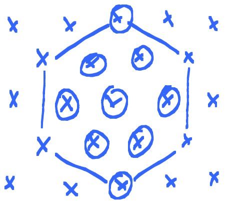
Tutorial - Part A Outline

1. Definitions: Partition, Construction — Vol(Λ), Modulo Λ
2. Figures of merit — $G(\Lambda)$
3. Dither & estimation — noise(Λ)
4. Entropy coding — $H(\Lambda)$
5. Infinite constellation — $Pe(\Lambda + \text{noise})$
6. Asymptotic goodness — $(n \to \infty)$
7. Error exponents
8. Nested lattices — $\Lambda_2 \subset \Lambda_1$
9. Lattice (Voronoi) shaping



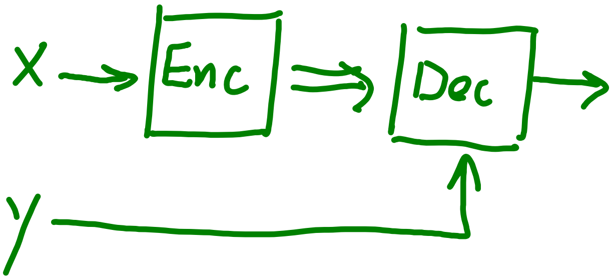
10. **Side-information problems** — Modulo$^2(\Lambda)$
11. Gaussian networks — Modulo$^n(\Lambda)$

Tutorial - Part A Outline

10. Side-information problems

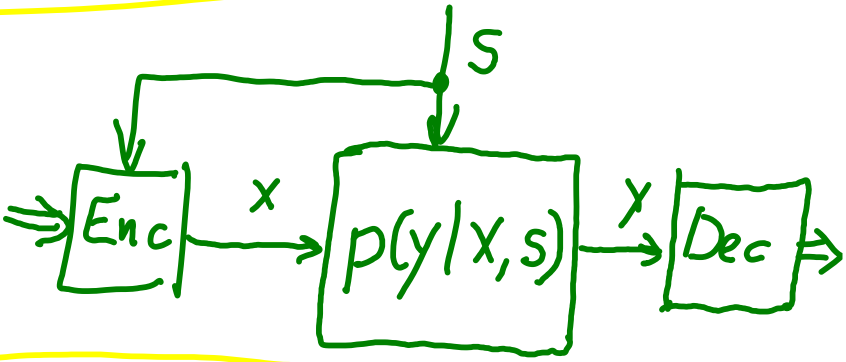
Modulo (Λ)

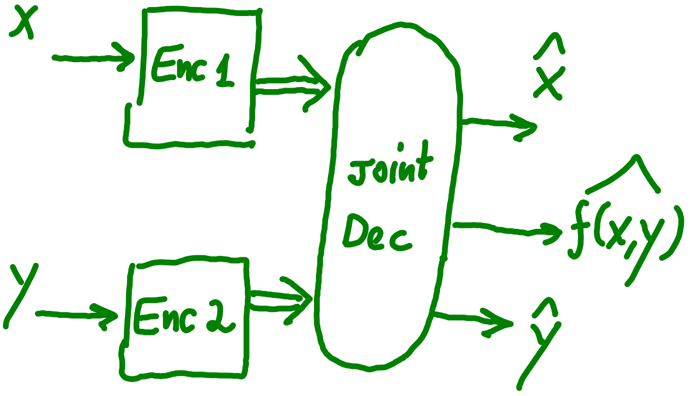
Lattices in Multi-Terminal Problems



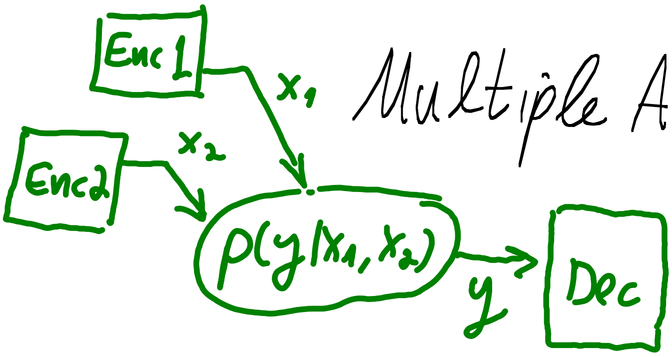
Source coding with Side Information

Channel Coding with Side Information

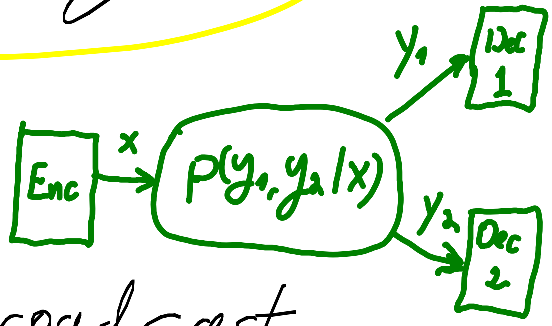




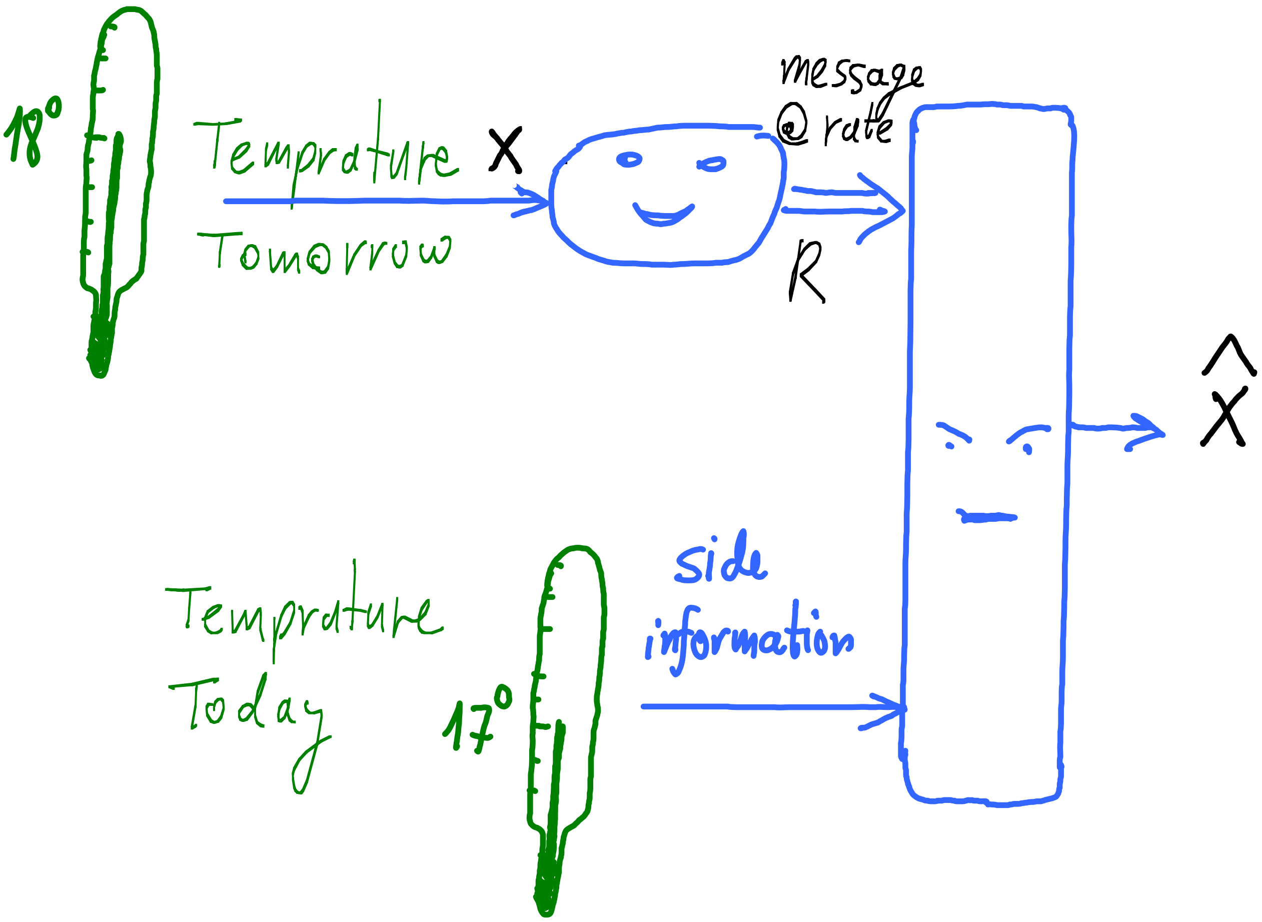
Multi-terminal Source coding



Multiple Access & Broadcast Channels



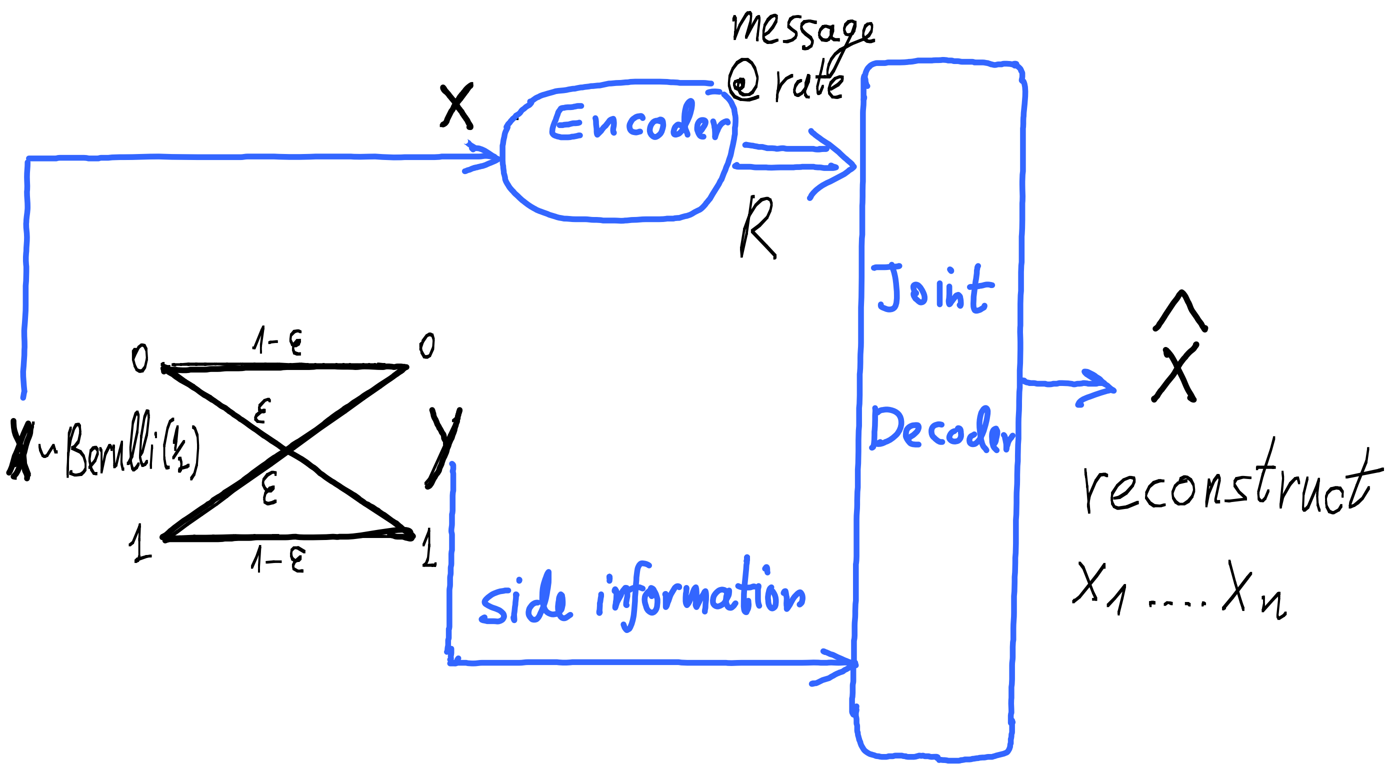
The Slepiàn-Wolf Problem



$$T_{tomorrow} = T_{today} \pm 1^{\circ}c$$

Can we send $T_{tomorrow}$ using only one bit?

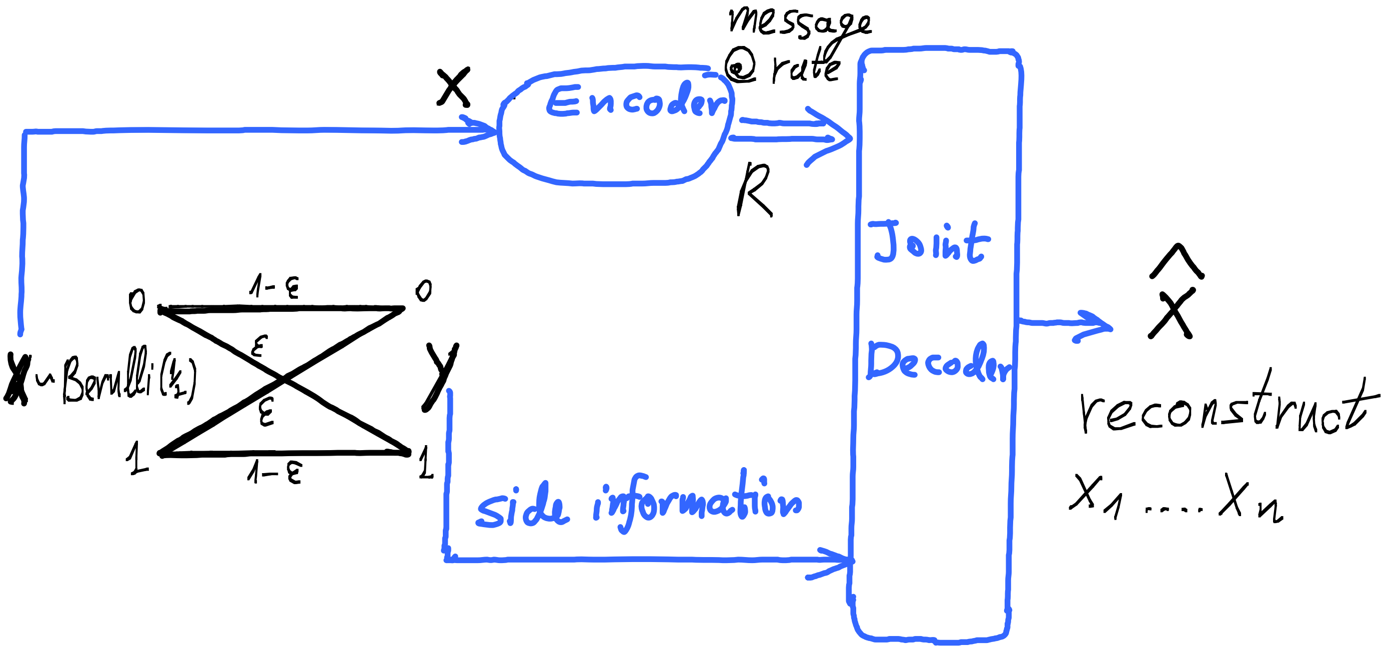
The Slepian-Wolf Problem



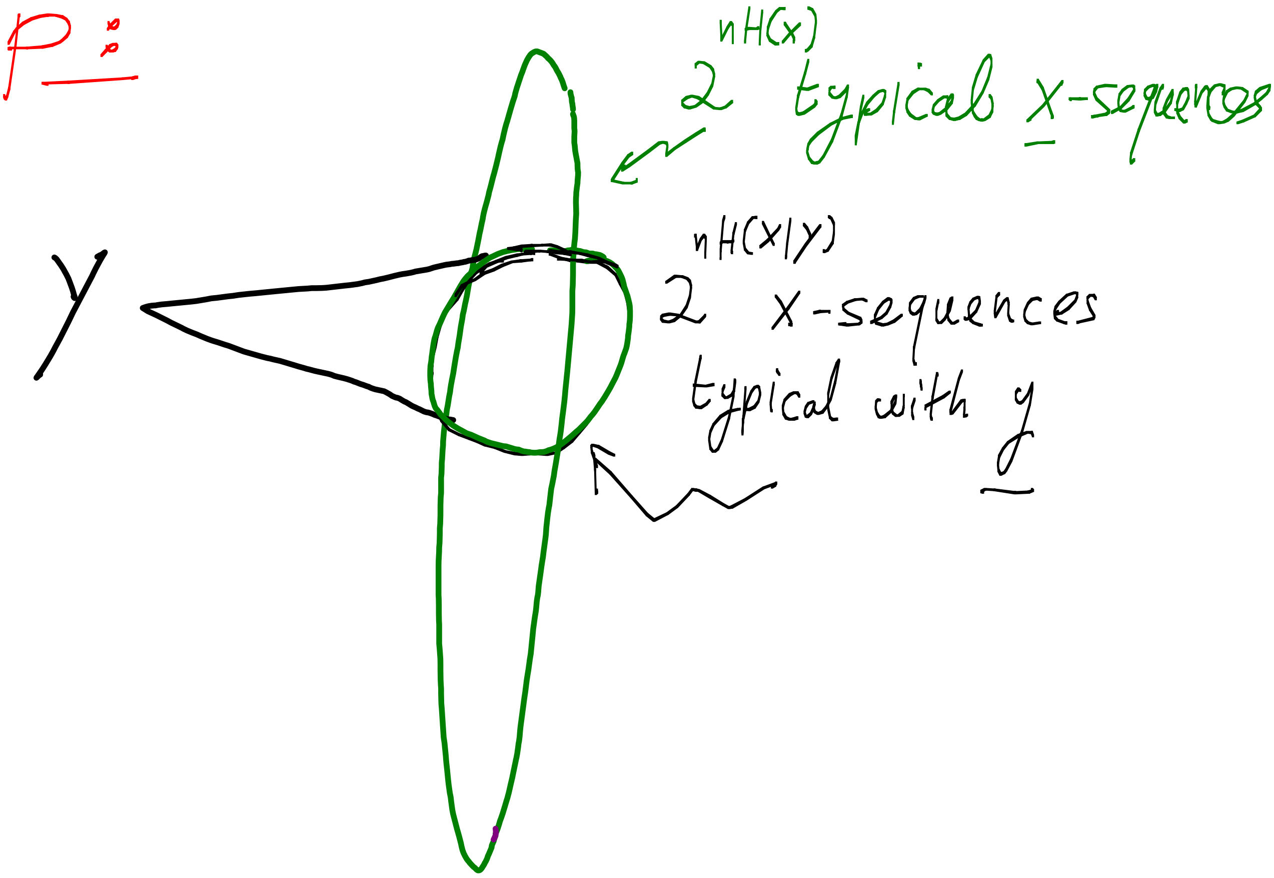
$$R = H(X|Y) = H(Z) = H_B(\varepsilon) = 0.1 \text{ Bit}$$

as if Y were available @ both encoder + decoder!

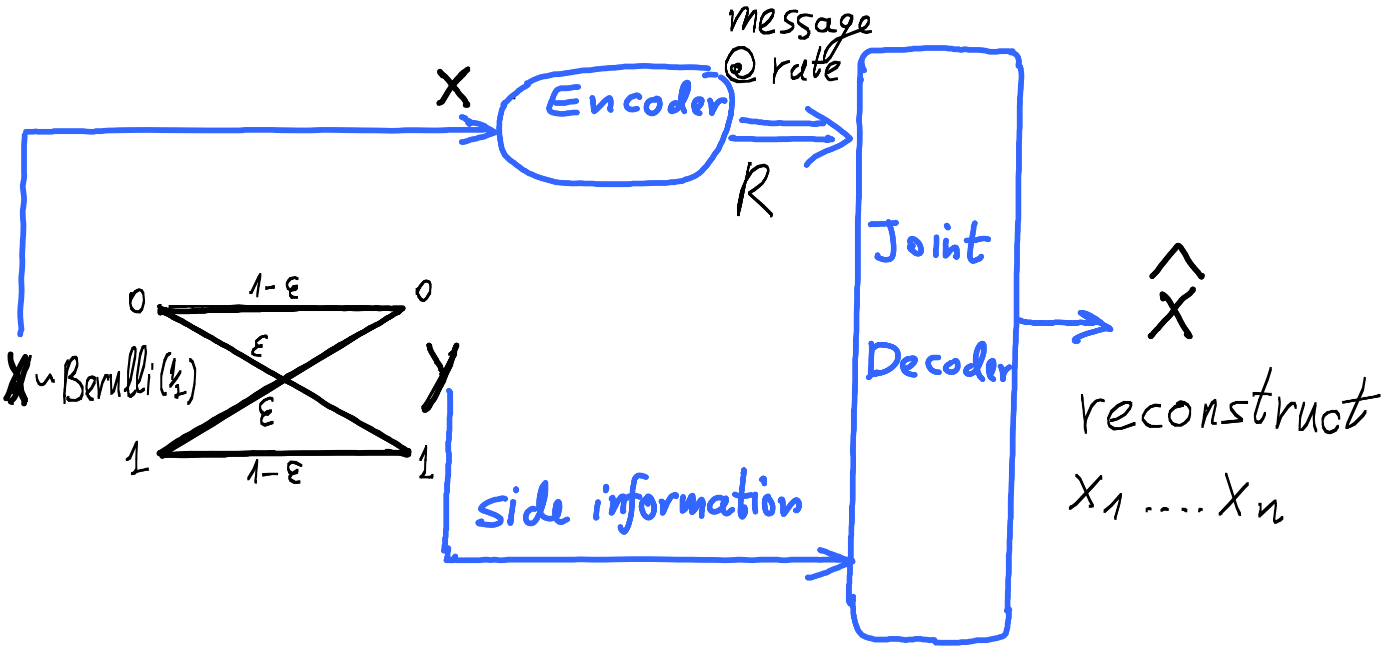
The Slepiàn-Wolf Problem

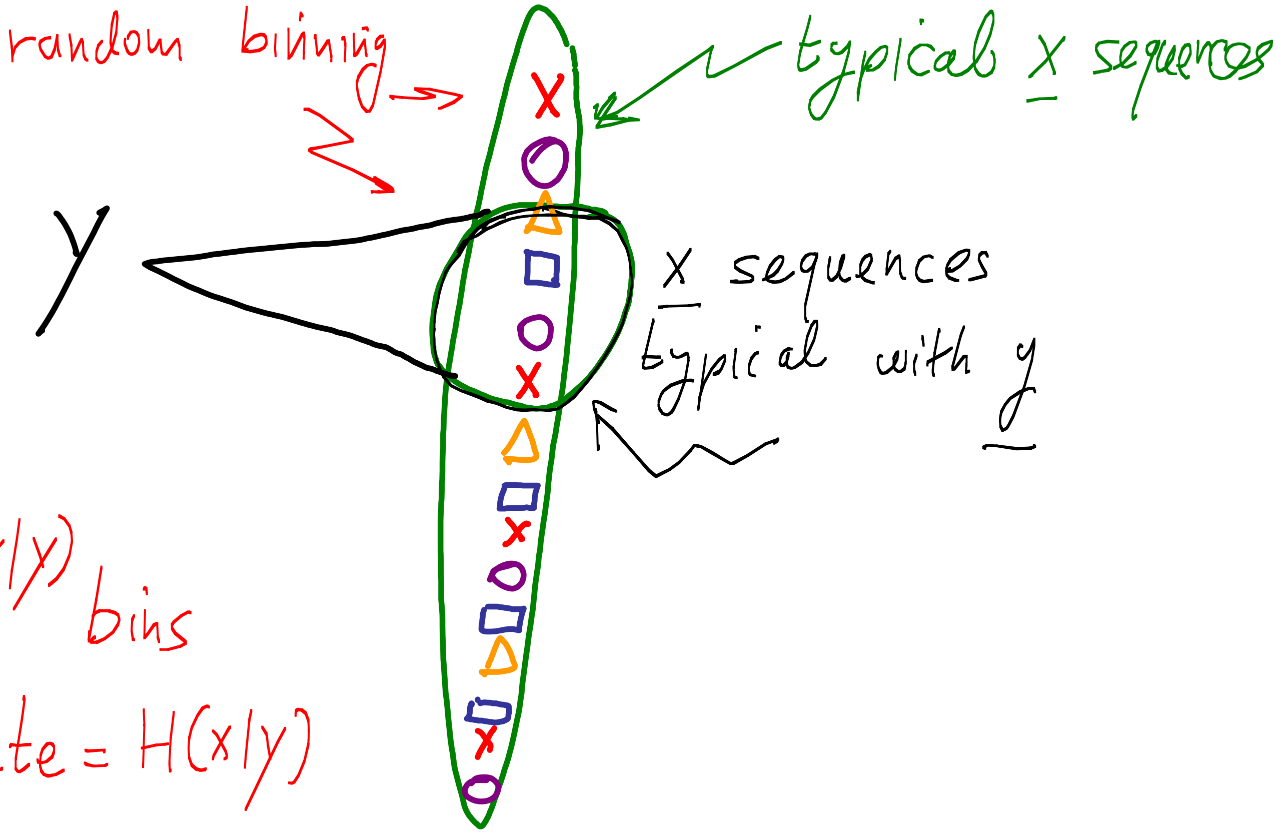


AEP:



The Slepian-Wolf Problem





$2^{nH(X|Y)}$ bins

$\Rightarrow$ Rate $= H(X|Y)$

Syndrome Coding

1. Good linear binary codes:

$\mathbb{C}$ = (n,k) linear code for B.S.C.(ε)

general properties: $k/n \simeq 1 - H_B(\varepsilon)$

generator matrix

$$\underset{n\times 1}{\underline{x}} = \underset{n\times k}{\underline{\underline{G}}} \cdot \underset{k\times 1}{\underline{i}}$$

parity-check

$$\underset{(n-k)\times n}{\underline{\underline{H}}} \cdot \underset{n\times 1}{\underline{x}} = \underline{0} \quad \text{for } \underline{x} \in \mathbb{C}$$

