אחת ורק אחת**.

← עבור קוד לינארי, ישנם q^e ($q\equiv|X|$) קוסטים, כל קוסט בגודל q^{n-e} הוא קוד תיקון מחיקות מושלם.

- עבור בעיית GP (זיכרון מקולקל) נתייחס לתאים המקולקלים כסימבולים **לא מחוקים** (n-e = np)
- הודעה מועברת ע"י בחירת קוסט: $q^{n(1-p)}=q^{e}=$ מספר הודעות.
- לכל תבנית של תאים מקולקלים ישנה השלמה אחת (ורק אחת) ולפיה בעצם בוחר המקודד את מילת הקוד בתוך הקוסט של ההודעה.

← מפענח יכול לזהות איזה קוסט שודר ללא שגיאה.

הרצאה מס' 10

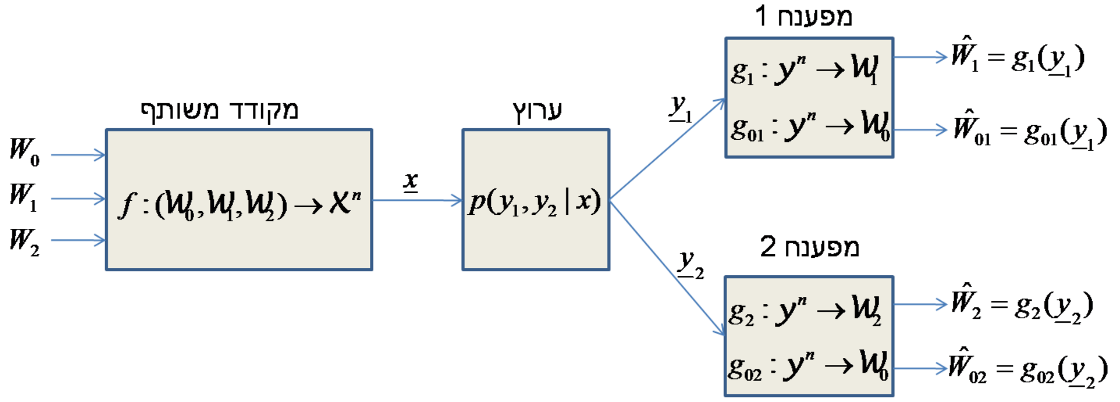
ערוץ הפצה (Broadcast Channel)

סוכם ע״י אבישי אנטמן

דוגמאות לערוצי .B.C

1. שידור רדיו \ טלוויזיה אנלוגי – הודעות ציבוריות
2. שידור יורד מתחנת בסיס סלולרית אל המכשירים הניידים - שידור הודעות פרטיות
3. router WiFi – הודעות פרטיות
4. מרכזיית כבלים – שידור מעורב של הודעות פרטיות וציבוריות

תרשים כללי של ערוץ .B.C



יש הודעות פרטיות W_1,W_2 והודעה משותפת W_0, שנבחרות מתוך הקבוצות הבאות:

$$W_0\in\{1,\ldots,2^{nR_0}\}$$
$$W_1\in\{1,\ldots,2^{nR_1}\}$$
$$W_2\in\{1,\ldots,2^{nR_2}\}$$

הסתברות שגיאה מוגדרת כך:

$$P_e=\Pr\{\hat{W}_1\neq W_1\bigcup\hat{W}_{01}\neq W_0\bigcup\hat{W}_2\neq W_2\bigcup\hat{W}_{02}\neq W_0\}$$

(מספיקה שגיאה של הודעה אחת בערוץ אחד, כדי שהדבר יחשב כאירוע שגיאה)

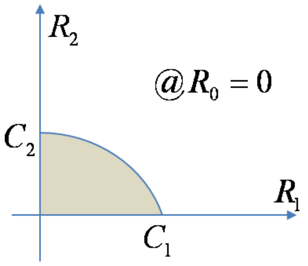
תחום קצבים בני-השגה – הגדרה אופרטיבית

שלישיית הקצבים (R_0,R_1,R_2) בת השגה אם קיימת סדרת מערכות $\left\{f^n,g_1^n,g_{01}^n,g_2^n,g_{02}^n\right\}$ בקצבים (R_0,R_1,R_2) כך ש $P_e\xrightarrow{n\to\infty}0$.

תחום הקיבול $\mathbf{C_{BC}}$ של ערוץ הוא סגור אוסף קצבים ברי השגה (קמור אינו נדרש בהגדרה אופרטיבית, ויכול להתקבל ע״י time-sharing בין פונקציות קידוד ופענוח שונות).

מקרים פרטיים:

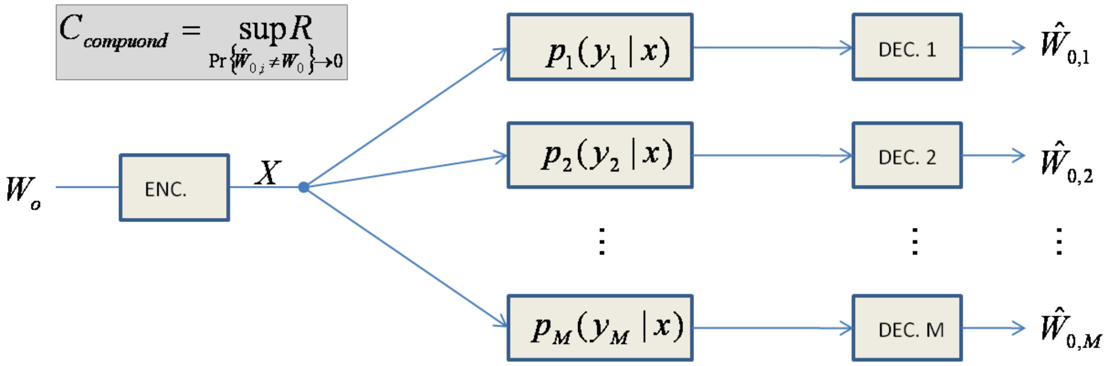
1. אין הודעה משותפת – סכמה של תחום הקיבול:



2. יש רק הודעה משותפת – ניתן לראות המקרה הזה גם כמודל 'ערוץ לא ידוע' \ 'משפחה של ערוצים' \ 'Compound Channel' (ערוץ עם פרמטר לא ידוע) – נדרשת העברת הודעה למקלט אחד כאשר הערוץ האמיתי יכול להיות אחד מבין קבוצה של ערוצים, והמקודד מעביר את ההודעה כך שהסתברות השגיאה בכל אחד מהערוצים תשאף ל-0. במקרה זה השאיפה היא למצוא פילוג כניסה שמביא למקסימום את האינפורמציה ההדדית בין הכניסה והמוצא בערוץ הכי גרוע עבור אותו פילוג.

$R_1 = R_2 = 0$ - רק הודעה ציבורית

$$C_{compound} = \sup_{\Pr\{\hat{W}_{0,i} \neq W_0\} \to 0} R$$

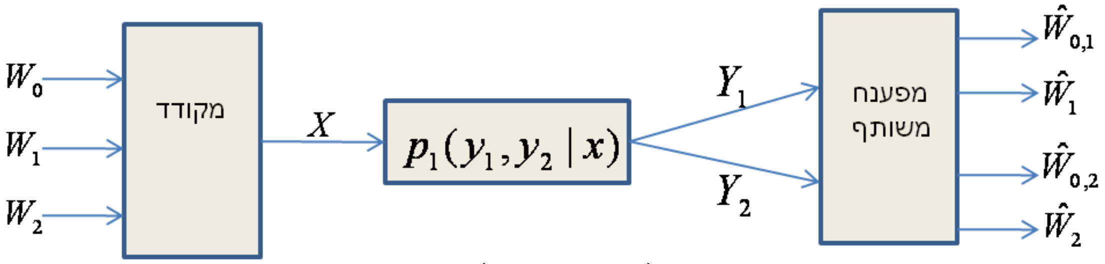


<u>משפט</u> תחום הקיבול $\mathbf{C_{BC}}$ תלויי רק בפילוג הערוצים השולי, ולא בתלות הסטטיסטית בין אותות המוצא, בהינתן אות הכניסה.

<u>הוכחה</u> הסתברות שגיאה קטנה מסכום הסתברויות השגיאה של כל ערוץ בנפרד, אם נשאיף כל הסתברות שגיאה נפרדת לאפס, בהכרח גם סכום ההסתברויות ישאף לאפס, יחד עם הסתברות השגיאה הכוללת.

$$\max_i \Pr(\hat{W}_i \neq W_i) \le P_e \le \sum_i \Pr(\hat{W}_i \neq W_i)$$

תרחיש יחוס - מקלט משותף (full receiver cooperation)



$$\mathbf{C}_{common} = \max\{R_0 + R_1 + R_2\} = \max_{p(x)} I(X;Y_1,Y_2) \quad \text{[P2P capacity]}$$

<u>הערה</u> $\mathbf{C}_{common}$ תלוי בפילוג המשותף של המוצאים.
כל פענוח מבוזר (כמו בערוץ BC) הוא מקרה פרטי של פענוח משותף, כאשר פונקציות הפענוח תלויות רק במוצא אחד ולא בשניהם. לכן –

$$\max_{(R_0,R_1,R_2)\in\mathbf{C}_{BC}} \{R_0 + R_1 + R_2\} \le \mathbf{C}_{common}$$

משפט SATO

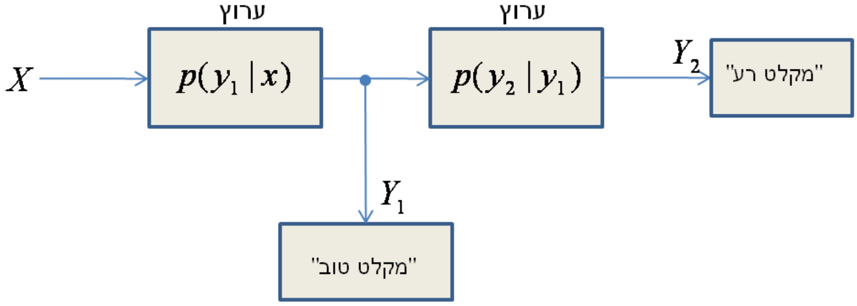
$$\max_{(R_0,R_1,R_2)\in\mathbf{C}_{BC}} \{R_0 + R_1 + R_2\} \le \min_{\left\{\substack{\tilde{p}(y_1,y_2|x): \\ \tilde{p}(y_1|x)=p(y_1|x) \\ \tilde{p}(y_2|x)=p(y_2|x)}\right\}} \left\{\mathbf{C}_{common}\left(\tilde{p}(y_1,y_2\,|\,x)\right)\right\}$$

סכום הקצבים בר ההשגה קטן מכל קיבול של ערוץ עם פענוח משותף (P2P) ופילוג מותנה שולי זהה לפילוג המותנה השולי בערוץ ההפצה הנתון.
*תרגיל בית
במקרה של BC גאוסי - $Y_1 = X + Z_1, \quad Y_2 = X + Z_2$ מה חסם Sato, כתלות בקורלציה בין Z_1, Z_2 ?

