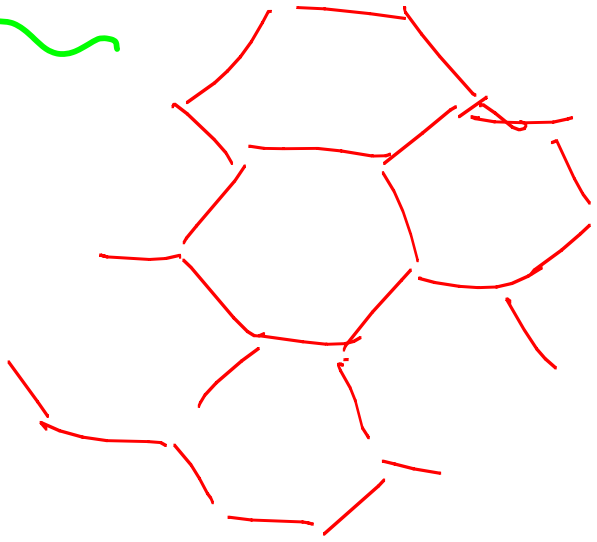
Lattices are Everywhere!



Rami Zamir

&

Meir Feder, Gregory Poltyrev, Shlomo Shamai
Uri Erez, Yael Frank-Dayan, Zvi Reznic,
Yuval Kochman, Tal Philosof, ...

Nature knows his Way...

* picture editing
by Kessem Zamir

Why Lattices in Communication?

1.

2.

3.

4.

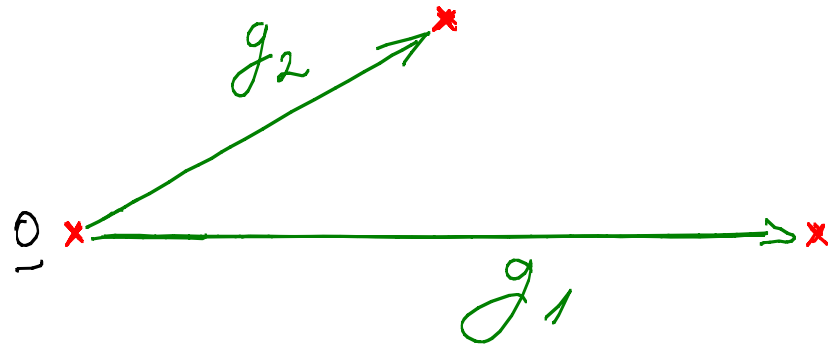
Lattice: Definition

$$\Lambda = \{ \underline{\underline{G}} \cdot \underline{i} \; : \; \underline{i} = \text{vector of integers } (0, \pm 1, \pm 2, \ldots) \}$$

- Λ: Lattice in $\mathbb{R}^k$
- $\underline{\underline{G}}$: Generator Matrix $k \times k$

Linearity: $\ell_1, \ell_2 \in \Lambda \Rightarrow \ell_1 + \ell_2 \in \Lambda$

$i \cdot \ell \in \Lambda$



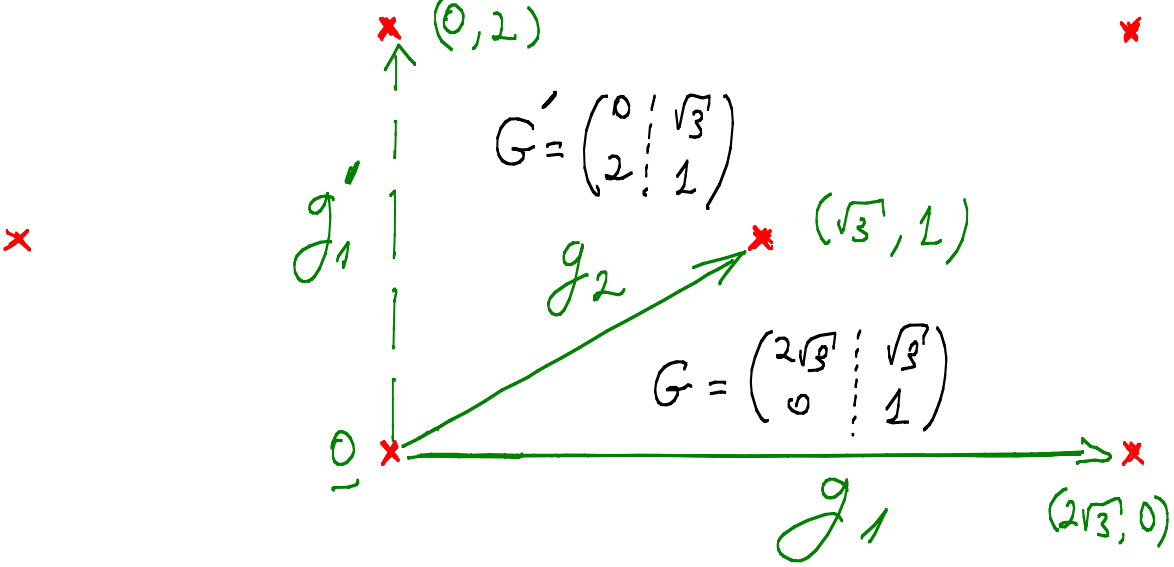
Lattice: Definition

$$\Lambda = \{ \underline{\underline{G}} \cdot \underline{i} \; : \; \underline{i} = \text{vector of integers} \}$$
$$(0, \pm 1, \pm 2, \ldots)$$

Λ: Lattice in $\mathbb{R}^k$

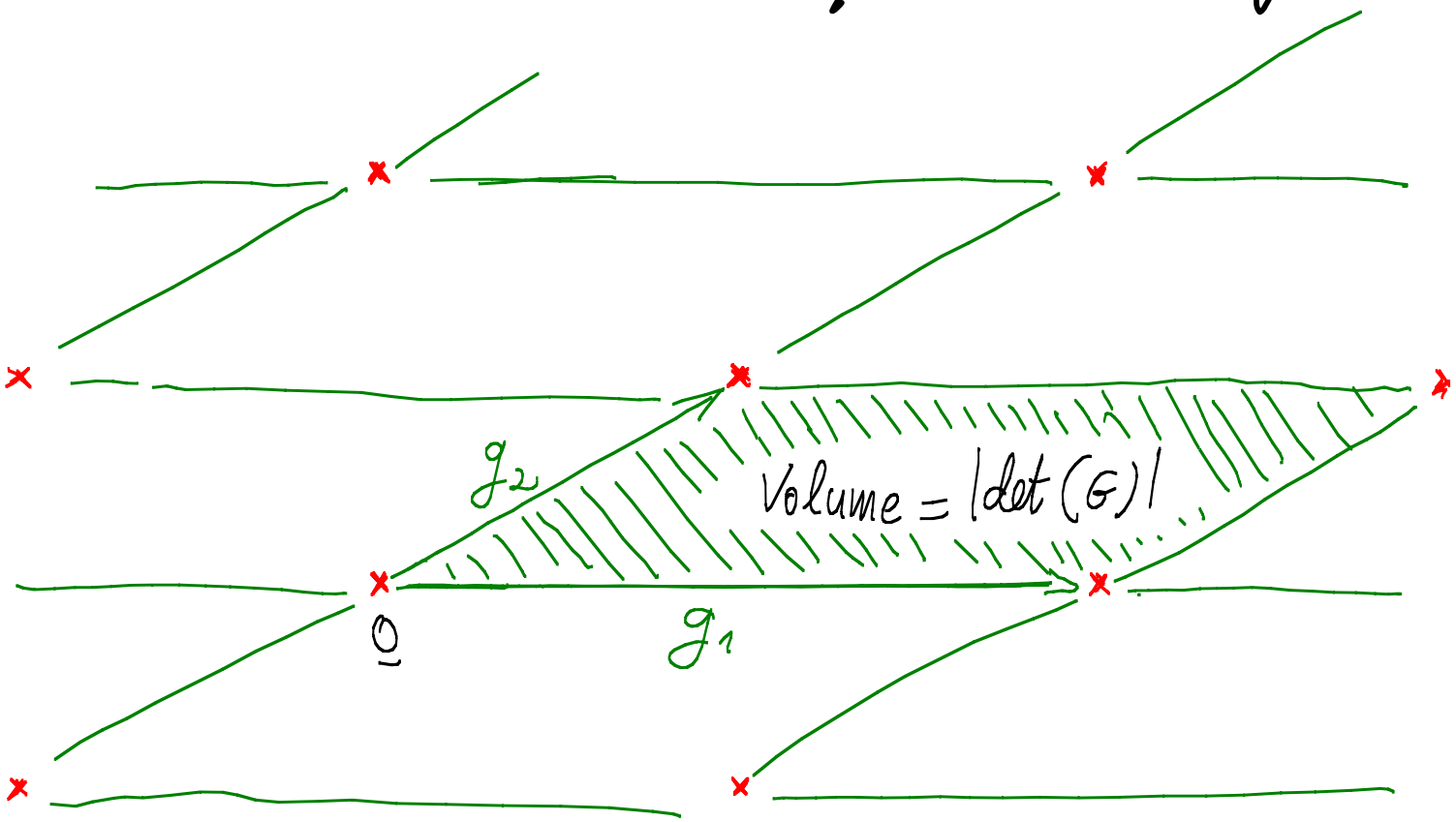
$\underline{\underline{G}}$: Generator Matrix $k \times k$

Linearity: $\underline{l}_1, \underline{l}_2 \in \Lambda \Rightarrow \underline{l}_1 + \underline{l}_2 \in \Lambda$



Lattice Partition:

Quantization / Decision Regions

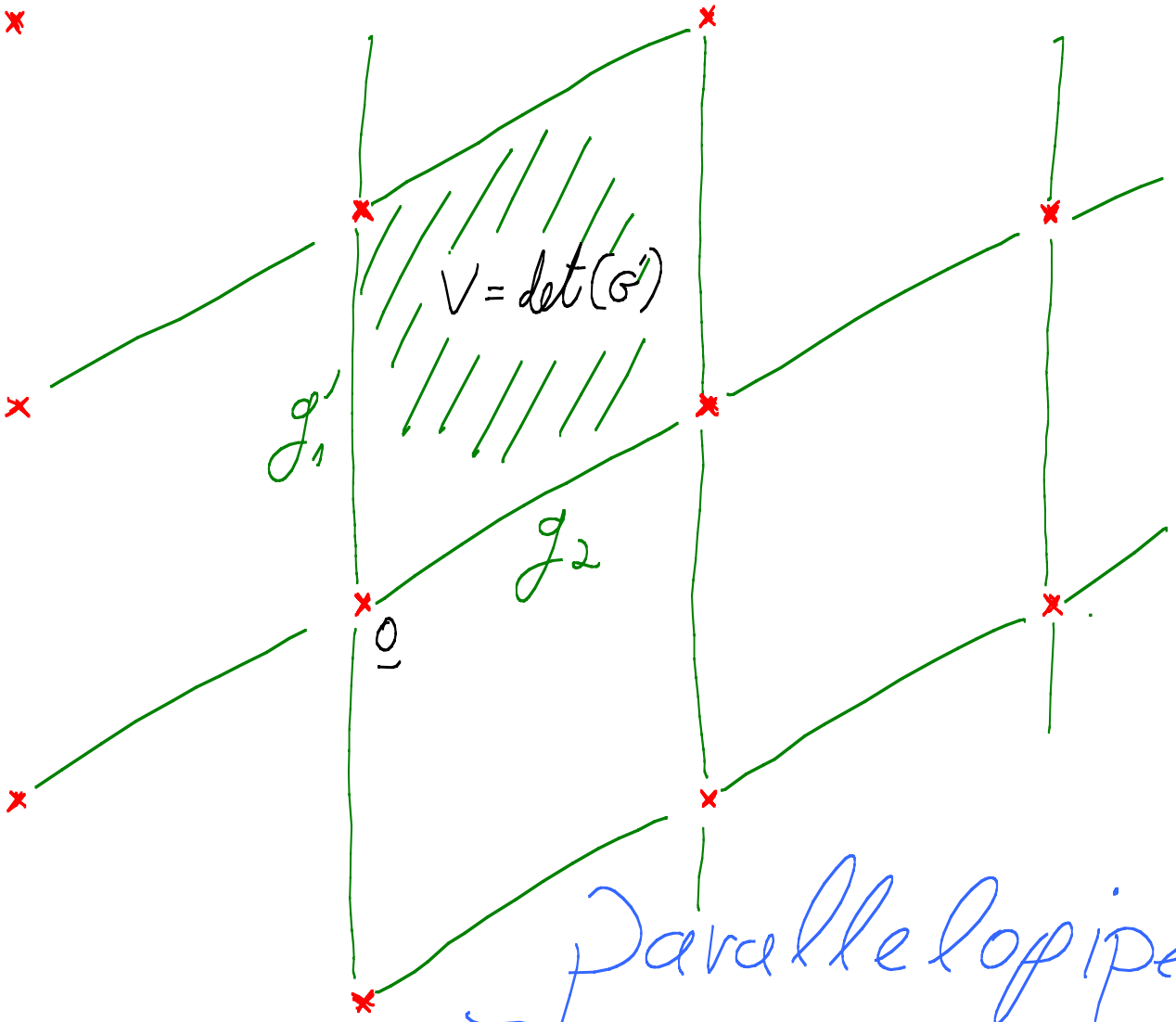


Parallelopipeds

$$P_0 = \{ \alpha_1 g_1 + \alpha_2 g_2 : \quad 0 \le \alpha_1, \alpha_2 \le 1 \}$$

$$\Lambda + P_0 = \mathbb{R}^k$$

Lattice Partition

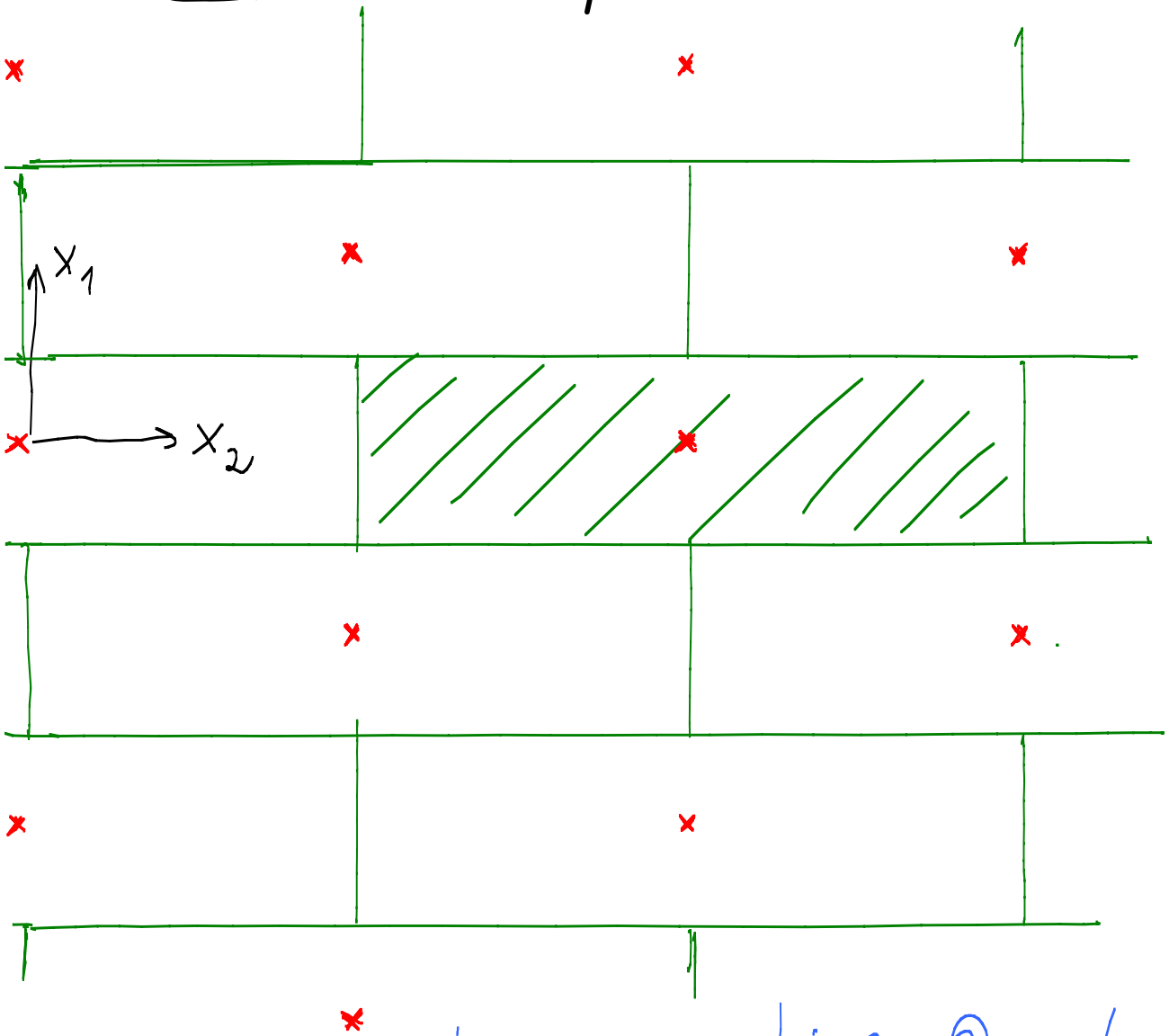


Parallelopipeds

$$P_0 = \{ \alpha_1 g_1' + \alpha_2 g_2 : \quad 0 \le \alpha_1, \alpha_2 \le 1 \}$$

Cell volume V is invariant of partition!