If $\underline{y} = \underline{x} \oplus \underline{z}$, where $\underline{z} \sim$ Bernulli(ε), then

$$\hat{\underline{z}}_{M.L.} = \text{error}(\underline{y}, \mathbb{C}) \triangleq f(\underbrace{H \cdot \underline{y}}_{s =\text{ syndrome of } \underline{y}}) = \underline{z} \quad \text{with high prob.}$$

$$P_e \underset{\uparrow}{=} Pr\{\hat{\underline{z}} \neq \underline{z}\} \longrightarrow 0$$

the same $\forall\ \underline{x} \in \mathbb{C}$

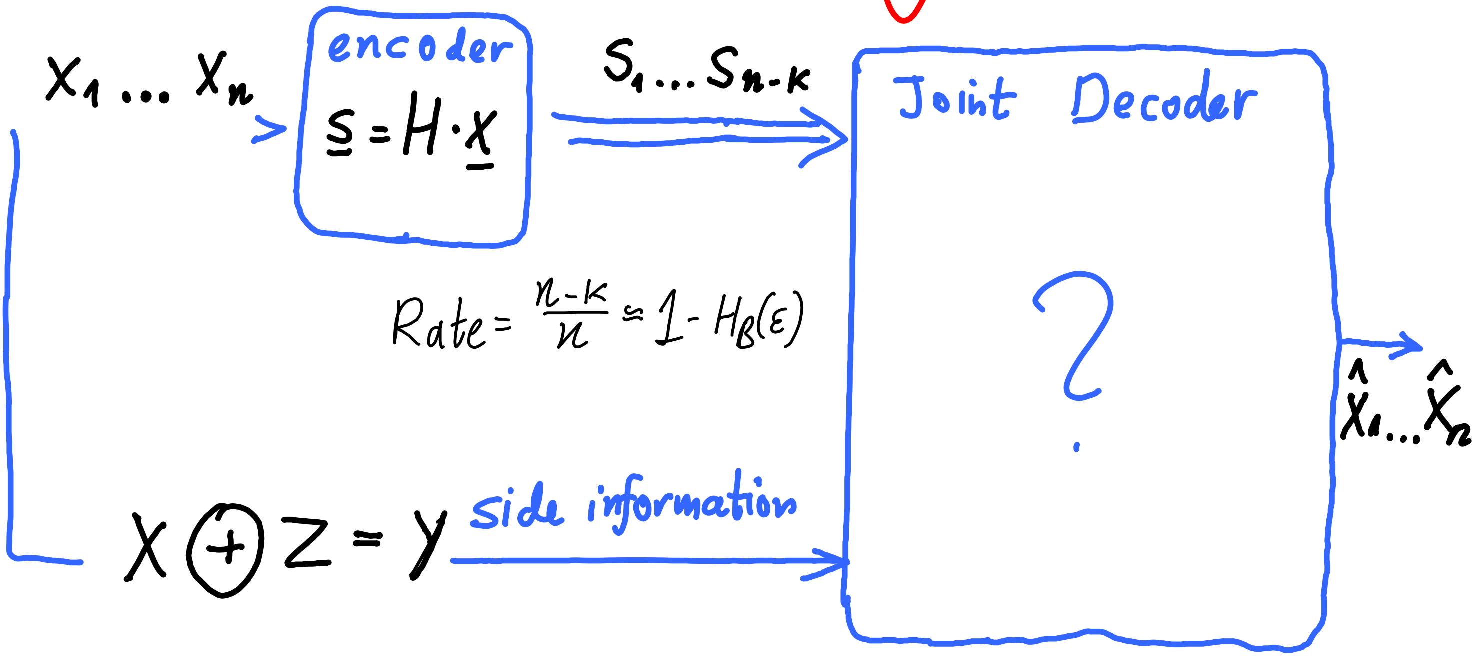
*** Def. Mod $\mathbb{C}$ ***

$$\text{error}(\underline{y}, \mathbb{C}) \triangleq \underline{y} \bmod \mathbb{C}$$

"coset leader of $\underline{y}$"

Syndrome Coding

2. -"- -"- for binary Slepian-Wolf:

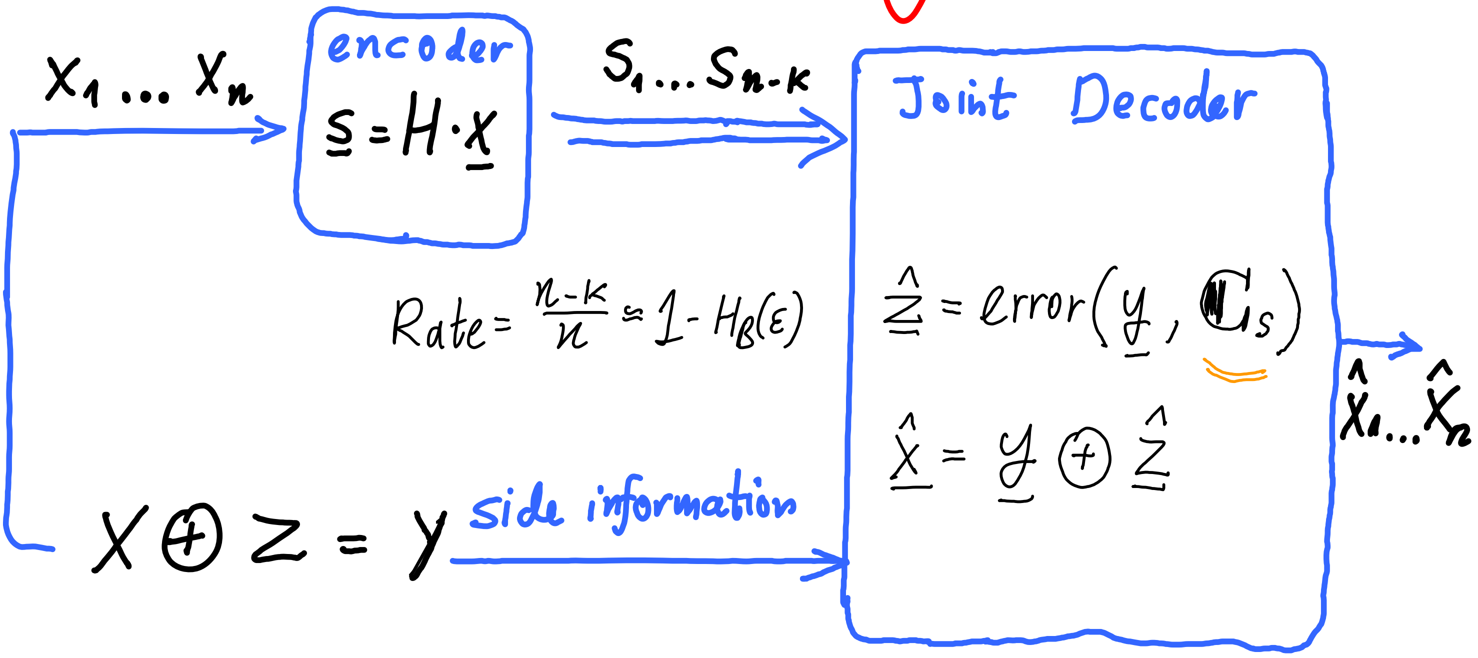


$$\text{Rate} = \frac{n-k}{n} \approx 1 - H_B(\varepsilon)$$

$$\mathbb{C}_s = \text{coset} \triangleq f(\underline{s}) \oplus \mathbb{C}$$

Syndrome Coding

2. -"- -"- for binary Slepian-Wolf:



$\mathbb{C}_s = \text{coset} = f(\underline{s}) \oplus \mathbb{C}$

Equivalent scheme

- **encoder:** $\text{message} = \underline{x} \bmod \mathbb{C}$
- **decoder:** $\hat{\underline{z}} = [(\underline{x} \underline{\bmod \mathbb{C}}) \oplus \underline{y}] \underline{\bmod \mathbb{C}}$

distributive law

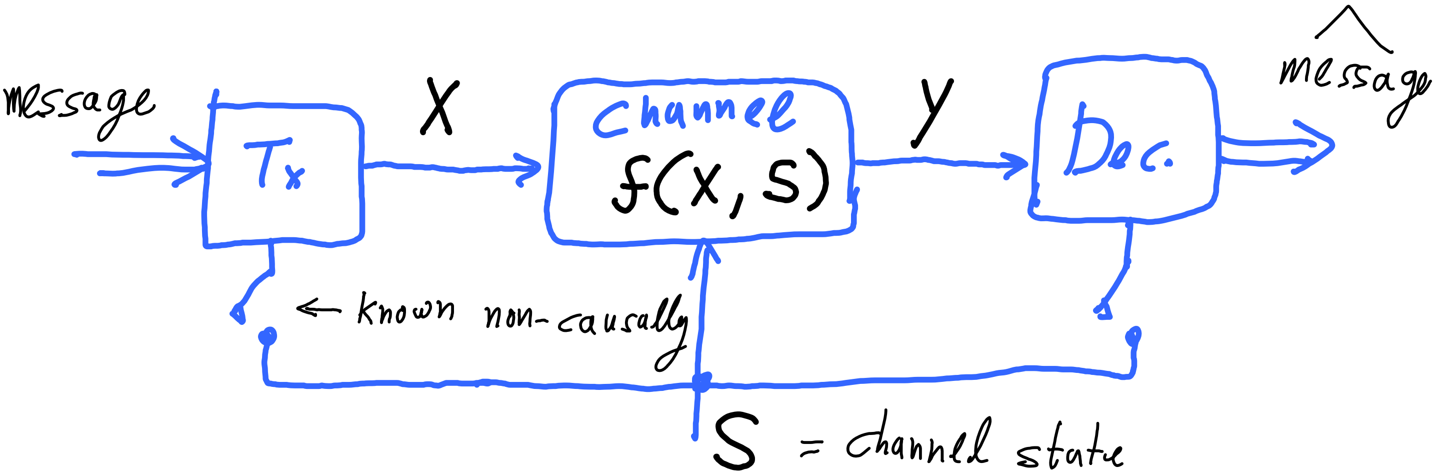
$= (\underline{x} \oplus \underline{y}) \bmod \mathbb{C}$

$= \underline{z} \bmod \mathbb{C}$

$= \underline{z}$ w. h. prob.

Deterministic Channels with State known at Transmitter

(the Gelfand-Pinsker [1980] problem)



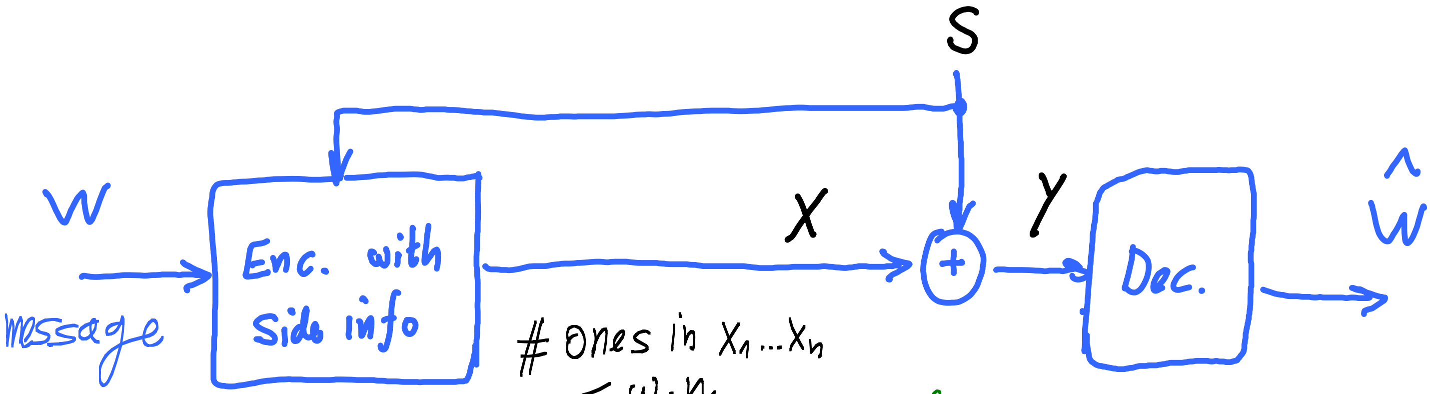
$$C_{SI@\underline{Tx}} = C_{SI@\underline{Both}} = \max_{\{\text{allowed } p(x)\}} H(y|S)$$

Examples:

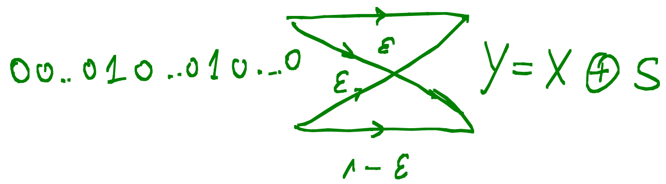
1. Hiding a binary "secret" in integer numbers
2. Memory with defects known at encoder
3. Hamming-constrained B.S.C. with known noise

Deteministic Gelfand-Pinsker Problem

(binary dirty-paper channel)

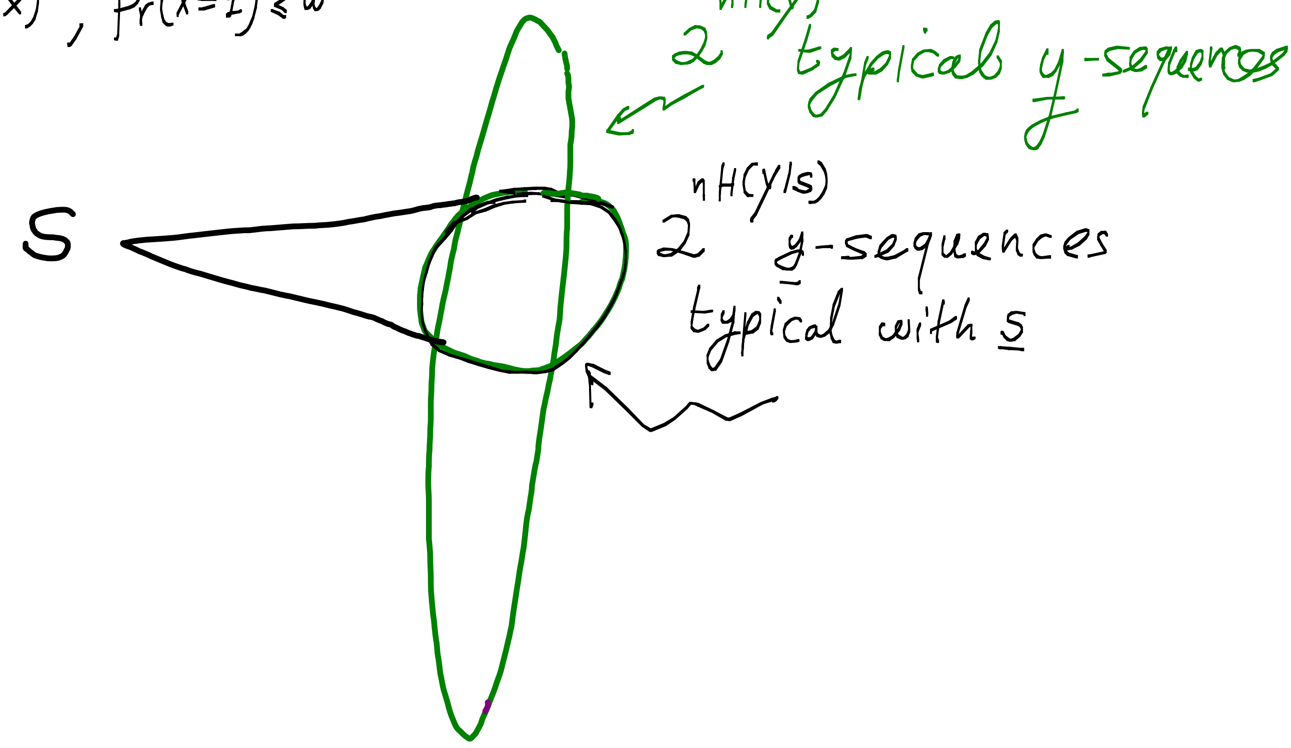


$\#$ ones in $X_1 \dots X_n$ $\leq w \cdot n$



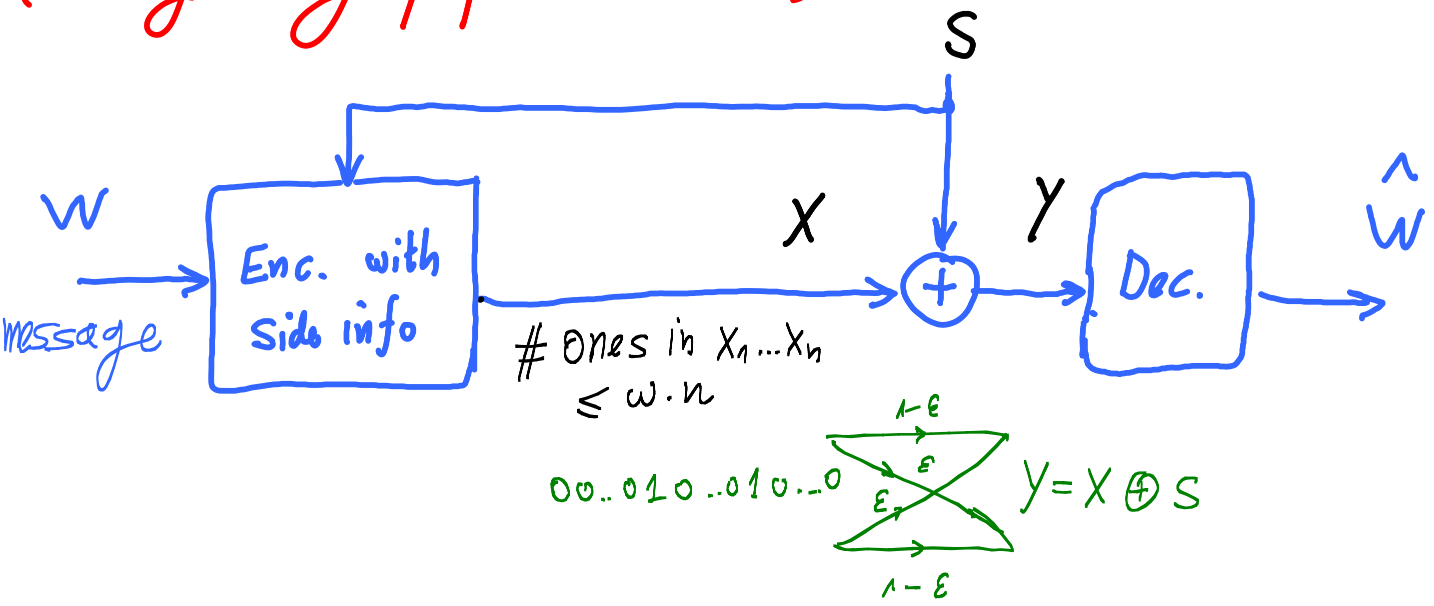
AEP:

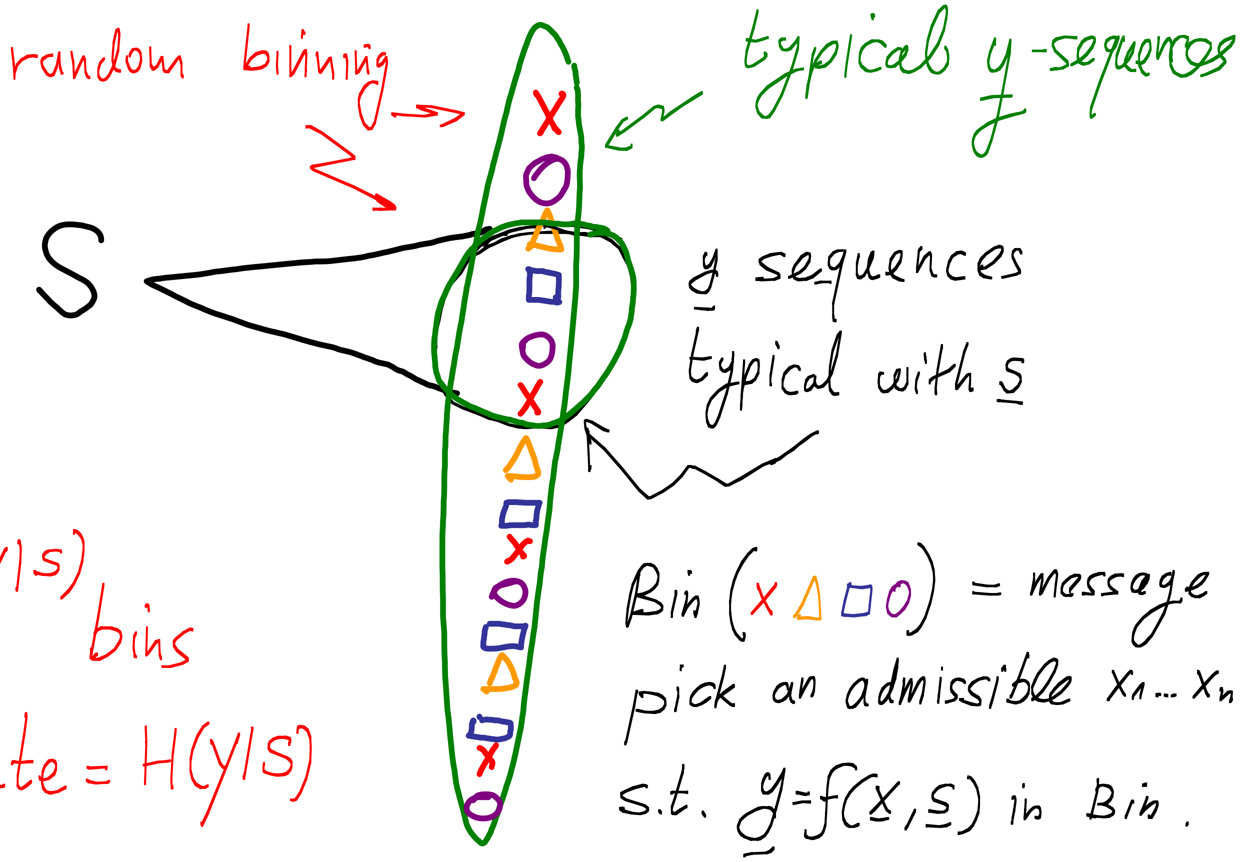
$X \sim p(x)$, $Pr(X=1) \leq w$



Deteministic Gelfand-Pinsker Problem

(binary dirty-paper channel)





$2^{nH(y|s)}$ bins

$\Rightarrow$ Rate $= H(y|S)$

Bin(x △ □ ○) = message

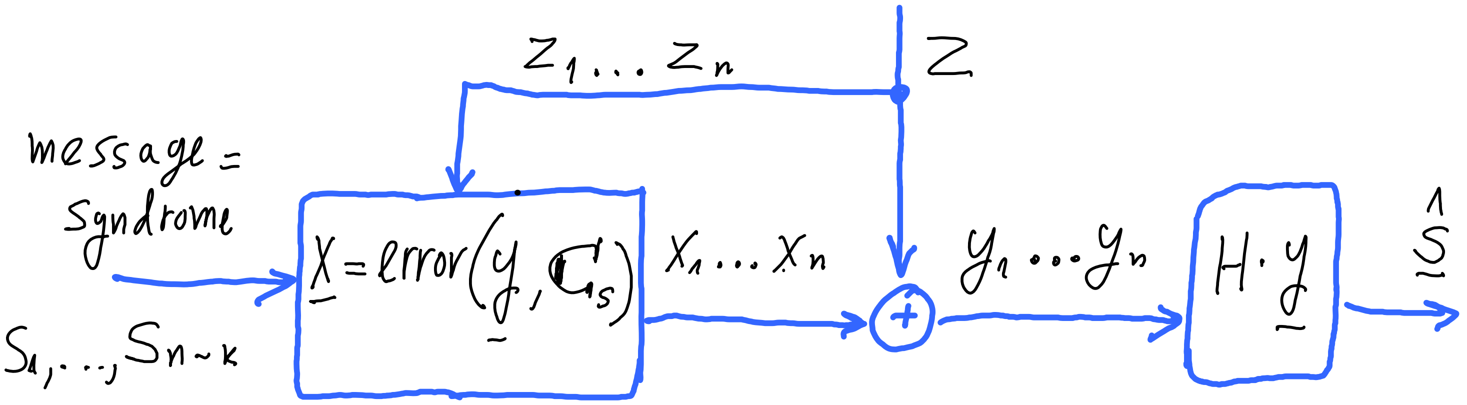
pick an admissible $x_1 \dots x_n$

s.t. $\underline{y} = f(\underline{x}, \underline{s})$ in Bin.

Syndrome Coding

3. -"- -"- for binary dirty-paper coding

$\mathbb{C}$ is a good binary quantizer:
for Bernoulli (1/2) source Z, at Hamming distortion D,
$E\{\underline{Z} \bmod \mathbb{C}\} = D$, $Rate = \frac{k}{n} \approx 1 - H_B(D)$



Set $D = w \Rightarrow \begin{cases} \text{Hamming input constraint} = w \\ Rate = \frac{n-k}{n} \approx H_B(w) = H(X) = H(Y|Z) \end{cases}$

equivalently:

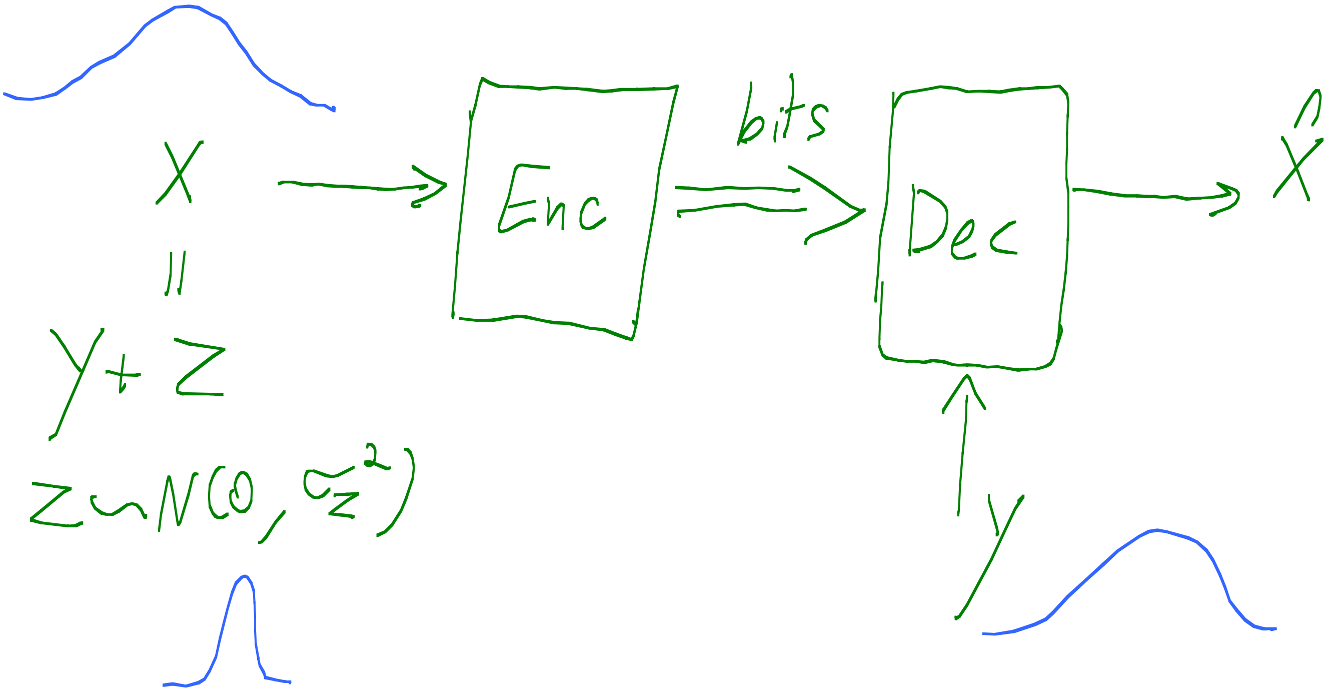
$\underline{v} = f(\underline{s}) \rightarrow \underline{v} \oplus \underline{z} \bmod \mathbb{C} \longrightarrow \overset{\downarrow \underline{z}}{\oplus} \longrightarrow \bmod \mathbb{C} \longrightarrow \hat{\underline{v}}$

$\Longrightarrow \hat{\underline{v}} = \left[(\underline{v} + \underline{z}) \underline{\bmod \mathbb{C}} \oplus \underline{z} \right] \underline{\bmod \mathbb{C}} = \underline{v}$

Two-Terminal Extensions

Noisy extensions ...