ערוץ הפצה מידרדר (DEGRADED BROAD-CAST CHANNEL)

ערוץ מידרדר פיזיקלית (physically degraded)

מתקיים הקשר המרקובי $X \leftrightarrow Y_1 \leftrightarrow Y_2 \quad \Leftrightarrow \quad p(y_1, y_2 | x) = p(y_1 | x)p(y_2 | y_1)$



ערוץ מידרדר סטכאסטית (stochastically degraded)

שקול מבחינת הפילוגים לערוץ הפצה מידרדר פיזיקאלית. , קיים ערוץ מידרדר פיזיקאלית 'מקביל' בעל פילוגים שוליים זהים לפילוגים השוליים של הערוץ הנתון $p(y_1 | x),\ p(y_2 | x)$.

הערוץ המקביל מתואר ע"י הפילוגים המותנים $\tilde{p}(y_2 | y_1)$, $\tilde{p}(y_1 | x)$ כך ש-

$$p(y_1 | x) = \tilde{p}(y_1 | x)$$

$$p(y_2 | x) = \sum_{y_1} p(y_1 | x)\tilde{p}(y_2 | y_1)$$

<u>הערות</u>

1. מהמשפט לגבי תלות רק בפילוג השולי נובע שתחום קיבול ערוץ מידרדר סטוכסטית זהה לערוץ הפיזיקאלי השקול.
2. מהקשר המרקובי נובע שכל הודעה שמקלט 'רע' יכול לפענח, גם מקלט 'טוב' יכול לפענח (בהסתברות גבוהה), כך שכל הודעה שנשלחת למקלט ה'רע' יכולה להיחשב כהודעה ציבורית. ולכן, אפשר להעביר כרצוננו קצב בין ההודעות הפרטיות למקלט ה'רע' ובין ההודעות הציבוריות:

$$\{(0, R_1, R_2) \in \mathbf{C_{BC}}\} \Rightarrow \{(R_0, R_1, R_2 - R_0) \in \mathbf{C_{BC}}\}, \quad \forall R_0 \in [0, R_2]$$

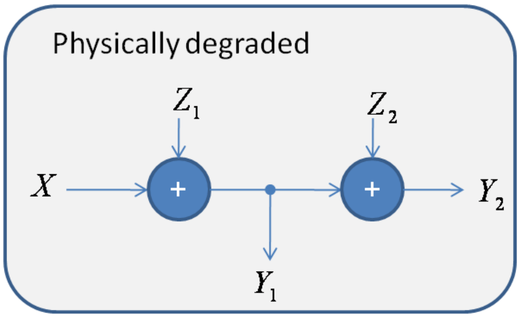
במקרה הכללי (לאו דווקא ערוץ מידרדר), תוספת קצב להודעות המשותפות תגרע משני הקצבים להודעות הפרטיות – לכל היותר בשיעור שנוסף לקצב המשותף:

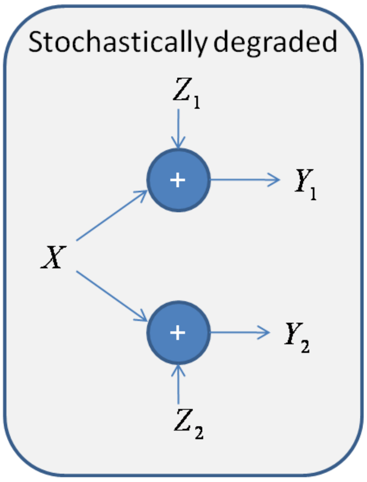
$$\{(0, R_1, R_2) \in \mathbf{C_{BC}}\} \Rightarrow \{(R_0, R_1 - R_0, R_2 - R_0) \in \mathbf{C_{BC}}\}, \quad \forall R_0 \in [0, \min\{R_1, R_2\}]$$

3. הגדרות כלליות ל'הידרדרות'

$$\forall p(x),\ I(X;Y_2) \le I(X;Y_1) \ \text{- "less capable" / "more noisy"}$$

4. השוואה בין ערוץ גאוסי מידרדר פיזיקלית וערוץ גאוסי מידרדר סטוכסטית





משפט קיבול לערוץ הפצה מידרדר

עבור ערוץ שמתקיים בו הקשר $X \leftrightarrow Y_1 \leftrightarrow Y_2$ מגדירים מ"א כך ש- $U \leftrightarrow X \leftrightarrow Y_1 \leftrightarrow Y_2$, הקצבים ברי ההשגה עבור פילוג כניסה $p(x,u)$:

$$C(p(x,u)) = \begin{Bmatrix} (R_1, R_2): \\ (R_0 =)R_2 \le I(U;Y_2) \\ R_1 \le I(X;Y_1 | U) \end{Bmatrix}$$

$$p(u,x,y_1,y_2) = p(u)p(x|u)p(y_1|x)p(y_2|y_1)$$

$$U \leftrightarrow X \leftrightarrow Y_1 \leftrightarrow Y_2$$

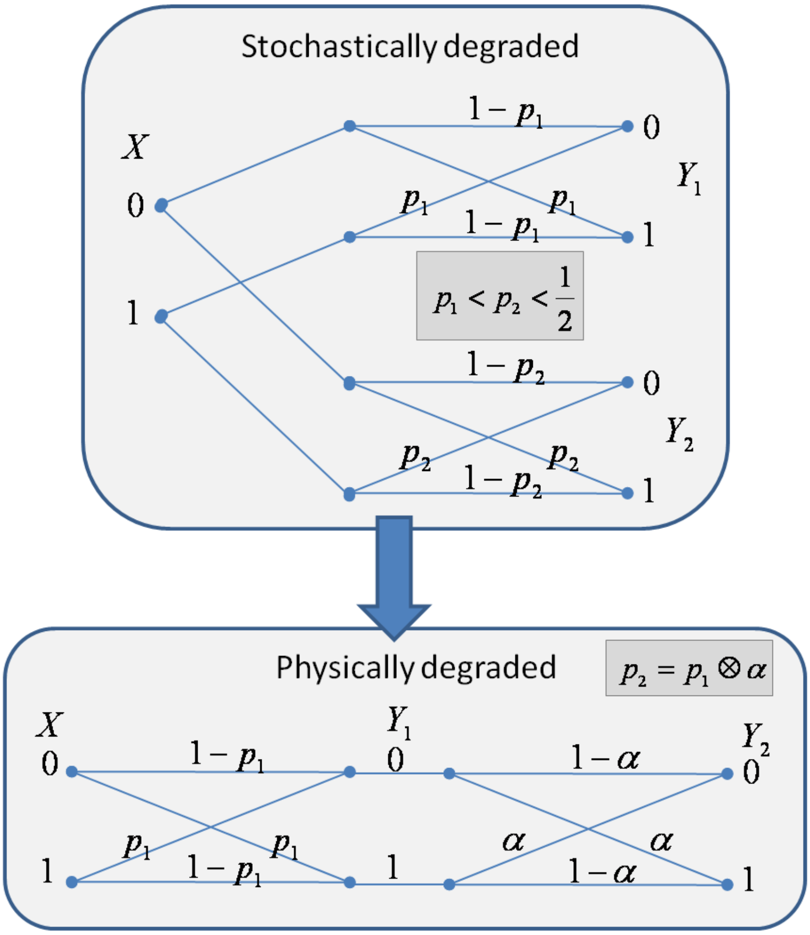
תחום הקיבול לערוץ הוא

$$\mathbf{C_{BC}} = convex\,hull\left(\bigcup_{p(x,u):U\leftrightarrow X\leftrightarrow Y_1\leftrightarrow Y_2} C(p(x,u)) \right)$$

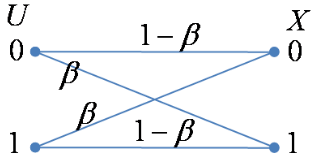
במקרה הבדיד, תמיד נוכל להשיג את תחום הקיבול ע"י שימוש במשתנה עזר U שגודל הא"ב שלו לא גדול מהא"ב המינימלי מבין שאר המשתנים במערכת - $|\mathcal{U}| \le \min\{|\mathcal{X}|,|\mathcal{Y}|,|\mathcal{Y}|\}$

Symmetric Binary B.C. – דוגמא

נתון ערוץ בינארי מידרדר סטוכסטית וממנו בונים ערוץ מידרדר פיזיקלית:



מגדירים את משתנה העזר U כך שהקשר בינו ובין X דומה לקשר בין מבוא ומוצא של ערוץ BSC בעל פרמטר β:



תחום הקיבול לפי המשפט:

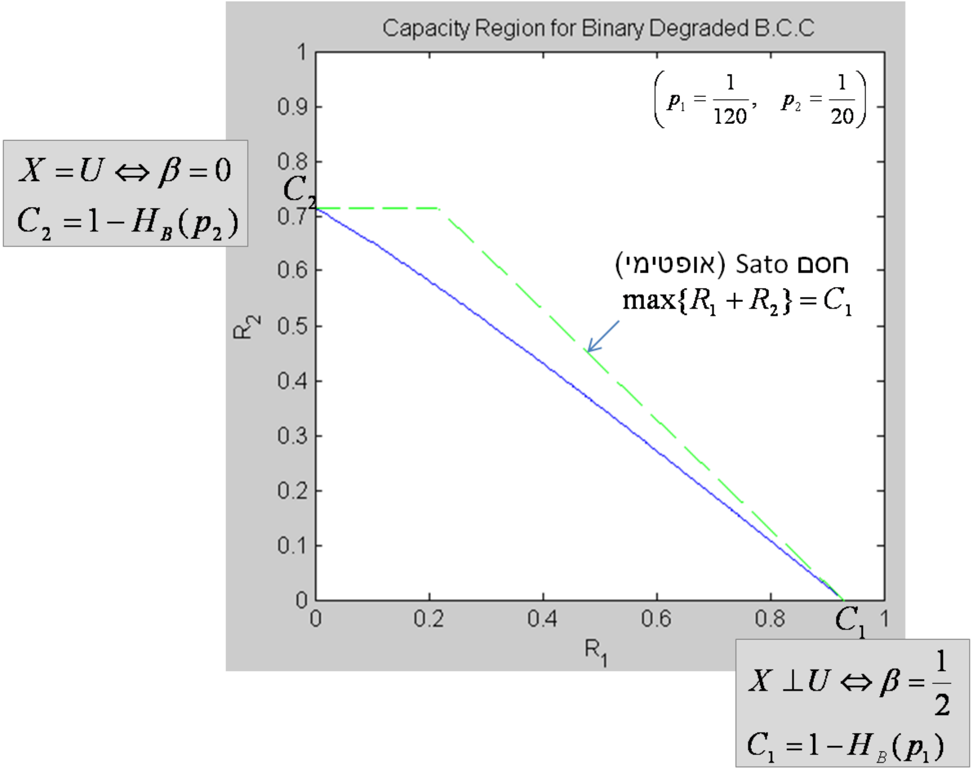
$$I(X;Y_1|U)=H(Y_1|U)-H(Y_1|X)=H_B(\beta\otimes p_1)-H_B(p_1)$$

$$I(Y_2;U)=1-H_B(\beta\otimes p_1\otimes\alpha)=1-H_B(\beta\otimes p_2)$$

$$C(p(x,u))=C(\beta)=\left\{\begin{array}{l}(R_1,R_2):\\ R_1\le H_B(\beta\otimes p_1)-H_B(p_1)\\ R_2\le 1-H_B(\beta\otimes p_2)\end{array}\right\}$$

$$\mathbf{C_{BC}}=convexhull\left(\bigcup_{0\le\beta\le\frac{1}{2}}C(\beta)\right)$$

גרף של תחום הקיבול בערוץ מסוג זה עם פרמטרים שנקבעו שרירותית:



הוכחת המשפט הישר

באמצעות קוד אקראי שמוגרל עבור בחירה נתונה של פילוג $p(x,u)$.

1. בניית קוד
   a. מגרילים 2^{nR_2} מילים $C_2=\{\mathbf{U}(i), i=1...2^{nR_2}\}$ עפ"י הפילוג השולי של U - $\mathbf{U}(i)_t \sim p(u), i.i.d. [t=1,...,n]$.
   b. עבור כל מילת קוד $\mathbf{U}(i)$ נגריל 2^{nR_1} וקטורים $C_1(i)=\{\mathbf{X}(k), k=1...2^{nR_1}\}$ לפי הפילוג של X מותנה ב $\mathbf{U}(i)$:

$$\mathbf{X}(i,k)_t \sim p(x|\mathbf{U}(i)_t) \Rightarrow \mathbf{X}(i,k) \sim \prod_{t=1}^{n} p(x|\mathbf{U}(i)_t)$$

2. קידוד
   בהינתן $W_2=W_0=i \quad W_1=k,$ נשדר $\mathbf{X}(i,k)$.

3. פענוח
   a. מקלט 'רע'
      בהינתן פלט ערוץ $\mathbf{Y}_2$ מחפש $\mathbf{U}(\hat{i}) \in C_2$ אופייני עם $\mathbf{Y}_2$
      $\left(\mathbf{U}(\hat{i}), \mathbf{Y}_2\right) \in A_\varepsilon^{(n)}(U,Y_2) \Rightarrow \hat{W}_2=\hat{i}$
   b. מקלט 'טוב'
      i. בהינתן פלט ערוץ $\mathbf{Y}_1$ מחפש $\mathbf{U}(i^*) \in C_2$ אופייני עם $\mathbf{Y}_1$
      $\left(\mathbf{U}(i^*), \mathbf{Y}_1\right) \in A_\varepsilon^{(n)}(U,Y_1)$

ii. מחפש בספר הקוד של X המתאים ל- $\mathbf{U}(i^*)$ שנמצא (הספר $C_1(i^*)$) מילת קוד אופיינית במשותף עם $\mathbf{Y}_1$.

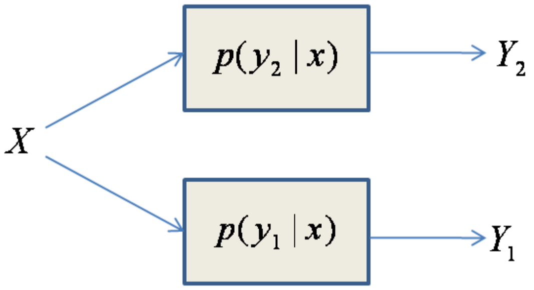
$$\left(\mathbf{X}(i^*,\hat{k}),\mathbf{Y}_1\right)\in A_\varepsilon^{(n)}(X,Y_!)\Rightarrow \hat{W}_1=\hat{k}$$

קביעת קצבים כדי לקרב הסתברות שגיאה לאפס

1. $R_2 < I(U;Y_2) \Leftarrow$ הסתברות ל- $\mathbf{U}$ מתחזה שואפת לאפס. $\mathbf{U}(i)$ האמיתי יפוענח בהסתברות גבוהה במקלט הרע (וברור שגם במקלט הטוב).
2. $R_1 < I(X;Y_1 \mid \underbrace{U}_{SI@both}) \Leftarrow$ בהינתן $\mathbf{U}$ ניתן לפענח נכון את $\mathbf{X}$ מתוך $\mathbf{Y}_1$ בהסתברות גבוהה (הסתברות ל- $\mathbf{X}$ מתחזה שואפת לאפס).

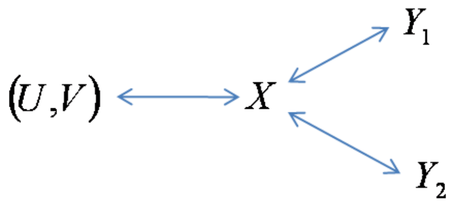
ערוץ הפצה בלתי מידרדר

נתייחס רק לפילוגים המותנים השוליים הנובעים מפילוג הערוץ:



חסמי מארטון (Marton 79') לקיבול ערוץ הפצה – חסם תחתון (inner bound)

עבור כל זוג מ"א (U,V) שמקיימים את הקשר המרקובי:



$$p(u,v,x,y_1,y_2)=p(u,v)p(x\,|\,u,v)p(y_1\,|\,x)p(y_2\,|\,x)$$

תחום הקיבול של הערוץ מכיל את התחום:

$$\mathbf{C_{BC}}\supset\left\{\begin{matrix}(R_1,R_2): \\ R_1\le I(U;Y_1) \\ R_2\le I(V;Y_2) \\ R_1+R_2\le I(U;Y_1)+I(V;Y_2)-I(V;U)\end{matrix}\right\}\quad,\quad W_0\equiv\phi\ \text{- no common message}$$

נשים לב שהגודל $[I(V;Y_2)-I(V;U)]$ זהה לקיבול ערוץ $V\to Y_2$ עם אינפורמציית צד $"S"=U$ ידועה למשדר (קיבול Gelfand Pinsker).

משדרים למקלט2 את ההודעה V, כאשר ההודעה U המיועדת למקלט1 מתפקדת כ"מצב ערוץ" ואינה ידועה למקלט2 (כאשר הערוץ לא מידרדר) אך ידועה למשדר.

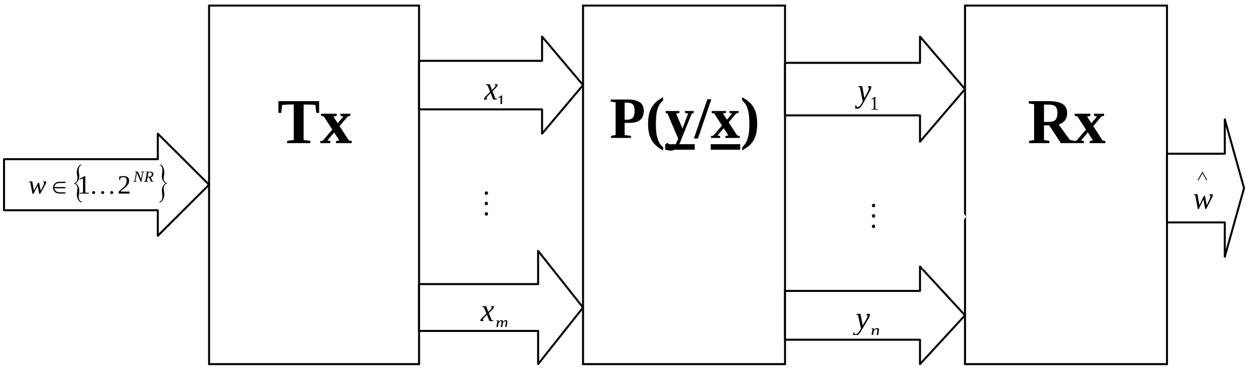
סכום הקצבים שווה לקצב שאפשר לשדר למקלט אחד בלי אינפורמציית צד ('הפרעות') - $C_{1,noSI}=I(U;Y_1)$, ועוד מה שאפשר לשדר למקלט השני כאשר ההודעה למקלט הראשון היא 'הפרעה' $C_{2,SI@Tx}=I(V;Y_2)-I(V;U)$.