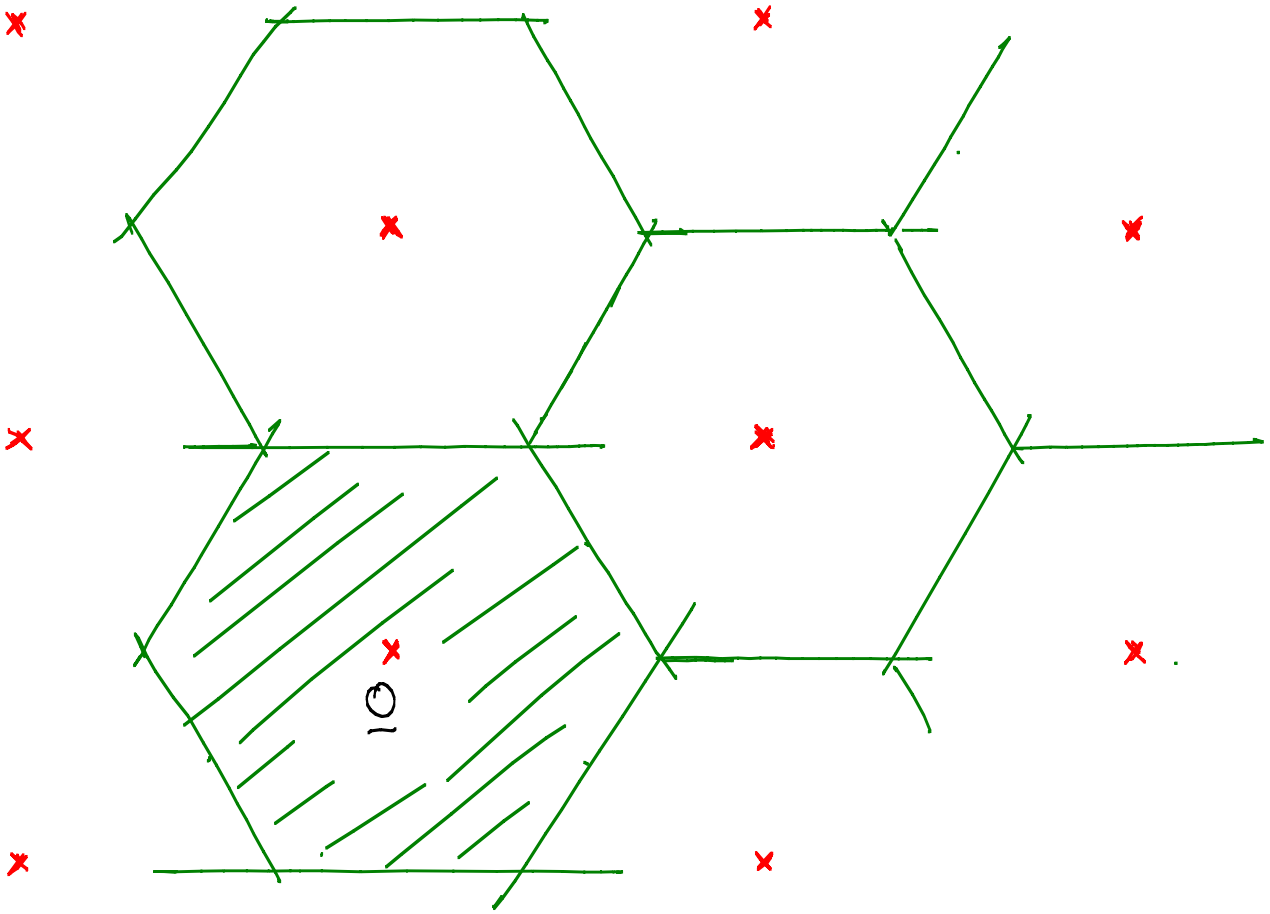
Lattice Partition



Sequential Quantization

$$Q(x_1, x_2) = \left(Q_1(x_1) \;,\; Q_2(x_2 \,;\, \text{parity}\{Q_1\}) \right)$$

Lattice Partition



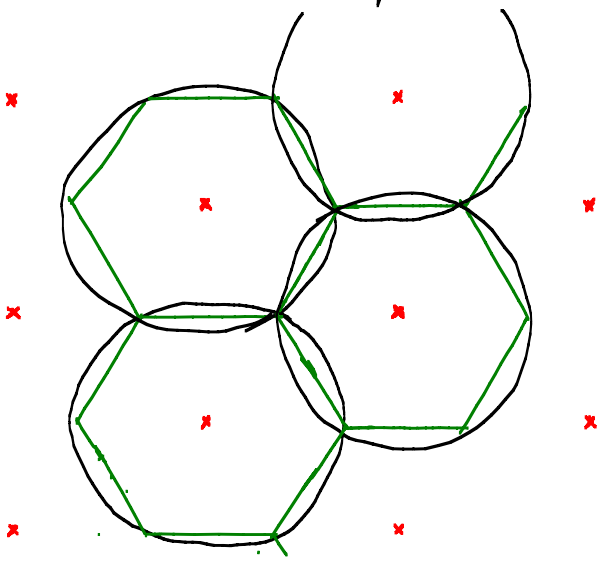
Voronoi Partition

$$V_0 = \left\{ x : \|x\| \leq \|x - l_i\|, \ \forall l_i \in \Lambda \right\}$$

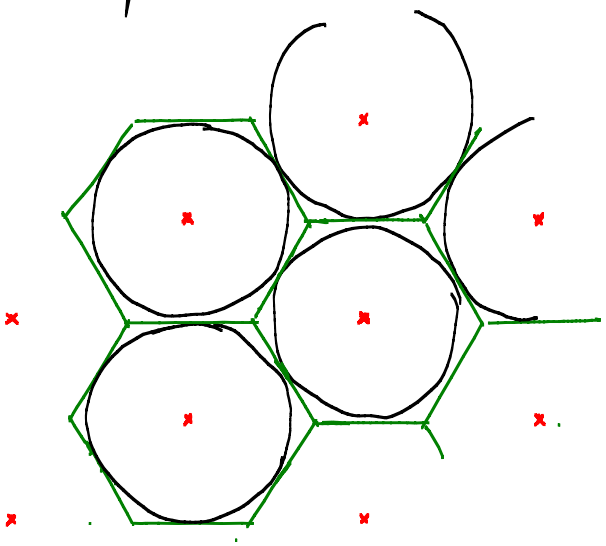
$\Rightarrow$ Minimum-Euclidean-distance quantization

Covering, Packing, Kissing Number & More....

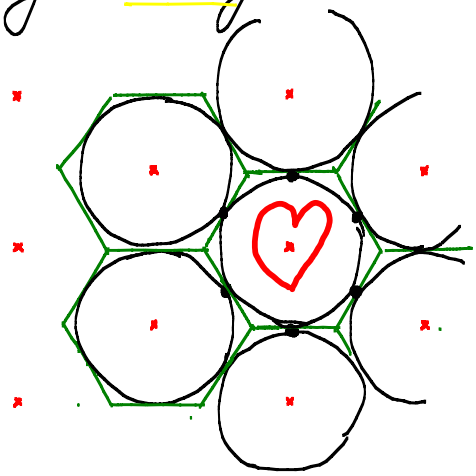
Covering $\mathbb{R}^k$ with (few) spheres



Packing (many) spheres in $\mathbb{R}^k$



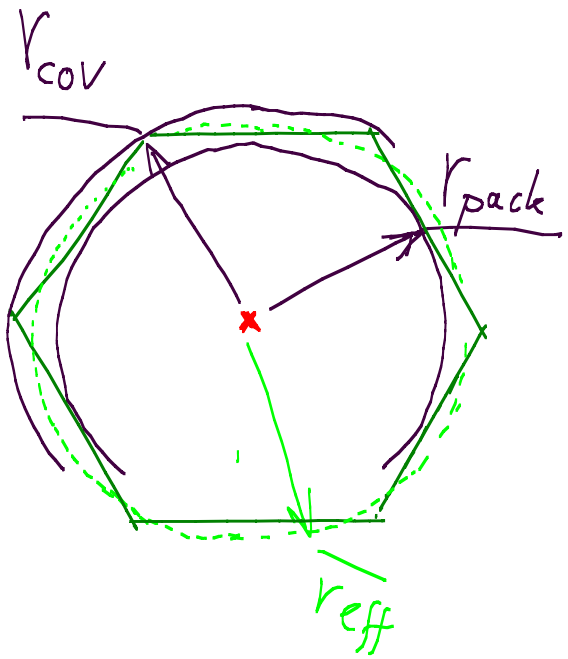
Kissing by (many) Spheres



&

good arrangements for quantization and AWGN channel coding

Figures of Merit



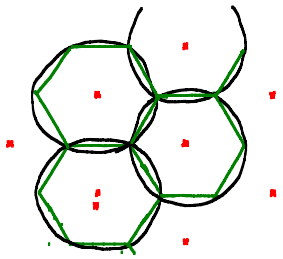
Radiuses:

r_{cov} = min sphere containing V_0

r_{pack} = max sphere contained in V_0

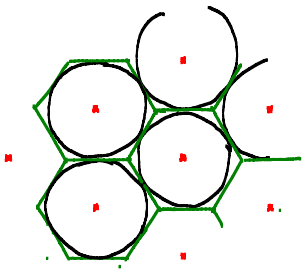
r_{eff} = Sphere with same volume

- **Covering efficiency:**



$$\rho_{cov}(\Lambda) = \frac{r_{cov}}{r_{eff}} > 1$$

- **Packing efficiency:**



$$\rho_{pack}(\Lambda) = \frac{r_{pack}}{r_{eff}} < 1$$

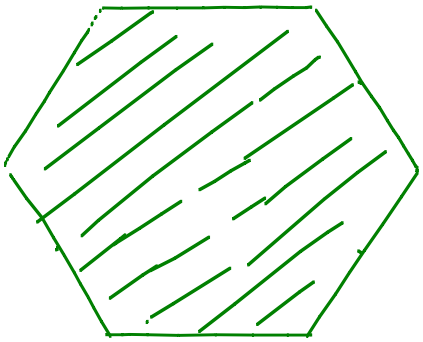
Figures of Merit (Continued)

- Quantization efficiency:

$\underline{X} \sim \text{Uniform}(\mathcal{V}_0)$

$\sigma^2(\Lambda) \triangleq \frac{1}{k} E\|X\|^2$

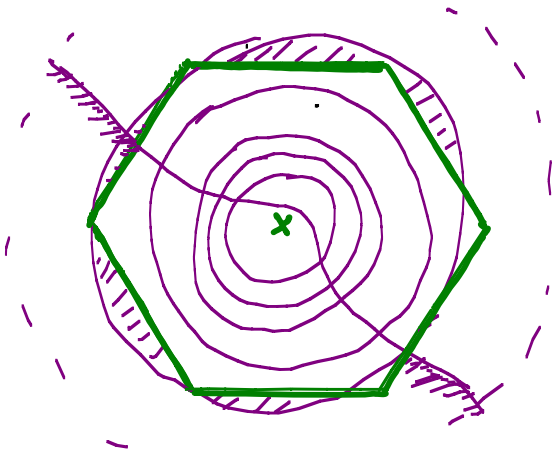
$G(\Lambda) \triangleq \frac{\sigma^2(\Lambda)}{V^{2/k}}$ = normalized second moment



- AWGN coding efficiency: $\underline{Z} \sim \text{AWGN } N(0, \sigma^2)$

$P_e \triangleq \Pr\{\underline{Z} \notin \mathcal{V}_0\}$

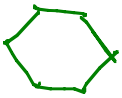
= "Poltyrev's error prob."



$\mu(\Lambda, P_e) \triangleq \frac{V^{2/k}}{\sigma^2}\Big|_{@P_e}$ = Volume-to-Noise Ratio

Good Lattices

* Best covering: $\min_{\Lambda \in \mathbb{R}^k} \theta_{cov}(\Lambda)$

$\mathbb{Z}$-lattice,  , B.C.C., ... ?

($k=1$) ($k=2$) ($k=3$)

* Best packing: $\max_{\Lambda \in \mathbb{R}^k} \theta_{pack}(\Lambda)$

$\mathbb{Z}$-lattice,  , F.C.C, ... ?

* Best lattice quantizer: $G_k \triangleq \min_{\Lambda \in \mathbb{R}^k} G(\Lambda)$

$G_1 = G(\mathbb{Z}) = \frac{1}{12}$, $G_2 = G($  $) = \frac{1}{12.5}$, ...

* Best AWGN channel code:

$$\mu_k(P_e) \triangleq \min_{\Lambda \in \mathbb{R}^k} \mu(\Lambda, P_e)$$

$\mu_1(P_e) = \mu(\mathbb{Z}, P_e) = 4 \cdot [Q^{-1}\{P_e/2\}]^2$ 

G_k as a function of k...

[Conway & Sloane Book 1988]

n.

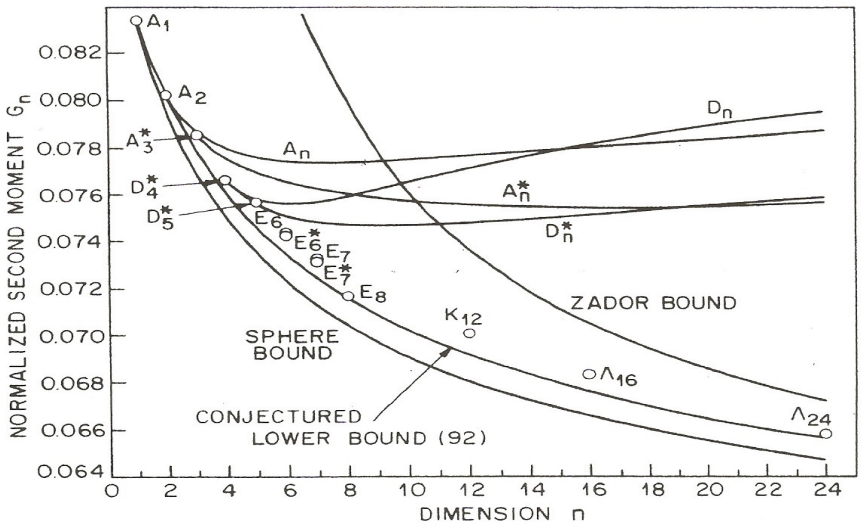


Figure 2.9. The best quantizers known in dimensions $n \leqslant 24$.

$\Lambda_k^{opt} \longrightarrow$

$G_k \longrightarrow$?

$\mu_k \longrightarrow$

Why Lattices in Communication?

1. a bridge from $n=1$  to $n=\infty$

   = non-asymptotic analysis per dimension

2.

3.

4.