The Wyner - Ziv Problem
(Lossy Source Coding with S.I. @ Decoder)

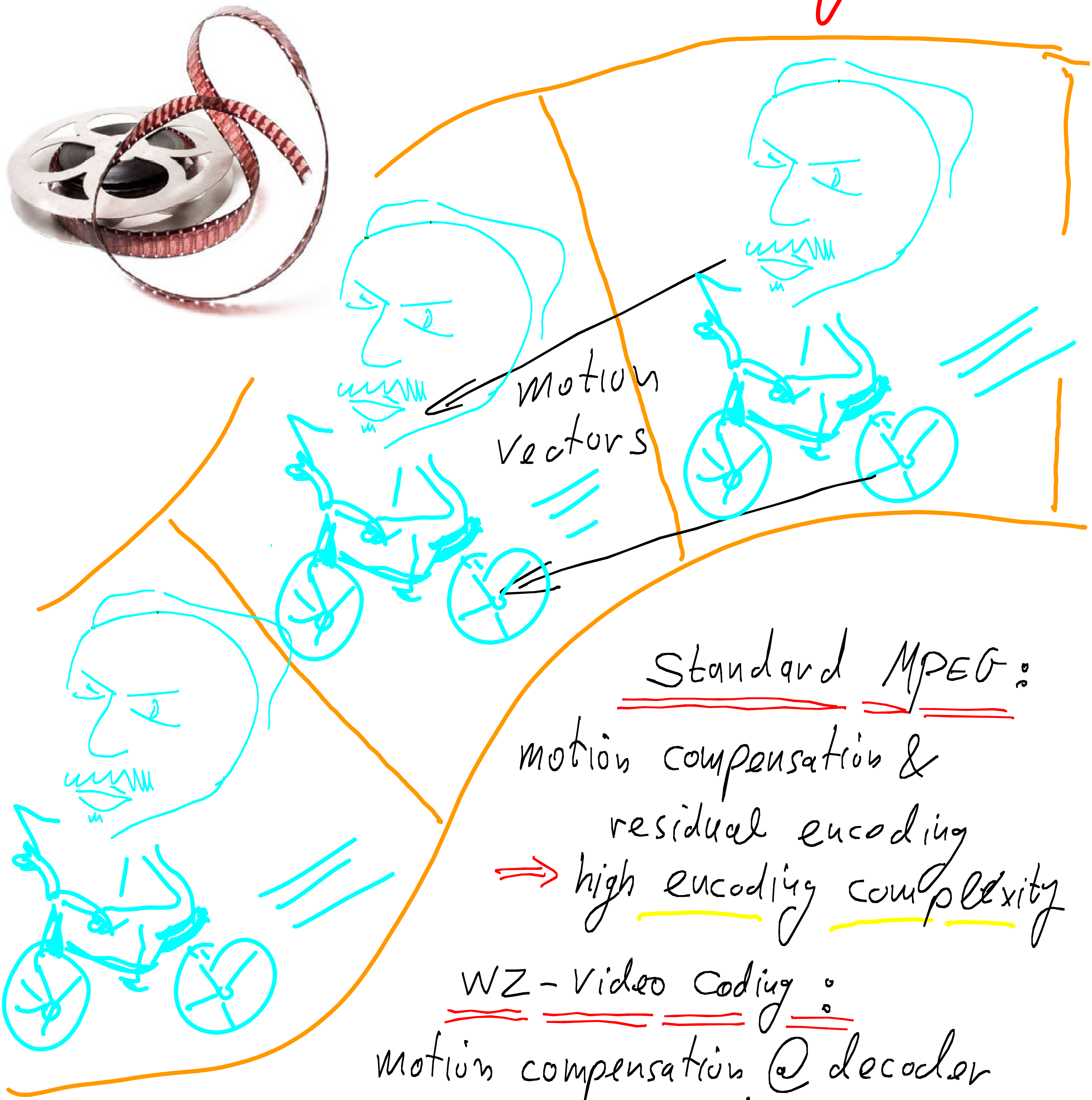


$$R^{WZ}_{X|Y}(D) = R_Z(D) = \frac{1}{2}\log\left(\frac{\sigma_z^2}{D}\right) \quad \frac{\text{bit}}{\text{source sample}}$$

Wyner-Ziv 1976

Wyner 1978

Wyner-Ziv Video Coding



Standard MPEG:

motion compensation & residual encoding

⇒ high encoding complexity

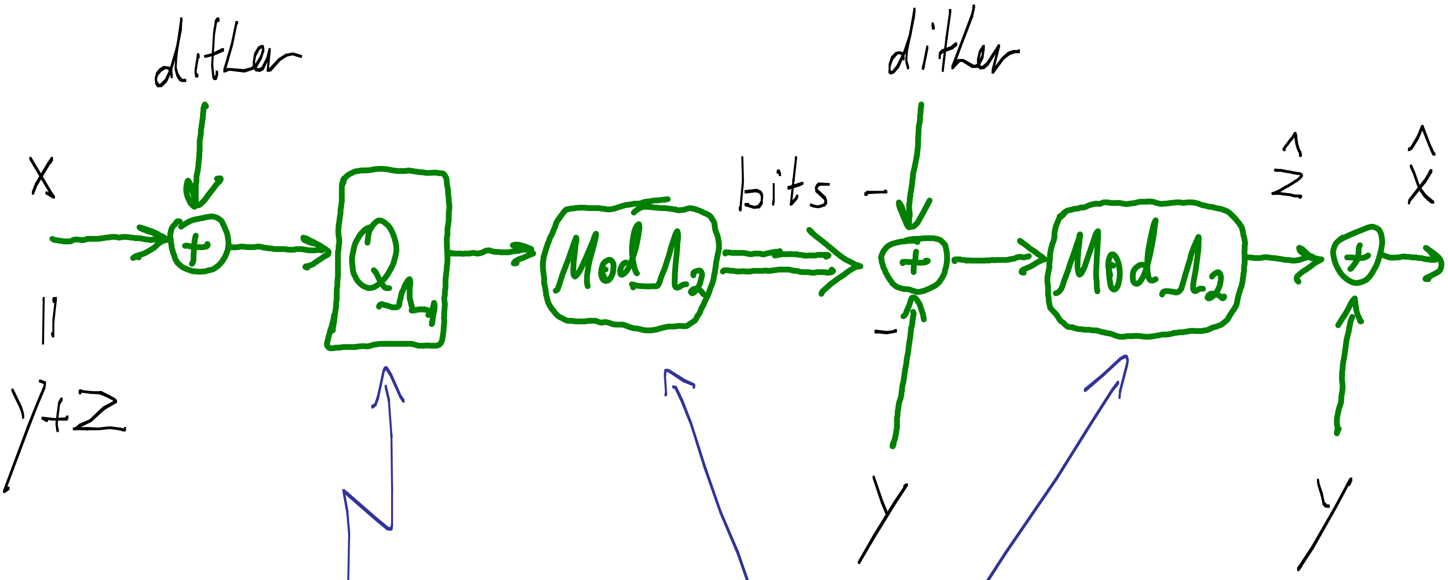
WZ-Video Coding:

motion compensation @ decoder

⇒ encoding = simple / deoding = complex

Lattice Wyner-Ziv Coding

[Z & Shamai Verdu]

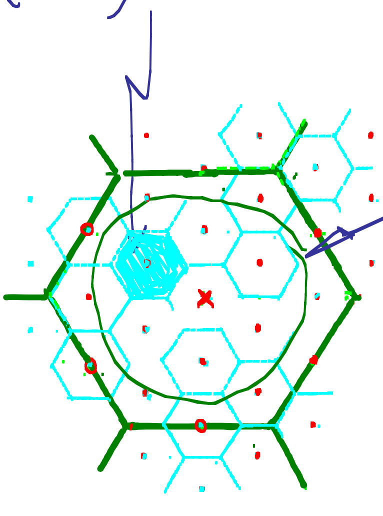


Good quantizer for desired distortion:

$\sigma^2(\Lambda_1) = D$

Good channel code for the noise Z:

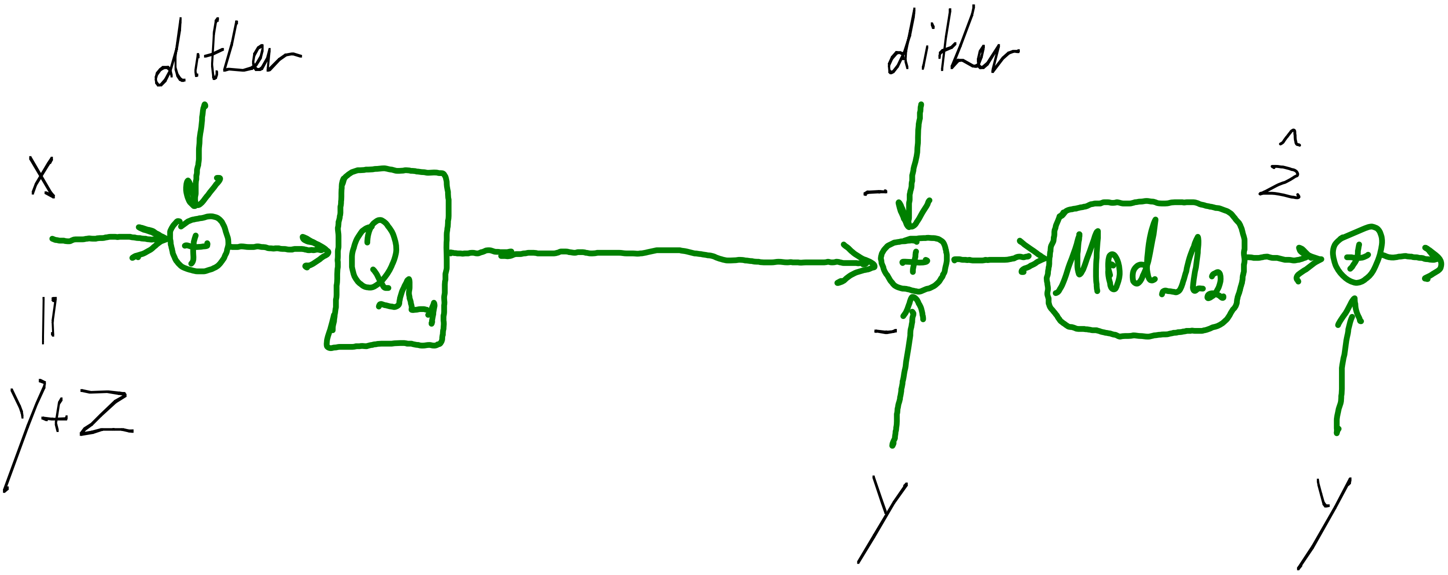
$Pe(\Lambda_2, \sigma_Z^2) < \varepsilon$



Lattice Wyner-Ziv Coding

$$(A \bmod \Lambda + B) \bmod \Lambda = (A+B) \bmod \Lambda$$

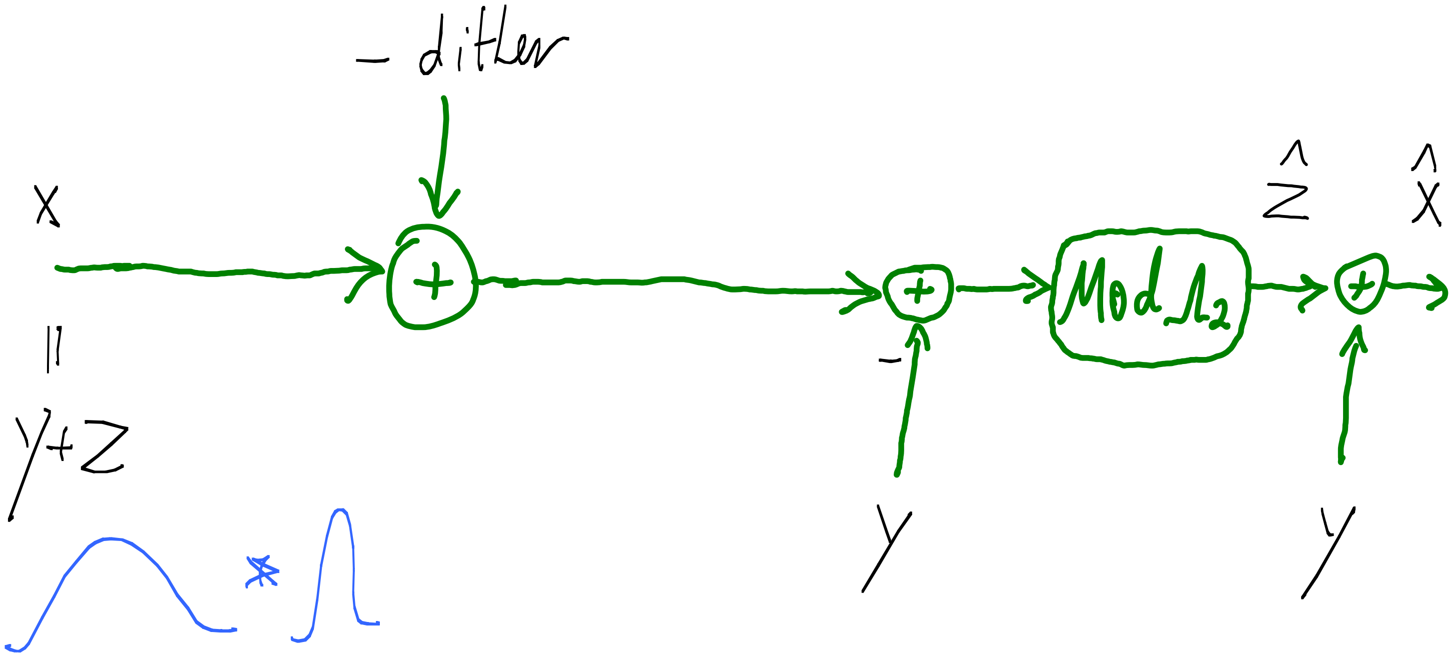
$\Longrightarrow$



Lattice Wyner-Ziv Coding

dithered quantization ≡ additive noise

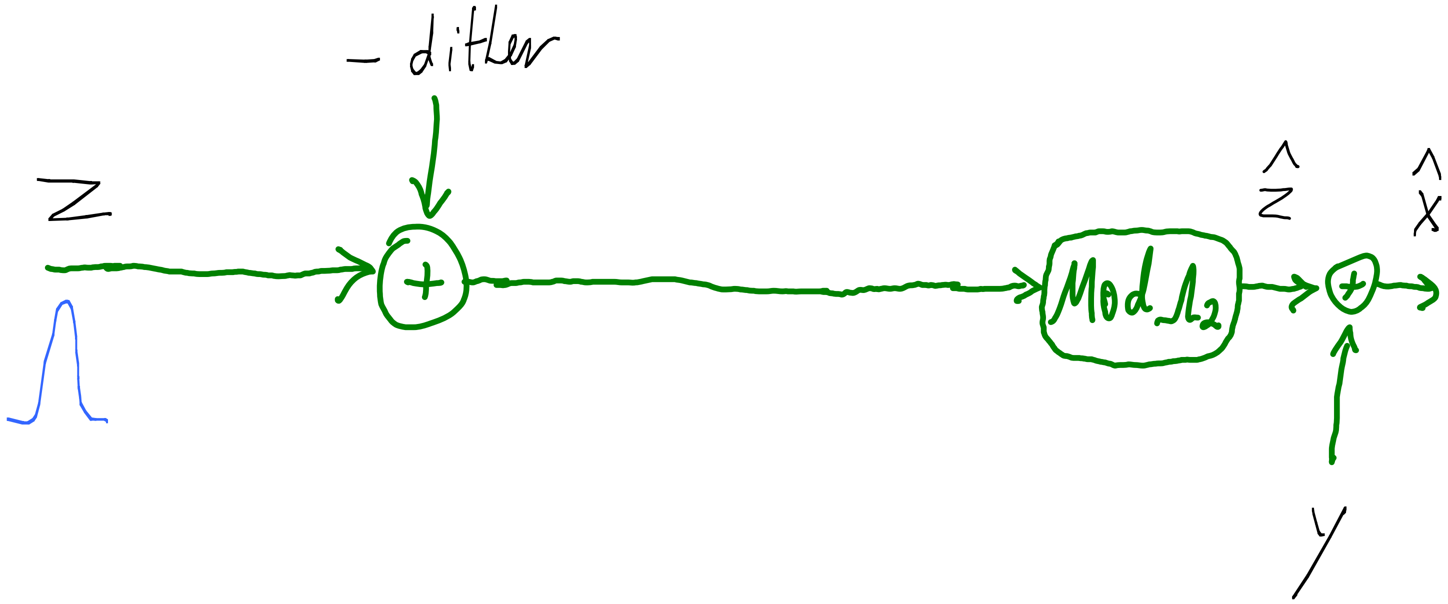
⇒



Lattice Wyner-Ziv Coding

dithered quantization ≡ additive noise

⟹

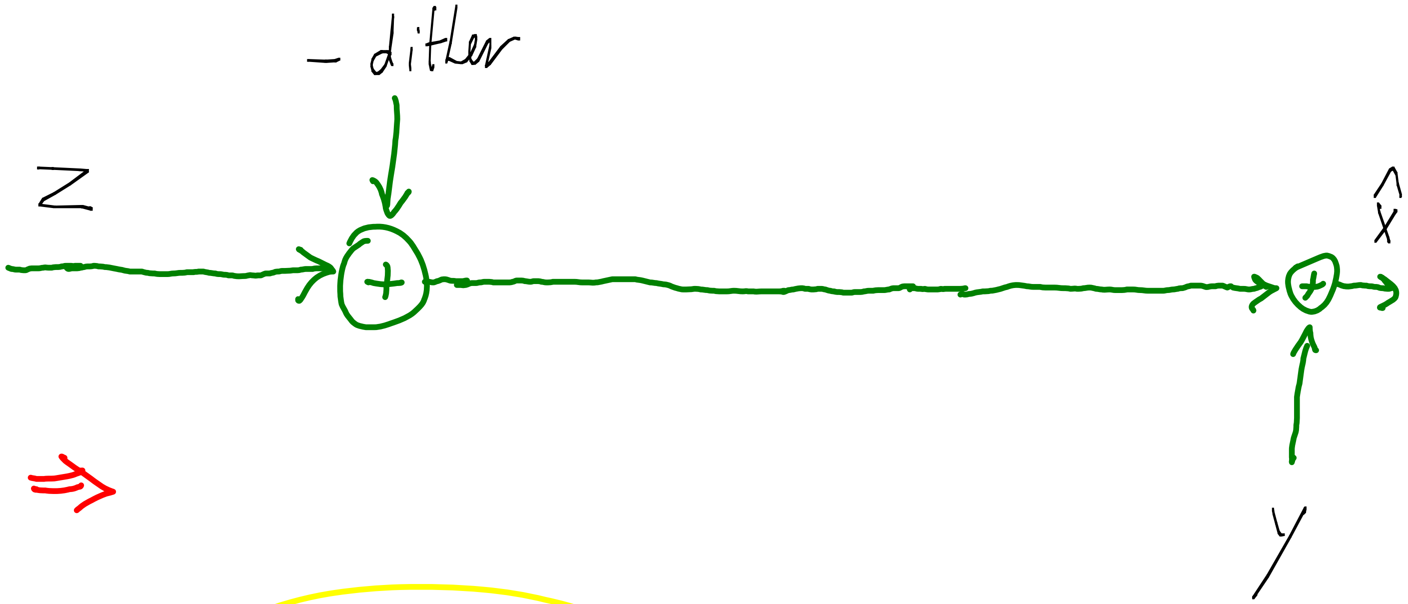


Lattice Wyner-Ziv Coding

Λ_2 = good channel code for $Z \sim \mathcal{N}(0, \sigma_Z^2)$.

$D \ll \sigma_Z^2$.

$\Rightarrow$ with prob. $> 1-\varepsilon$,



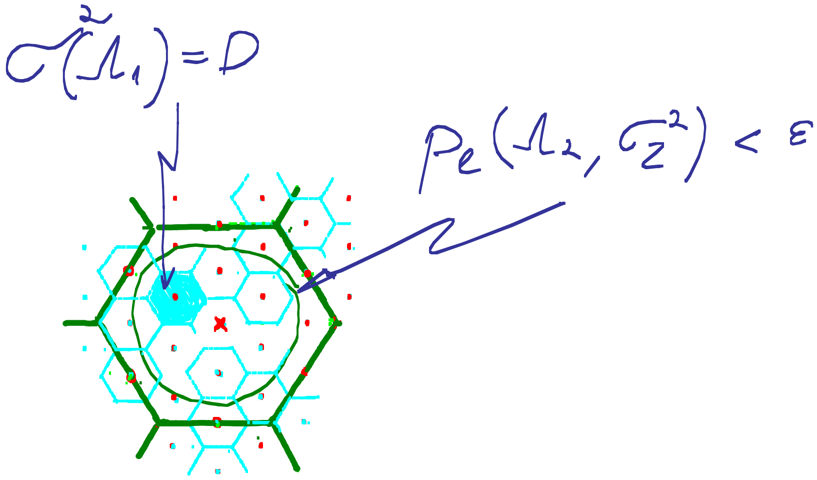
$\Rightarrow$

$\hat{X} = X - \text{dither}$, w.p. $> 1-\varepsilon$

$\Rightarrow$ distortion $= \sigma^2(\Lambda_1) = D$

Lattice Wyner-Ziv Coding

Nesting Ratio:



$\Longrightarrow$

$$\text{Rate} = \frac{1}{k}\log\left(\frac{V_2}{V_1}\right) \text{ bit/sample}$$

$$= \underbrace{\frac{1}{2}\log\left(\frac{\sigma_Z^2}{D}\right)}_{R_Z(D)} + \underbrace{\frac{1}{2}\log\left(G(\Lambda_1)\cdot\mu(\Lambda_2,\varepsilon)\right)}_{\text{Redundancy} \to 0}$$

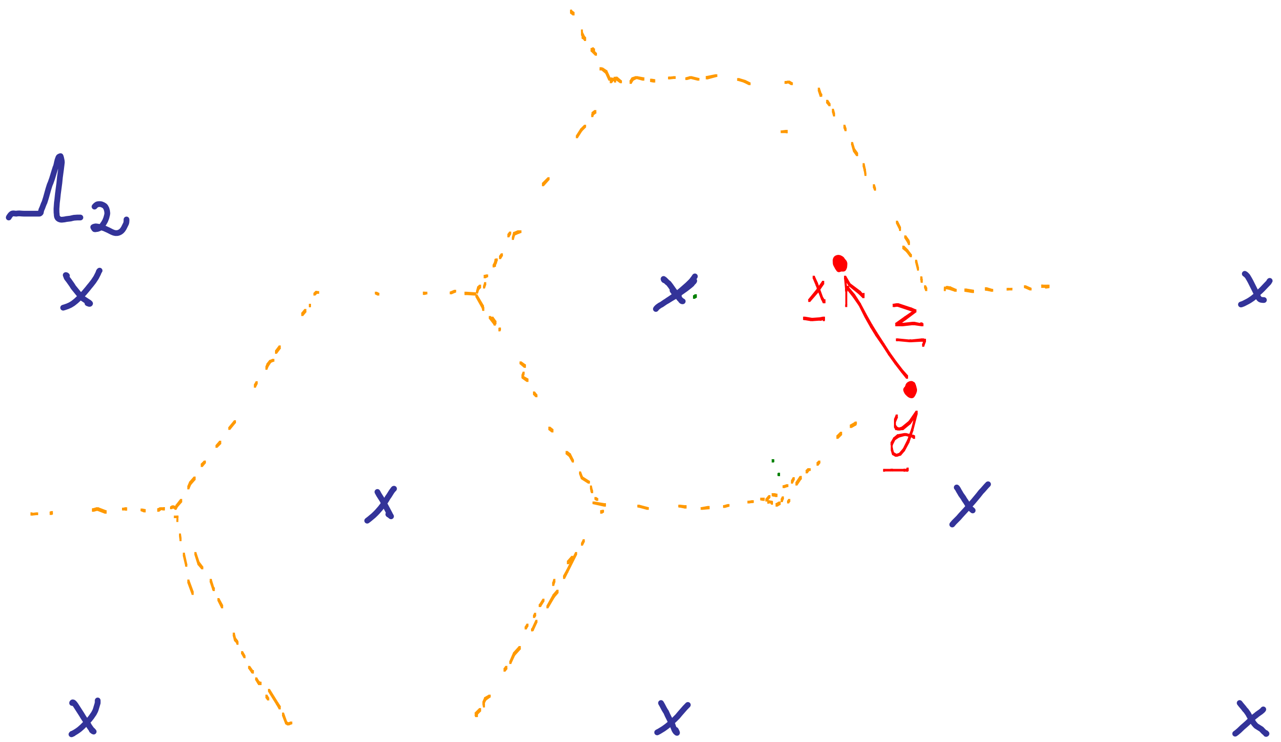
NSM (Λ_1)

VNR (Λ_2)

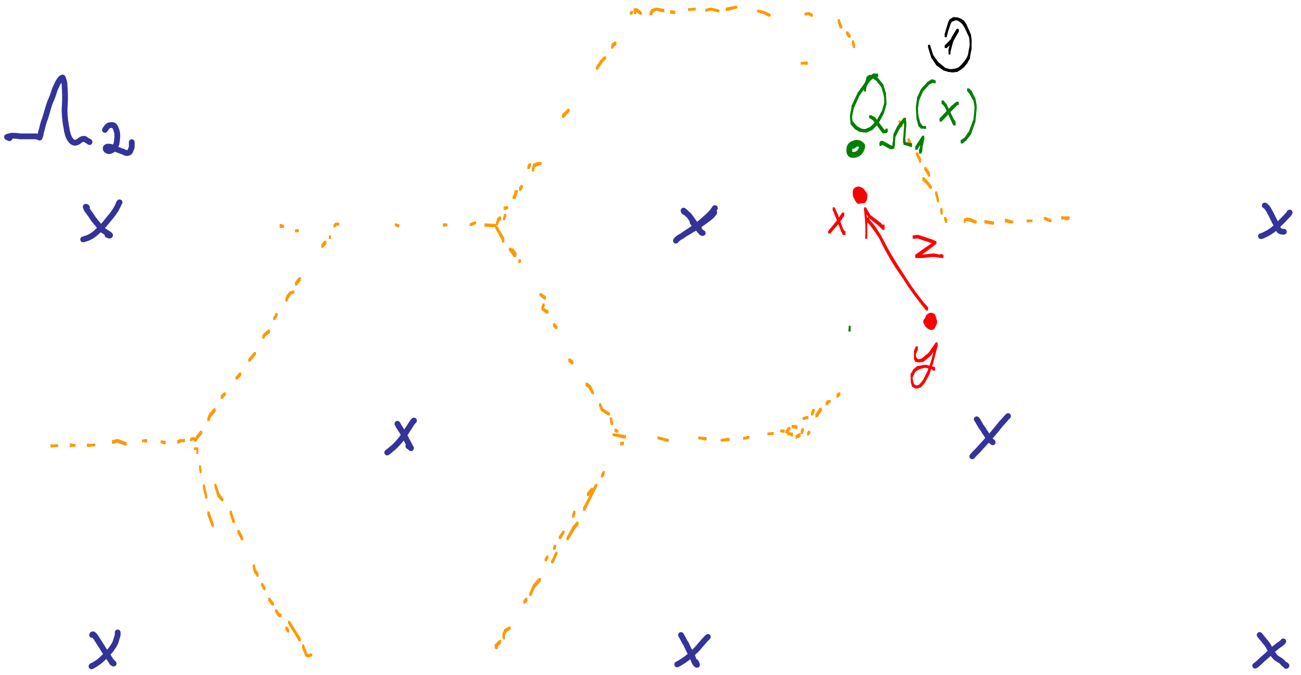
$k \to \infty$

for good lattices ....