הרצאה מס' 11

ערוצים מרובי כניסות ומוצאים (MIMO)

סוכם ע"י עמנואל אורנשטיין

ערוצים וקטוריים גאוסיים P2P



Memoryless
לאורך ציר הזמן

$E\left\|x^2\right\| \le P$

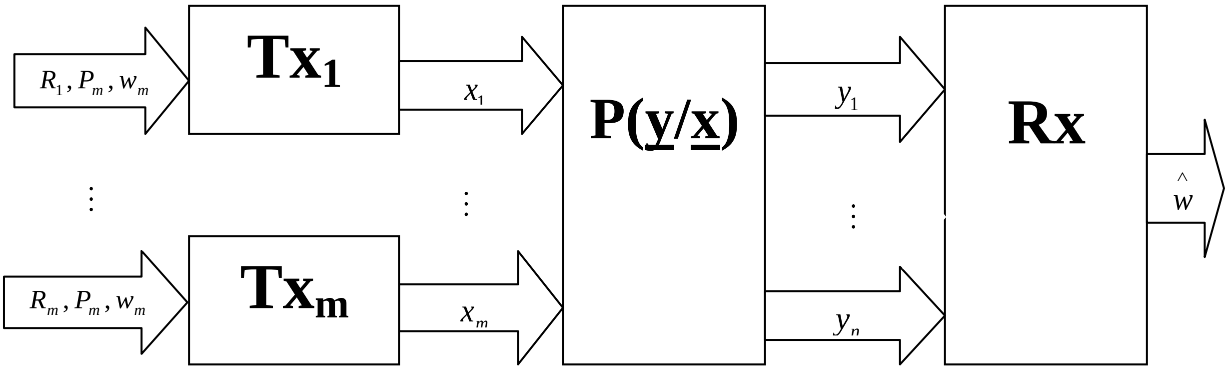
לאורך ציר הזמן "מילת קוד" היא סדרת וקטורים m מימדיים $x_1(w) \ldots x_N(w)$:

$\frac{1}{N}\left\{\left\|x_1(w)^2\right\| + \ldots + \left\|x_N(w)^2\right\|\right\} \le P$

$w \in \{1 \ldots 2^{NR}\}$

$C_{p2p} = \max_{p(\underline{x}):E\left\|x^2\right\| \le P} I(\underline{x};\underline{y})$

MAC משדרים מבוזרים



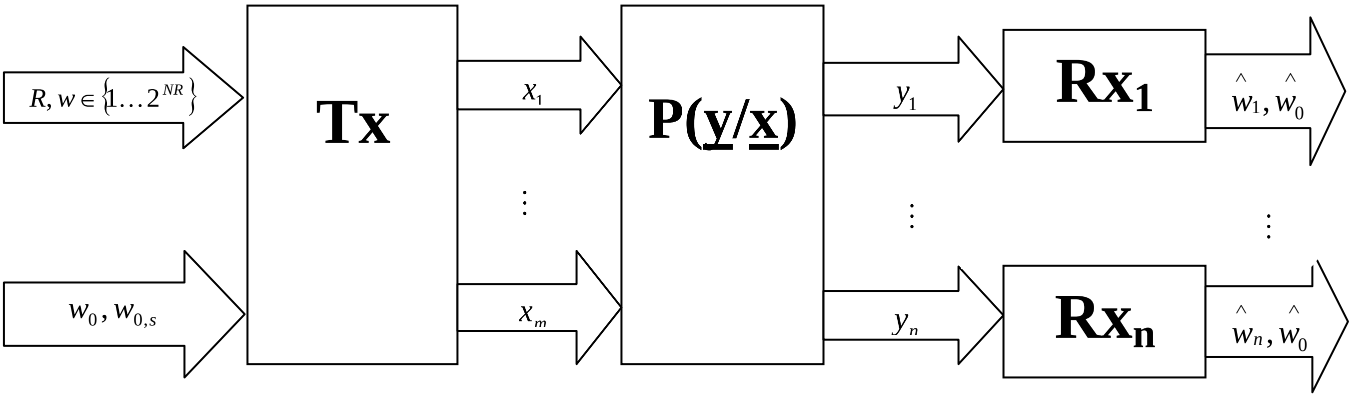
$C_{MIMO-MAC}^{CONVEX-HULL-CLOSURE} = \underline{R} = R_1 \ldots R_m : \sum_{i \in s} R_i \le I(\underline{x}_s ; \underline{y} / \underline{x}_{s^c}) \ \ \forall s \subset \{1 \ldots m\}$

עבור איזשהו פילוג מבוא $p(x_1) \ldots p(x_m)$

$E x_i^{\ 2} \le p_i ; i = 1 \ldots m$

מותר לקחת קומבינציה ליניארית של תחומים שכל אחד מהם בנפרד לא מקיים אילוץ אבל לאחר פעולת הקמור האילוץ מתקיים.

B.C.C. משדר משותף מקלטים מבוזרים



1. Degraded

עבור $C_{B.C.}$ ידוע שאם $x \leftrightarrow y_1 \leftrightarrow y_2 \leftrightarrow \dots y_n$

$R_2 \le I(u;y_2)$

$R_1 \le I(x;y/u)$

$C_{B.C.} =$ 1972 Cover תחום של $\underset{\forall n=2}{=} \{R_1, R_2 = R_0$

2. **חסמי מארטון:** inner, outer

קצבים בני השגה

3. **חסמי סאטו:**

$$C_{SUM} = \sum_{\{\underline{R}\in C_{B.C.}\}} R_i \le \min_{\left\{p(\underline{y}/\underline{x}) : p(\underline{y};\underline{x}) \tilde{=} p(\underline{y};\underline{x})\right\}} C_{p2p}\left[\tilde{p}(\underline{y}/\underline{x})\right]$$

ערוצים וקטוריים ליניאריים תחת אילוץ הספק

$$\underline{y}_t = \underline{\underline{H}} \cdot \underline{x}_t + \underline{Z}_t \qquad t = 1,2\dots N \qquad \underline{Z}_t \amalg \underline{x}_t$$

$$\underline{y}_t : N \times 1, \qquad \underline{\underline{H}} : N \times m, \qquad \underline{x}_t : m \times 1, \qquad \underline{Z}_t : N \times 1$$

$\underline{\underline{H}}$ מטריצה קבועה בזמן

חסר זיכרון בציר הזמן

$Z \sim N(\underline{0}, K_z)$

$White \sim N(\underline{0}, \sigma_Z^2 I)$

הנחה: מקלט ומשדר יודעים את הערוץ (H, K_Z) כלומר CSI@BOTH

קיבול P2P

$$C_{p2p} = \max_{E\|\underline{x}\|^2} I\left(\underline{x};\underline{\underline{H}}\,\underline{x}+\underline{Z}\right)$$

פרוק I לאנטרופיה דיפרנציאלית

$$C_{p2p} = \max_{E\|\underline{x}\|^2}\left\{h\left(\underline{\underline{H}}\,\underline{x}+\underline{Z}\right)\right\}-h\left(\underline{Z}\right)$$

$$C_{p2p} = \max_{K_x:tr(K_x)\le p}\left\{\begin{matrix}\text{Re}: \frac{1}{2}\cdot\log\left(2\pi e\right)^n\left|HK_xH^t+K_Z\right| \\ \log\left(2\pi e\right)^n\left|HK_xH^t+omplex:1\cdot\log\left(2\pi e\right)^n\right|HK_xH^t+K_Z\right|\end{matrix}\right\}-\log\left(2\pi e\right)^n\left|K_Z\right|$$

$$C_{p2p} = \max_{K_x:tr(K_x)\le p}\log\frac{\left|HK_xH^t+K_Z\right|}{\left|K_Z\right|}$$

$$C_{p2p} = \max_{K_x:tr(K_x)\le p}\log\left|\frac{1}{\sigma_z}HK_xH^t+I\right| \qquad \forall Z-white$$

<u>הערה:</u>
מטריצת הפרש אי שלילית מוגדרת

$$\text{cov}\left(\underline{x}\right)\le K_x$$
$$\text{cov}\left(\underline{x}\right)=K_x$$
$$E\|\underline{x}\|^2=tr\left(K_x\right)\equiv\sum_{i=1}^{n}K_{xi}$$

נרצה להבין (לקבל Insight) למספר היבטים של הבעיה:

1. המקרה $m\neq n$ לעומת $m=n$.
2. כלל מזיגת המים (Waterfilling Solution) S.V.D.
3. עיצוב אלומה Beamforming הרווח לעומת שידור איזוטרופי (חד כיווני).
4. גילוי אופטימלי לעומת G.D.F.E. = Succesive Decoding (פענוח בשלבים).
5. מדוע MIMO (SIMO,MISO).
6. הכללה מ P2P ל MAC ול B.C.

מדוע MIMO

רווח עיצוב אלומה (B.F.)
רווח גיוון (Diversity)
רווח ריבוב (Multiplexing)

דוגמה

$$n=3$$
$$m=2$$
$$\begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix}=\begin{bmatrix}h_{11} & h_{12}\\ h_{21} & \\ & h_{32}\end{bmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}+\begin{pmatrix}Z_1\\Z_2\\Z_3\end{pmatrix}$$
$$y_1=h_{11}x_1+h_{12}x_2+Z_1$$
$$\vdots$$

א. כתיבה מצורת "MISO"

$$y_i=\left\langle\underline{h}_i,\underline{x_i}\right\rangle+Z_i \qquad i=1\ldots n$$

$y_i = \|h_i\| \cdot \|x\| \cdot \cos\theta$

התאבכות בונה $\theta = 0$ או $\theta = 180^0$

ב. כתיבה מצורת "SIMO"

$\underline{y} = x_1 [\underline{h}_1]_{|@ x_2 = 0} + \underline{Z}$

$\underline{y} = x_1 [\underline{h}_2]_{|@ x_1 = 0} + \underline{Z}$

ג. כתיבה מצורת "SISO"

$\tilde{y} = \langle \underline{y}, \underline{u} \rangle \qquad \underline{x} = \tilde{x} \cdot v$

$\tilde{y} = \underline{u}^t \left[\underline{\underline{H}} \cdot \tilde{x} \cdot \underline{v} + \underline{Z} \right]$

$\tilde{y} = \tilde{x} \cdot u^t \cdot \underline{\underline{H}} \cdot \underline{v} + \tilde{Z}$

$\tilde{Z} = u^t \cdot Z$

$u^t : 1 \times N, \qquad \underline{\underline{H}} : N \times m, \qquad v : m \times 1$

רווח גיוון $\Leftarrow$ שיפור הסתברות השגיאה בתנאים של אי וודאות לגבי הערוץ

<u>דרגות חופש</u>

טענה: מספר דרגות החופש של המערכת - $rank \ H$

כלומר

א. $C \approx (rankH) \cdot \log\left(\frac{p}{\sigma_Z^2}\right)$ בגבול של יחס אות לרעש גבוה מתקיים שוויון

ב.אם הרעש Z לבן,אזי קיימת מטריצה A בשידור ואו מטריצה B בקליטה כך שללא הפסד אינפורמציה הערוץ השקול

$\underline{\tilde{y}} = B \cdot \left[H \cdot A \cdot \underline{\tilde{x}} + \underline{Z} \right]$

$\underline{\tilde{y}} : \tilde{n} \times 1, \qquad B : \tilde{n} \times N, \qquad \underline{\underline{H}} : N \times m, \qquad A : m \times \tilde{n}, \qquad \underline{\tilde{x}} : \tilde{n} \times 1, \qquad \underline{Z} : N \times 1$