It's Like Linear Codes in the Binary (Finite) Alphabet?

$$\mathcal{C} = \{ G \cdot \underline{u} : \underline{u} \in \{0,1\}^k \}$$

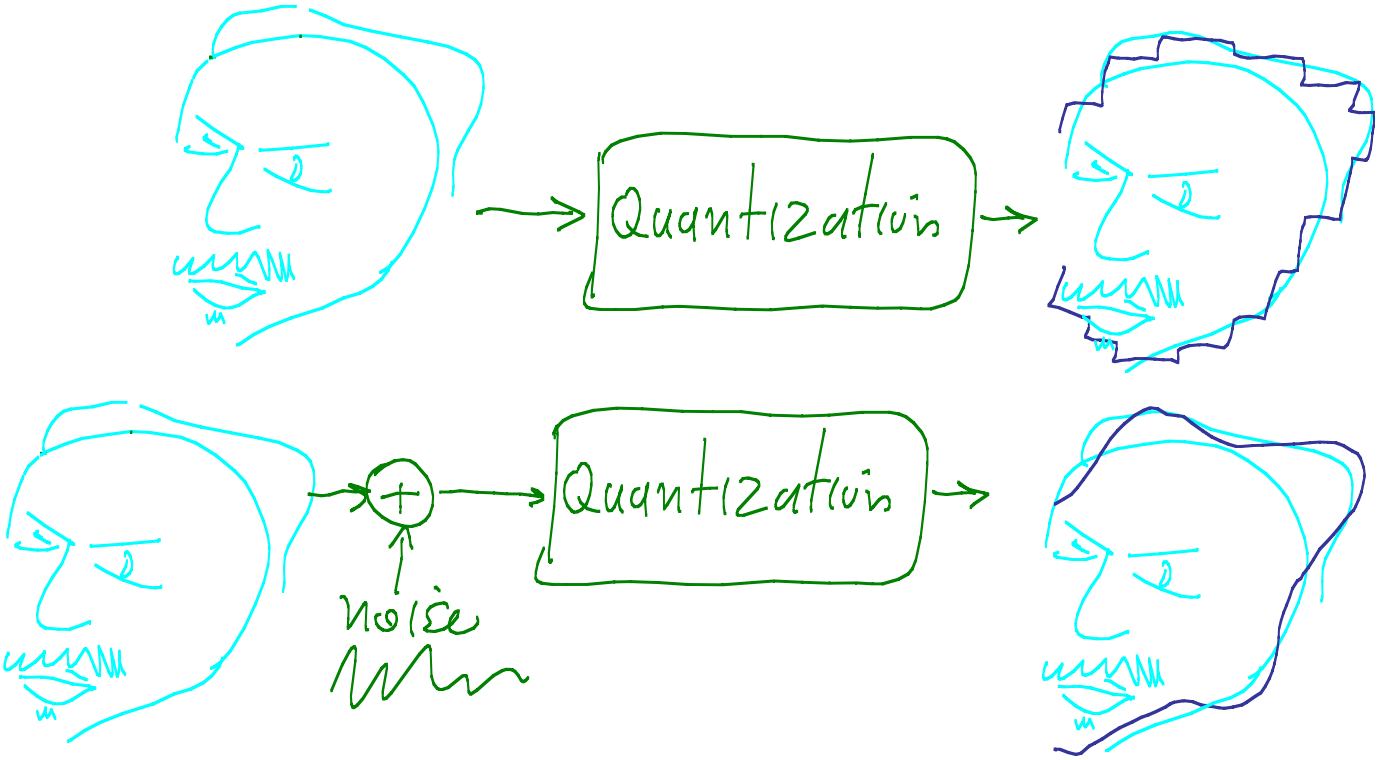
G: $n \times k$ generator matrix

Linear k-dim subspace

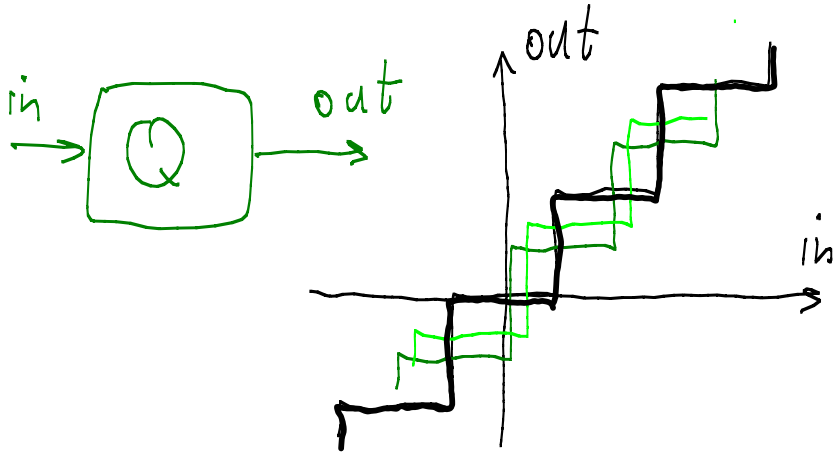
- $\underline{0} \in \mathcal{C}$
- Parity check: $\underline{\underline{H}} \cdot \underline{c} = \underline{0}$, $\forall \underline{c} \in \mathcal{C}$ ($\underline{\underline{H}}$: $(n-k) \times n$, $\underline{0}$: $(n-k) \times 1$)
- Linearity: $c_1, c_2 \in \mathcal{C} \Rightarrow c_1 \oplus c_2 \in \mathcal{C}$
- Coset: $\{ \underline{x} : \underline{\underline{H}} \cdot \underline{x} = \underline{s} \}$ ($\underline{x}$: $n \times 1$, $\underline{\underline{H}}$: $(n-k) \times n$, $\underline{s}$: $(n-k) \times 1$)

Dithered Quantization

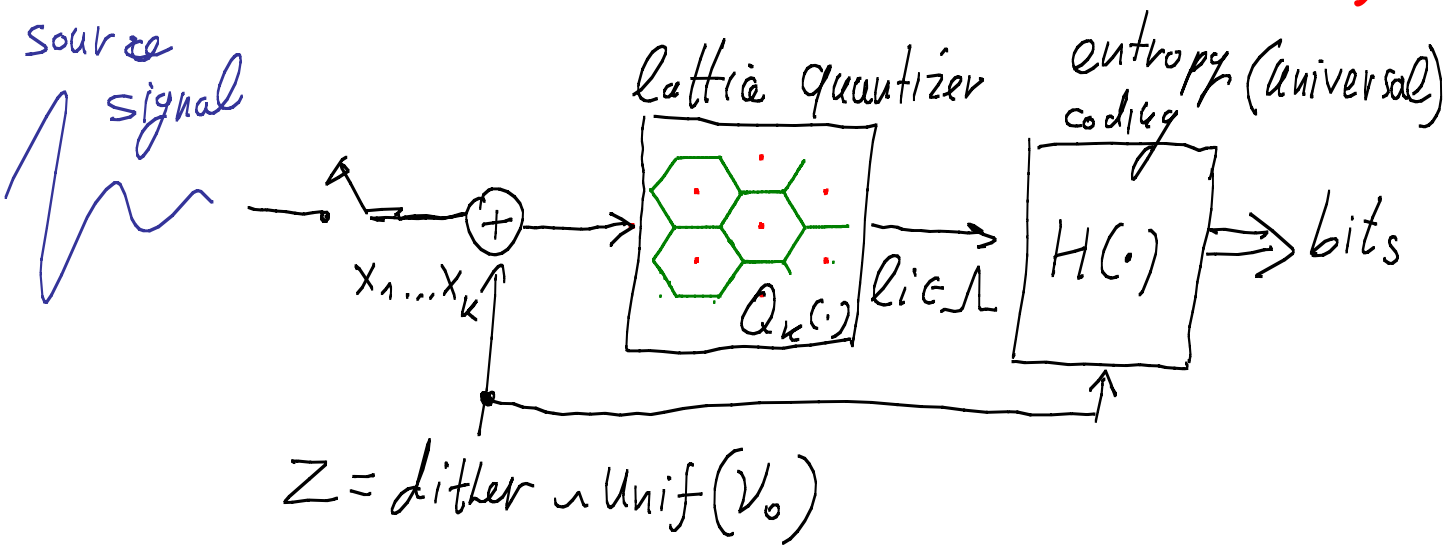
- dither for perceptual reasons:



- dither for analytical reasons:



Universal Quantization (Zi 85)



- Subtractive Dither (Pseudo Random Noise) $\Rightarrow$

$$\text{Distortion} = E\|Q_k(x+Z) - Z\|^2 = E\|Z\|^2$$

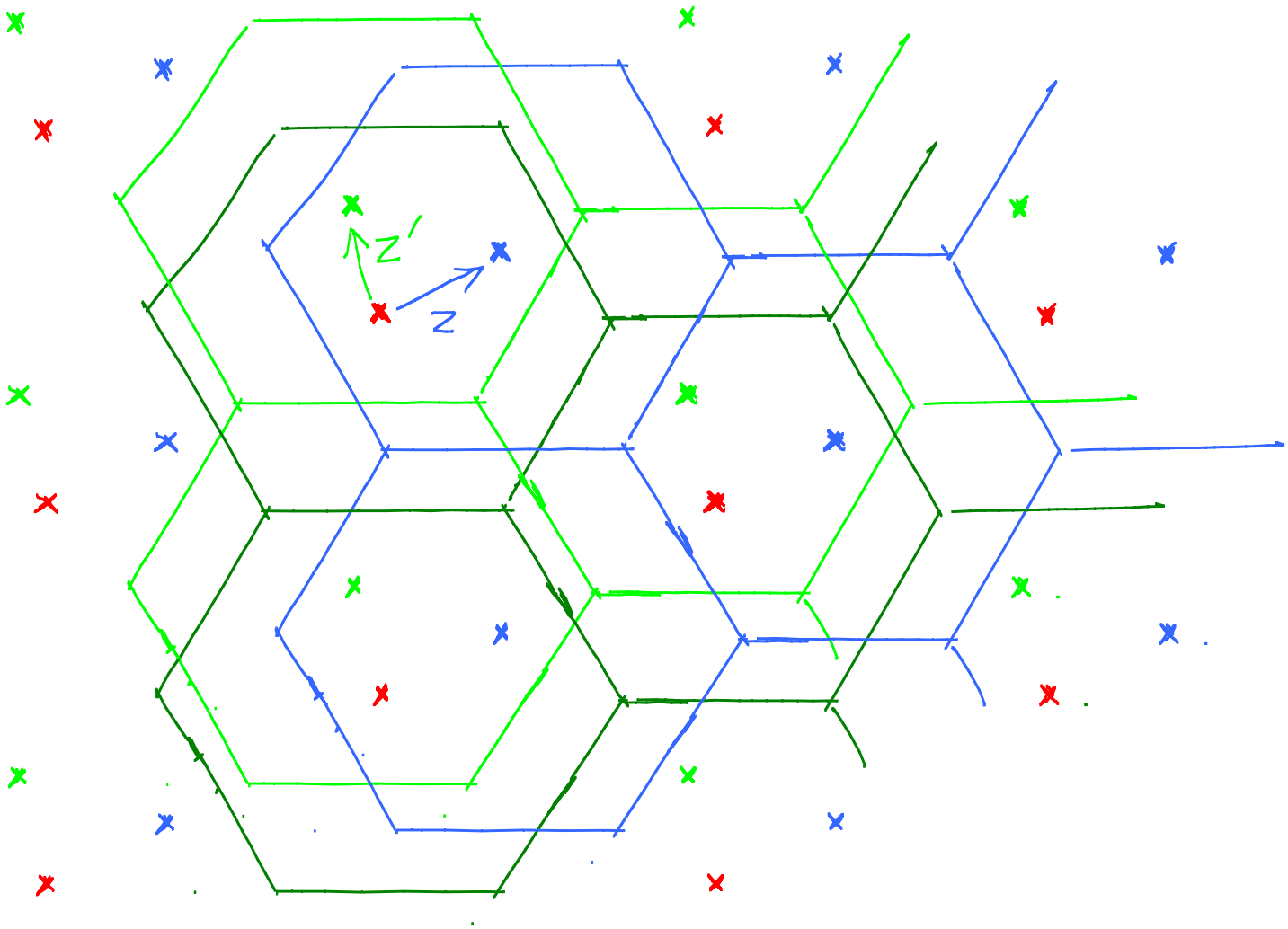
$$= k \cdot G(\Lambda) \quad \text{invariant with } x$$

- Rate Redundancy: $H(Q_1(X+Z)|Z) - H(Q_1^{opt}(X)) \leq 0.754$ Bit

- If Gersho's conjecture is true for good lattices

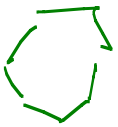
$\Rightarrow \lim_{k\to\infty} H(Q_k|Z) - H(Q_k^{opt}) \leq \frac{1}{2}$ Bit

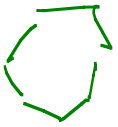
$$Q_k(x+Z) - Z$$



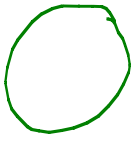
$\Rightarrow$ Random shift of the lattice quantizer

Gersho's Conjecture

The best space-filling-polytope  in $\mathbb{R}^k$ satisfies

$$G\left(\text{  }\right) \xrightarrow[k\to\infty]{} \frac{1}{2\pi e}$$

Note that...

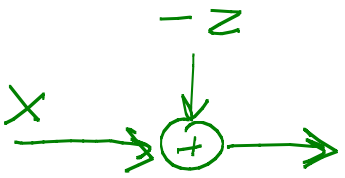
(1) $G_k^* \triangleq G\left(\text{  }\right) \xrightarrow[k\to\infty]{} \frac{1}{2\pi e}$

(2) Iso-perimetric inequality:
Ball has the minimum diameter & second moment among all shapes of given volume!

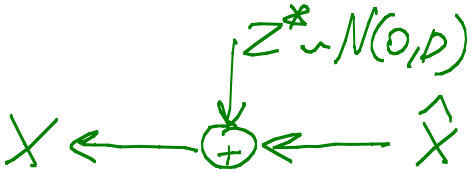
Can "good" lattice cells approximate Balls (as $k\to\infty$)?...

Universal Quantization (Cont. Z & Feder 91)

$$H(Q_\Lambda|Z) = I(X; X-Z)$$



$$R(D) = I(X;\hat{X})$$



Universal Bound

$$\frac{1}{k}H(Q_k|Z) - R(D) \le \frac{1}{2} + \frac{1}{2}\log(2\pi e G_k) \xrightarrow[k\to\infty]{\text{gcl}} \frac{1}{2}$$

worst case: $X \sim N(0,\sigma^2)$, $D=\sigma^2$

High Resolution Quantization

$$\frac{1}{k}H(Q_k|Z) - R_{SLB}(D) = \frac{1}{k}D(\Xi;\Xi^*) = \frac{1}{2}\log(2\pi e G_k)$$

gcl → 0 as $k\to\infty$

Shannon Lower Bound

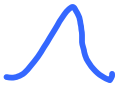
Divergence of Dither from Gaussianity

Can the Dither be Gaussian ??

Morals...