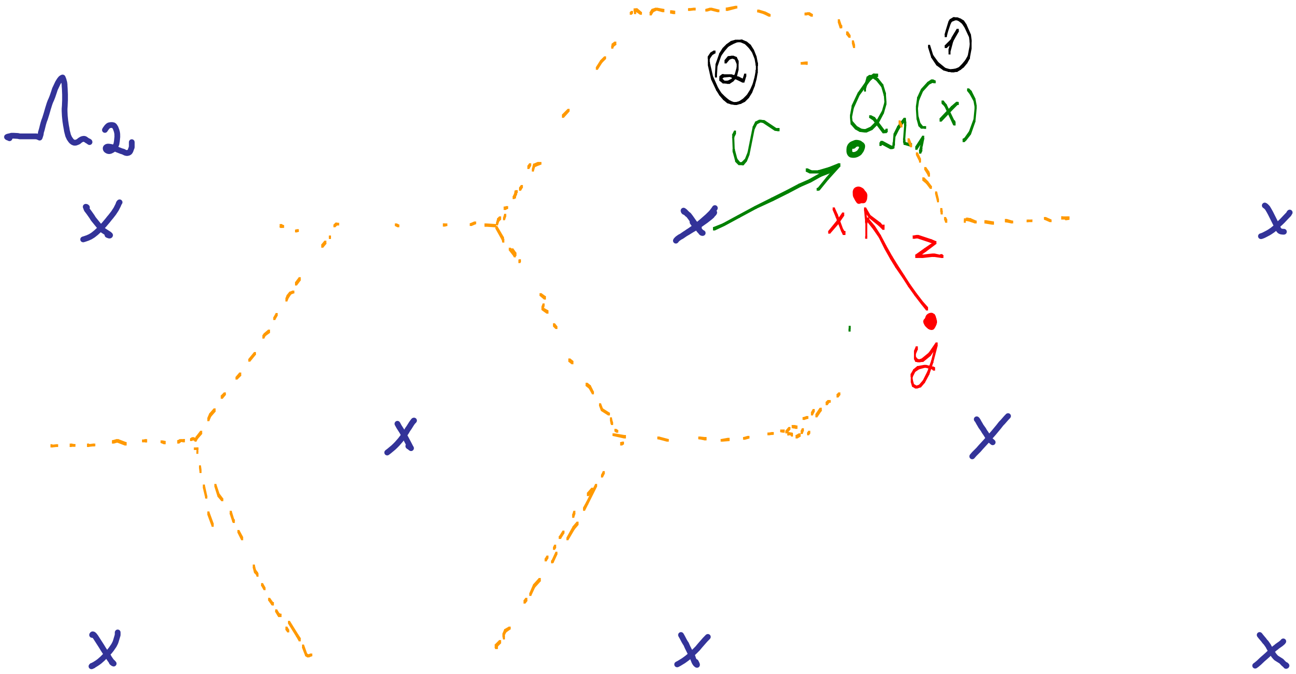
Geometric Picture in Signal Space



Geometric Picture in Signal Space

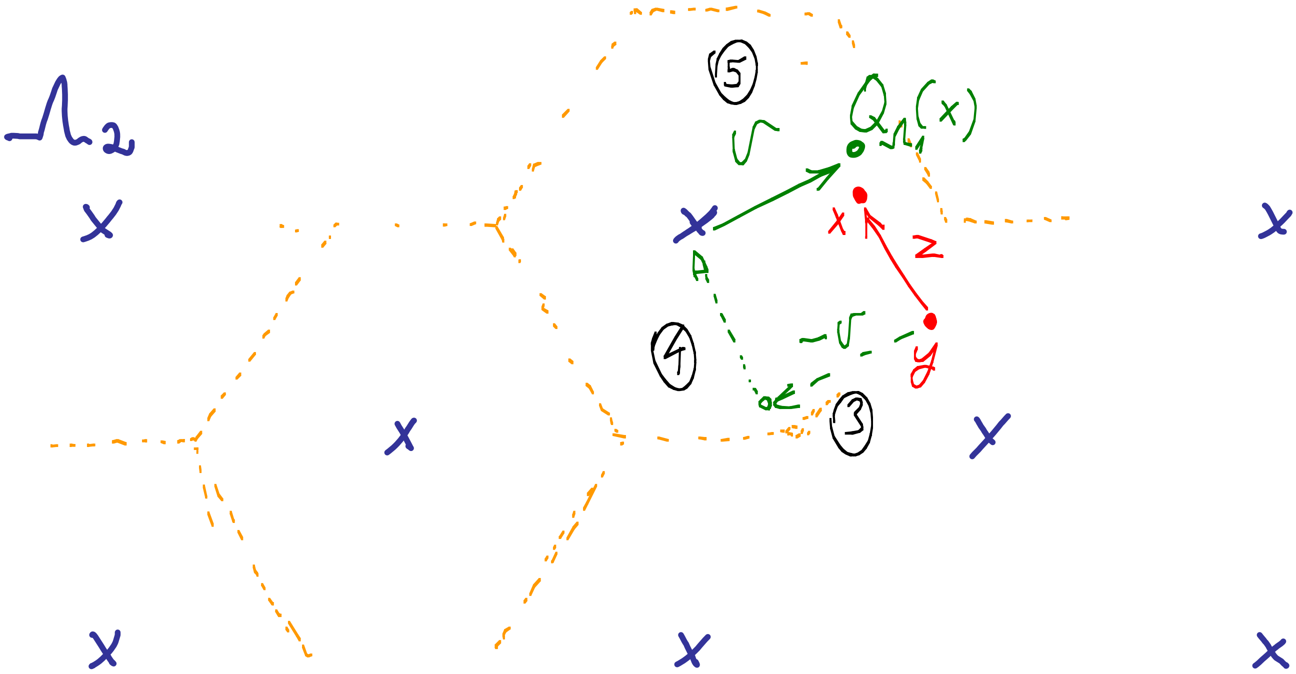


Geometric Picture in Signal Space

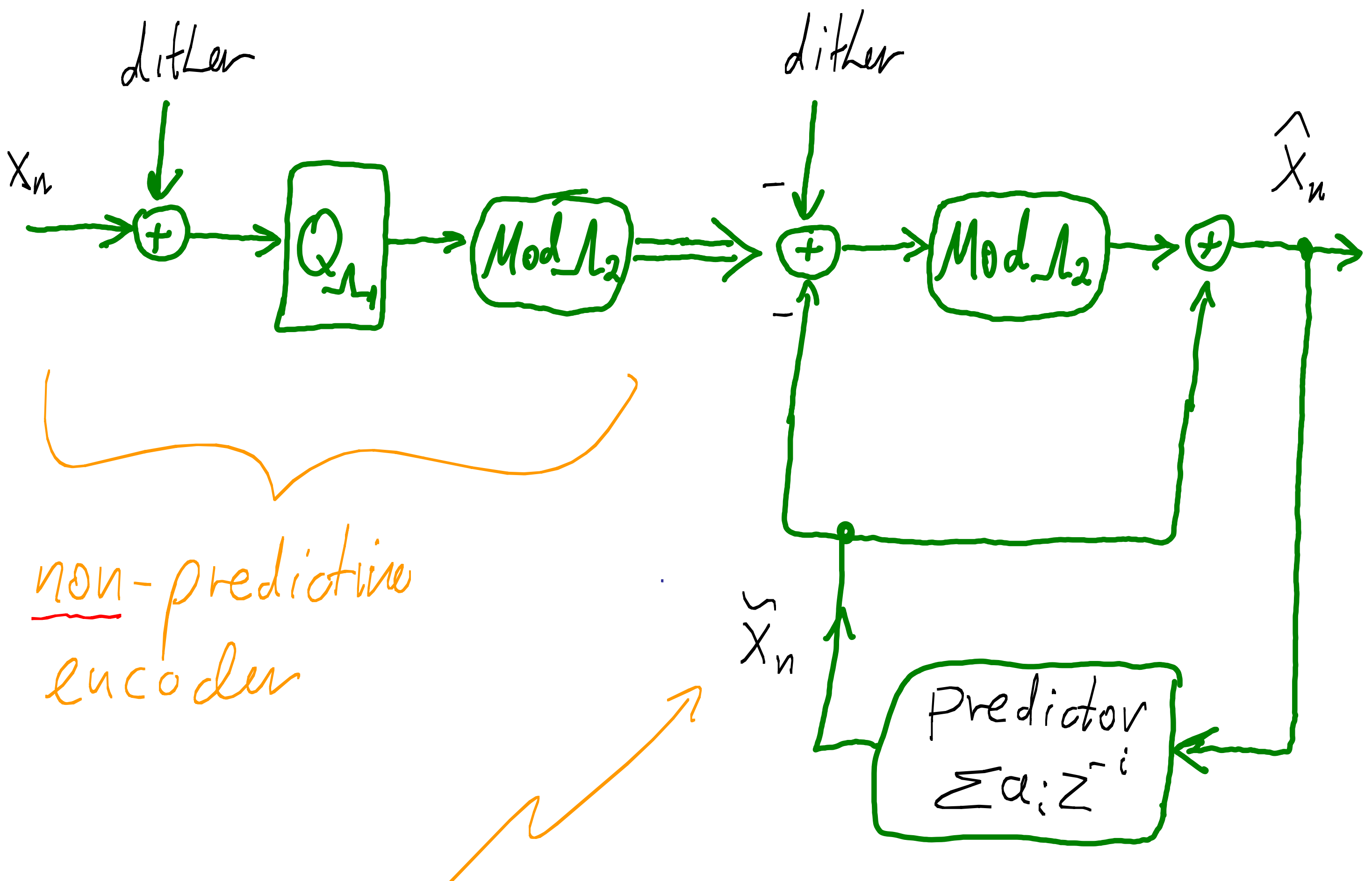


v = relative coset ("syndrome")

Geometric Picture in Signal Space



Wyner-Ziv - D.P.C.M.

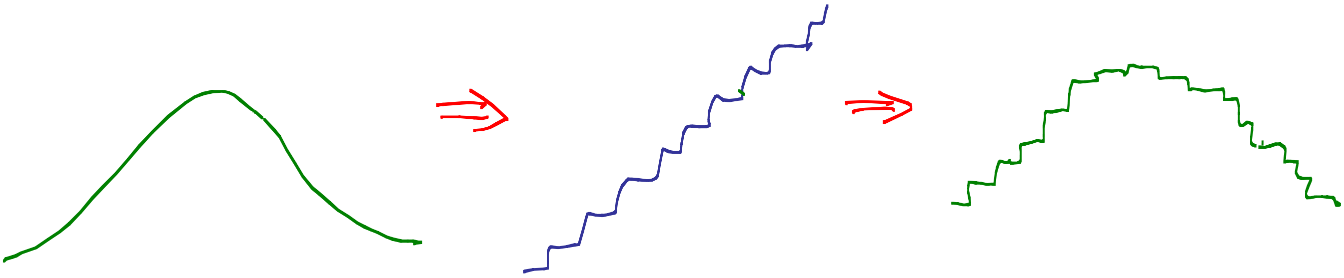


non-predictive encoder

"side information" @ decoder

predictive decoder

So far, under high-resolution approximation...



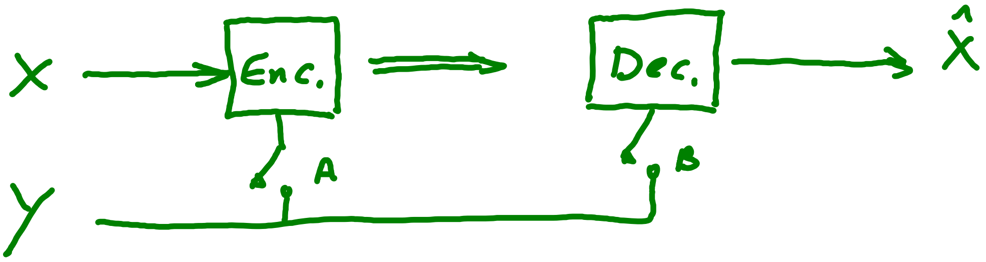
distortion << innovation

$$(z+\text{dither}) \bmod \Lambda \approx z \bmod \Lambda$$

$$I(z\,;\, z+\text{dither}) \approx h(z) - h(\text{dither})$$

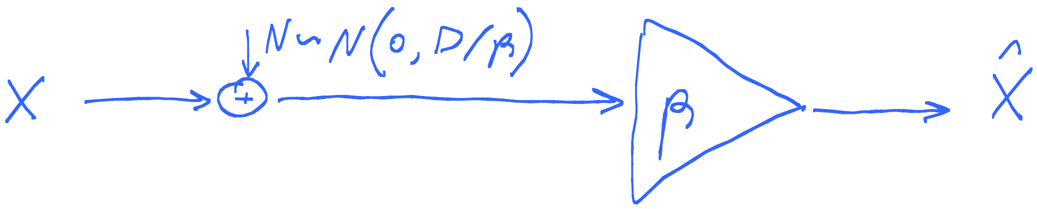
how can we extend to general resolution?

Rate-distortion with Side-Information



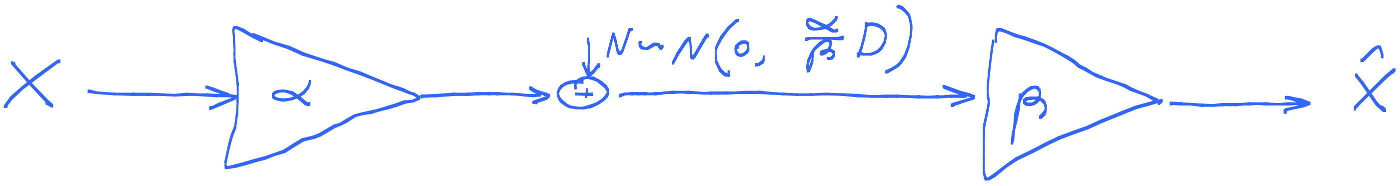
1. **no SI** : $R_X(D) = \min_{\{\hat{X}:\, E(\hat{X}-X)^2 \le D\}} I(X;\hat{X})$

If $X \sim N(0, \sigma_x^2)$ white Gaussian, $R_X(D) = \frac{1}{2}\log(\sigma_x^2/D)$, achieved by "forward test channel":



β = Wiener cofficient $= \dfrac{\sigma_x^2}{\sigma_x^2 + \sigma_N^2} = 1 - \dfrac{D}{\sigma_x^2}$

Or "pre/post-filtered" form:

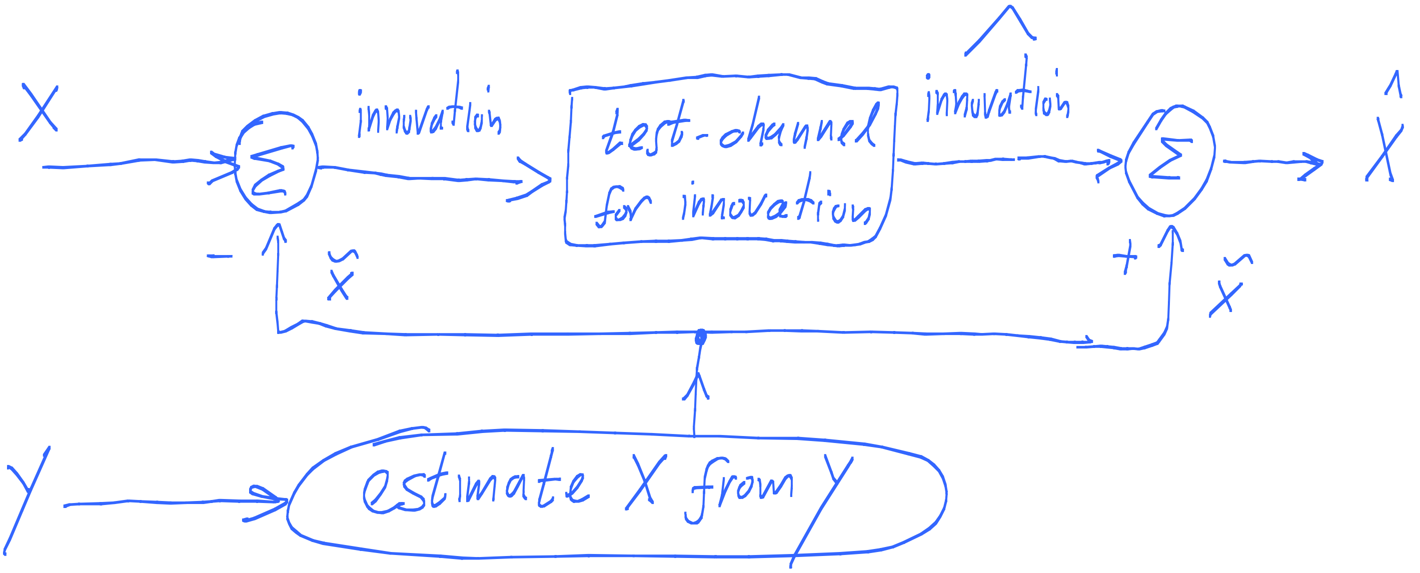


any α, β s.t. $\alpha \cdot \beta = 1 - \dfrac{D}{\sigma_x^2}$

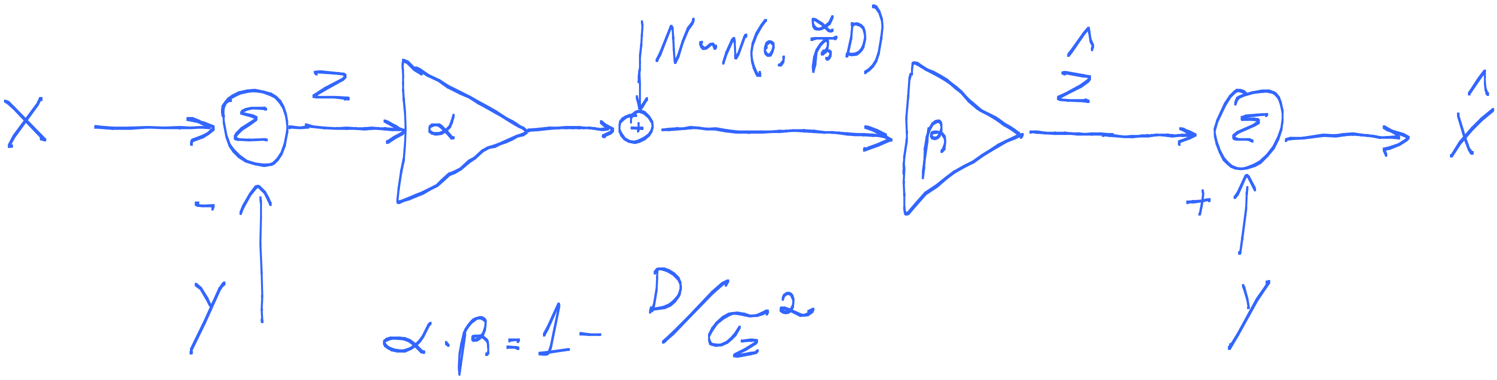
Rate-distortion with Side-Information

2. <u>SI @ Both</u>: $R_{x|y}(D) = \min_{\{\hat{x}:\ E(\hat{x}-x)^2 \le D\}} I(x;\hat{x}|y)$

If $X|y \sim N(0,\sigma^2_{x|y})$ jointly Gaussian, $R_{x|y}(D) = \frac{1}{2}\log\left(\frac{\sigma^2_{x|y}}{D}\right)$

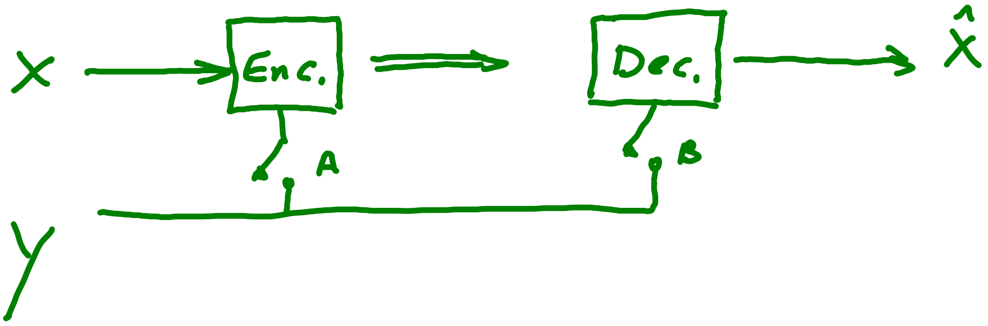


For $X = Y + Z$, $Y \perp\!\!\!\perp Z$ (w.l.o.g.):



$\alpha\cdot\beta = 1 - D/\sigma_z^2$

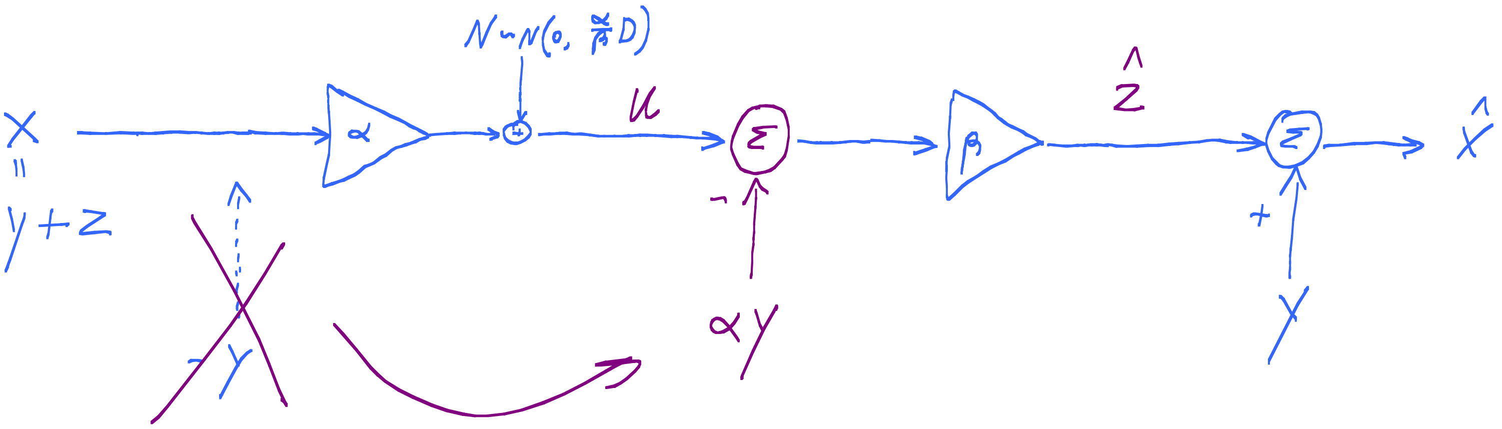
Rate - distortion with Side - Information



3. SI @ decoder:

$$R_{WZ}(D) = \min_{\left\{\begin{array}{l}\text{auxiliary } U: \\ U \leftrightarrow X \leftrightarrow Y \\ \mathrm{Var}(X|U,Y) = D\end{array}\right\}} I(X;U|Y)$$

If $X|y \sim N(0,\sigma^2_{x|y})$ jointly Gaussian, $R_{WZ}(D) = R_{X|Y}(D)$



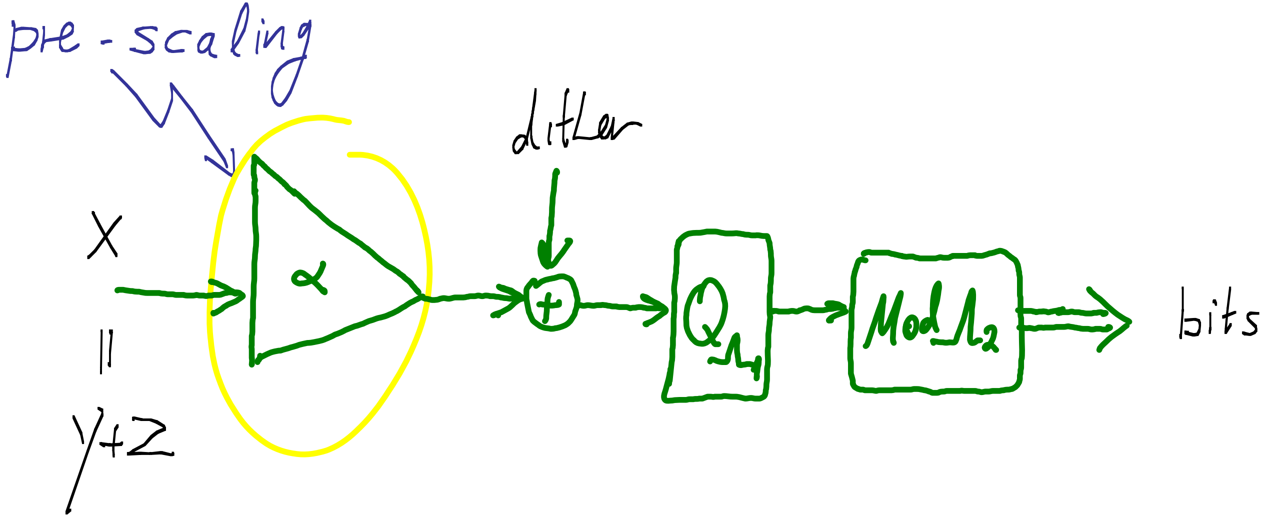
$$\alpha \cdot \beta = 1 - D/\sigma_Z^2$$