$\underline{x} = A \cdot \underline{\tilde{x}}$

הוכחה

$N > m = rankH$ (עודף אנטנות קליטה)

$\underline{\underline{H}} \cdot \underline{x} = x_1 [\underline{h}_1] + \ldots + x_m [\underline{h}_m] \quad \in R^N$

$R^N \subset$ תת מרחב לינארי ממימד m = תת מרחב העמודות $\in$

B – בסיס של תת מרחב העמודות $(m \times N)$

$B_\perp$ - בסיס של תת מרחב המשלים $(N - m) \times N$

$I(\underline{x}; \underline{y}) = I(\underline{x}; B\underline{y}; B_\perp \underline{y})$

$I(\underline{x}; \underline{y}) = I(\underline{x}; BH\underline{x} + B\underline{Z}; B_\perp \underline{Z}) \qquad \underline{B_\perp \underline{\underline{H}} \underline{x} = 0}$

אם Z לבן אזי $B\underline{Z} \amalg B_\perp Z$ $\qquad$ $B_\perp Z$ בת"ס בכל מרכיבי הביטוי

$I(\underline{x}; \underline{y}) = I(\underline{x}; BH\underline{x} + B\underline{Z};)$

כלל מזיגת המים

אם H $N\times N$ מדרגה מלאה

$$\underline{y}=H\underline{x}+\underline{W}\quad\Rightarrow H^{-1}\underline{y}=\underline{x}+\underline{Z}\qquad \underline{Z}=H^{-1}\underline{W}$$

$$K_Z=\left(H^{-1}H^{-t}\right)\sigma_Z^2$$

"לכסון רעש"

$$\Lambda=T^tK_ZT\qquad K_Z=T\Lambda T^t$$

$$T^tT=TT^t=1$$

המרה למרחב הוקטורים העצמיים

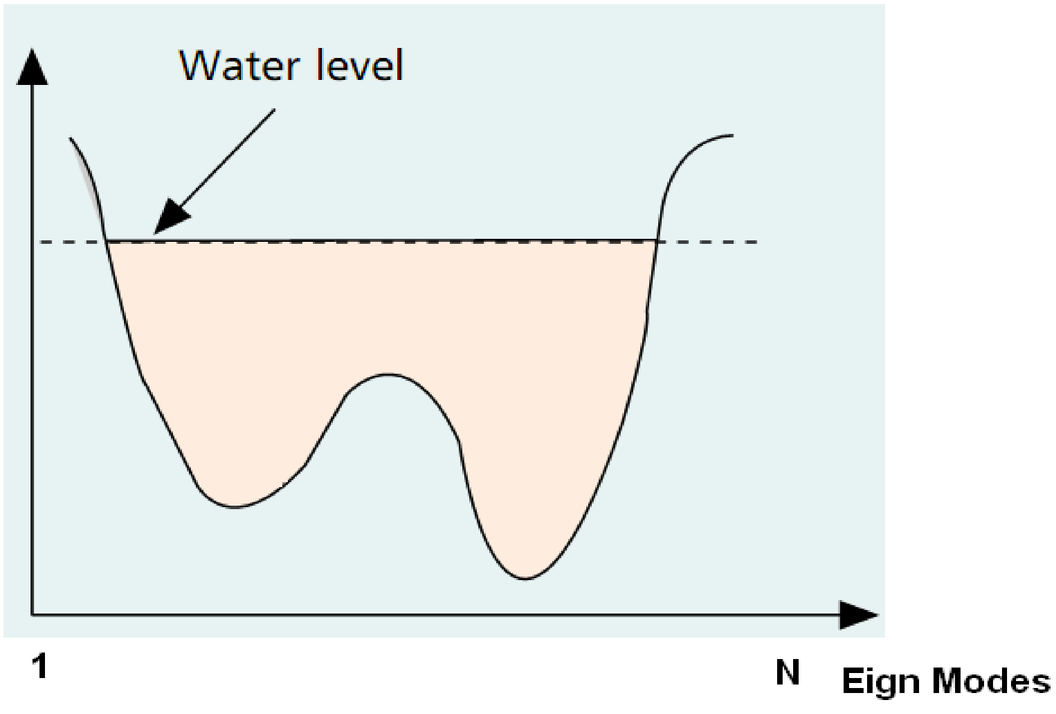
$$\underline{\tilde{y}}=T^t\underline{y}$$

$$\underline{x}=T\underline{\tilde{x}}$$

$$\Rightarrow\underline{\tilde{y}}=T^t\left(T\underline{x}+\underline{Z}\right)=\underline{\tilde{x}}+\underline{\tilde{Z}}+\operatorname{cov}\left(\underline{Z}\right)=T^tK_ZT=\Lambda$$

ערוצים מקביליים

$$\tilde{y}_1=\tilde{x}_1+\tilde{Z}_1$$
$$\vdots$$
$$\tilde{y}_N=\tilde{x}_N+\tilde{Z}_N$$
$$Z_i\sim N\left(0,\lambda_i\right)$$



Water Level = θ, Total amount of water = p

$$C_{p2p}=\sum_{i=1}^{N}\log\left(1+\frac{p_i}{\lambda_i}\right)\qquad p_i=\left[\theta-\lambda_i\right]^t$$

θ נבחר כך ש $\sum p_i=p$

הערות

1. סה"כ המרה T^t, T, B, A מקבלים את קווריאנס השדור K_x^{OPT} שמשיג את נוסחת הקיבול.
2. אם $\theta \ge \lambda_{\max}$ אזי $C = C_{SUB} = N\log\left(\frac{p+tr(K_Z)}{N}\right) - \log|K_Z|$
3. ניתן ע"י לכסון ישיר של H לקבל $\tilde{y}_i = \alpha_i \tilde{x}_i + \tilde{W}_i \quad i=1\ldots N \quad \tilde{W}_i \sim N(0,\sigma^2)$

$$\alpha_i = \frac{1}{\sqrt{\lambda_i}}$$

שידור איזוטרופי (כלל כיווני)~$\underline{x}$ לבן

$$C = N\log\left(\frac{p}{N\sigma_Z^2}\right) + \log(HH^t) \qquad \begin{matrix} O(1)\to 0 \\ OR \\ p\to\infty \end{matrix} \qquad C = \log\left|\frac{p}{n\delta_Z^2}HH^t\right| + O(1)$$

מושג ע"י $K_x = \frac{p}{N}\underline{\underline{I}}$

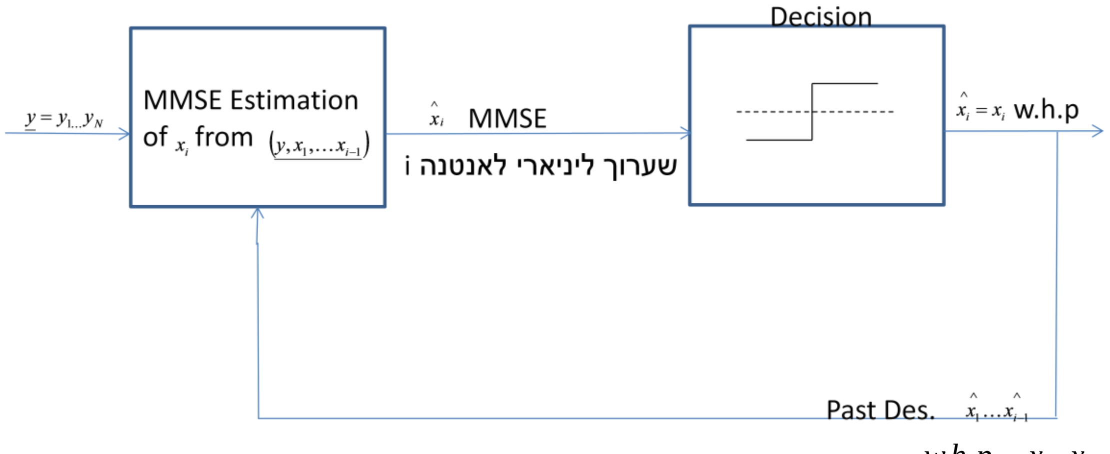
חסם אוניברסאלי (נכון לכל SNR)

$$C - I(White_Input) \le N\frac{\log(e)}{2e} \approx N\cdot {}^1\!/_4\, bit \quad \forall SNR$$

Successive Refinement = GDFE

מקלט פשוט

הנחה: $x_1\ldots x_N$ בת"ס



$= w.h.p = x_{1\ldots}x_{i-1}$

על"פ סדר $i=1\ldots N$ שרירותי שנקבע מראש.

טענה: פענוח GDFE אינו מפסיד קיבול ! (למרות הפסד מבחינת הסתברות השגיאה)

הוכחה:

טענות עזר

1. $e = x - \hat{x}^{MMSE}(y) \Rightarrow e \perp y$ And any function of y
2. במקרה הגאוסי (ניצבות הופכת לחוסר תלות היות ו $E(e)=0$)
3. אם x,y גאוסיים במשותף

$$I(\underline{y};\underline{x}) = I\left(x;\hat{x}^{MMSE}(\underline{y})\right) = I\left(\hat{x}^{MMSE}+e;\hat{x}^{MMSE}\right) = \log\left(\frac{Var(x)}{MMSE}\right)$$

<u>הוכחה:</u>

$$I(\underline{y};\underline{x}) = \sum_{i=1}^{N} I(\underline{y};x_i/x_1^{i-1})$$

$$I(\underline{y};x_i/x_1^{i-1}) = I\left(\underline{y}, f(\underline{y},x_1^{i-1},x_1^{i-2});x_i/x_1^{i-1}\right)$$

$$I(\underline{y};x_i/x_1^{i-1}) = I\left(\hat{x}_i,\hat{x}_i+e_i/x_1^{i-1}\right)+I\left(\underline{y},\hat{x}_i+e_i/\hat{x}_i,x_1^{i-1}\right) \qquad e_i = x_i-\hat{x}_i$$