1. Entropy Coded Dithered (Lattice) Quantization (E.C.D.Q.) simulates an "additive noise test channel"

2. As $k \to \infty$, simulates AWGN channel —
   — provided Gersho's Conjecture for Lattices is true....



3. Universal system looses $\frac{1}{2}$ bit @ low resolution
   Optimal @ H.R.Q. —
   — provived G.C.L. is true...

Good Lattices

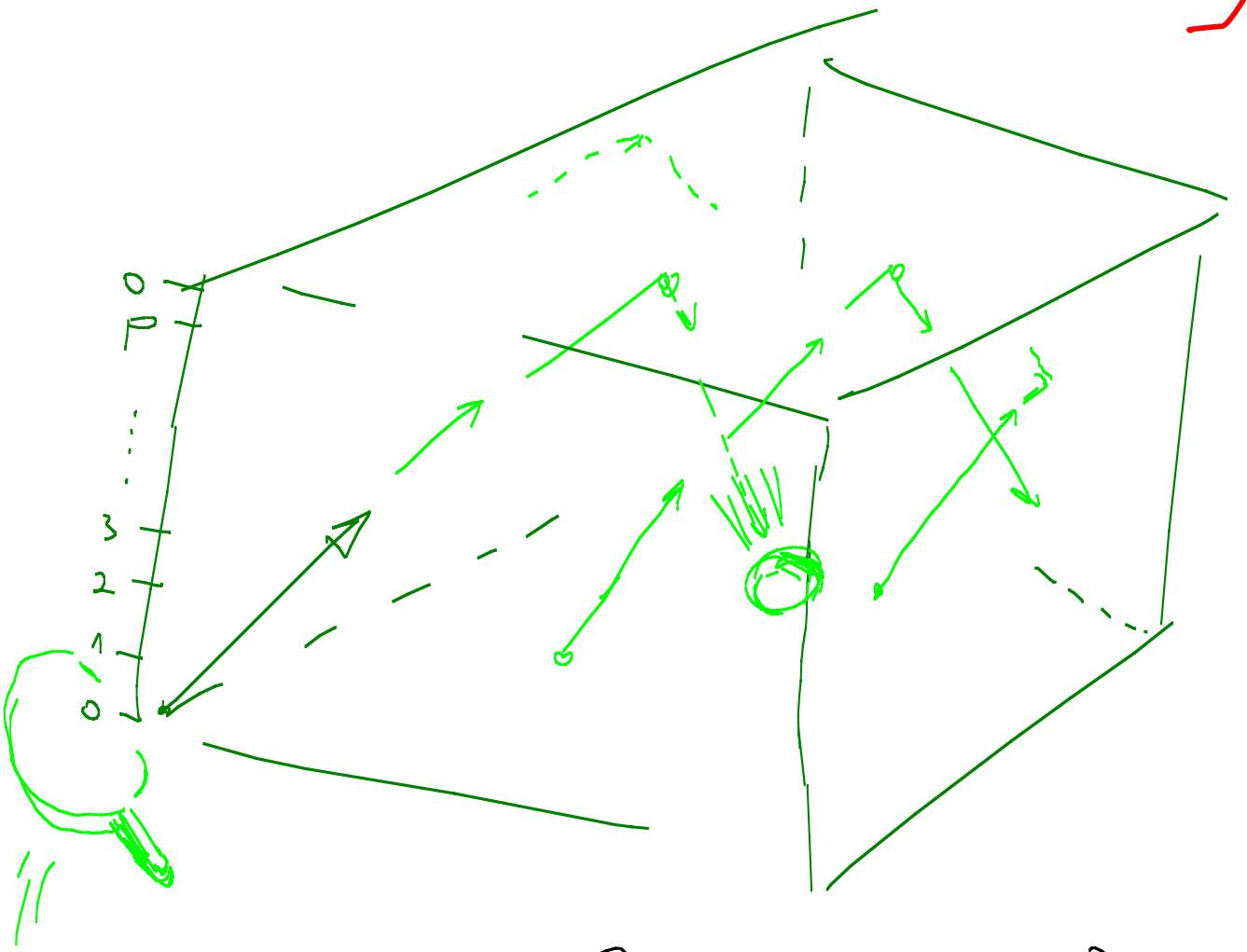
- ✓ good coverings exist $\quad \rho_{cov}(\Lambda_k^*) \to 1$ [Rogers]
- ✓ packings exist with $\quad \rho_{pack}(\Lambda_k^*) > \frac{1}{2}$ [Minkowski-Hlawka]
- ✓ good channel codes exist with $\quad \mu(\Lambda_k^*, p_e) \to 2\pi e$ [de-Buda, Loeliger]
- ✓ Covering $\Rightarrow$ Quantization [Poltyrev, Z&Feder]
- ✓ $\mathrm{cov}(\mathrm{dither}) = \sigma^2(\Lambda_k^*) \cdot \underline{\underline{I}} \Rightarrow$ dither is white [Z&F]
- ✓ dither projection $\longrightarrow$ AWGN [Z&Feder]
- ✓ Simultaneous goodness ($k \to \infty$) [Erez Litsyn Z]

(covering, packing, quantization, AWGN ch.)

- ✓ Other distance measures [ELZ], other dither distrib. [Gariby Erez]

The Loeliger-Erez Random Lattice Ensemble

Λ_∞

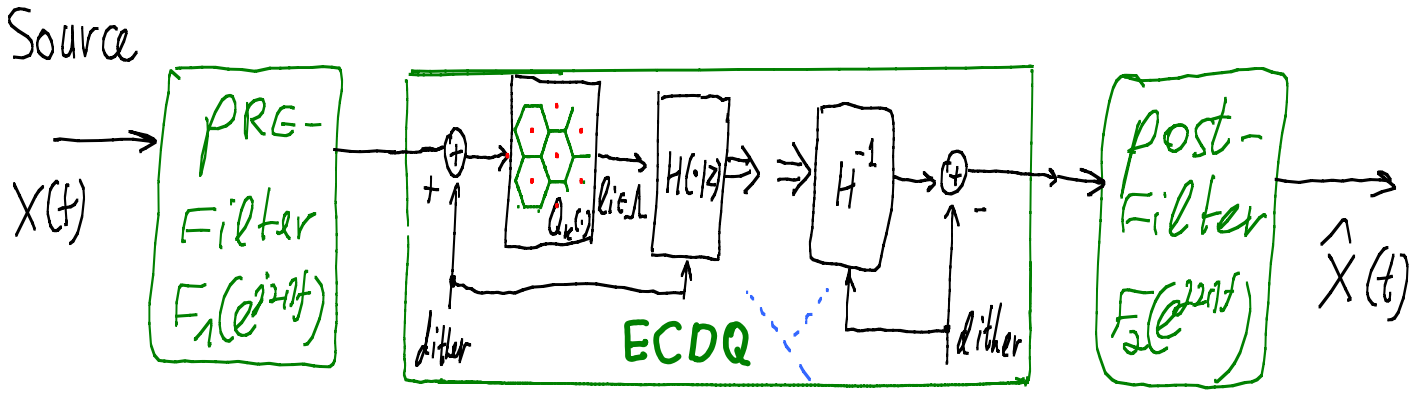


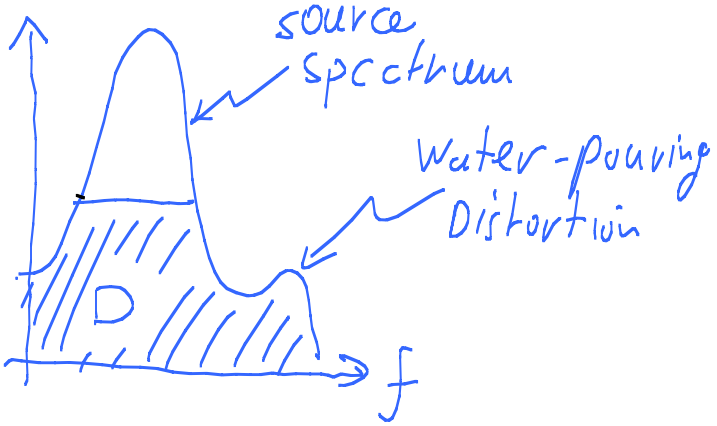
$$\Lambda \cap \text{cube} = \{ i \cdot \underline{X} \bmod p \}$$

$$\Lambda = \text{construction A}$$

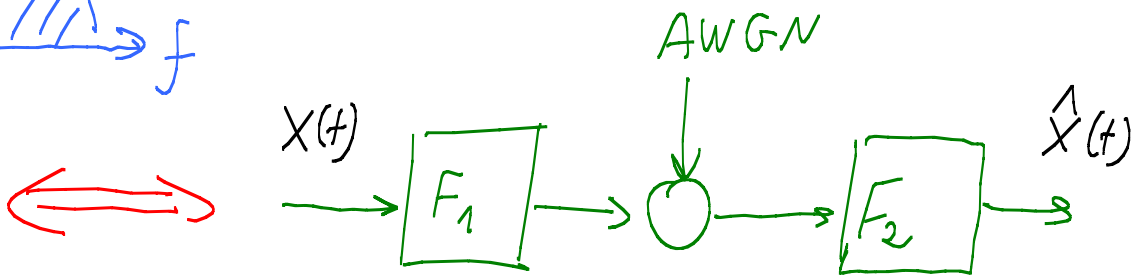
p = prime , $\underline{X} \sim \text{unif}\{p \times p \times \cdots \times p\}$

Pre-/post-Filtered ECDQ for Colored Sources





Entropy coding with memory



$$\Longrightarrow \quad \bar{H}(Q_k|z) = R^*(D) + \frac{1}{2}\log(2\pi e G_k)$$

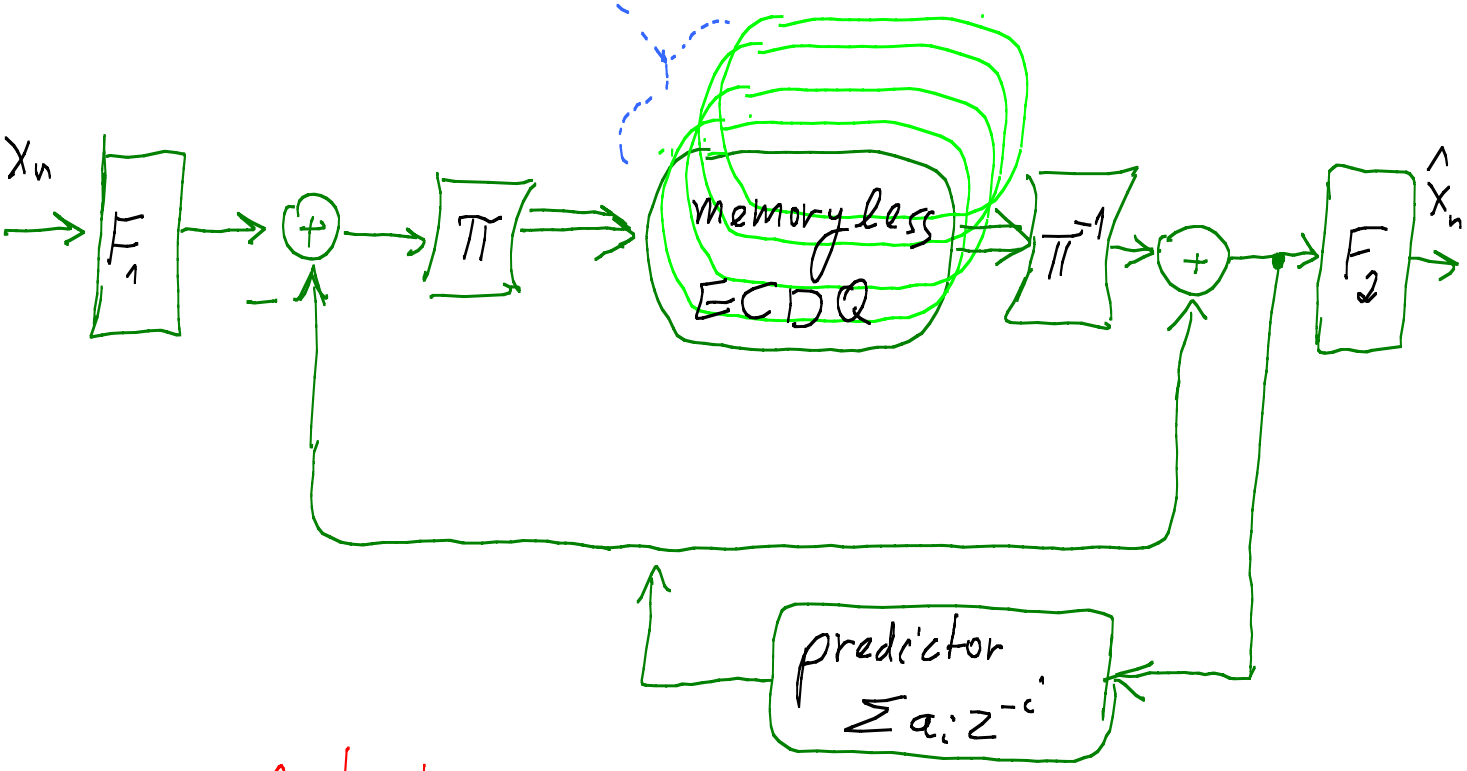
$\rightarrow$ Gaussian R-D-F

$k \to \infty$

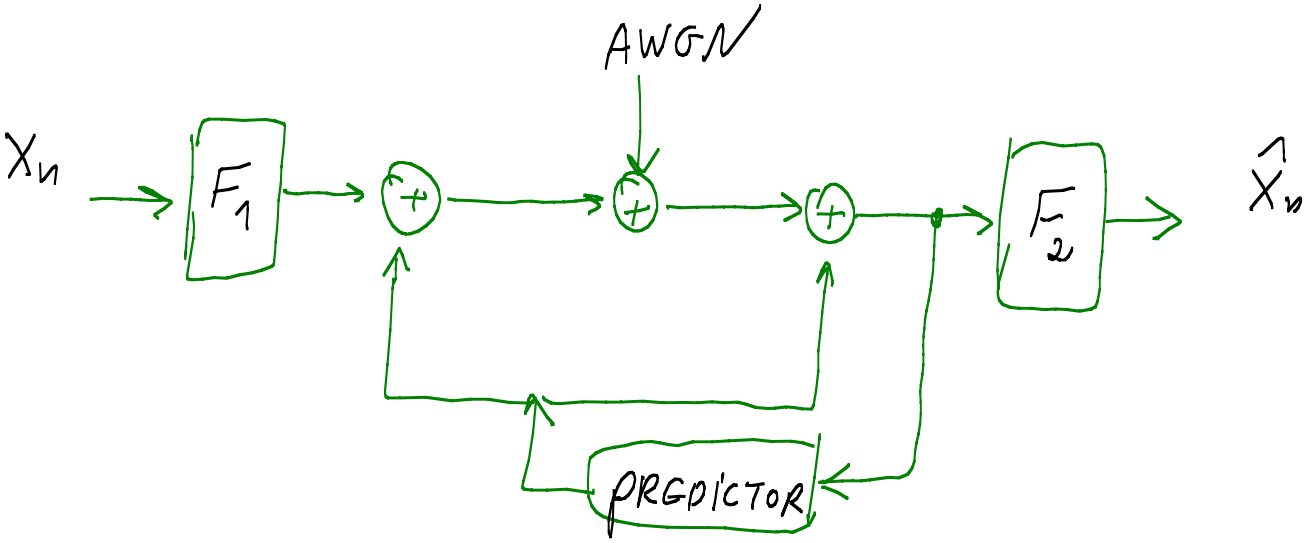
ECDQ in Predictive Coding (DPCM)

Q_Λ over parallel prediction loops

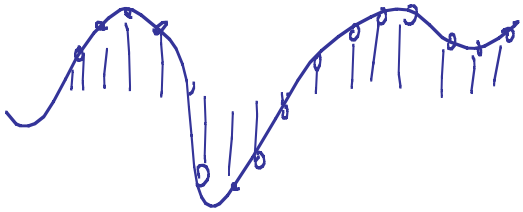
[Z & Kochman & Erez]

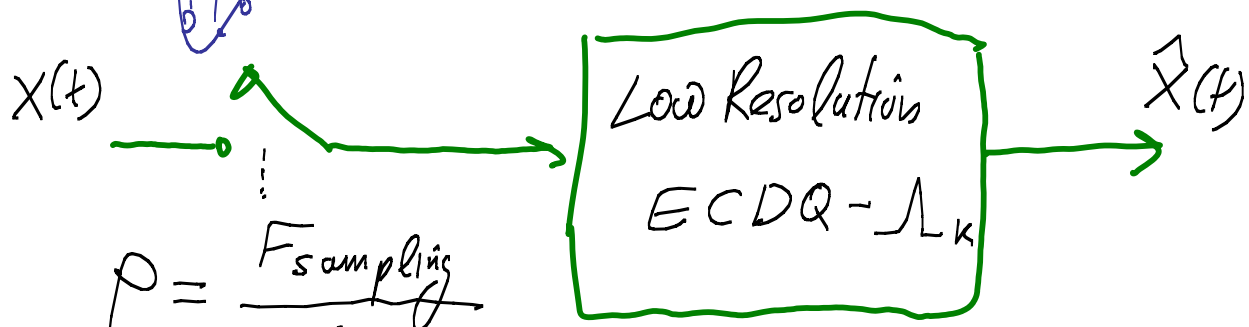


equivalent to ...