Lattice Wyner-Ziv: general resolution

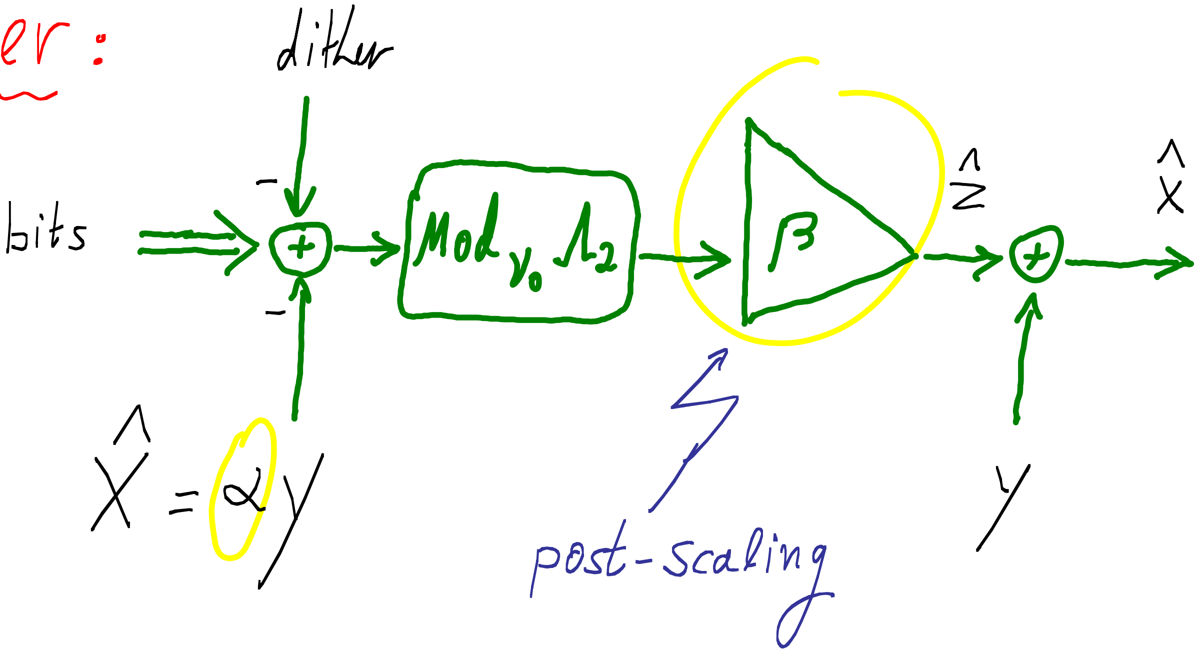
pre/post-scaling

$$\alpha \cdot \beta = 1 - D/\sigma_z^2$$

encoder:



decoder:

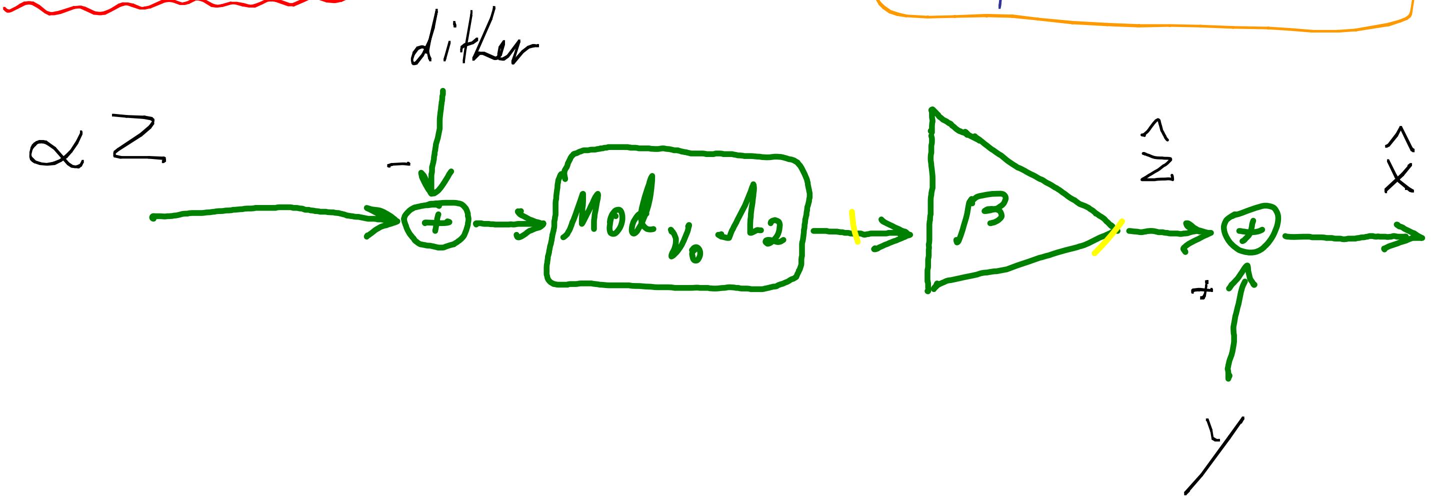


Lattice Wyner-Ziv: general resolution

pre/post-scaling

$\alpha \cdot \beta = 1 - D/\sigma_z^2$

equivalent channel:



correct decoding $\Rightarrow$ $\alpha Z + u_{eq} \in \mathcal{V}_0(\Lambda_2)$

$$\hat{Z} = \beta(\alpha Z + u_{eq})$$

distortion $= E\left[Z - \beta(\alpha Z + u_{eq})\right]^2 = D$

Rate $\triangleq \frac{1}{n}\log|\Lambda_2/\Lambda_1| = \underbrace{\frac{1}{2}\log\left(\frac{\sigma_z^2}{D}\right)}_{R_{WZ}(D)} + \underbrace{\frac{1}{2}\log\left(G(\Lambda_1)\cdot\underbrace{\mu_{mix}(\Lambda_2, P_e)}_{\text{NVNR @ mixture Gaussian + dither}}\right)}_{\text{redundancy}}$

Noise-Matched WZ-Decoding

If quantization dimension is low ⇒ U_{eq} non Gaussian

If also resolution is low $(D \not< \sigma_Z^2)$ ⇒ $\underbrace{\alpha Z + U_{eq}}_{\triangleq Z_{eq}}$ non Gaussian

⇒ Euclidean decoding $(\bmod_{V_0} \Lambda_2)$ is not optimal!

Noise-matched decoder (NMD):

$$Q_\Lambda(a) \underset{\uparrow\ \text{w.r.t } Z_{eq}}{\triangleq} \underset{\lambda\in\Lambda}{\arg\max}\ P_{Z_{eq}}(a-\lambda) \underset{\uparrow\ \text{if } Z_{eq}=\text{AWGN}}{=} \arg\min \|a-\lambda\|$$

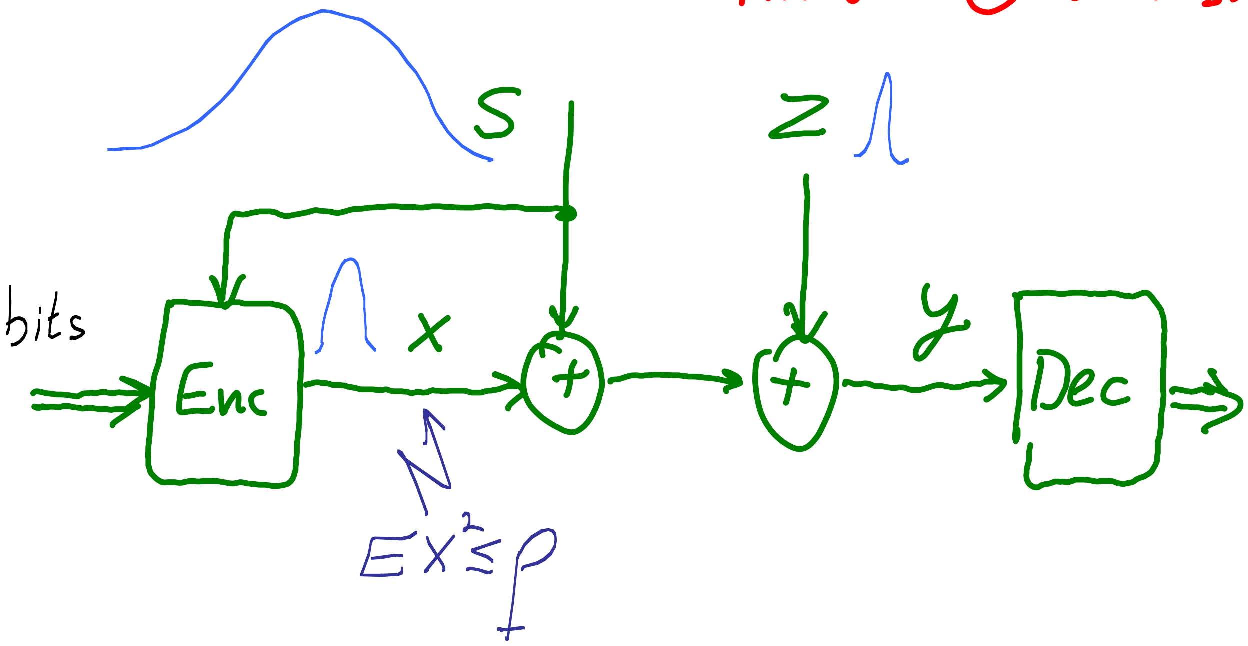
Thm. [High dim coarse lattice with noise-matched dec.]

If $n(\Lambda_2) \to \infty$, and $n(\Lambda_1)$ arbitrary, then

$$\text{Rate} = \frac{1}{n(\Lambda_1)} I\left(\underbrace{Z;\ \alpha Z}_{n(\Lambda_1)\text{ dim}} + U_{eq}\right) = \text{Rate}\left(\text{ECDQ of } Z\right)$$

"Writing on Dirty Paper"

(AWGN channel coding with Interference known @ transmitter)



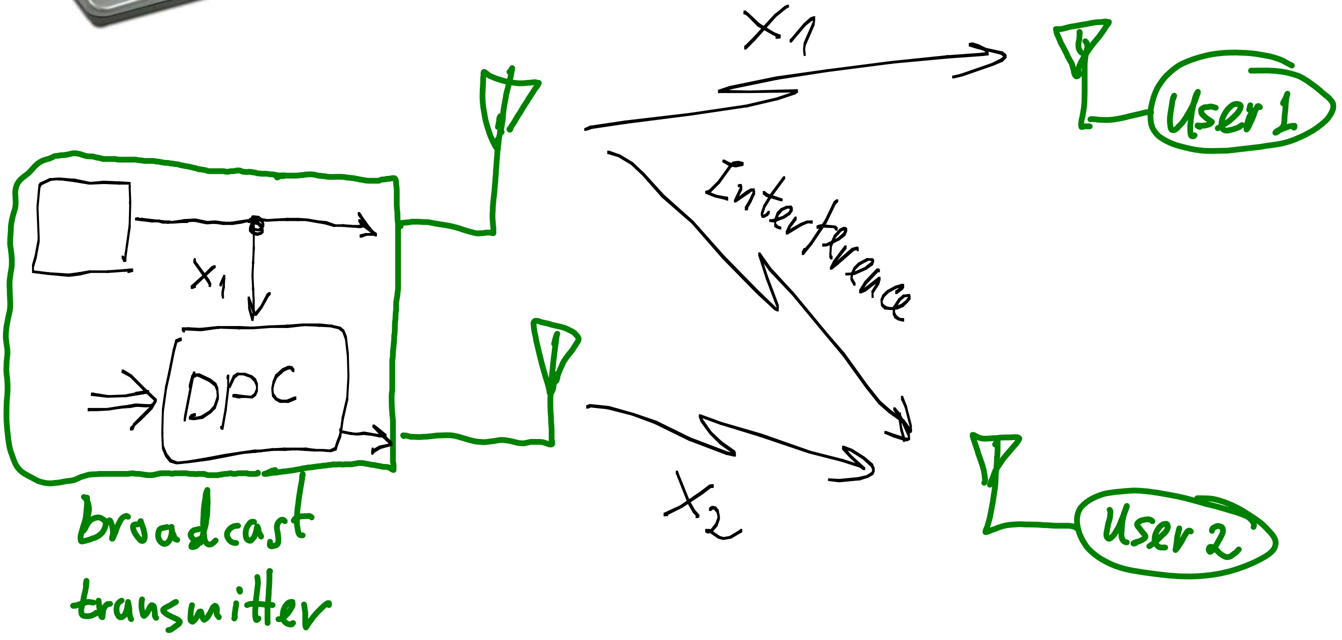
$$C_{SI@T_x} = \frac{1}{2}\log\left(1+\frac{P}{\sigma_z^2}\right) = C_{AWGN}$$

Gelfand-Pinsker 1980

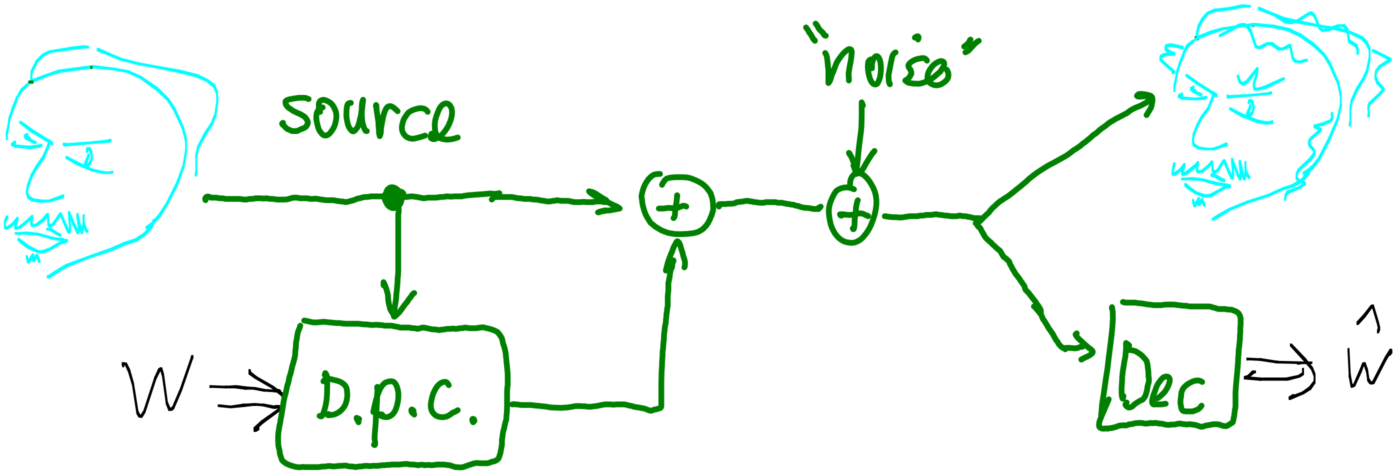
Costa 1983

Surprising: interference cancellation with no power penalty?

MIMO - Broadcast using D.P.C

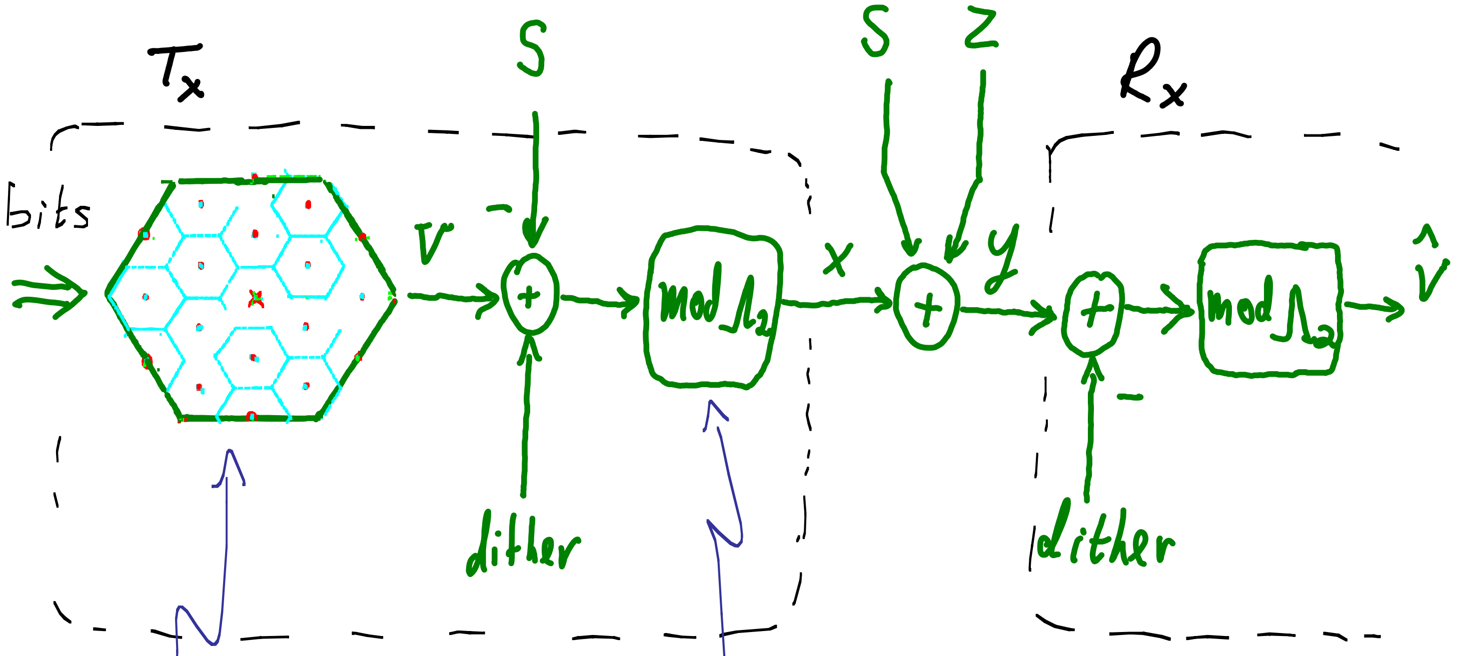


Information Embedding ("Watermarking")



Lattice Dirty Paper Coding

[Tomlinson-Harashima / Erez-Shamai-Zamir]

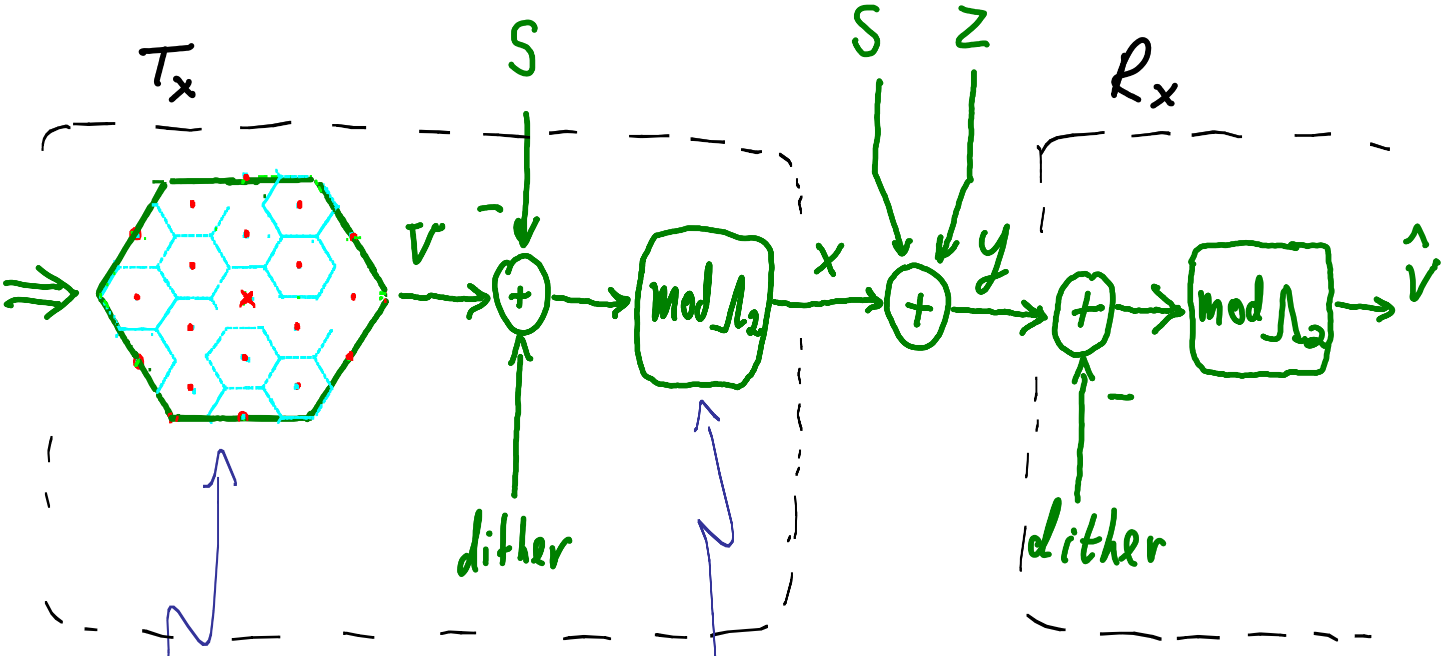


Λ_1/Λ_2
Voronoi
Constellation

Λ_2 = Good quantizer
$\sigma^2(\Lambda_2) = P$

Λ_1 = good channel code for $N(0,\sigma_Z^2)$

Lattice Dirty Paper Coding



Λ_1 / Λ_2
Voronoi
Constellation

Λ_1 = good channel
code for $N(0,\sigma_Z^2)$

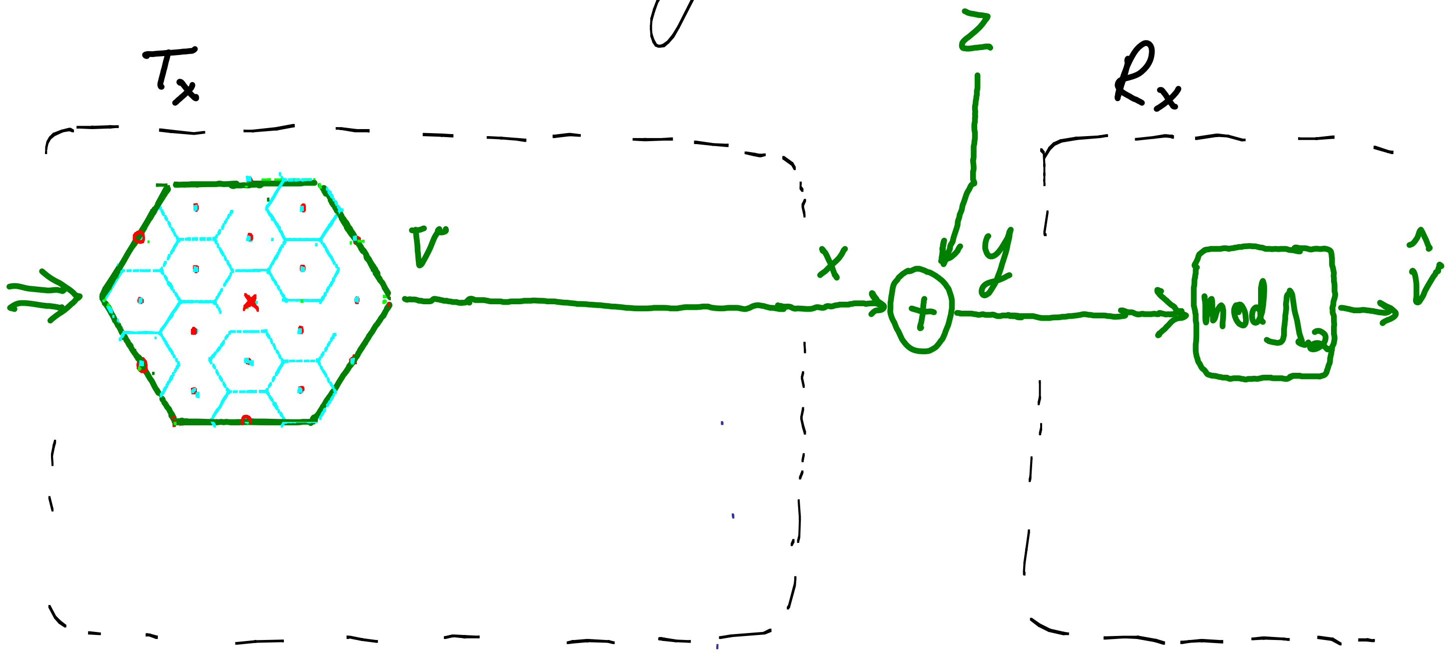
Good quantizer
$\sigma^2(\Lambda_2) = P$ + dither

$$E \, \frac{1}{k} \|X\|^2 = P$$

for any codeword!