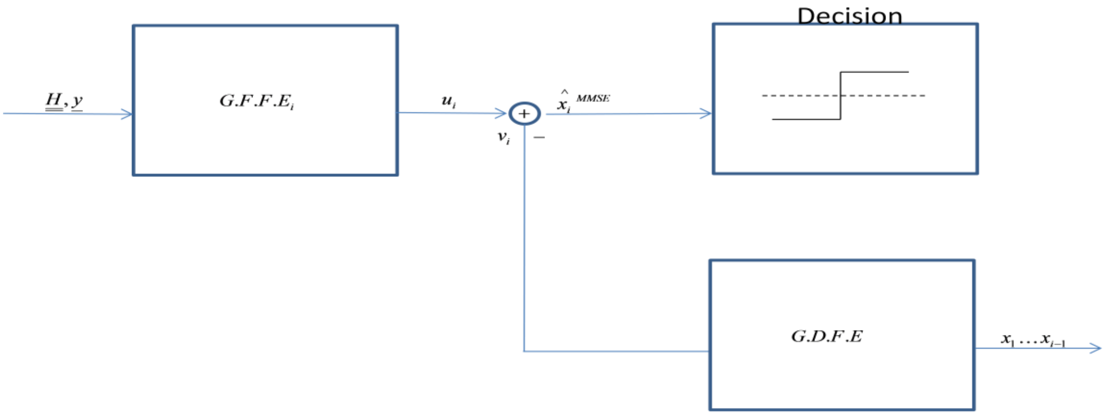
$I(\underline{y};x_i/x_1^{i-1}) = I\left(\hat{x}_i^{MMSE},\hat{x}_i^{MMSE}+e_i/x_1^{i-1}\right)+0$.משערך MMSE ⇐ אורתו

Suff. Statistics $\Rightarrow 0$

$$I(\underline{y};x_i/x_1^{i-1}) = h(x_i/x_1^{i-1})-h(e_i) = h(x_i)-h(e_i) = I\left(\hat{x}^{MMSE};x\right)$$

$$I(\underline{y};x_i/x_1^{i-1}) = \log\left(\frac{p_i}{MMSE_i}\right) \quad i=1\ldots N$$

ניתן לפרק את המשערך הלינארי $2\times L$ לשני משערכים נפרדים



טענה: עבור G.F.E.E. נתון אם $x_1\ldots x_N$ בת"ס

$$u_i = \sum_{j=1}^{N} a_{ij}x_1 + \tilde{Z}_i$$

ה G.D.F.E. האופטימאלי $\quad v_i = \sum_{j=1}^{i-1} a_{ij}x_j$

פתרון נוח ל G.D.F.E. ב SNR גבוה Gram schmidt $\Leftrightarrow$ QR Decomposition

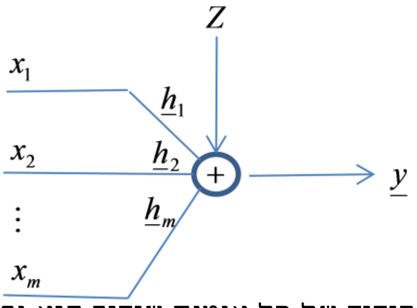
רעש $+ y_1 = r_{11}x_1$ $\quad \underline{\underline{H}} = QR \Rightarrow$ ניתן לבצע טרנספורמציה

רעש $+ y_2 = r_{22}x_2 + r_{21}x_1$

רעש $+ y_3 = r_{33}x_{3+}r_{32}x_2 + r_{31}x_1$

$\Leftarrow$ G.D.F.E. מקזז את איברי ה Off Diagonal של $\underline{\underline{R}}$

MIMO MAC

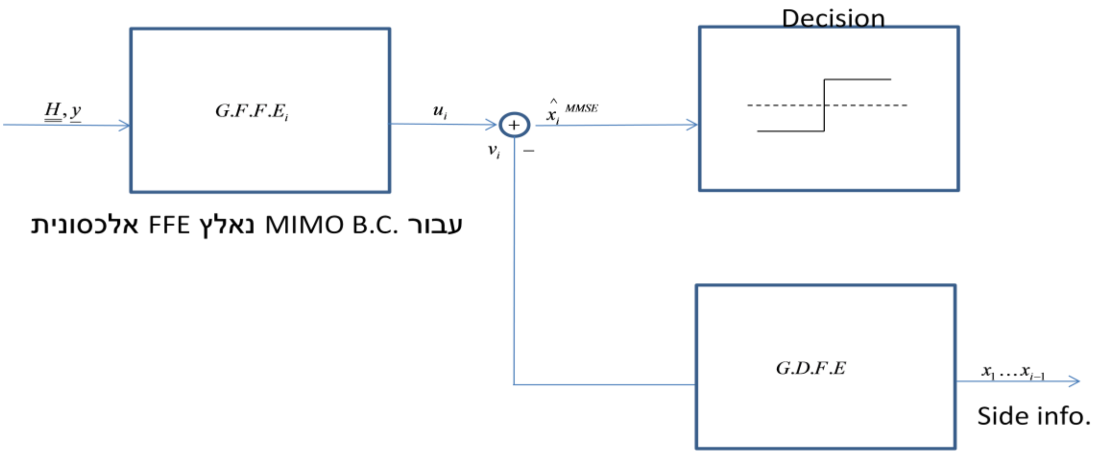


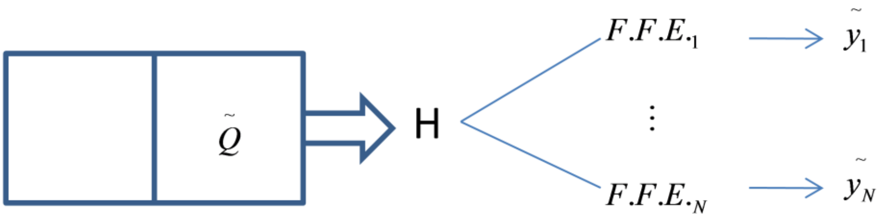
קידוד של כל אנטנת שידוד הוא נפרד

MIMO MAC להשיג קיבול G.D.K.E $\Leftarrow$

$$C = \max\log \frac{\left|HH^t + K_Z\right|}{\left|K_Z\right|}$$

MIMO BC Channel





DPC

$$C_{MIMO B.C.} = \quad x_1 \ldots x_{i-1}$$

קצבים בני השגה - מקסימום סכום קצבים:

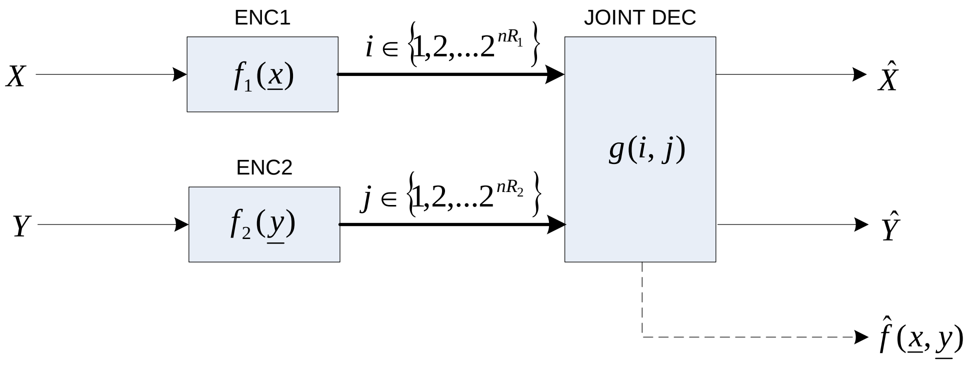
$$C_{sumMIMO B.C.} = \max_{p : p_1 + \ldots + p_N \le p} C_{MIMO_MAC}\left(H^t\right) = \max_{\tilde{K}_x : tr\left(\tilde{K}_x\right) \le p} \log\left|\frac{1}{\sigma_Z^2} H^t \tilde{K}_x + I\right|$$

הרצאה מס'12

קידוד מקור מבוזר עם עיוות

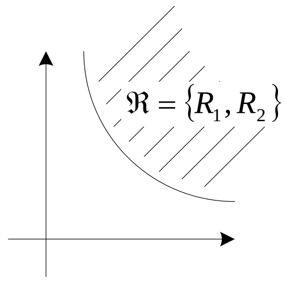
סוכם ע"י יובל דומב

1. **סכמת המערכת**:



2. **קריטריון העוות**
   - כללי $D = E\{d(\underline{x},\underline{y};\underline{\hat{x}},\underline{\hat{y}})\}$
   - לפי פונקצית שחזור $D = E\{d(f(\underline{x},\underline{y});\hat{f})\}$
   - מספר אילוצים $D = E\{(x-\hat{x})^2\}$, $D = E\{(y-\hat{y})^2\}$

3. נדרש למצוא את תחום הקצבים ברי ההשגה:

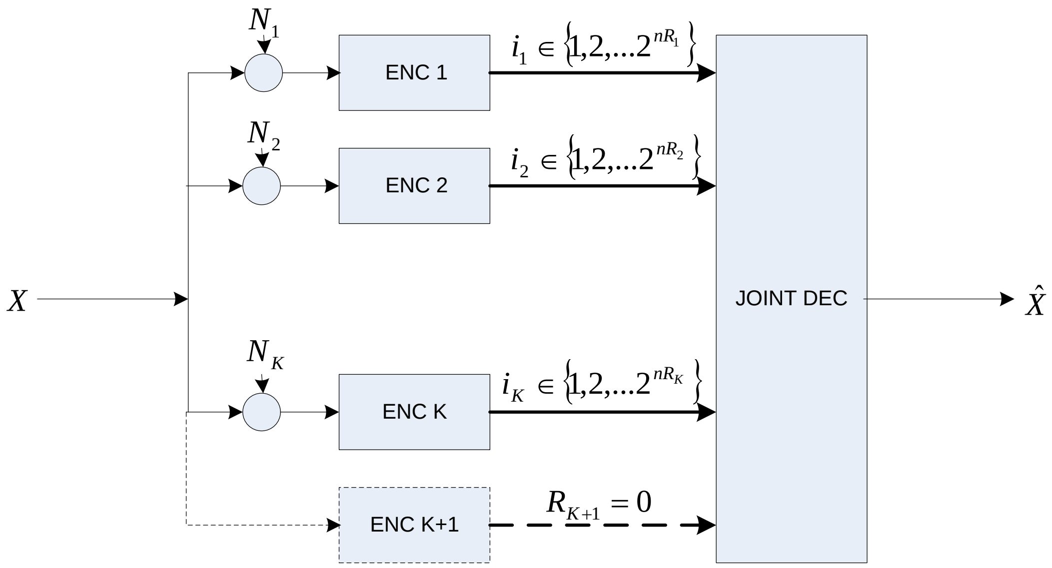


4. מקרים פרטיים מעניינים:
   - בעיית Wiener-Ziv
     - Y ידוע במדוייק למפענח
     - הכללות: Y דיסקרטי, $R_2 \geq H(Y)$ ומשוחזר ללא עוות $p(\hat{y} \neq y) \to 0$
   - בעיית ה-CEO
   - בעיית העוזר/ים (WAK)
   - בעיית Korner-Marton