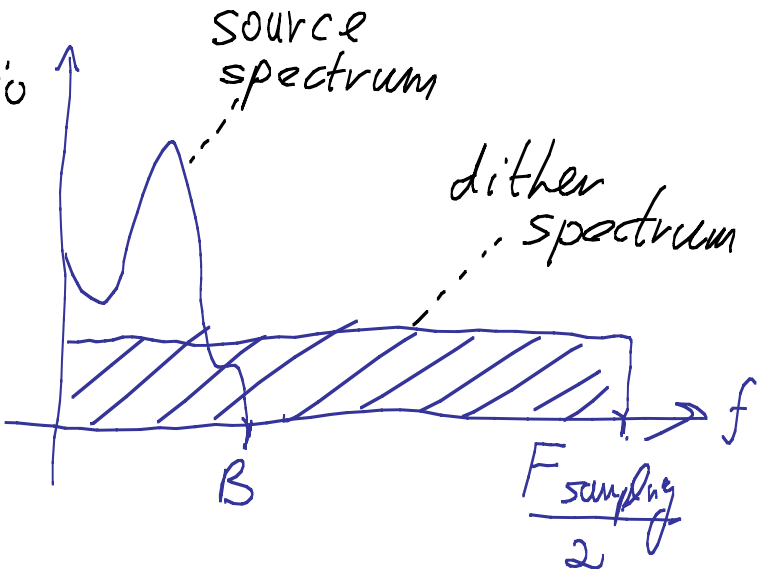
Oversampling ECDQ





$$\rho = \frac{F_{sampling}}{2B}$$

= oversampling ratio

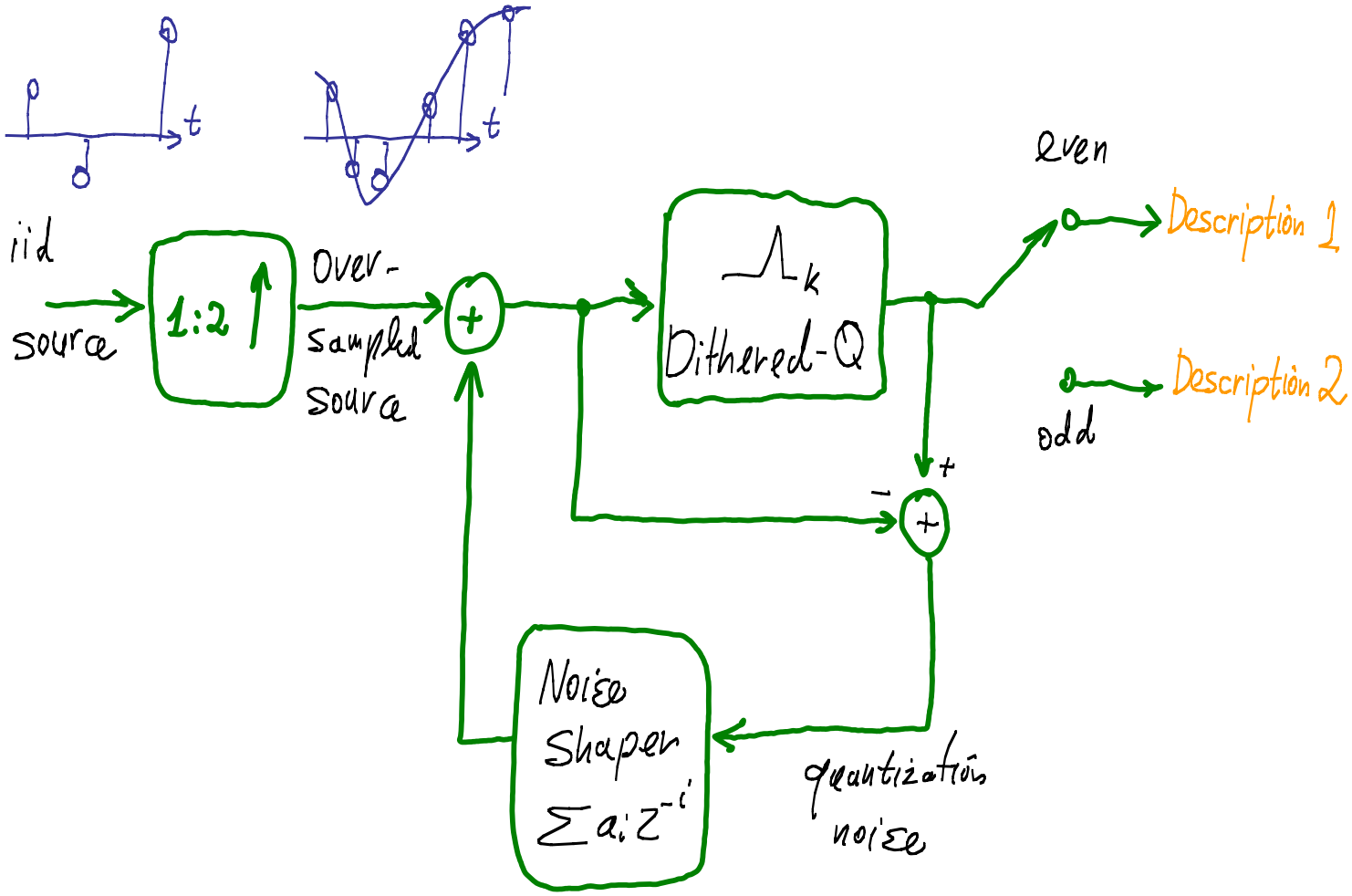


Conclusions:

$K = \infty \Rightarrow$ R-D performance invariant to ρ

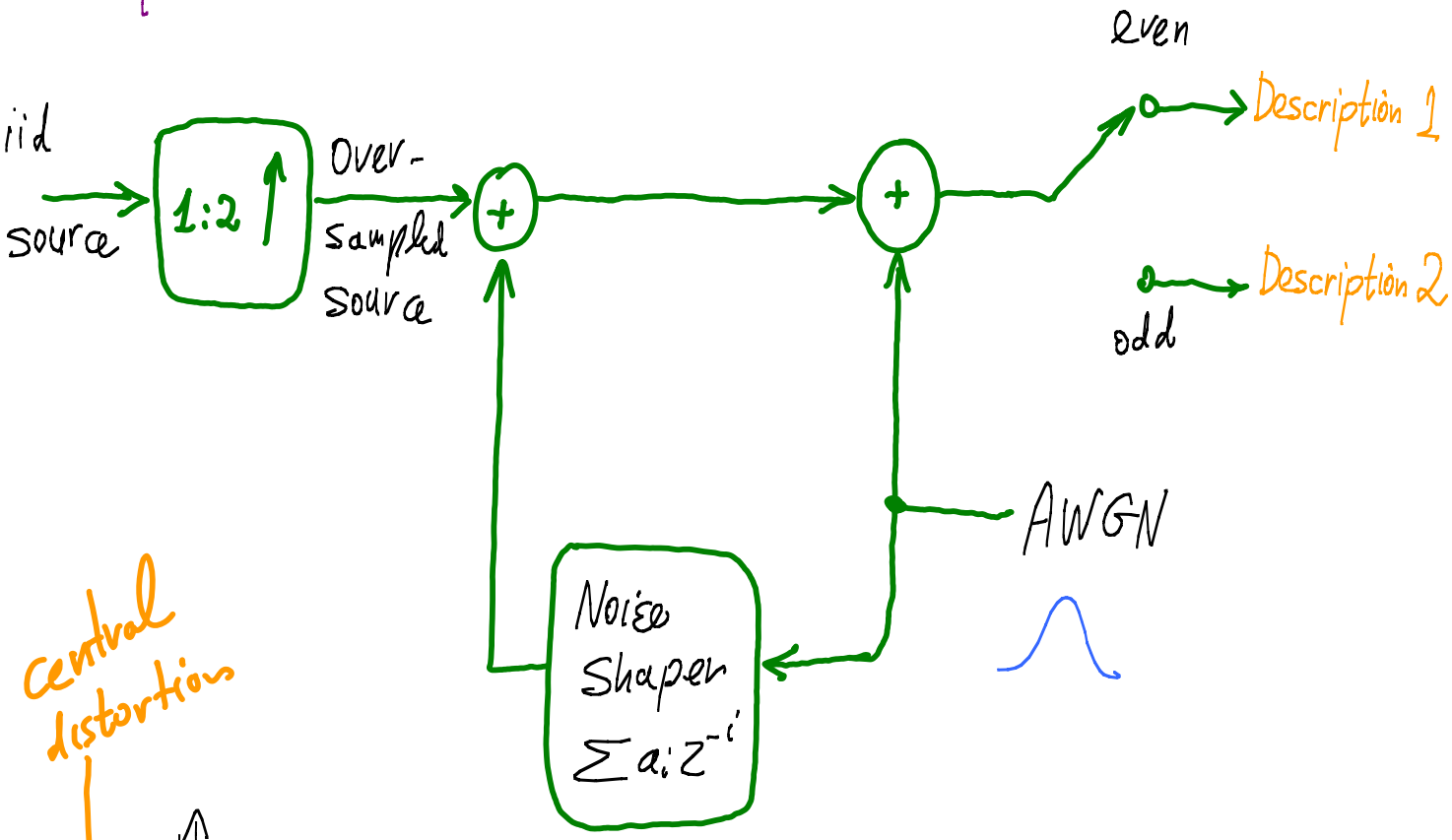
$K < \infty \Rightarrow$ R-D performance $\searrow$ ρ.

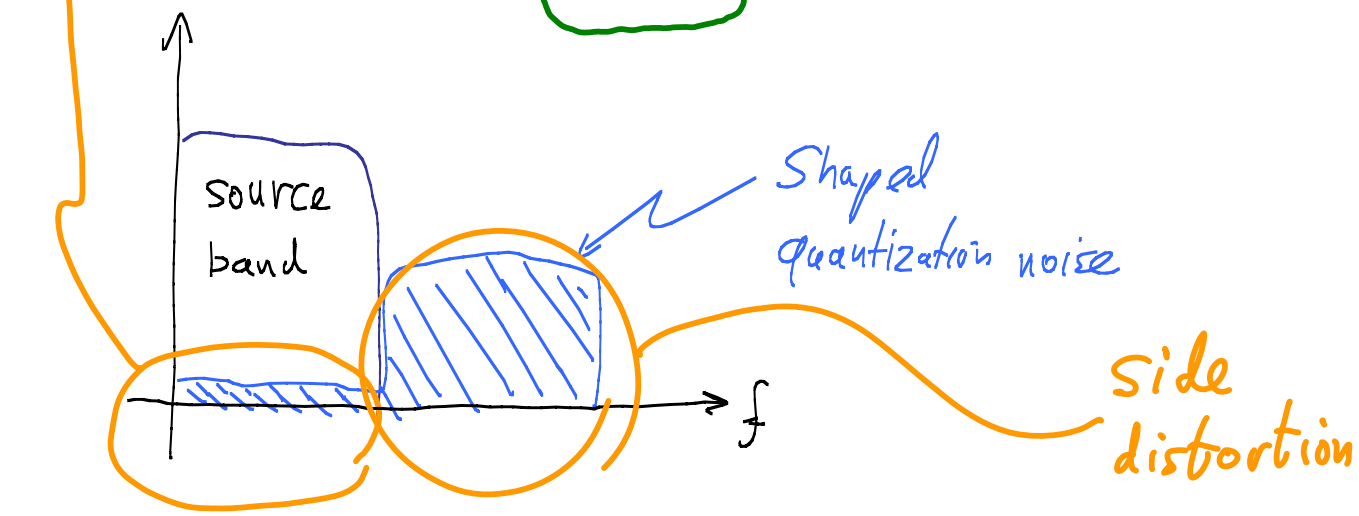
Multiple Descriptions by Oversampling & Noise Shaping



Multiple Descriptions by Oversampling & Noise Shaping

equivalent to ...





Why Lattices in Communication?

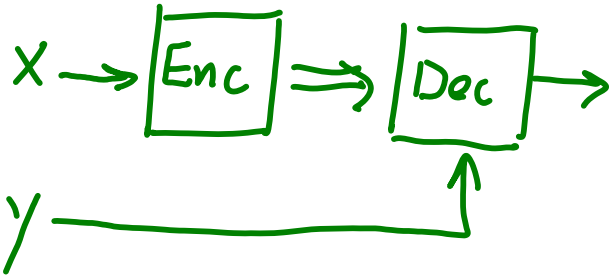
1. a bridge from $n=1$  to $n=\infty$
   = non-asymptotic analysis per dimension

2. Algebraic (low complexity) Binning
   = structured coding schemes for networks

3.

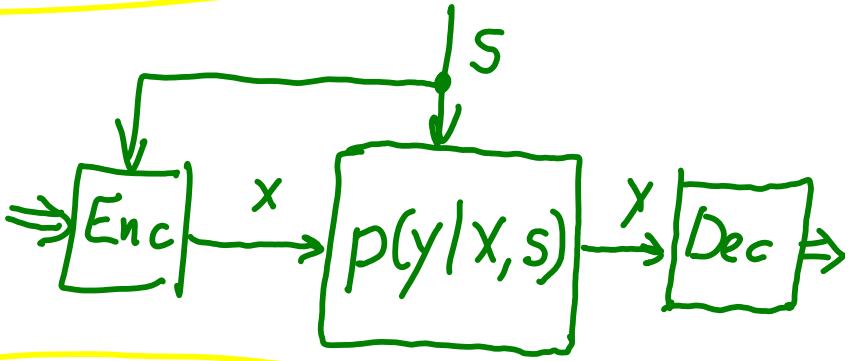
4.

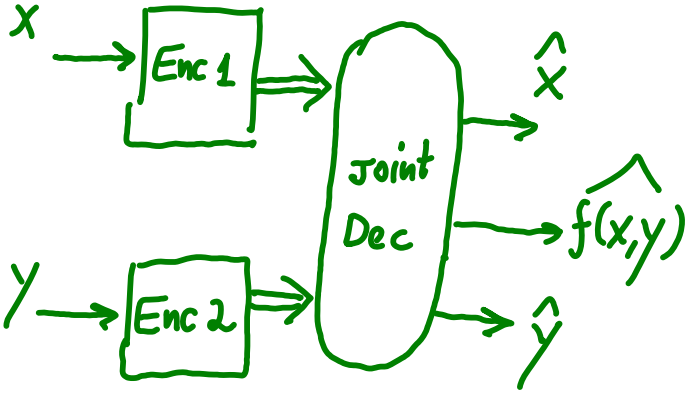
Lattices in Multi-Terminal Problems



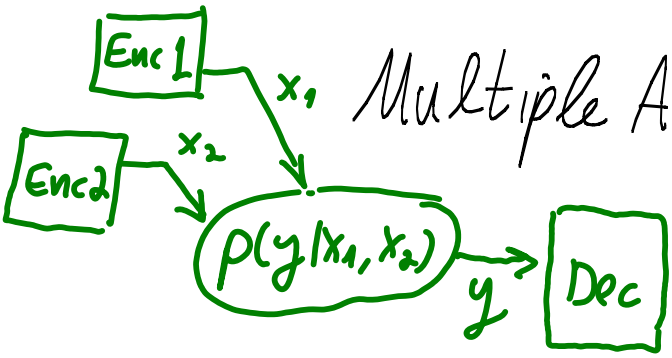
Source coding with Side Information

Channel Coding with Side Information

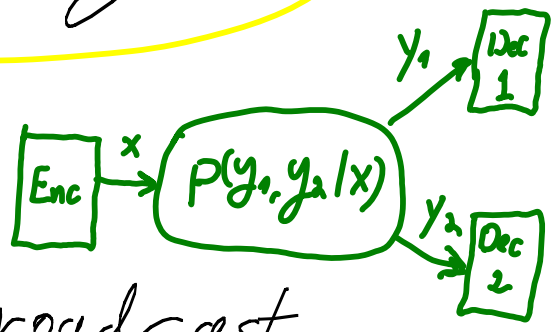




Multi-terminal Source coding



Multiple Access & Broadcast Channels



Nested Lattices

$$\Lambda_2 \subset \Lambda_1 \Rightarrow \underline{\underline{G_2}} = \underline{\underline{G_1}} \cdot \underline{\underline{J}}$$