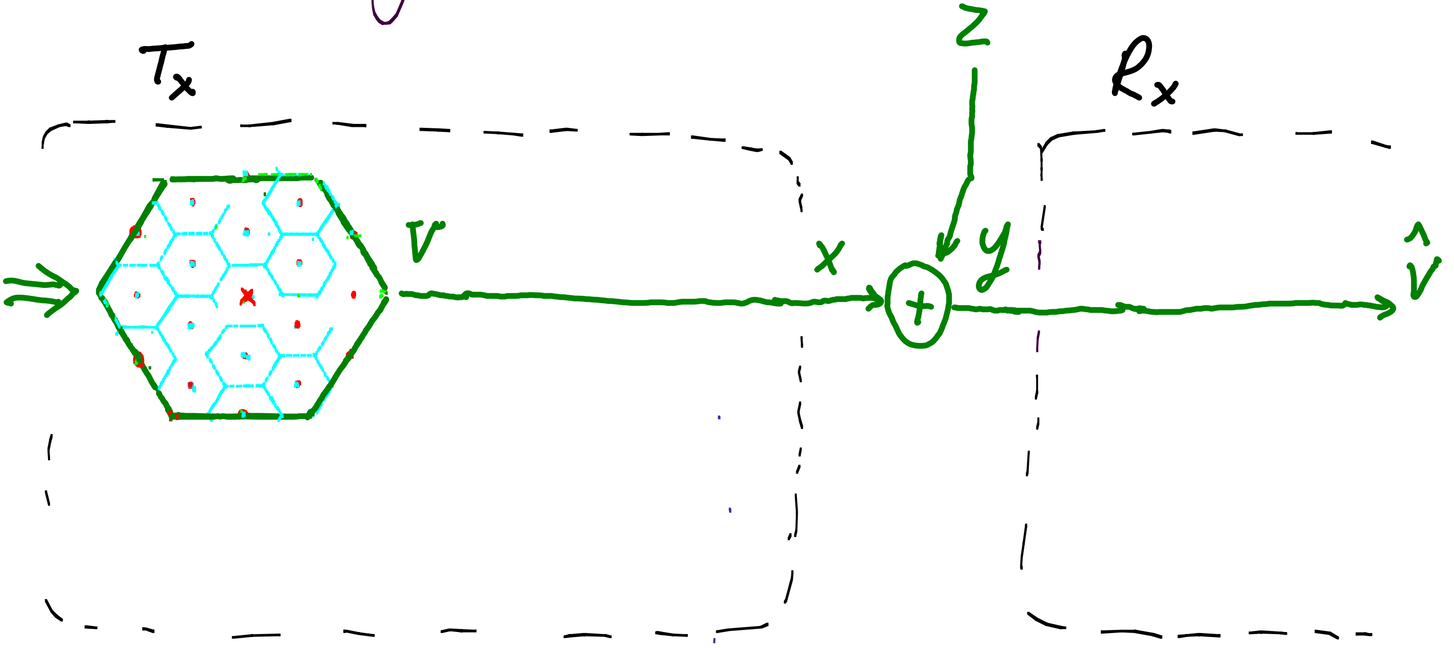
Lattice Dirty Paper Coding

Modulo property ⇒



Lattice Dirty Paper Coding

Λ_1 = good for $N(0,\sigma_z^2)$ $\Rightarrow$ $P_e < \varepsilon \ \forall v$



$$\text{Rate} = \frac{1}{k}\log\left(\frac{V_2}{V_1}\right) \quad \text{bit / channel use}$$

NSM(Λ_2)
VNR(Λ_1)

$$= \underbrace{\frac{1}{2}\log\left(\frac{P}{\sigma_z^2}\right)}_{\text{AWGN capacity @ High SNR}} - \underbrace{\log\left(G(\Lambda_2)\cdot\mu(\Lambda_1,\varepsilon)\right)}_{\text{Redundancy} \longrightarrow 0}$$

$k \to \infty$

for good lattices ....

Costa (Random Binning) ⇒ Lattice Coding

1. Code design

binning ⇒ relative cosets

2. Transmission

message ⇒ Coset

typicality encoding ⇒ quantization @ $MSE = P$

$$\text{"}u\text{"} = Q_{\Lambda_2}(S + V - \text{dither}) - V + \text{dither}$$

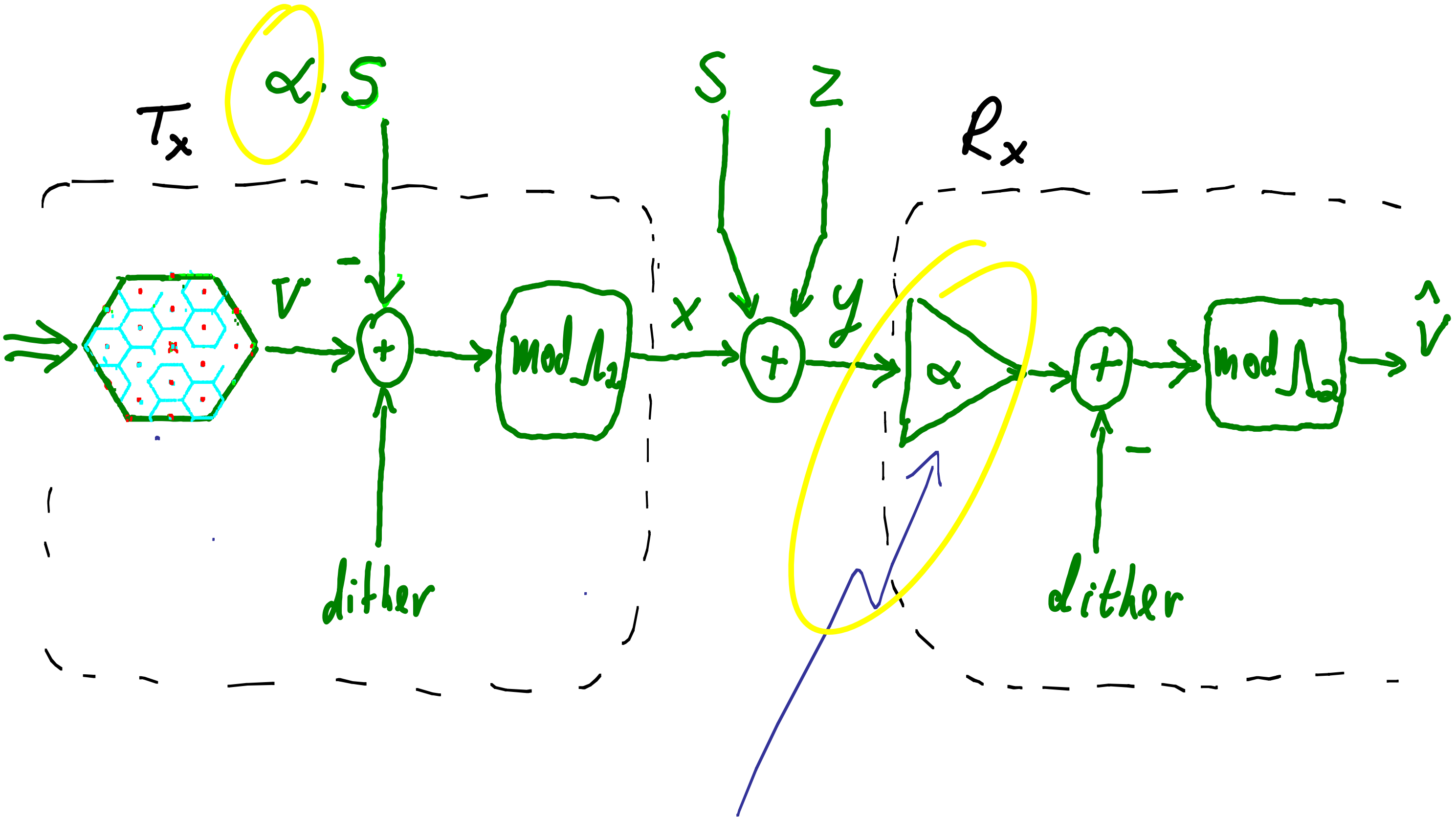
3. Reception

typicality decoding ⇒ lattice decoding

$$\text{"}\hat{u}\text{"} = Q_{\Lambda_1}(y - \text{dither} \bmod \Lambda_2)$$

Achieving $\frac{1}{2}\log(1+SNR)$ @ general SNR

$(SNR = P/\sigma_z^2)$



Where a good choice for α is:

$$\alpha = \text{MMSE (Wiener) Coefficient}$$

$$= \frac{P}{P+\sigma_z^2} \approx 1 \text{ @ HSNR}$$

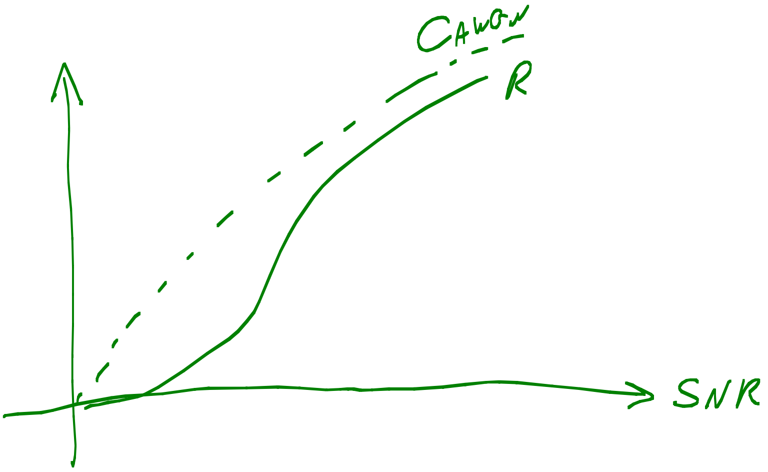
Noise-Matched D.P.-Decoding

If quantization dimension is low ⇒ U_{eq} non Gaussian

If also SNR is low ⇒ Z_{eq} non Gaussian

⇒ Euclidean decoding $(\text{mod}_{\mathcal{V}_0} \Lambda_2)$ is not optimal!

$$\Rightarrow \quad \text{Rate} \cong I(X;\ X + Z_{eq} \bmod \Lambda_2)$$



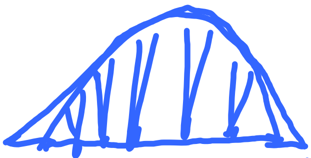
Why Lattices in Communication?

① a bridge from $n=1$ to $n=\infty$

= non-asymptotic analysis per dimension

② Algebraic (low complexity) Binning

= structured coding schemes for networks



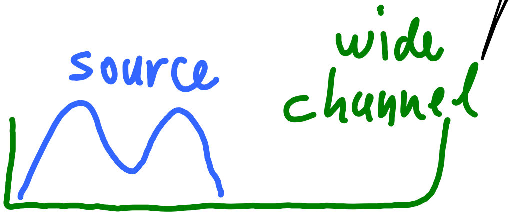
③ bridge from Analog-to-Digital

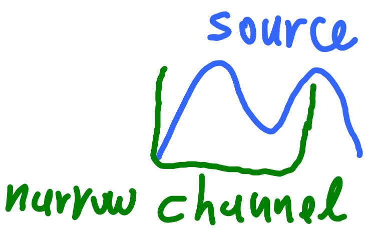
= Robust joint source-channel coding

④

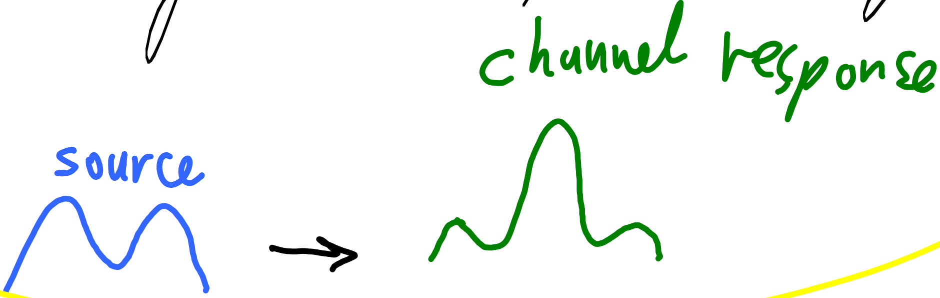
Joint Source-channel Coding

Bandwidth Expansion & Compression

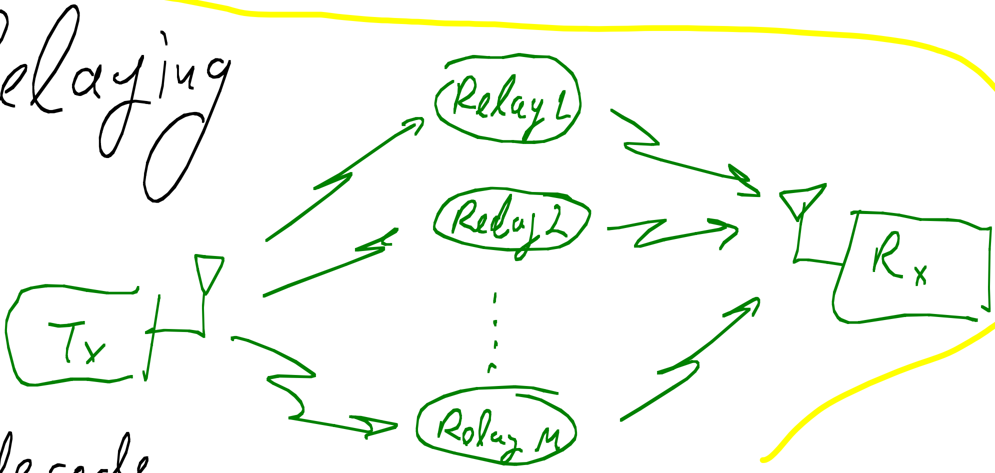




Analog (colored) Matching



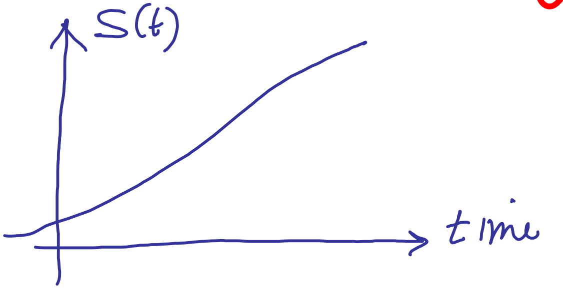
Analog Relaying

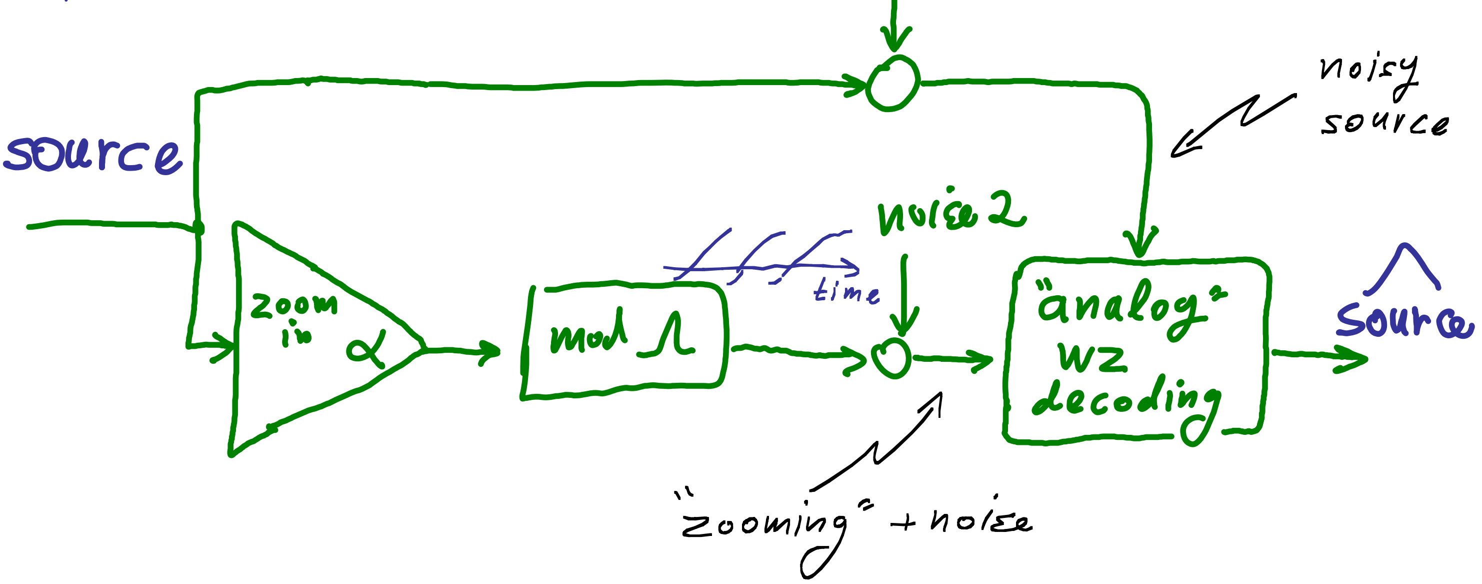


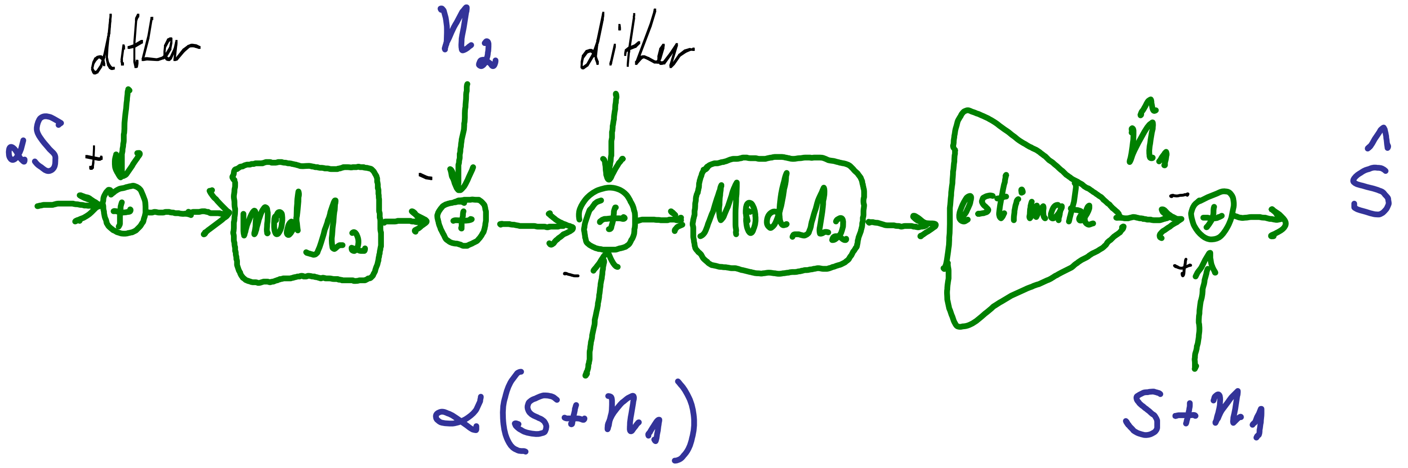
relays cannot decode ...

Modulo-Lattice Modulation for Analog Wyner-Ziv coding

[Reznic Feder Z, Kochman Z]

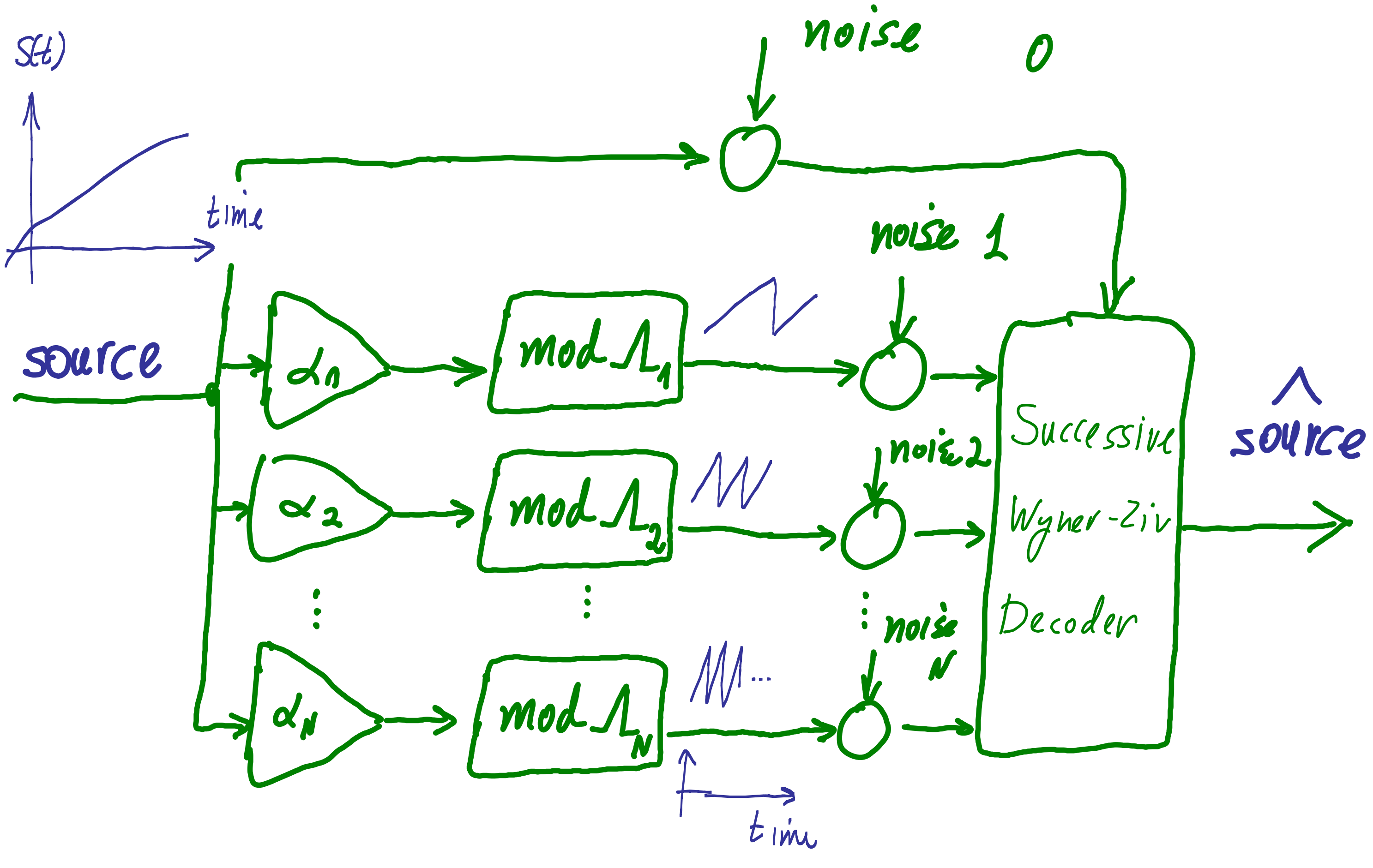






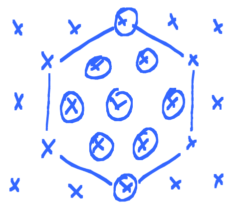
Modulo-Lattice Modulation for Bandwidth Expansion

(analog error-correction codes: Chen & Wornell)



Tutorial - Part A Outline

1. Definitions: Partition, Construction $\mathrm{Vol}(\Lambda)$ Modulo Λ
2. Figures of merit $G(\Lambda)$
3. Dither & estimation $\mathrm{noise}(\Lambda)$
4. Entropy coding $H(\Lambda)$
5. Infinite constellation $P_e(\Lambda + \mathrm{noise})$
6. Asymptotic goodness $(n \to \infty)$
7. Error exponents
8. Nested lattices $\Lambda_2 \subset \Lambda_1$
9. Lattice (Voronoi) shaping



10. Side - information problems $\mathrm{Modulo}^2(\Lambda)$
11. Gaussian networks $\mathrm{Modulo}^n(\Lambda)$

Tutorial - Part A Outline

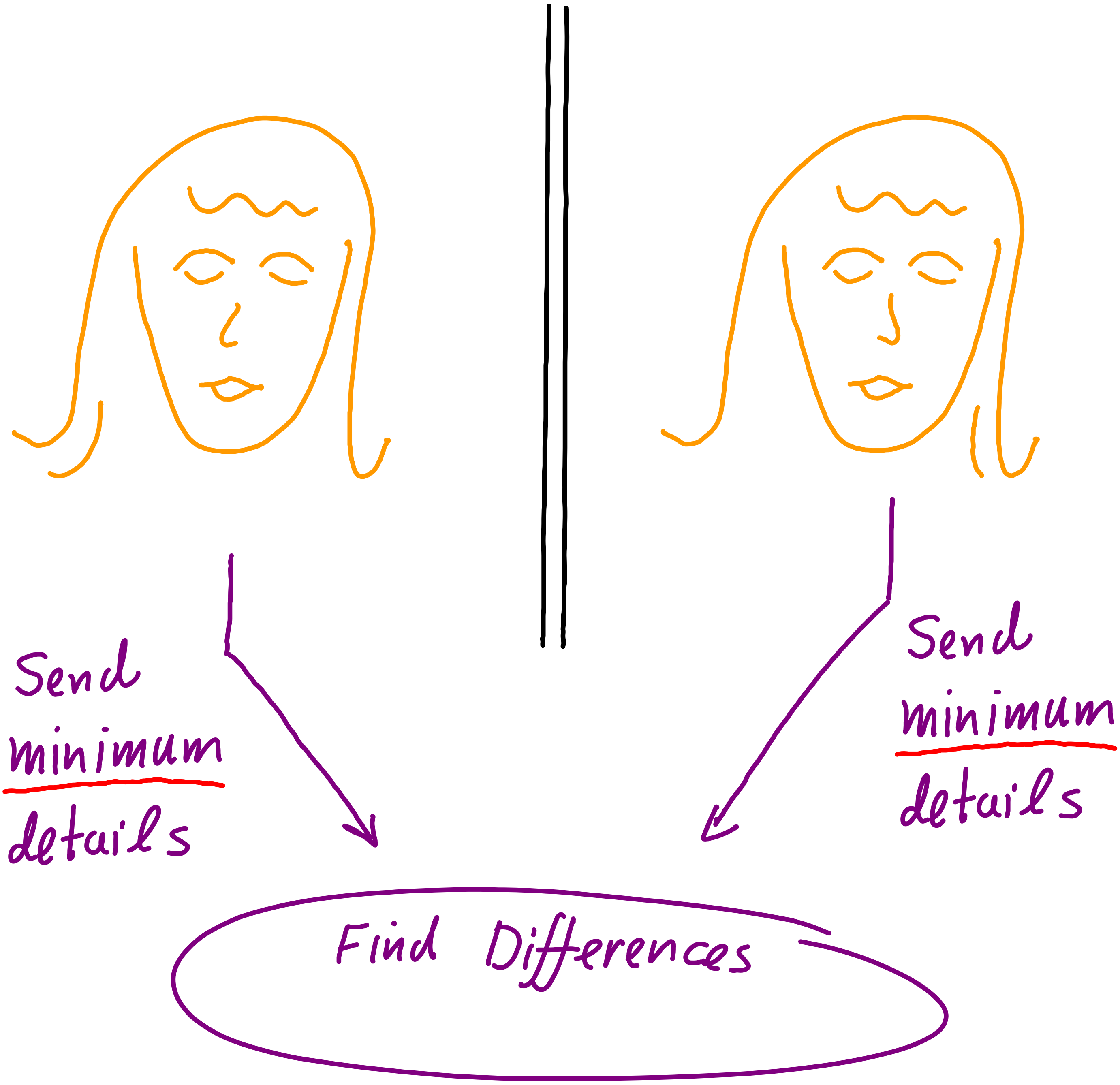
11. Gaussian networks

$\text{Modulo}^n(\Lambda)$

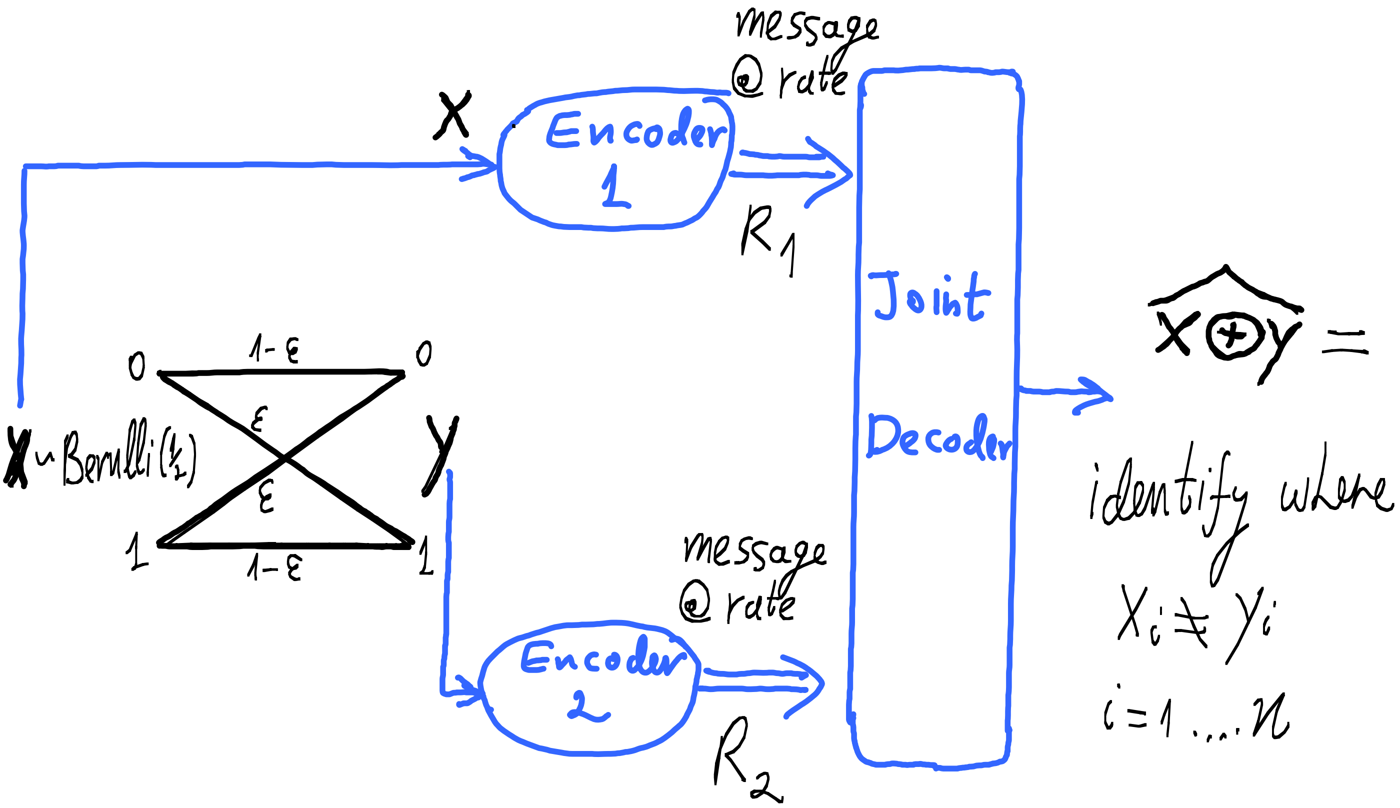
Find the Differences

?