בעיית ה-CEO

Berger-Zhang-Viswanathan

- קידוד מבוזר של מדידות רועשות לצורך פענוח ושחזור של המקור

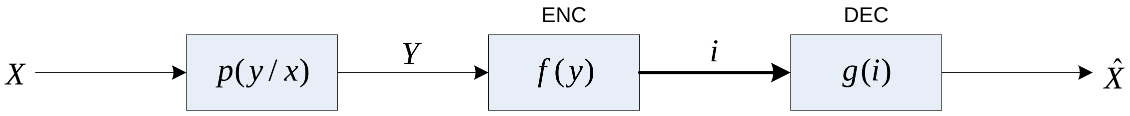


$$p(x, y_1, y_2, \ldots y_K) = p(x) p(y_1 \mid x) \ldots p(y_K \mid x)$$

$$D = E\{d(x, \hat{x})\}$$

גרסה סקלרית (קידוד משותף) של ה-CEO

remote/noisy/indirect source coding



$$D = d(x, \hat{x})$$

$$R_{XviaY}(D) = ?$$

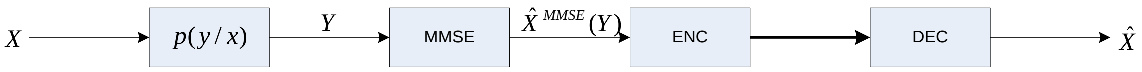
1. **Dobrushin-Tsybakov:**

$$R_{XviaY}(d, D) = R_Y(\tilde{d}, D)$$

$$\tilde{d}(y, \hat{y}) \equiv E_{p(x|y)}\{d(x, \hat{y}) \mid Y = y\}$$

2. **Wolf-Ziv (1970)**:

- אם מדד העוות הוא ריבועי $d(x,\hat{x})=(x-\hat{x})^2$



$$R_{XviaY}(MSE,D)=R_{\hat{X}^{MMSE}}(MSE,D-MMSE)$$
$$D=MMSE+\text{compression distortion}$$

- התוצאה נובעת מעקרון האורתוגונליות: העוות הריבועי השקול בין $\hat{X}$ ל- X שווה לסכום של ה-$MMSE$ ושגיאת הקידוד, כאשר המרכיב הראשון הוא קבוע שלא תלוי במקודד.

3. **סטטוס של בעיית ה-CEO**:

- פתורה עבור:
  - מקרה גאוסי עם מדד עוות ריבועי
  - מקרה כללי כאשר $K\to\infty$
- מסקנה מהפתרון במקרה הגאוסי ריבועי כאשר $K\to\infty$ (Ohama):

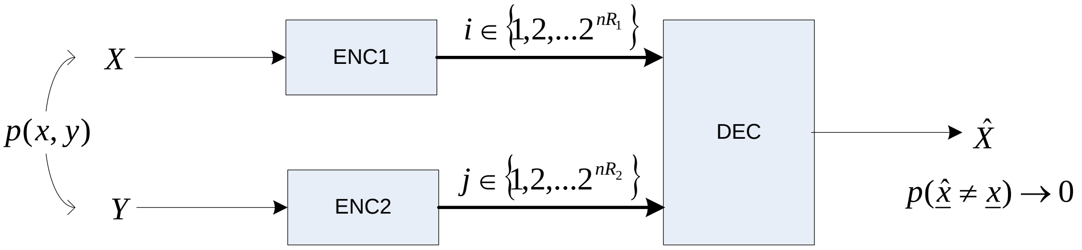
$$D\propto\frac{\sigma_N^2}{R_{sum}}$$
$$R_{sum}=\sum_{1}^{K}R_i$$

- לשם השוואה עם שערוך משותף ואז דחיסה בגבול $K\to\infty$:

$$D=D(R)=\sigma_X^2\,2^{-2R_{sum}}$$
$$\left[R(D)=\frac{1}{2}\log\left(\frac{\sigma_X^2}{D}\right)\right]$$

בעיית העוזר 1 help 1

Wyner, Ahlswede – Korner (WAK)

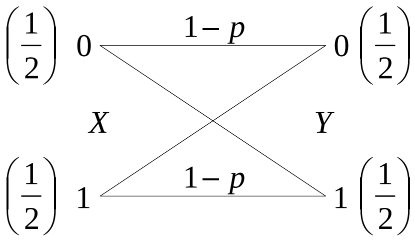


$$\Re=\text{convex hull}\left\{\bigcup\left\{\begin{matrix}R_1\ge H(X|V)\\ R_2\ge I(Y;V)\end{matrix}\right\}\right\}$$
$$X\leftrightarrow Y\leftrightarrow V$$

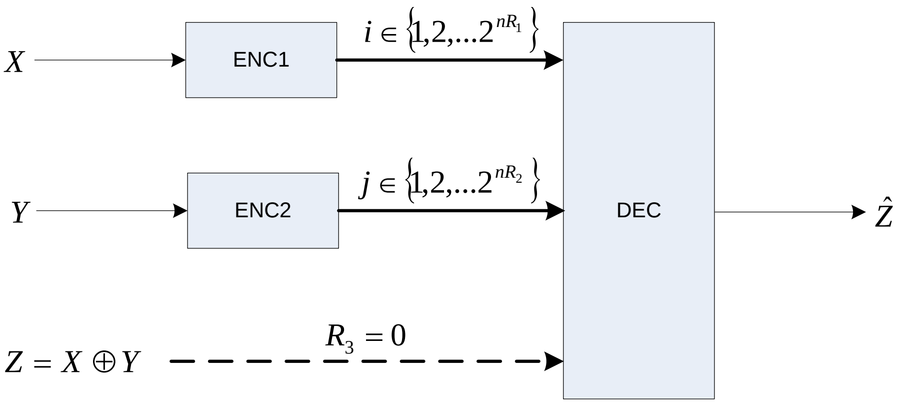
- האיחוד הוא על כל ה- V שמקיימים את התנאי המרקובי.
- ניתן לחשוב על V כקוונטיזציה של Y או כ-"context".

בעיית העוזר הכפול modulo sum(2 help 1)

Korner-Marton (1979)

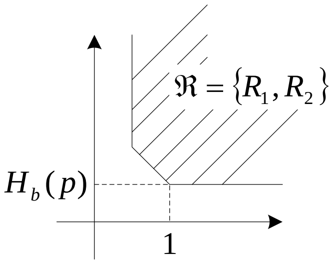


- (X,Y) מקור בינרי סימטרי כפול (doubly symmetric binary source)



- $Z \sim Ber(p)$ ולכן קדוד משותף היה משיג $R = H_b(p)$

1. **גישת Slepian-Wolf**:



$$\Rightarrow R_{sum} = H(X,Y) = 1 + H_b(p)$$

2. **גישת Korner-Marton**:

$$R_{sum} = R_1 + R_2 = 2H_b(p)$$

converse

אם נתייחס ל- Y בתור מידע צד אזי $R_1 \geq H_b(p)$

זה כמובן מתקיים גם עבור הצד השני ולכן $R_1 + R_2 \geq 2H_b(p)$

direct

אם C הוא קוד ליניארי כך ש-$C = \{\underline{c} : H\underline{c} = 0\}$ כאשר H היא מטריצת בדיקת הזוגיות ו-C הוא בר-פענוח בהסתברות גבוהה בערוץ BSC אזי:

$$\exists f, \hat{\underline{z}} = f(H\underline{y}) = \underline{z} \text{ w.h.p.}$$

כאשר $H\underline{y}$ הוא הסינדרום ($H\underline{y} = H(\underline{x} \oplus \underline{z}) = H\underline{z}$)

- לפי גישת SW (תזכורת: קדוד של X עם אינפורמצית צד Y במפענח)
  - קידוד: $\underline{s} = H\underline{x}$
  - פענוח: $H\underline{y} \oplus \underline{s} = H(\underline{x} \oplus \underline{y}) = H\underline{z}$ כאשר $\underline{y}$ הוא מידע צד

    אם $\hat{\underline{z}} = f(H\underline{z})$ שייך לתא החלטה אזי $\hat{\underline{z}} = \underline{z}$ בהסתברות גבוהה

  מימדי המטריצה $H_{(n-k)\times n}$ נותנים $R_1 = H_b\left(\frac{n-k}{n}\right) \approx H_b(p)$

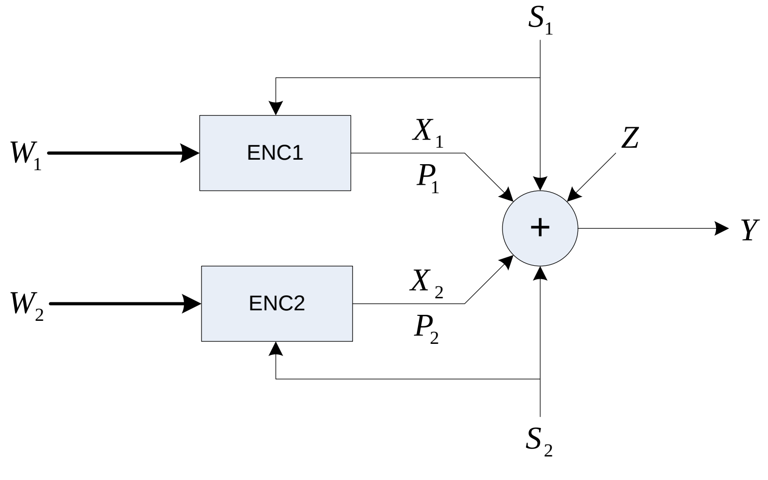
- לפי גישת KM:
  - X מקודד עם מידע צד Y: $\underline{s}_1 = H\underline{x}$

    Y מקודד עם מידע צד X: $\underline{s}_2 = H\underline{y}$

    כאשר H היא מטריצת בדיקת הזוגיות של קוד בינרי שמתקרב לקיבול ה-BSC הנתון
  - פענוח: $\hat{\underline{z}} = f(\underline{s}_1 + \underline{s}_2) = f(H(\underline{x} \oplus \underline{y})) = f(H\underline{z}) = \underline{z}$ w.h.p.