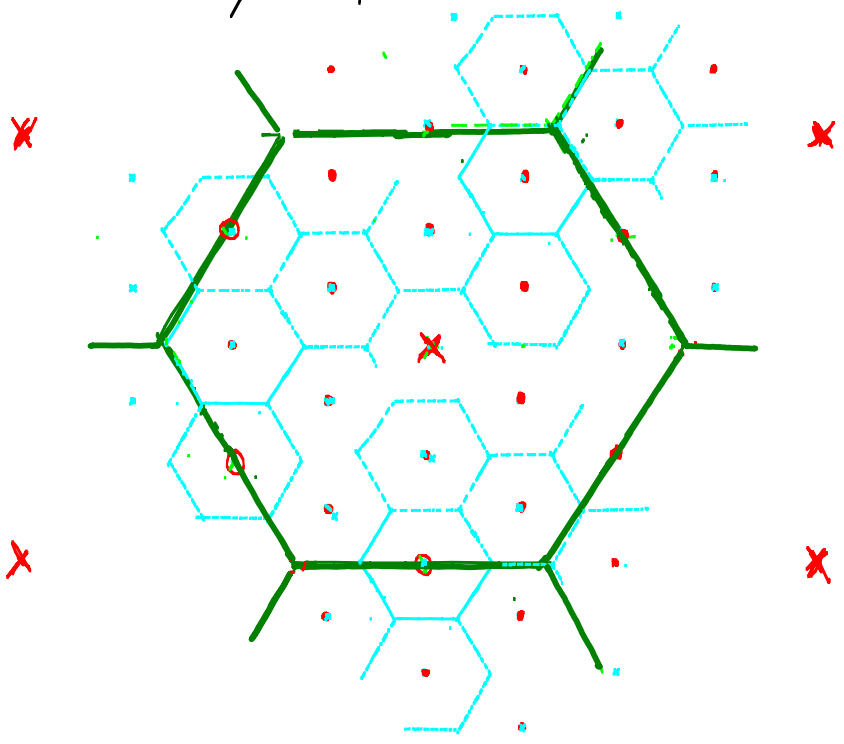
course lattice

fine lattice

integer matrix

$$\text{Nesting Ratio} = \left(\frac{V_2}{V_1}\right)^{1/k} = \left|\det(J)\right|^{1/k}$$

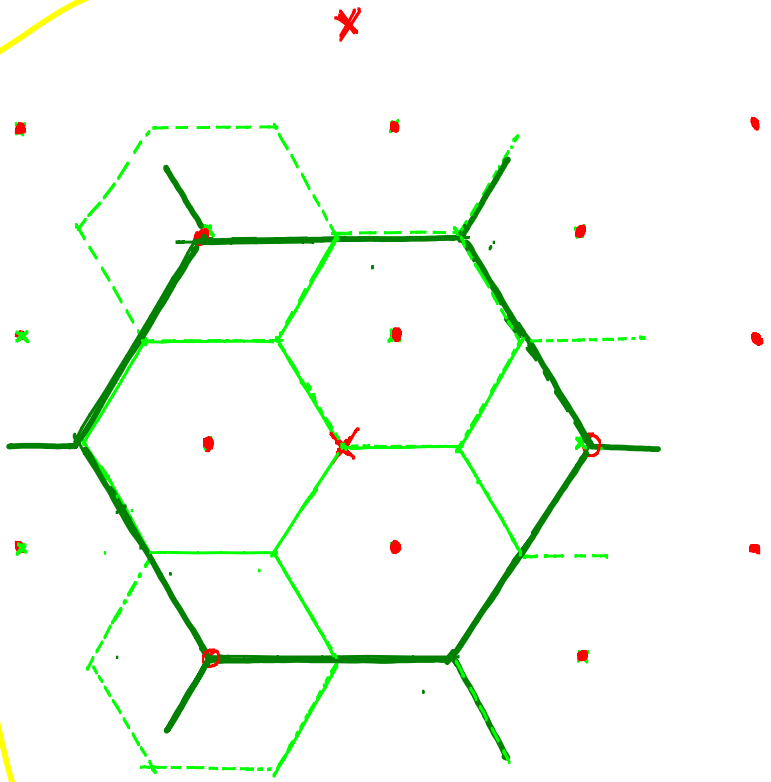
$$\text{Relative Cosets} = \Lambda_2/\Lambda_1$$



4:1

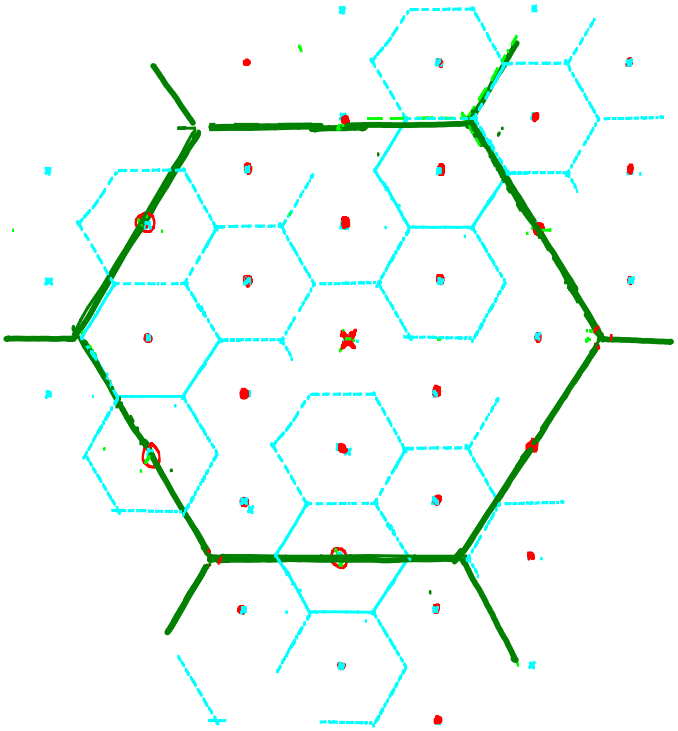
Not necessarily "Self Similar"!

$\Rightarrow V_{o_2} \not\subset V_{o_1}$



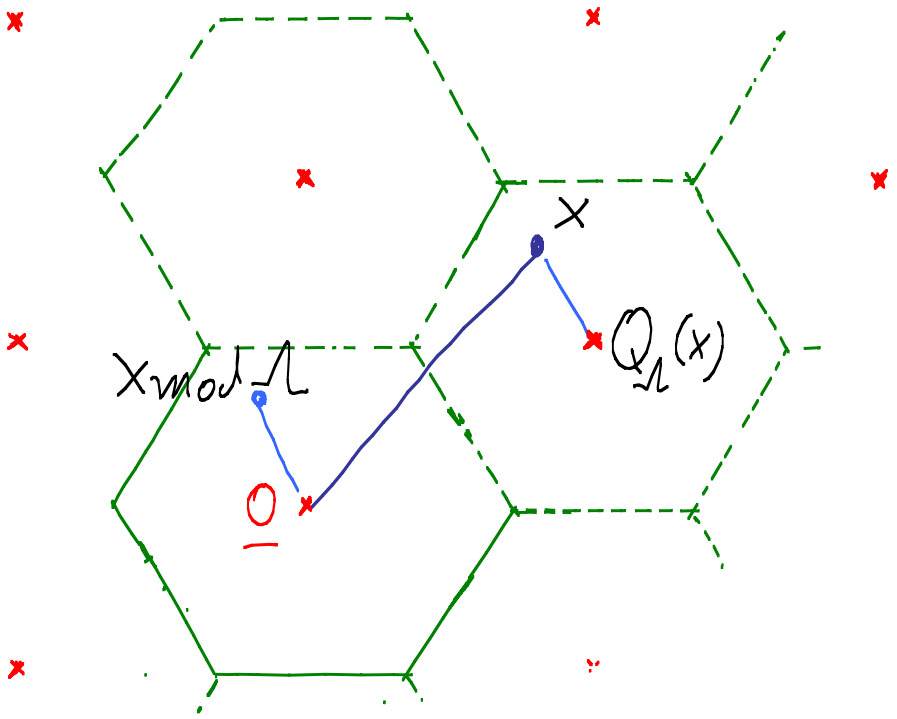
Relatively periodic
(non nested)

Nested & self Similar

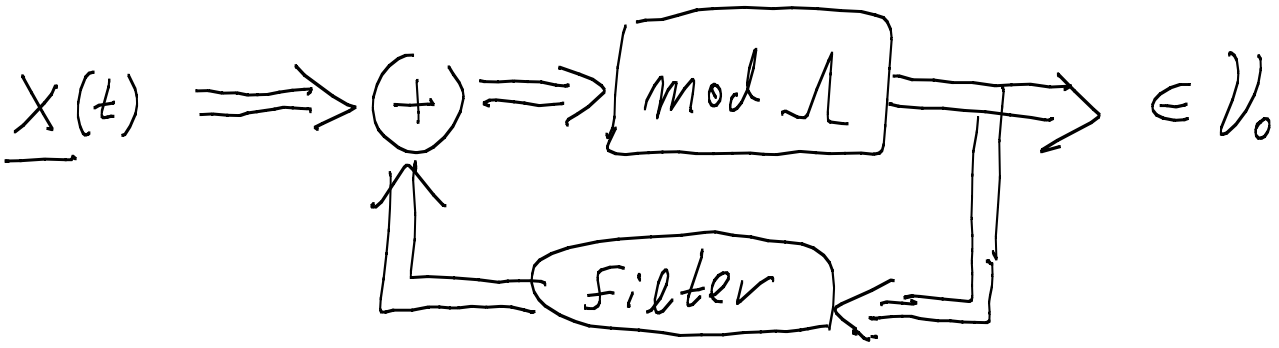


Modulo-Lattice Arithmetic

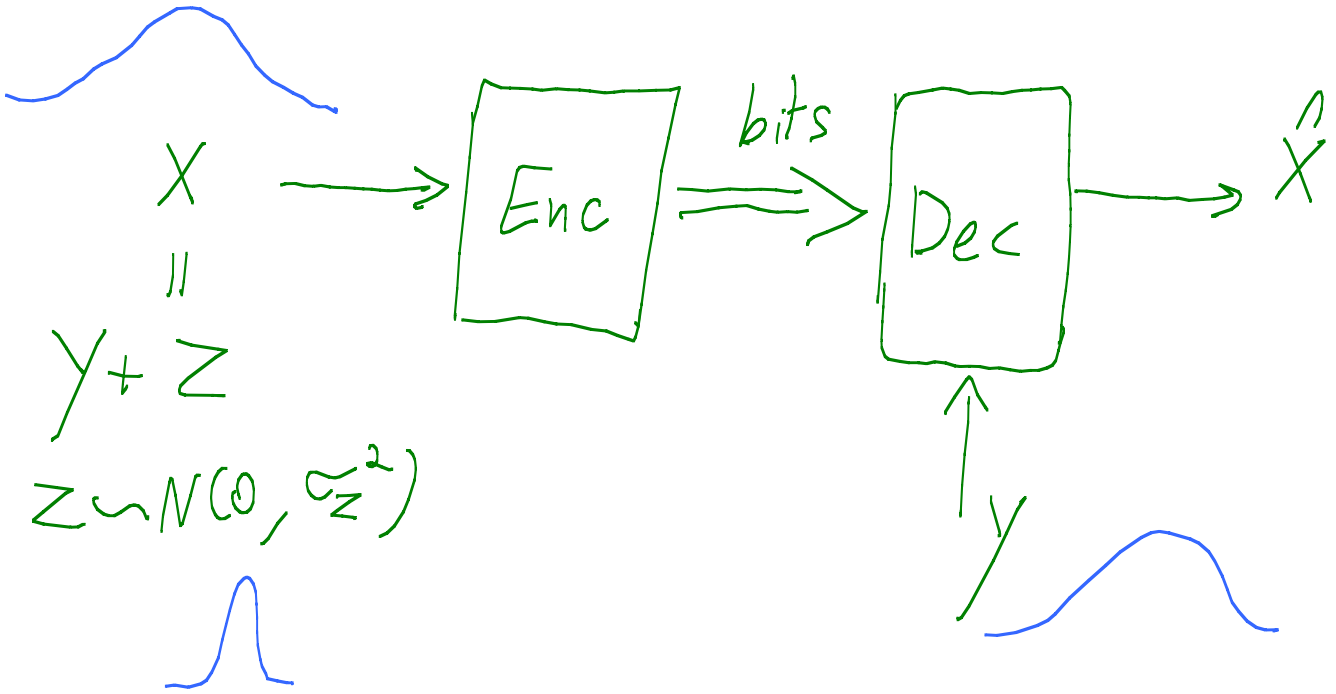
$$x \bmod \Lambda \triangleq x - Q_\Lambda(x)$$



$$x \pm y \bmod \Lambda \in V_0$$



The Wyner-Ziv Problem
(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

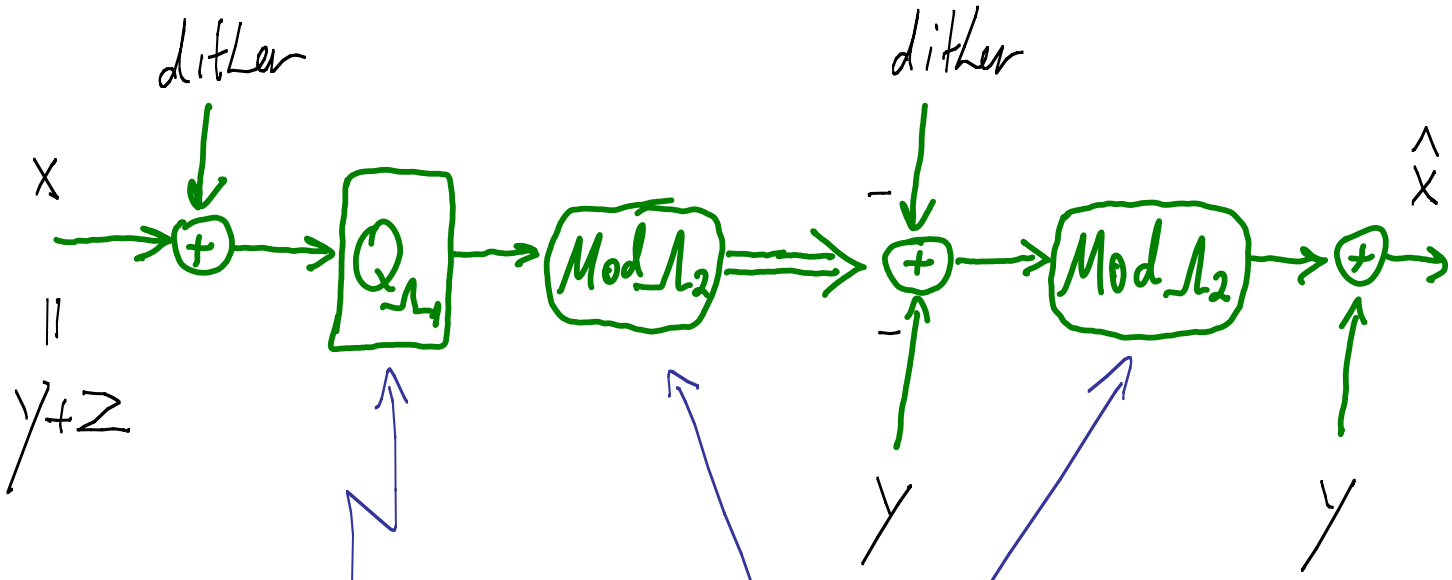
WZ-Video Coding:

motion compensation @ decoder

⇒ encoding = simple / decoding = complex

Lattice Wyner-Ziv Coding

[Z & Shamai Verdu]

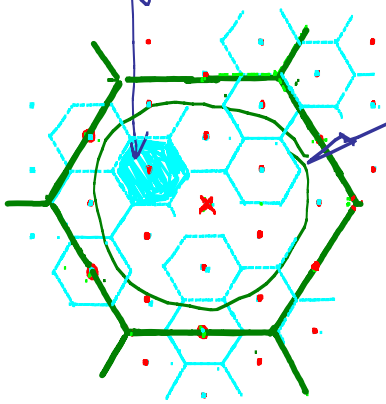


Good quantizer for desired distortion:

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

Good channel code for the noise Z:

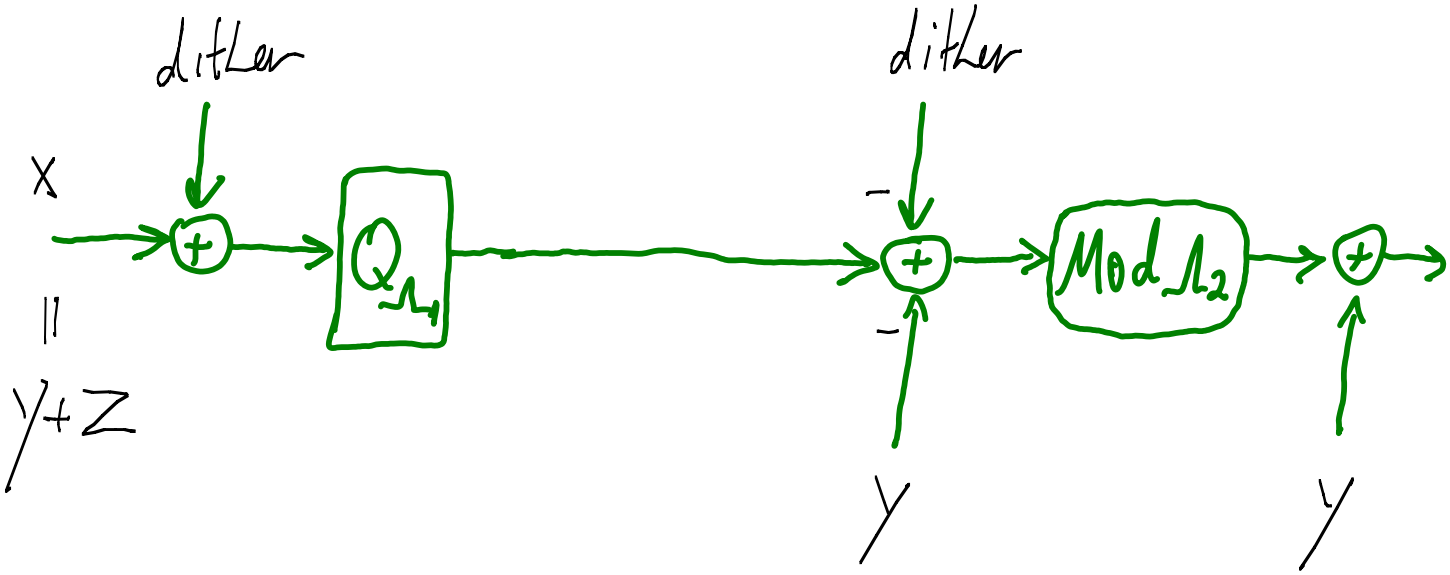
$P_e(\Lambda_2, \sigma_Z^2) < \varepsilon$



Lattice Wyner-Ziv Coding

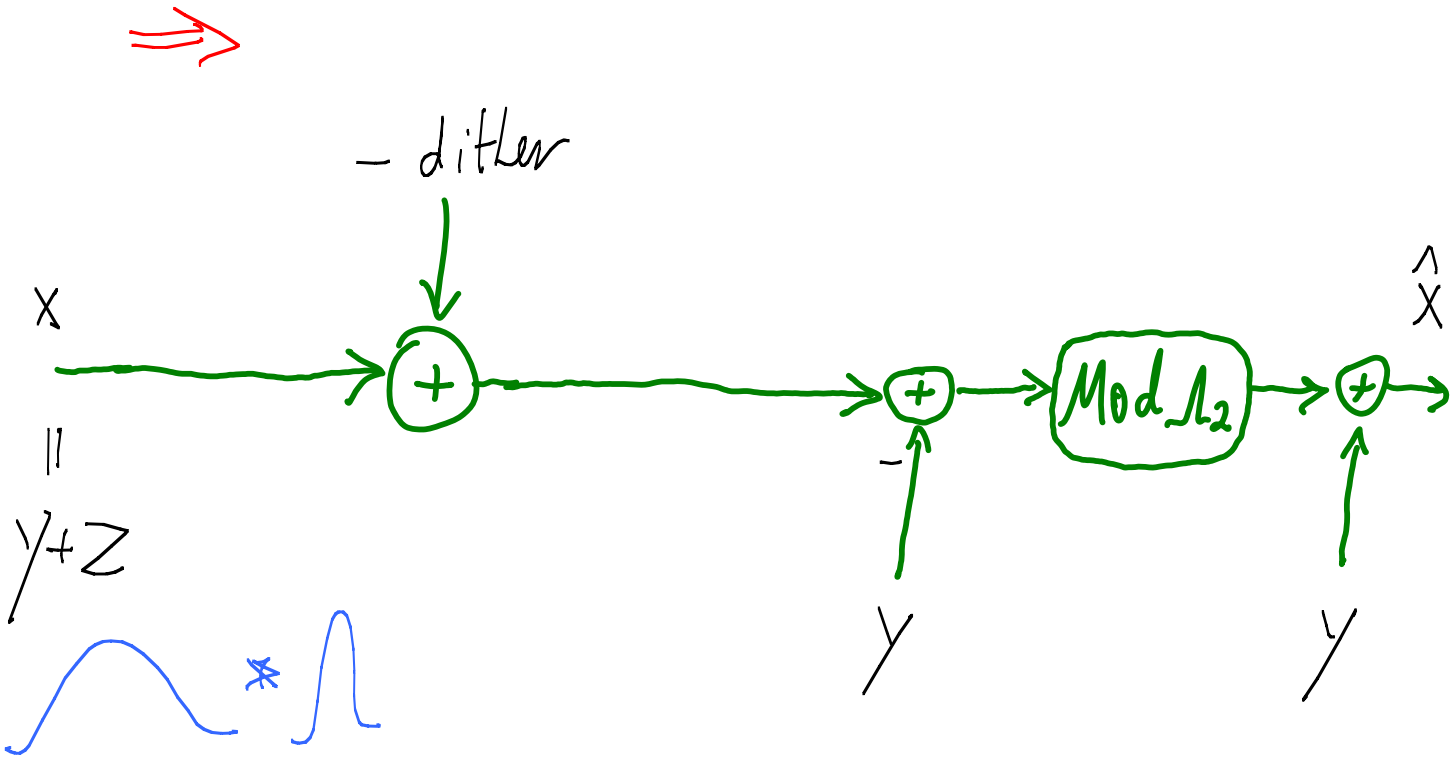
$$(A \bmod \Lambda + B) \bmod \Lambda = (A + B) \bmod \Lambda$$

$\Rightarrow$



Lattice Wyner-Ziv Coding

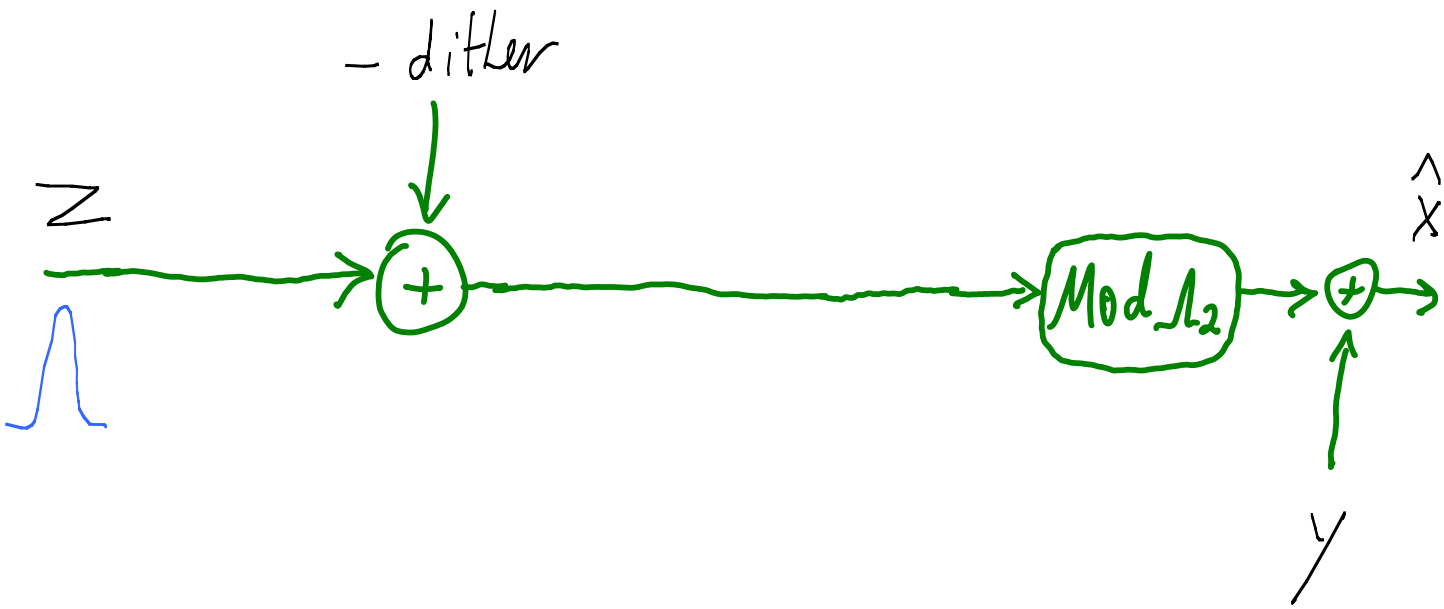
dithered quantization ≡ additive noise.



Lattice Wyner-Ziv Coding

dithered quantization $\equiv$ additive noise

$\Rightarrow$



Lattice Wyner-Ziv Coding

Λ_2 = good channel code for $Z \sim N(0, \sigma_Z^2)$.
$D \ll \sigma_Z^2$.

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

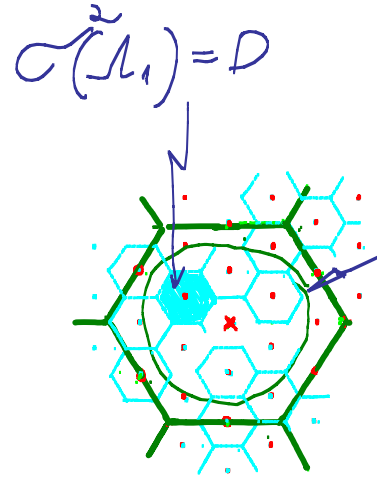
$\Rightarrow$

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

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

Lattice Wyner-Ziv Coding

Nesting Ratio:



$\Rightarrow$

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

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

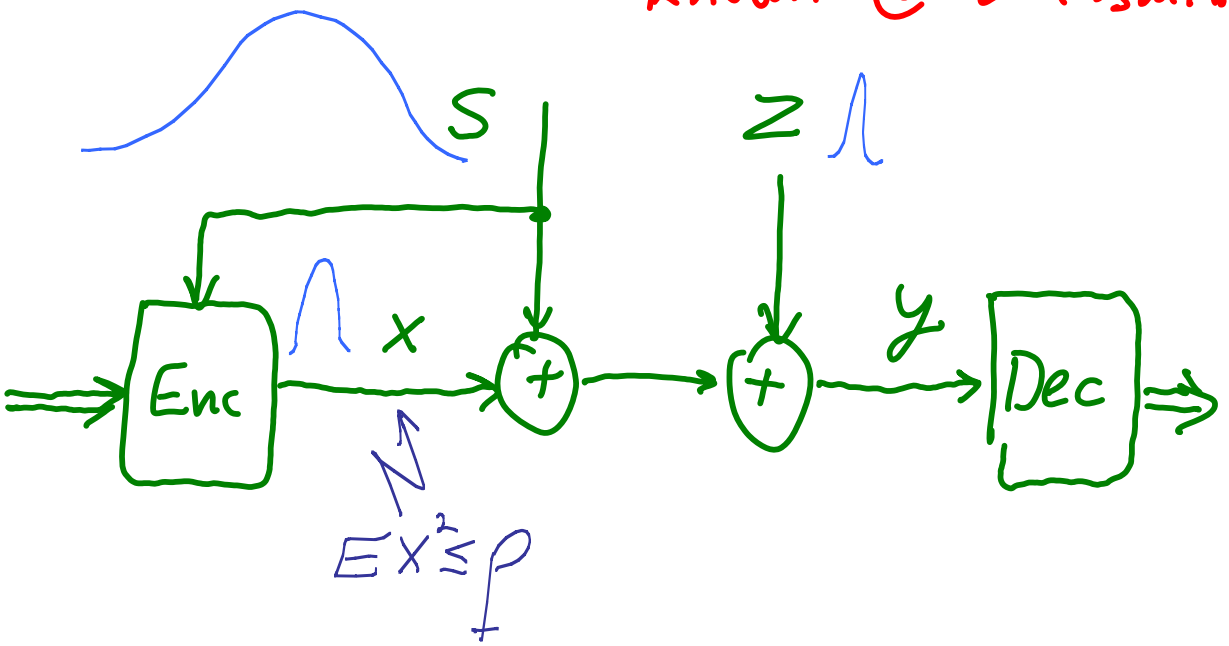
NSM (Λ_1)

VNR (Λ_2)

$k \to \infty$

for good lattices ...

"Writing on Dirty Paper"
(channel coding with Interference known @ transmitter)

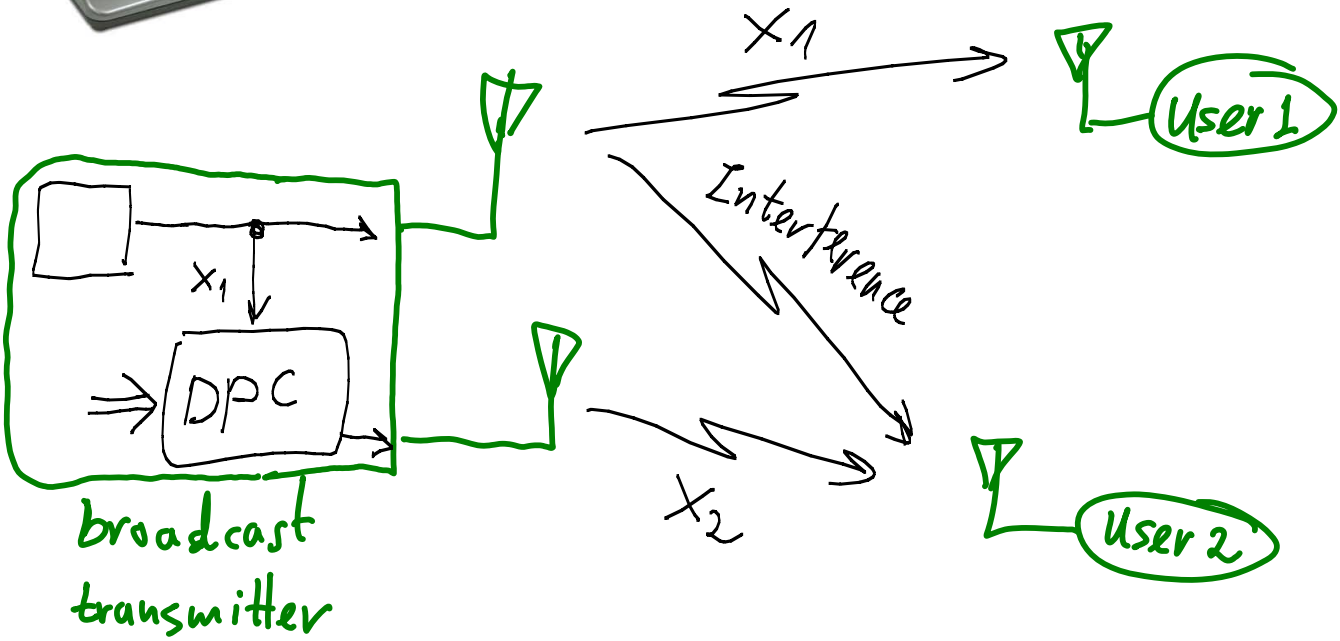


$$C_{SI@Tx} = \frac{1}{2}\log\left(1+\frac{P}{\sigma_z^2}\right) = C_{AWGN}$$

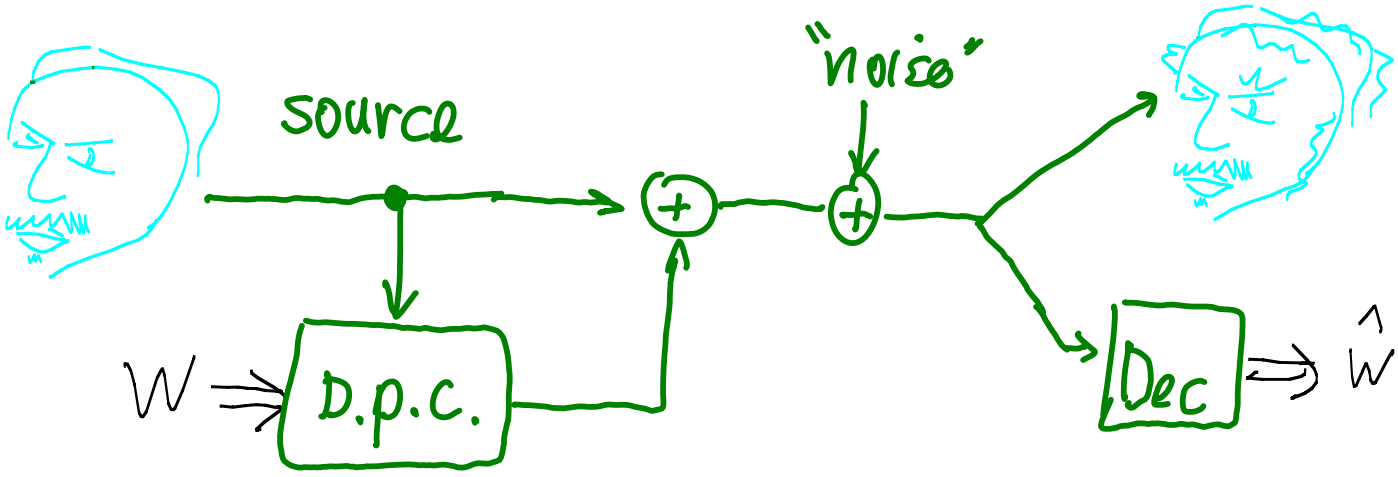
Gelfand-Pinsker 1980
+
Costa 1983

Surprising: interference cancellation with no power penalty?