Communicate the Differences



The Korner-Marton Problem



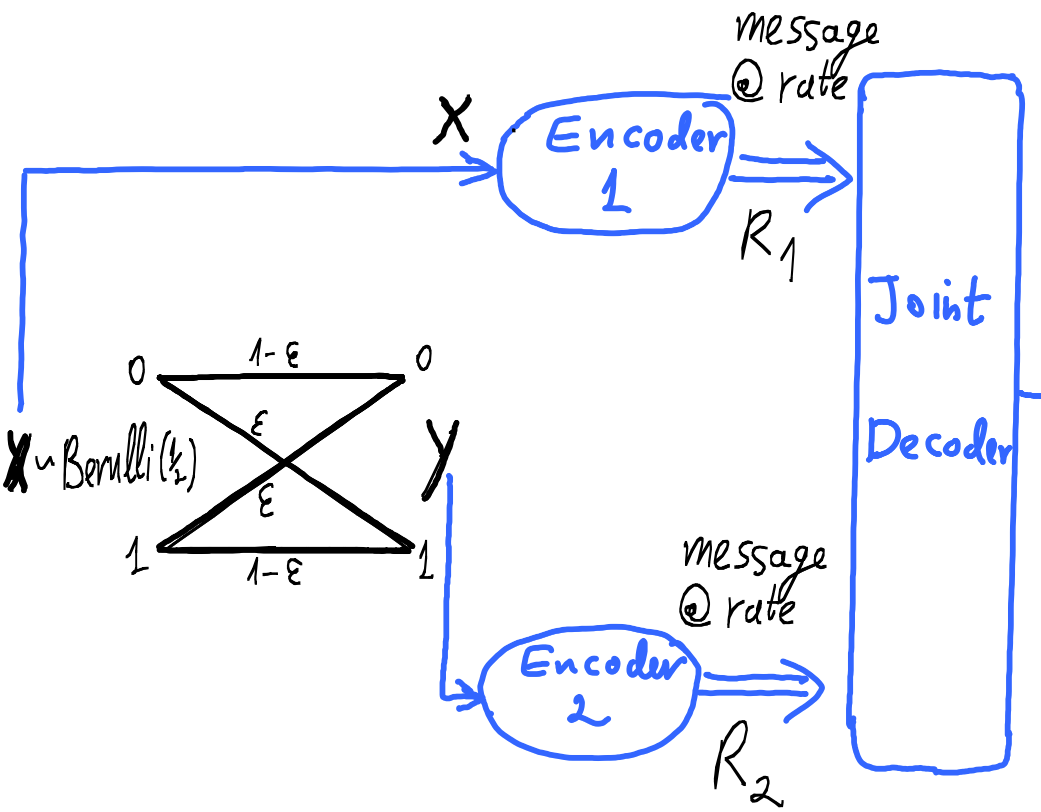
$Z = X \oplus Y$

Compress & estimate:

$H(X) + H(Y) = 1 + 1 = 2$ bit

Rate $\overset{?}{=}$

The Korner-Marton Problem



$\widehat{X \oplus Y} =$ identify where $X_i \neq Y_i$

$i = 1 \dots n$

$Z = X \oplus Y$

$\text{Rate} \overset{?}{=}$

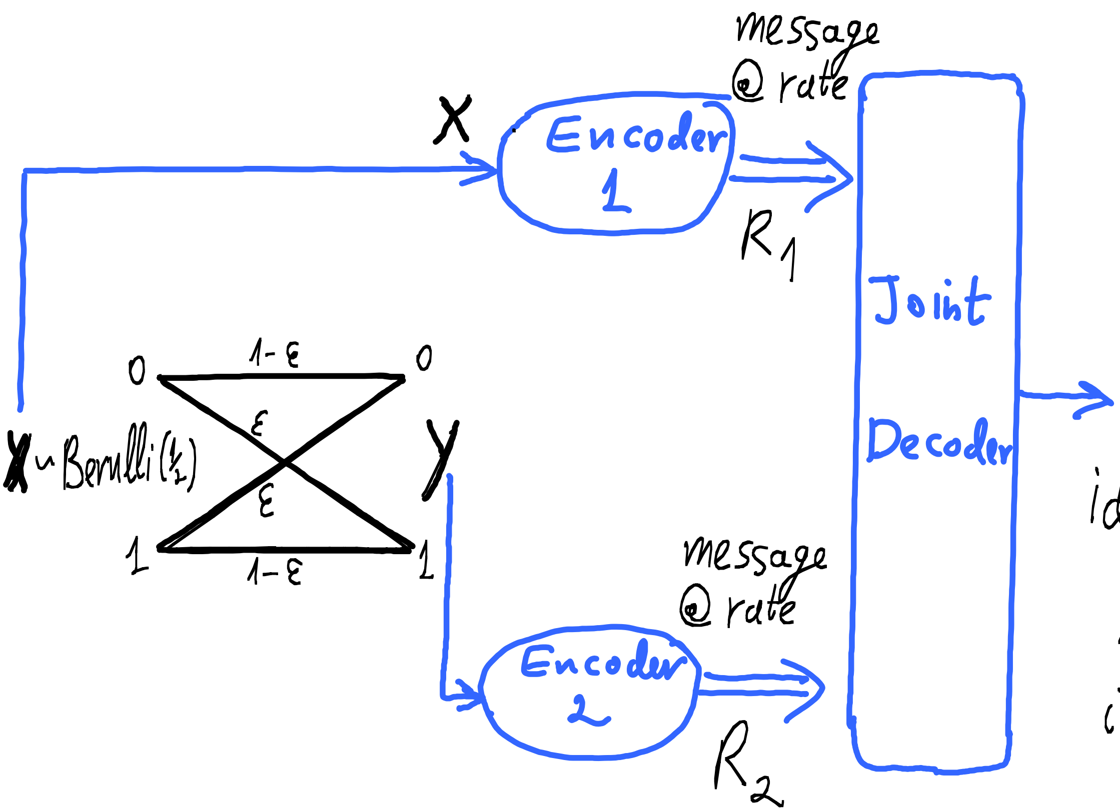
Compress & estimate:

$H(X) + H(Y) = 1 + 1 = 2$ Bit

Compress **well** & estimate:

$H(X,Y) = H(X) + H(Z) = 1 + H_B(\varepsilon) = 1.1$ Bit

The Korner - Marton Problem



$\widehat{X \oplus Y} =$

identify where

$X_i \neq Y_i$

$i = 1 \ldots n$

$Z = X \oplus Y$

$\text{Rate} \overset{?}{=}$

compress & estimate:

$H(X) + H(Y) = 1 + 1 = 2$ Bit

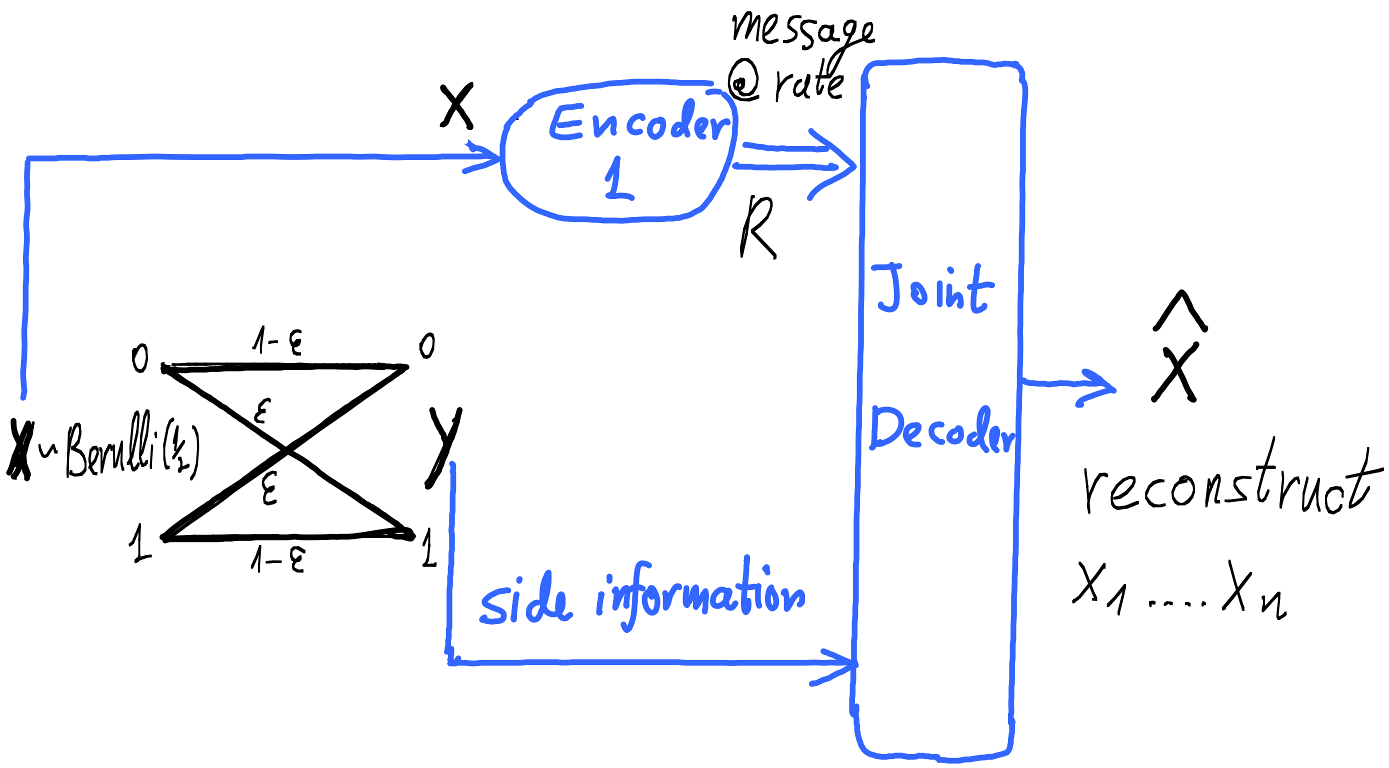
compress **well** & estimate:

$H(X,Y) = H(X) + H(Z) = 1 + H_B(\varepsilon) = 1.1$ Bit

estimate & compress:

$H(Z) = H_B(\varepsilon) = 0.1$ Bit

The Slepian-Wolf Problem



$$R = H(X|Y) = H(Z) = H_B(\varepsilon) = 0.1 \text{ Bit}$$

Back to Korner-Marton: Solution

$\mathbb{C}$ = (n,k) linear code for B.S.C.(ε)

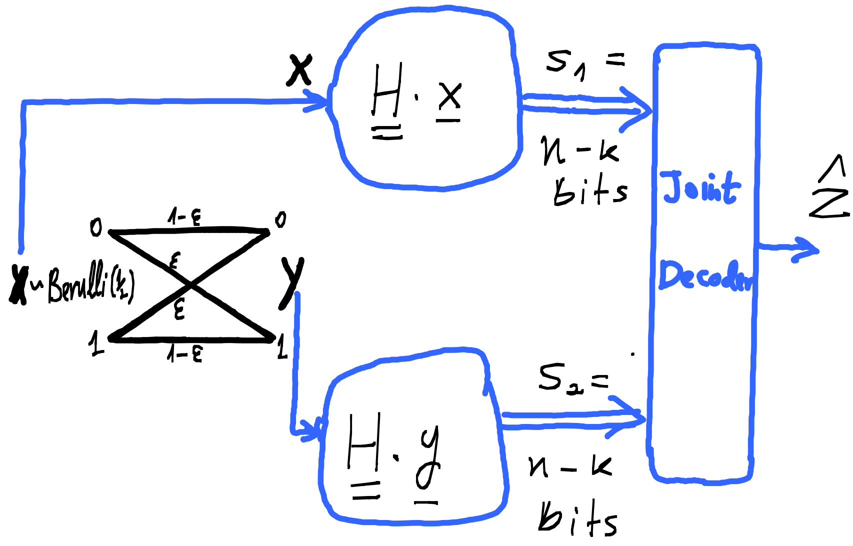
general properties:

$k/n \simeq 1 - H_B(\varepsilon)$

$\underset{n\times 1}{\underline{x}} = \underset{n\times k}{\underline{\underline{G}}} \cdot \underset{k\times 1}{i}$ $\qquad$ $\underset{(n-k)\times n}{\underline{\underline{H}}} \cdot \underset{n\times 1}{\underline{x}} = \underline{0}$ for $\underline{x} \in \mathbb{C}$

If $\underline{y} = \underline{x} \oplus \underline{z}$, where $\underline{z} \sim \text{Bernulli}(\varepsilon)$, then

$\hat{\underline{z}} \triangleq f(\underbrace{H \cdot \underline{y}}_{\text{syndrome}}) = \underline{z}$ with high prob.



$$\hat{\underline{z}} = f(s_1 \oplus s_2)$$
$$= f(\underline{\underline{H}} \cdot (\underline{x} \oplus \underline{y}))$$
$$= f(\underline{\underline{H}} \cdot \underline{z})$$
$$= \underline{z} \quad \text{w. high prob.}$$

Total Rate $= 2 \times \frac{n-k}{n} = 2 \times H_B(\varepsilon) \simeq 0.2$ bits

$P_e = \Pr\{\hat{\mathbf{z}} \neq \mathbf{z}\}$ = independent of $\mathbf{x}$

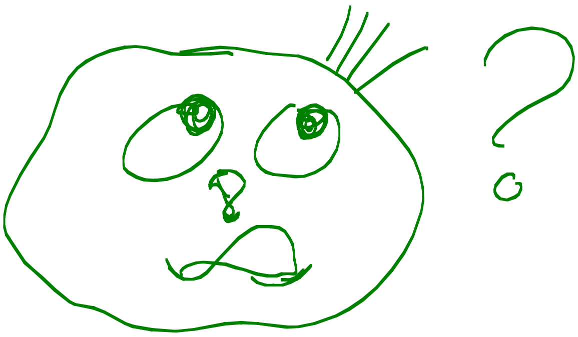
A comment by KM: best known "single letter" = SW = 1.1 bit

- Do we really need structured Codes?

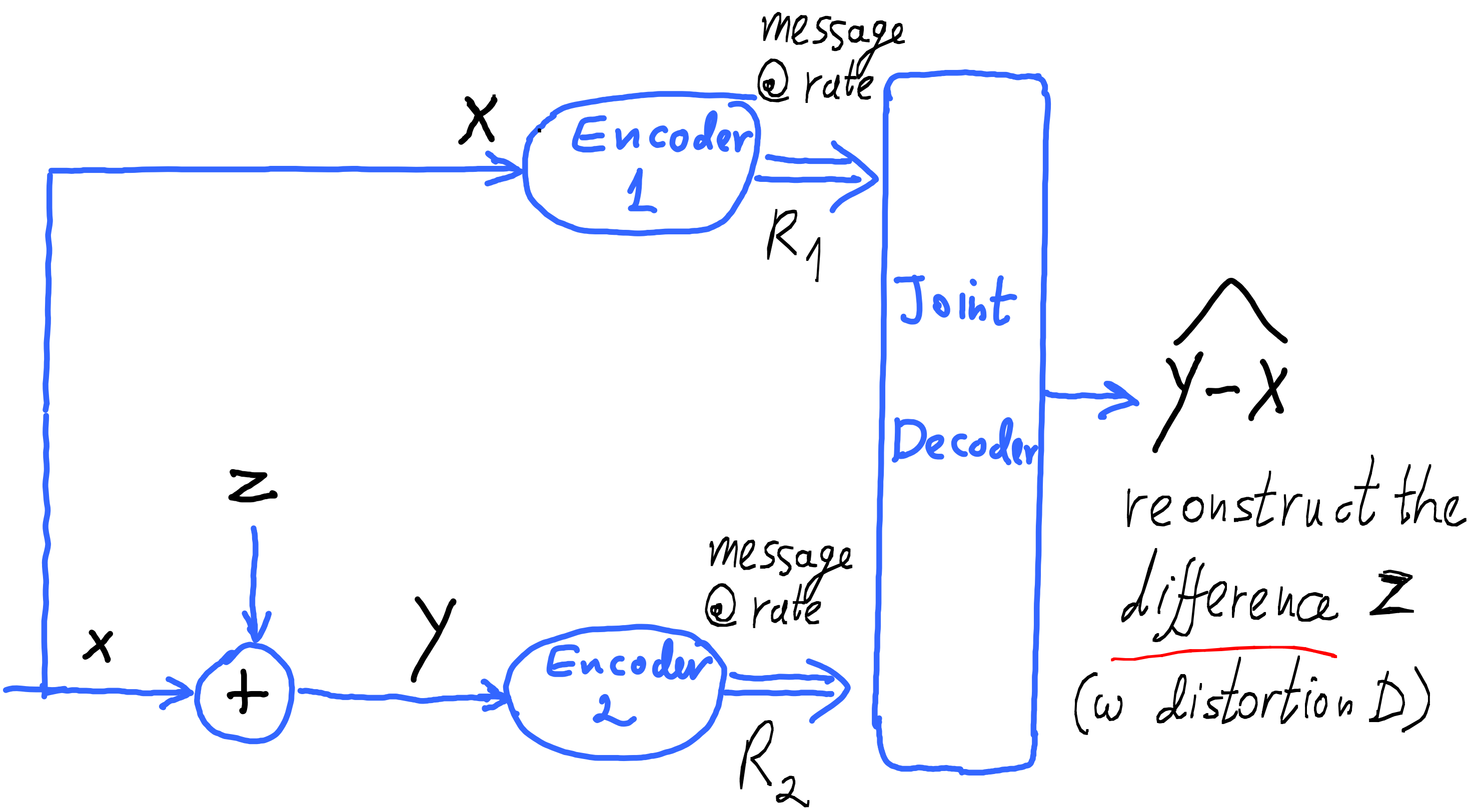
- How do we extend to real signals?

- How do we measure code goodness?

  {rate, error prob., distortion...}



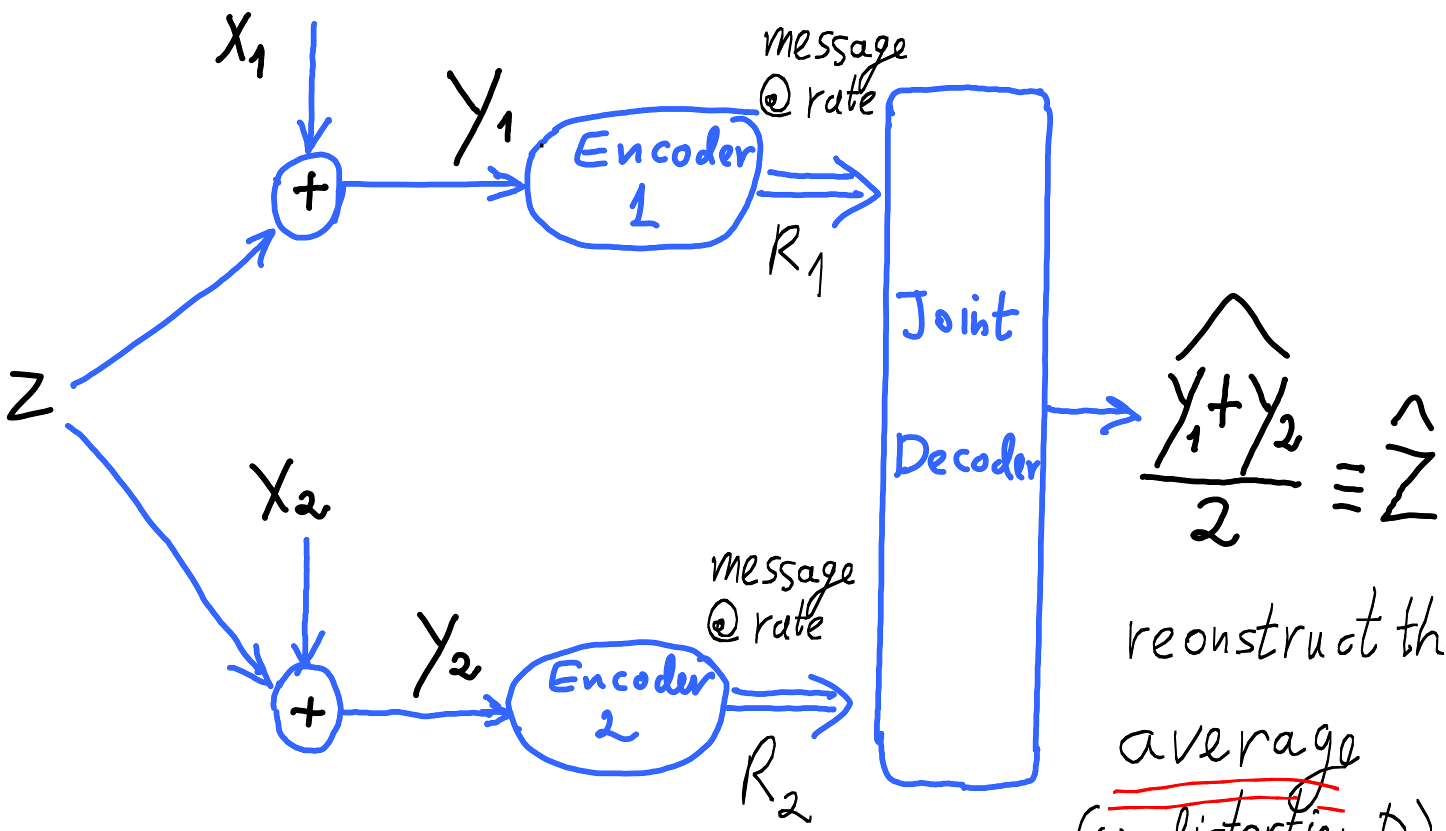
Lattice Korner-Marton Coding



Rate = ?