3. בעיות דומות:

- בעיית העוזר הכפול הגאוסי
  - נפתרה ע"י Pradhan בעזרת שריגים מקוננים (השריגים זהים בשני המקודדים) בדומה לפתרון שריג לבעיית WZ.
- בעיית ה-dirty MAC
  - טופלה ע"י Tal Philosof בערת שריגים זהים (עד כדי מתיחה/כיווץ)
  - קצב קוסטה שואף ל-0 כאשר $\sigma_S^2 \to \infty$



$S_1 \perp S_2$

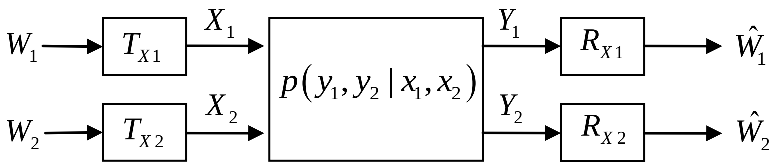
$C \approx C_{CleanMAC}$

הרצאה מס' 13

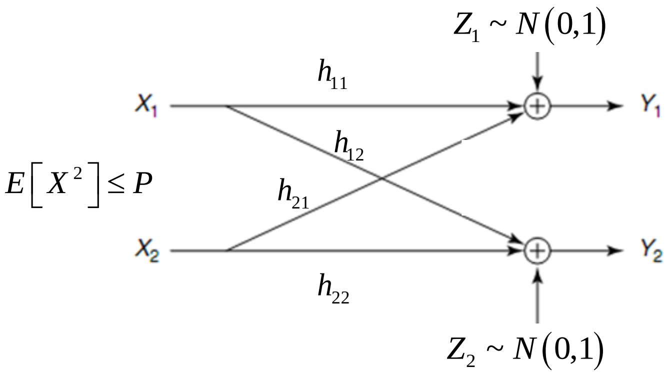
ערוץ הפרעה

סוכם ע"י עֹפר שפירא

מודל ערוץ כללי



המקרה הגאוסי



<u>הערה</u>: בלי הגבלת הכלליות, נניח כי אילוצי ההספק זהים ושונויות הרעש הם 1, הודות לכך שניתן להכיל כל מקרה אחר באמצעות המקדמים $\{h_{ij}\}$.

מתקיים:

$$SNR_1 = h_{11}^2 P$$
$$SNR_2 = h_{22}^2 P$$
$$INR_1 = h_{21}^2 P$$
$$INR_2 = h_{12}^2 P$$

באופן אינטואיטיבי, כל מקלט רואה ערוץ MAC.

<u>תזכורת</u>: *תחום הקיבול בערוץ* MAC

$$\underset{\text{Convex hull}}{\text{Closure}} \{R_1 \le I(X_1; Y | X_2), \quad R_2 \le I(X_2; Y | X_1), \quad R_1 + R_2 \le I(X_1; X_2 | Y)\}$$

ראינו בשיעורי בית: $C_1 = \max_{x_2, p(x_1)} I(X_1; Y_1 | X_2 = x_2)$

במקרה הגאוסי נוכל לבחור $x_2 \equiv 0$ ואז: $C_1 = C(SNR_1)$

חסמים

חסם פנימי טריוויאלי מתקבל מעיקרון ה- *Time Sharing* (משולש) וחסם חיצוני טריוויאלי ממודל של ערוצים מקבילים (מלבן).

אם y_1 מתייחס ל- x_2 כרעש אז: $R_1 \le I\left(X_1;Y_1\right)$. באותו אופן: $R_2 \le I\left(X_2;Y_2\right)$.

$Coded-Time\ Sharing: i=1,2$, $R_i \le I\left(X_i;Y_i \mid Q\right)$.

מקרה גאוסי: כל משתמש מגדיר ספר קוד גאוסי תוך התייחסות למשתנה האחר כרעש גאוסי: $R_i \le C\left(\frac{SNR_i}{1+INR_i}\right), i=1,2$

שכלול המודל: מקלט T_{Xi} מקבל כקלט מדידה y_i ואת ההפרעה x_j:

$$R_i \le I\left(X_i, Y_i \mid X_j, Q\right)$$

$$X_1 - Q - X_2$$

מקרה גאוסי: $R_i \le C\left(SNR_i\right)$

מה לגבי חסם על ה-*Sum Rate*?

ניצור שיתוף פעולה במודל: כל מקלט יקבל את זוג המדידות:

$R_1 + R_2 \le I\left(X_1, X_2; Y_1, Y_2 \mid Q\right)$ כאשר שוב מתקיים תנאי המרקוביות: $X_1 - Q - X_2$.

נותר לבצע אופטימיזציה על תחום הקיבול. לשם כך ניעזר ב-*Sato*:

נבחר $\tilde{p}\left(y_1, y_2 \mid x_1, x_2\right)$ שמקיים את הפילוגים השוליים הנתונים: $p\left(y_i \mid x_1, x_2\right)$.

כעת $I\left(X_1, X_2; Y_1, Y_2 \mid Q\right)$ מוגדר היטב בהינתן הפילוג: $p(q)\,p\left(x_1 \mid q\right)p\left(x_2 \mid q\right)$, ונוכל לבצע מקסימיזציה.

לאחר מכן, נבצע מינימיזציה על-פני תחומי קיבול שונים (חיתוך של כל התחומים) כדי לקבל חסם הדוק ככל האפשר.

<u>הערה</u>: אם $p\left(y_1 \mid x_1, x_2\right) = p\left(y_2 \mid x_1, x_2\right)$ אז כל מקלט רואה אותו מודל של *MAC* (ריאליזציית ערוץ שונה). כאשר נחפש לפי *Sato* $\tilde{p}\left(y_1, y_2 \mid x_1, x_2\right)$ שמקיים פילוגים שוליים נתונים, ניתן לבחור בפרט $y_1 = y_2$ ואז:

$\tilde{p}\left(y_1, y_2 \mid x_1, x_2\right) = p\left(y_1 \mid x_1, x_2\right) \cdot \delta\left(y_2 - y_1\right)$.

לסיכום:

$$R_1 \le \min\left\{I\left(X_1;Y_1 \mid X_2, Q\right), I\left(X_1;Y_2 \mid X_2, Q\right)\right\}$$

$$R_2 \le \min\left\{I\left(X_2;Y_1 \mid X_1, Q\right), I\left(X_2;Y_2 \mid X_1, Q\right)\right\}$$

$$R_1 + R_2 \le \min\left\{I\left(X_1;X_2 \mid Y_1, Q\right), I\left(X_1;X_2 \mid Y_2, Q\right)\right\}$$

קביעת התחום במקרה הגאוסי, למשל, הופך לבעיית מציאת ה- *CH* של כל חיתוכי זוגות של מחומשים.

נדון בסיטואציה שבה לא צריך לפענח את ההודעה של השני.

נציע מאורע שגיאה, שבו לא משנה לנו שגיאת פענוח בהודעה השנייה:

$$P_\varepsilon = \Pr\left\{\hat{W}_1 = w_1, \hat{W}_2 \ne w_2\right\}$$

ניתן להוכיח שאז תחום הקיבול יוצא כמו *MAC* שרואה את y_1.

נבחן את הבעיה בעוד שני מקרים מעניינים:

הפרעה חזקה מאוד

הפרעה חזקה

הפרעה חזקה מאוד:

$$I\left(X_1;Y_1 \mid X_2\right) \le I\left(X_1;Y_2\right)$$
$$I\left(X_2;Y_2 \mid X_1\right) \le I\left(X_2;Y_1\right)$$

בהפרעה חזקה, ניסיון של מקלט 2 לפענח את 2 הוא קשה, אבל לפענח את 1 אפשרי, על-אף שהוא לא מעניין אותו. יותר מכך, אי-השוויון מלמד ששערוך X_1 על-פי Y_1 בהינתן שההפרעה X_2 ידועה, ושערוך X_1 על-פי Y_2 בלבד, יעמוד באותו קריטריון טיב.

במקרה הגאוסי, התנאי מיתרגם לאי-שוויון: $SNR_1 \le \dfrac{INR_2}{1+SNR_2}$

לאחר קילוף הודעה 1 במקלט 2, חזרנו למודל ה- *Genie Aided*, ולכן זה חסם חיצון בר-השגה, כלומר תחום הקיבול מתואר לפי: $R_i = I\left(X_i;Y_i \mid X_j, Q\right)$, ושוב במקסימיזציה על פילוגים שמקיימים תנאי מרקובי.

הפרעה חזקה (לא מאוד)

$$I\left(X_1;Y_1 \mid X_2\right) \le I\left(X_1;Y_2 \mid X_2\right)$$
$$I\left(X_2;Y_2 \mid X_1\right) \le I\left(X_2;Y_1 \mid X_1\right)$$

$$\begin{aligned} I\left(X_1;Y_1 \mid X_2\right) &\le I\left(X_1;Y_2\right) = H\left(X_1\right) - H\left(X_1 \mid Y_2\right) = H\left(X_1 \mid X_2\right) - H\left(X_1 \mid Y_2\right) \\ &\le H\left(X_1 \mid X_2\right) - H\left(X_1 \mid Y_2, X_2\right) = I\left(X_1;Y_2 \mid X_2\right) \end{aligned}$$

במקרה הגאוסי:

$$SNR_1 \le INR_2$$
$$SNR_2 \le INR_1$$

תחום הקיבול עבור הפרעה חזקה:

$$R_1 \le I\left(X_1;Y_1 \mid X_2, Q\right)$$
$$R_2 \le I\left(X_2;Y_2 \mid X_1, Q\right)$$
$$R_1 + R_2 \le \min\left\{I\left(X_1;X_2 \mid Y_1, Q\right), I\left(X_1;X_2 \mid Y_2, Q\right)\right\}$$

מקרה גאוסי:

$$R_1 \le C\left(SNR_1\right)$$
$$R_2 \le C\left(SNR_2\right)$$
$$R_1 + R_2 \le \min\left\{C\left(SNR_1 + INR_1\right), C\left(SNR_2 + INR_2\right)\right\}$$

תחום הקצבים בני-ההשגה הטוב ביותר הידוע – Han-Kobayashi

מחלקים כל אחת מההודעות לשני חלקים:

- חלק פומבי – מפוענח בשני המפענחים
- חלק פרטי – מפוענח רק ע"י המפענח שבאמת מעונין בהודעה

מקבלים תחום קצבים שמורכב מתחומי הקצבים של שני ערוצי ה-MAC (ערוץ MAC לכל משתמש).