- $R_{X,Y}(D_1, D_2)$ where $D_1 + D_2 = D$ — Berger-Tang
- $R_Z(D)$ — over optimistic
- $2R_Z(D)$, $2R_Z(D/2)$ ... ? — outer/inner

Compare: The CEO Problem



reconstruct the average (w distortion D)

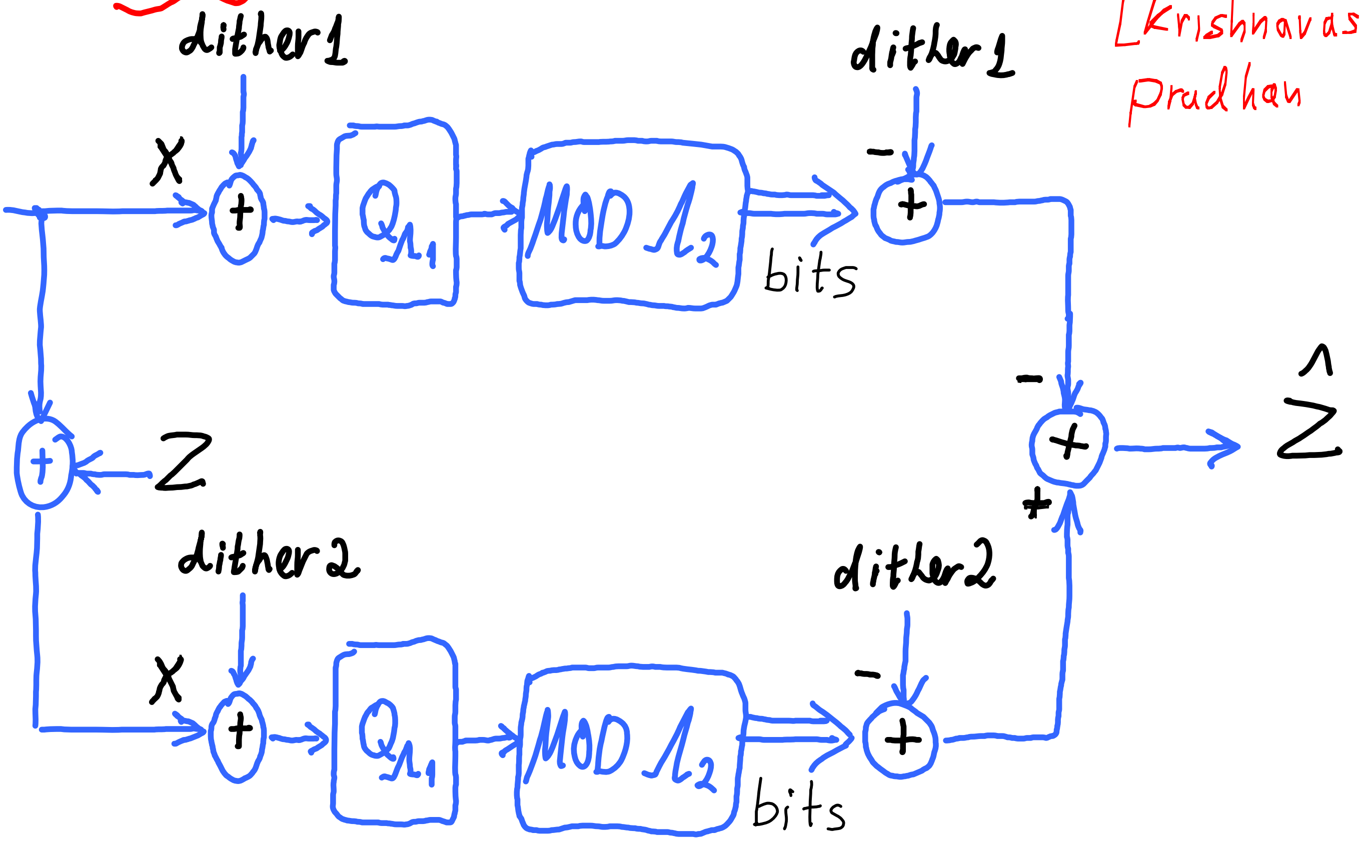
optimum rate:

$$\text{Rate} = \underset{\text{Berger-Tung}}{R_{y_1 y_2}(D_1, D_2)} \qquad \text{where } D_1 = D_2 = 2D$$

achieved by random codes!

The Gaussian Korner - Marton Problem

[Krishnavasan Pradhan]



* modulo distributive law ⇒

$$\hat{Z} = Z + \widetilde{dither\ 1} + \widetilde{dither\ 2} \quad w.h.p$$

$$\Rightarrow R_1 = R_2 = R_Z(D/2) + \frac{1}{2}\log(NSM_1 * VNR_2)$$

gap of ½ bit from outer bound

redundancy → 0 @ dim → ∞

Why Random Loses ?

Distributed Coding ⇒ Need Commutativity:

$$\boxed{\text{Binning}(y) - \text{Binning}(x) = \text{Binning}(y-x)}$$

⇒ Binning should be <u>aligned</u>

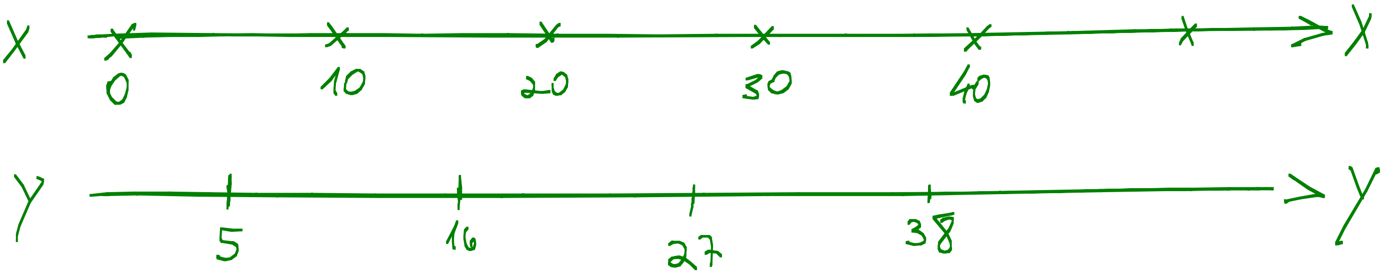
Example of <u>mis-aligned</u> ("pseudo random") binning:

$y = x + z$, $z \sim \text{unif}[0,9]$, $x \sim \text{unif}[0,999]$

code1 = $x \bmod 10$

code2 = $y \bmod 11$ (= higher rate but mis aligned)

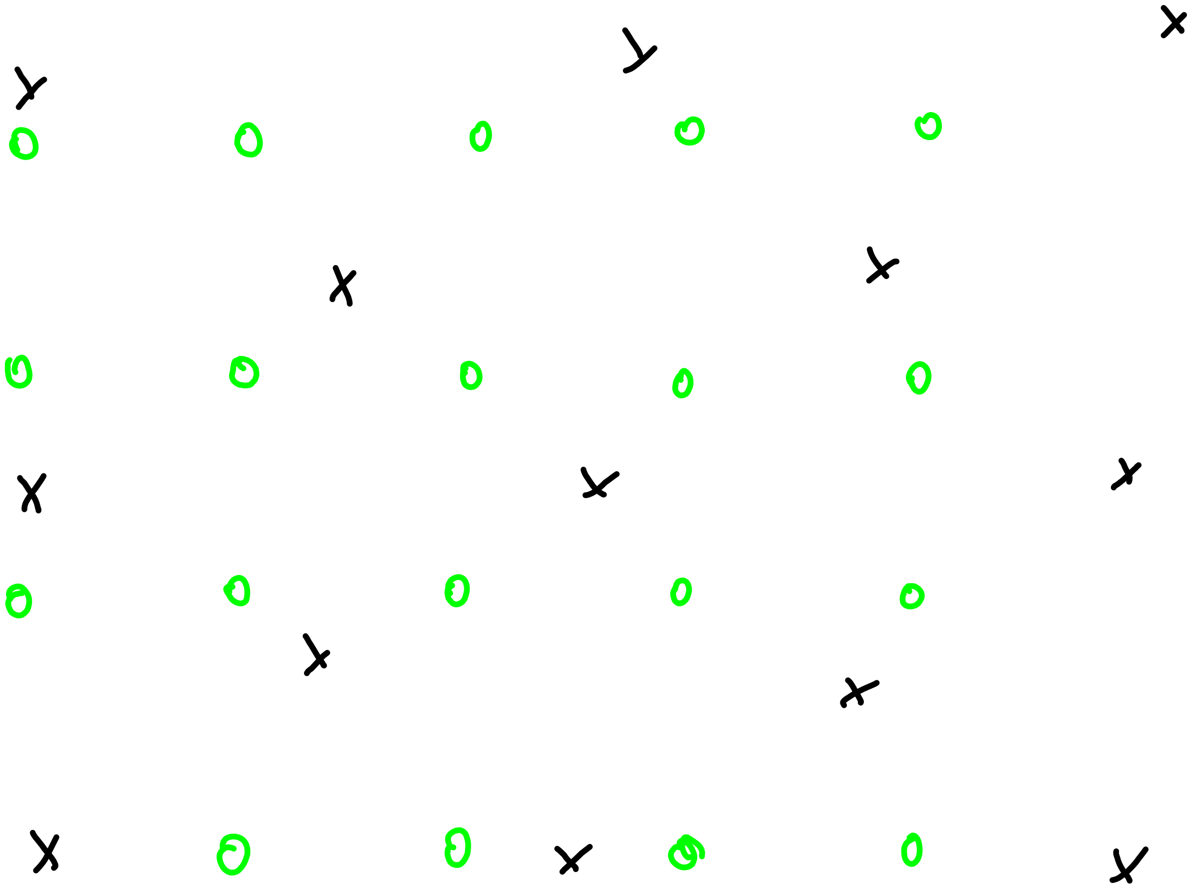
If code 1 = 0 code 2 = 5



⇒ $Z = 5$ or 6 or 7 or ..... ?

Why Random Loses ?

2-dim example of mis-aligned binning:

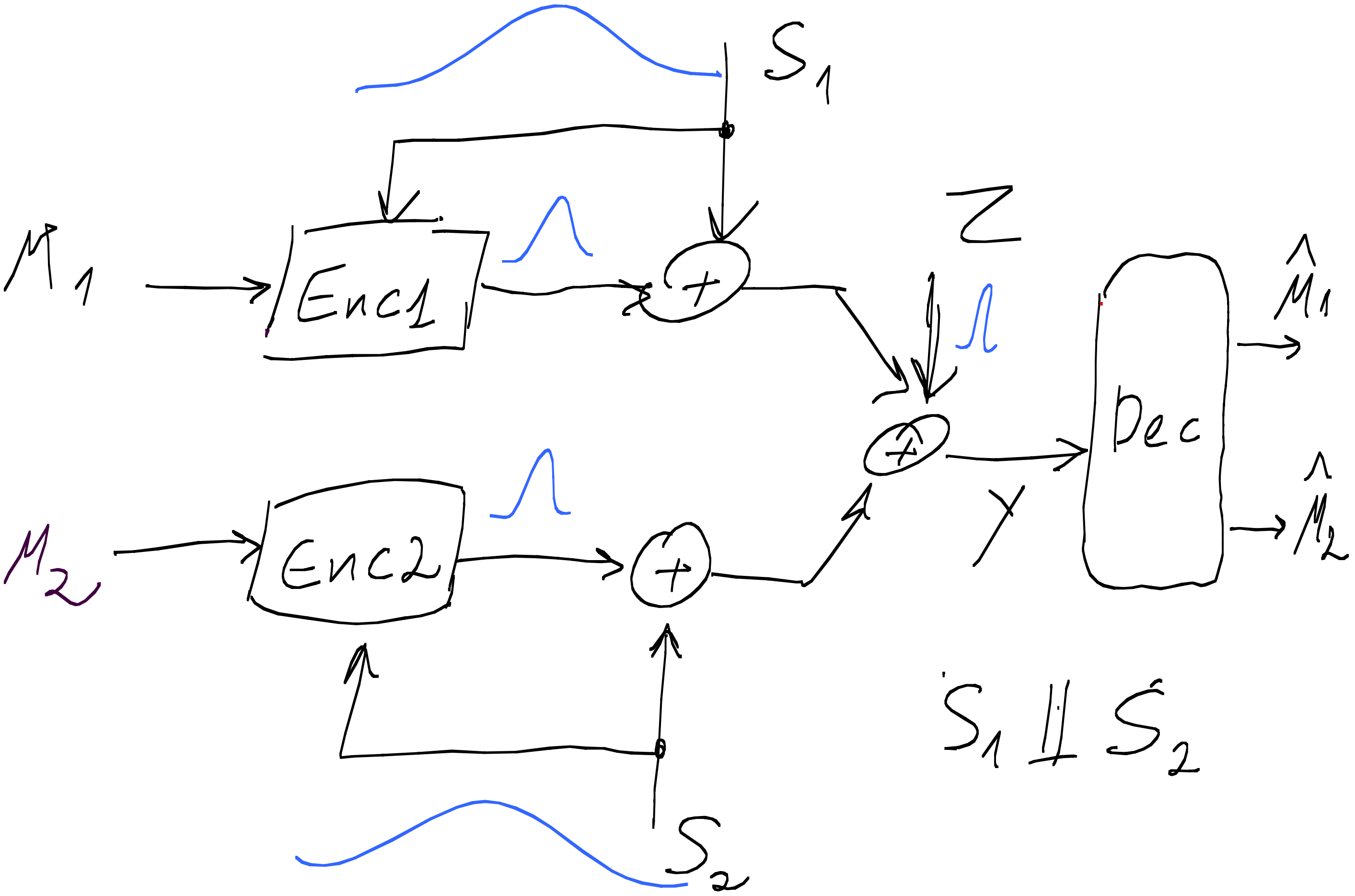


$$\boxed{\det(\Lambda_1) = \det(\Lambda_2)}$$

Distributed Structured Codes

- Korner - Marton Problem
- Dirty Multiple - Access Channel
- Noisy Network Coding (C&F)
- Interference Alignment

"Doubly - Dirty" Multiple - Access Channel



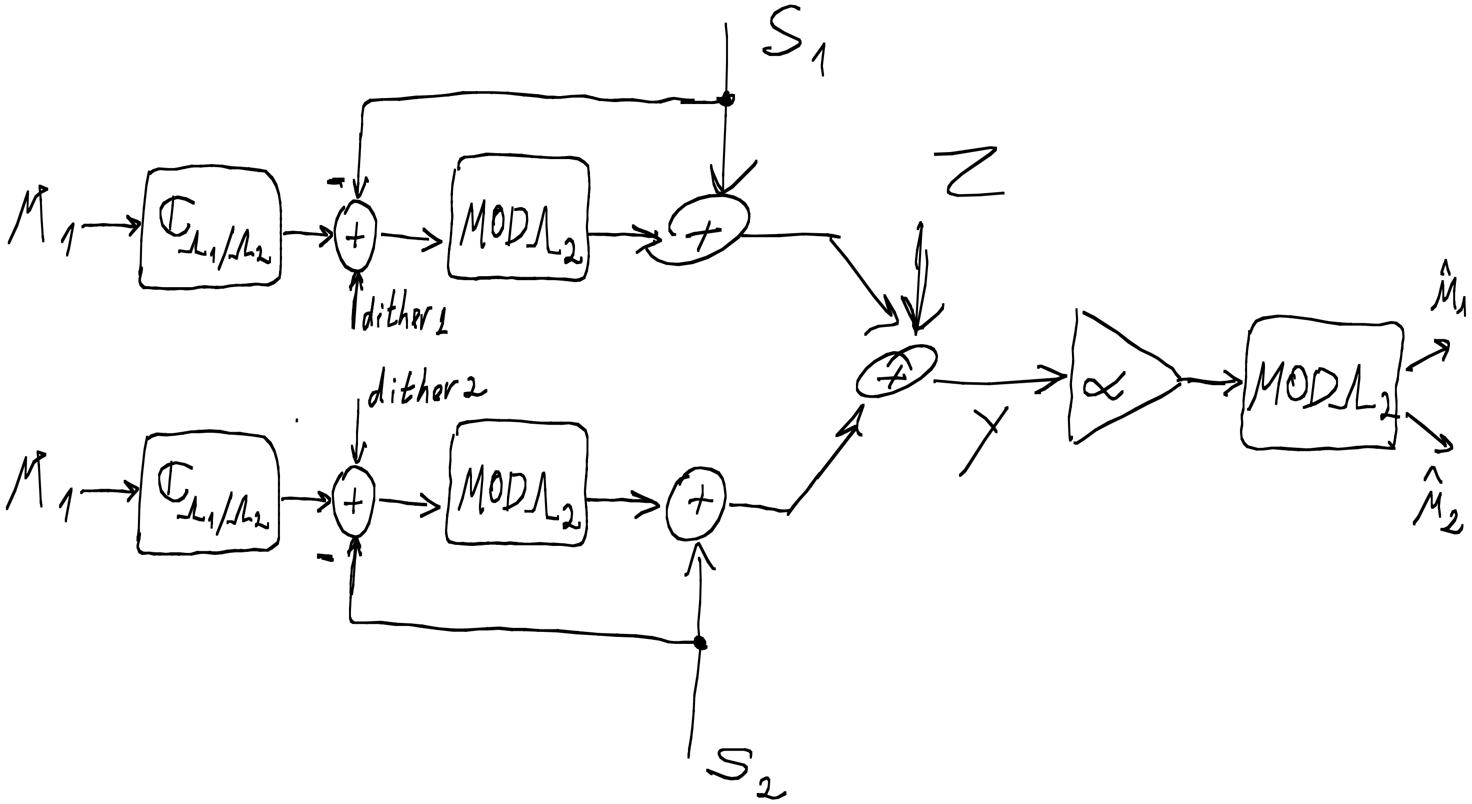
$S_1 \perp\!\!\!\perp S_2$

Knowledge of the interference (S_1, S_2) is split between two independent encoders

"Doubly-Dirty" Multiple-Access Channel

* Costa's (Gaussian) random binning Capacity $\longrightarrow 0$ as $\sigma_S^2 \longrightarrow \infty$!

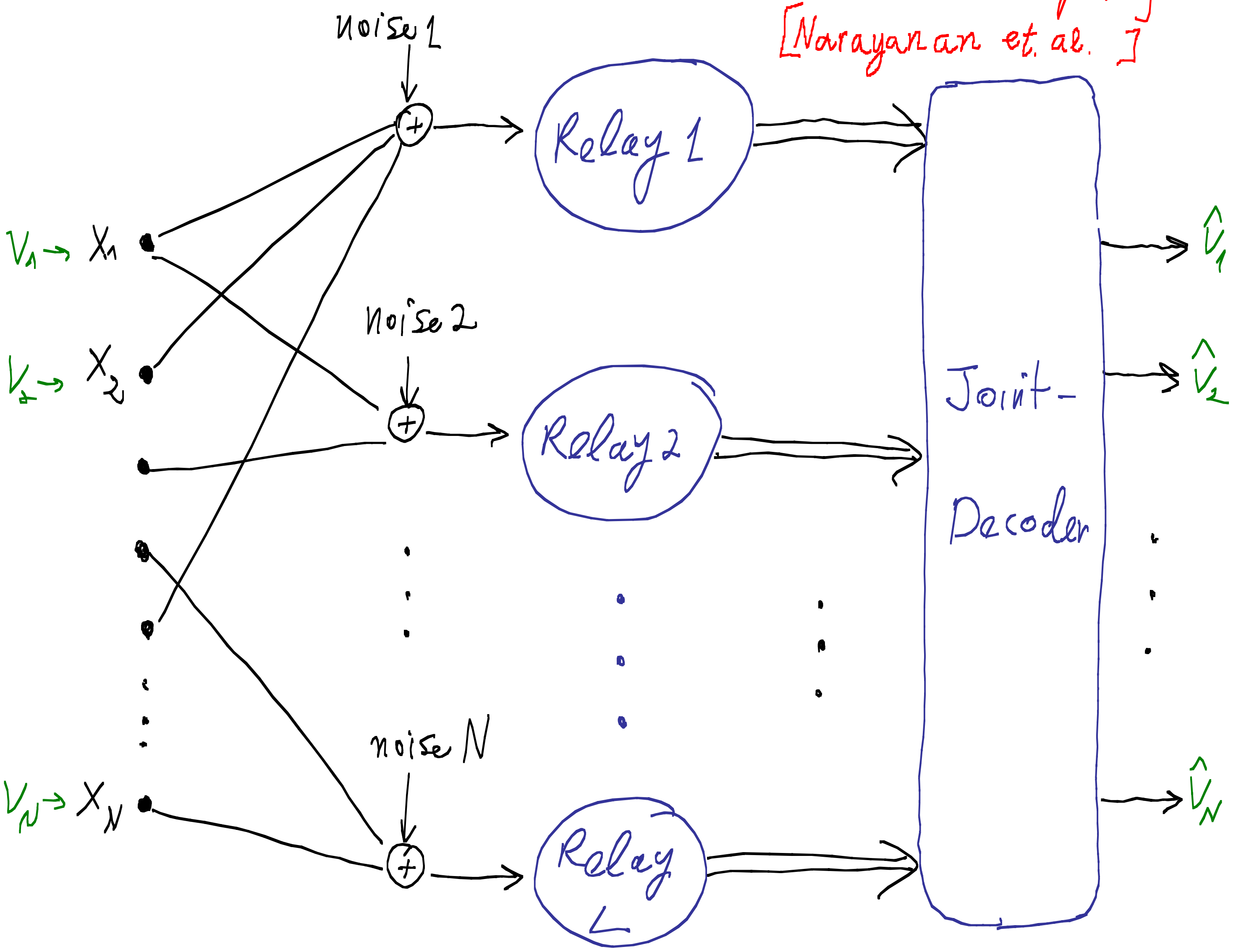
* In contrast, lattice DPC ...



...achieves rate sum $= \frac{1}{2}\log\left(\underset{=}{\frac{1}{2}} + SNR\right)$!

Lattice Coding for Noisy-Linear-Networks

[Nazer-Gastpar]
[Narayanan et. al.]



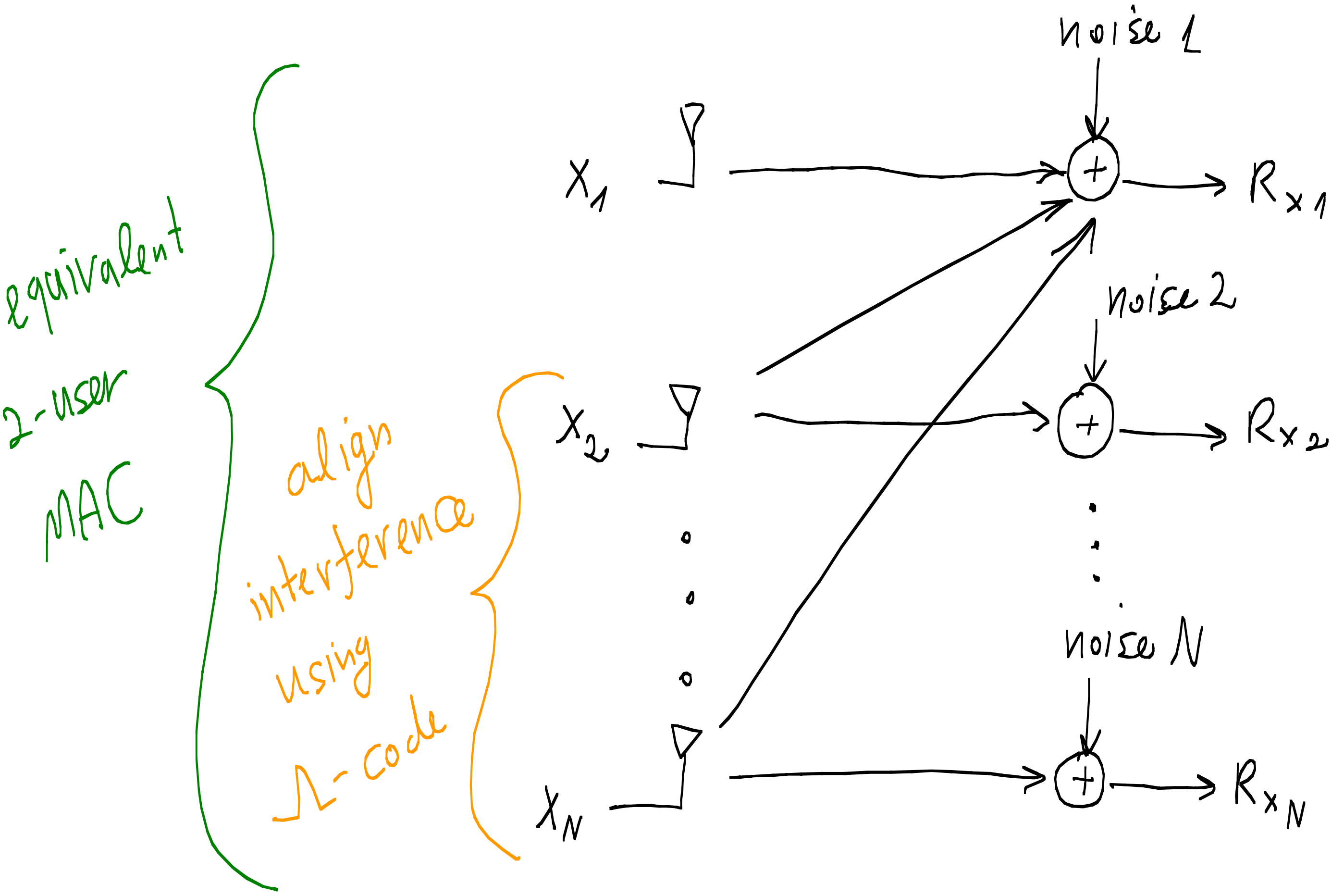
"digital" network coding : noiseless, bit pipes, random ✓ \ linear ✓ code

"analog" network coding : noisy, linear channels (interference), ~~random~~ \ lattice ✓ code

Interference Alignment

(in amplitude domain)

[Bresler - Parekh - Tse]

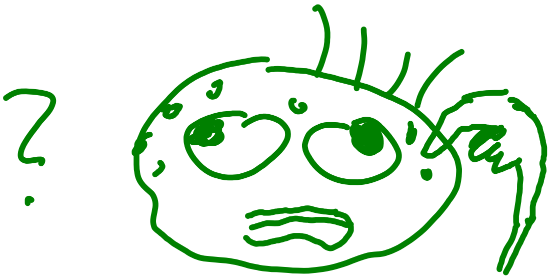


Lattice Alignment

	Align	must be linear	can be random
KM	reference signals =>	coarse lattice	fine (quantize) code
DMAC	i concentration points =>	coarse lattice	fine (channel) code
CO&F	desired codewords =>	fine lattice	coarse (shaping) code
IC	interefer codewords =>	fine lattice	coarse (shaping) code

Open Q 12:

More cases ?....



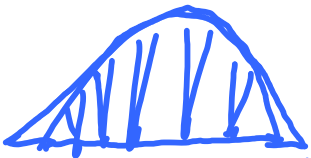
Why Lattices in Communication?

① a bridge from $n=1$  to $n=\infty$

= non-asymptotic analysis per dimension

② Algebraic (low complexity) Binning

= structured coding schemes for networks

③ bridge from Analog-to-  Digital

= Robust joint source-channel coding

④ Better than Random-Coding!

in distributed side-information problems

More ...

- * The gain of structure : interference channel [Ordentlich, Bresler, ...]
  error exponent in MAC [Haim, Kochman, Erez]
  a proof ?
- * Lattices in wire-tap channel [Yener, Poor, Shamai, Belfiore, Oggier ...]
- * General (non-additive) channels [Pradhan]
- * Simulation of Sources/Channels
- * How to design, encode & decode "good" lattices ?

Thank You !