MIMO - Broadcast using D.P.C

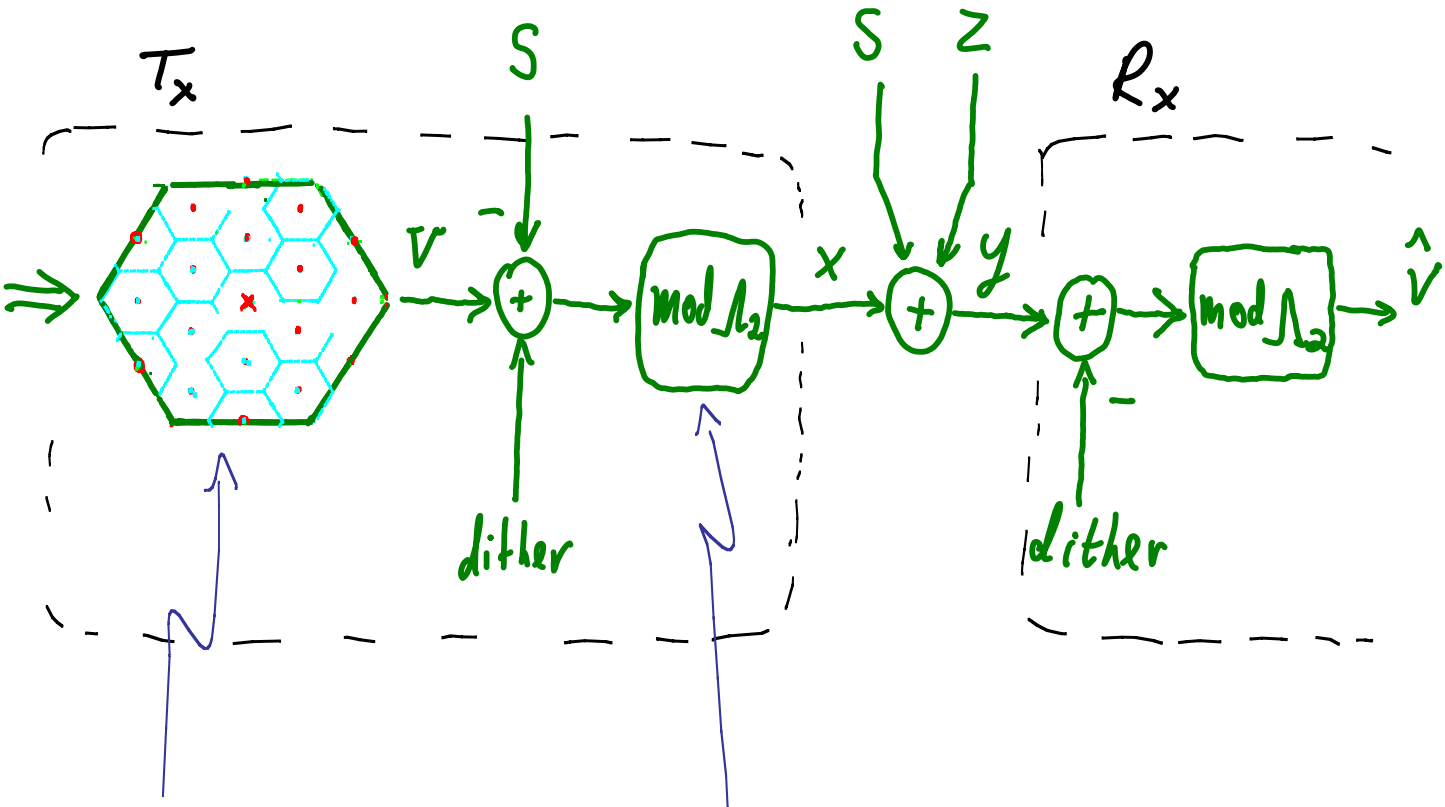


Information Embedding ("Watermarking")



Lattice Dirty Paper Coding

[Erez Shamai & Z]



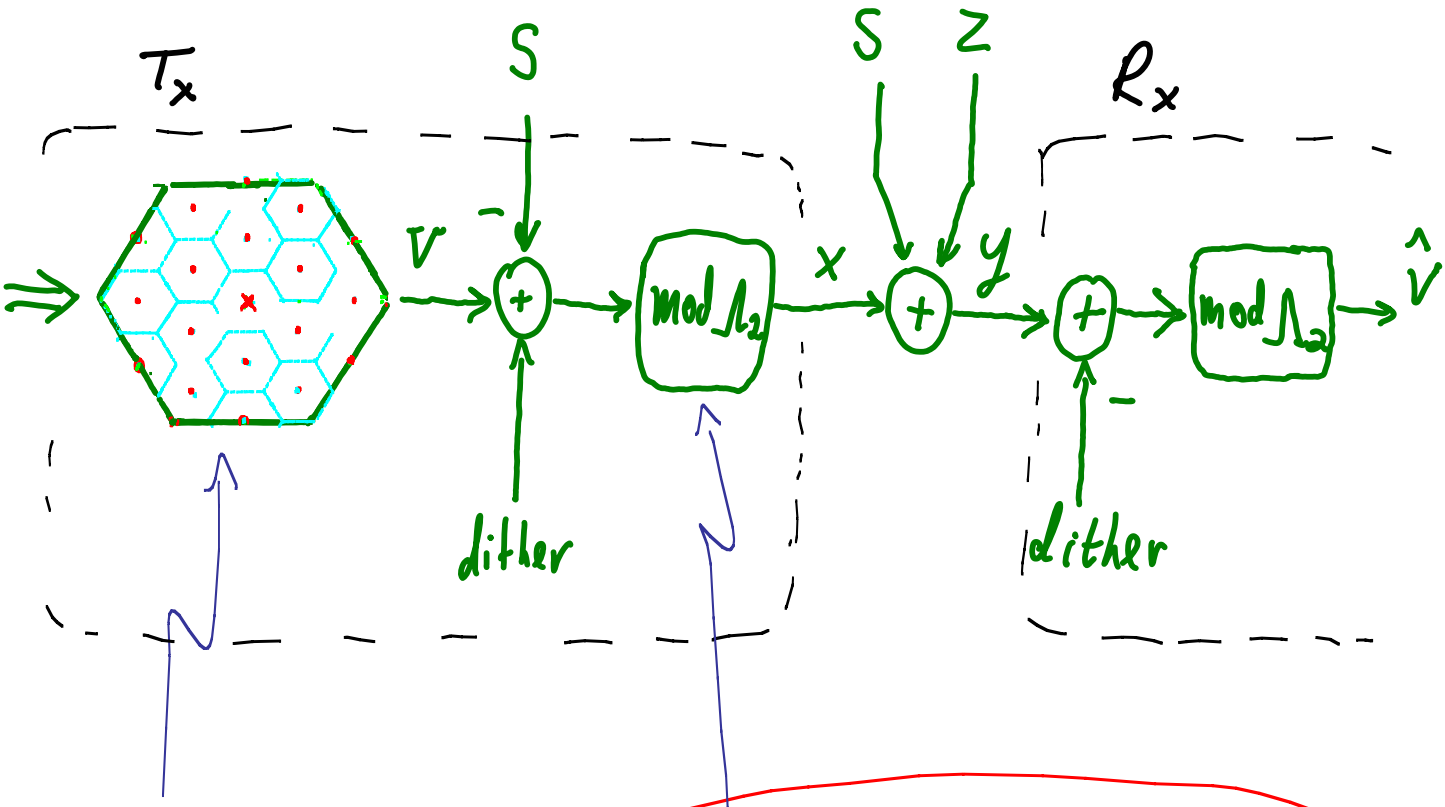
Λ_1 / Λ_2 Voronoi Constellation

Λ_2 = Good quantizer

$\sigma^2(\Lambda_2) = P$

Λ_1 = good channel code for $N(0, \sigma_2^2)$

Lattice Dirty Paper Coding



Λ_1/Λ_2 Voronoi Constellation

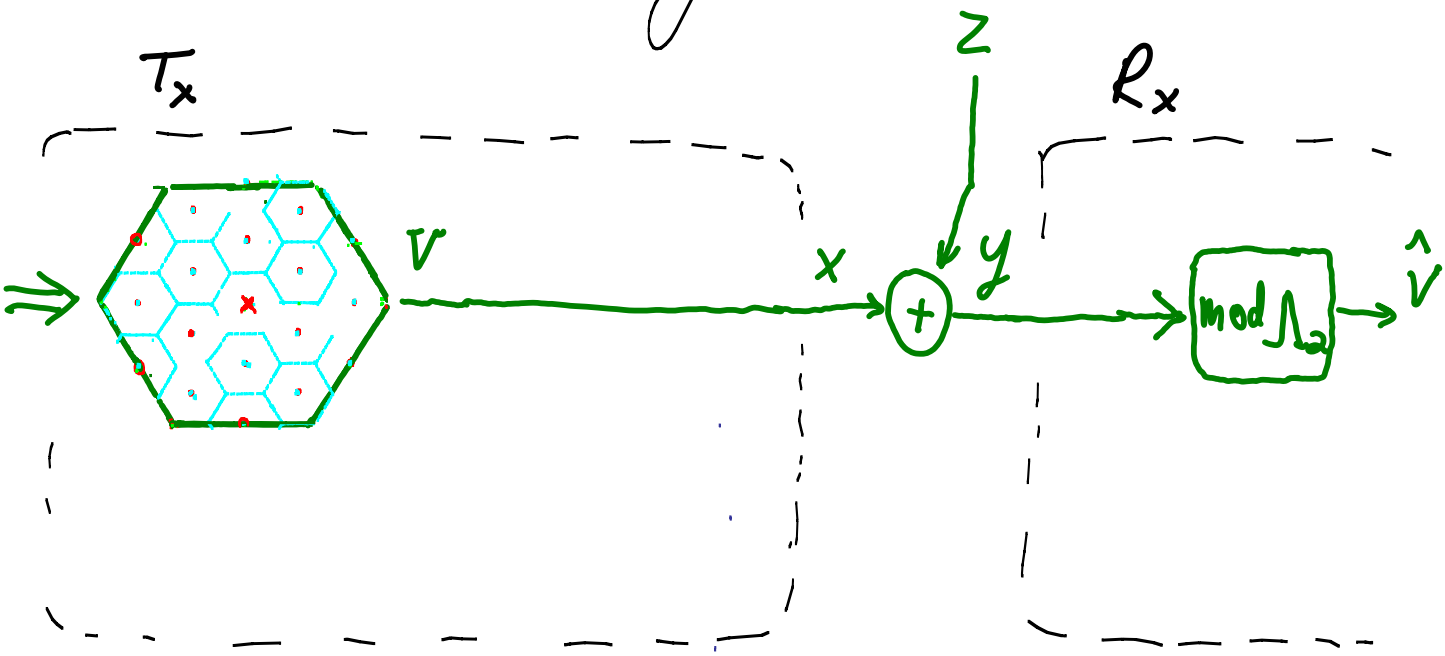
Good quantizer $\sigma^2(\Lambda_2) = P$ + dither

Λ_1 = good channel code for $N(0, \sigma_2^2)$

$E\frac{1}{k}\|X\|^2 = P$ for any codeword!

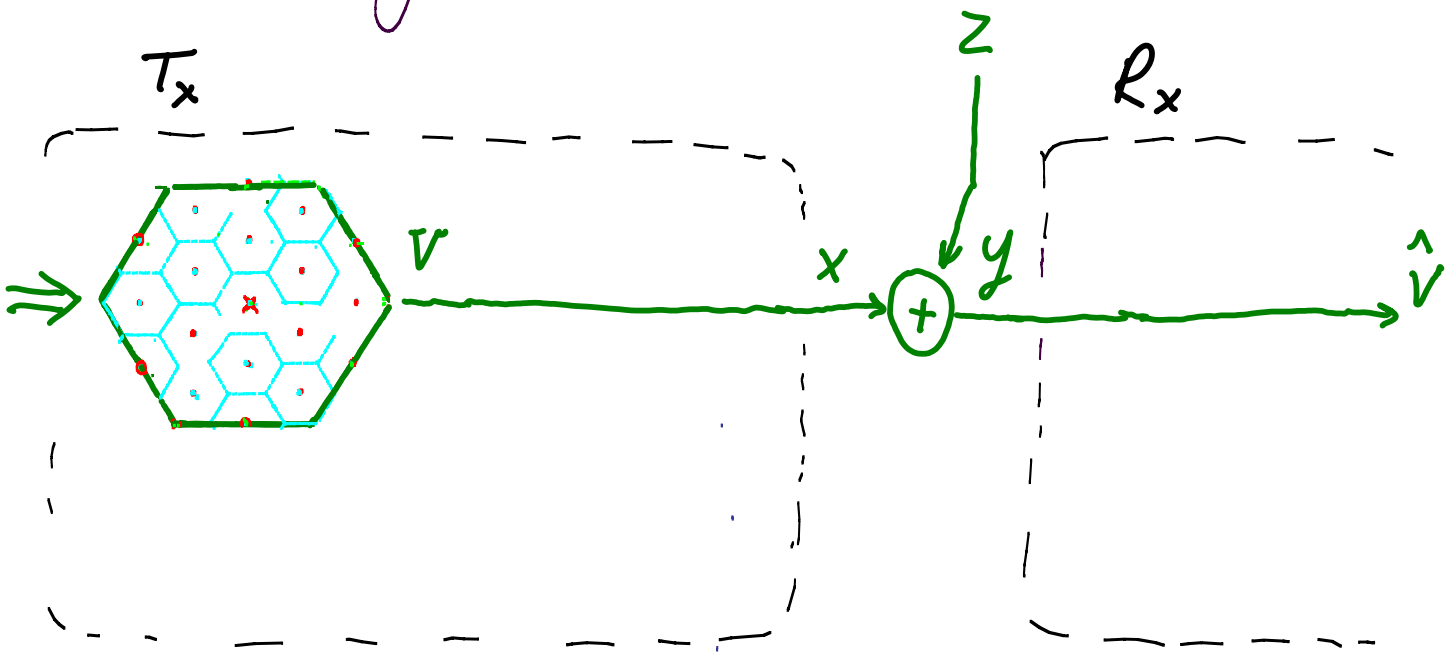
Lattice Dirty Paper Coding

Modulo property $\Rightarrow$



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)

$$= \frac{1}{2}\log\left(\frac{P}{\sigma_z^2}\right) - \frac{1}{2}\log\left(G_k \cdot \mu_k\right)$$

Λ_2 Λ_1

AWGN capacity @ High SNR

Capacity Loss $\xrightarrow{\alpha \to \infty} 0$

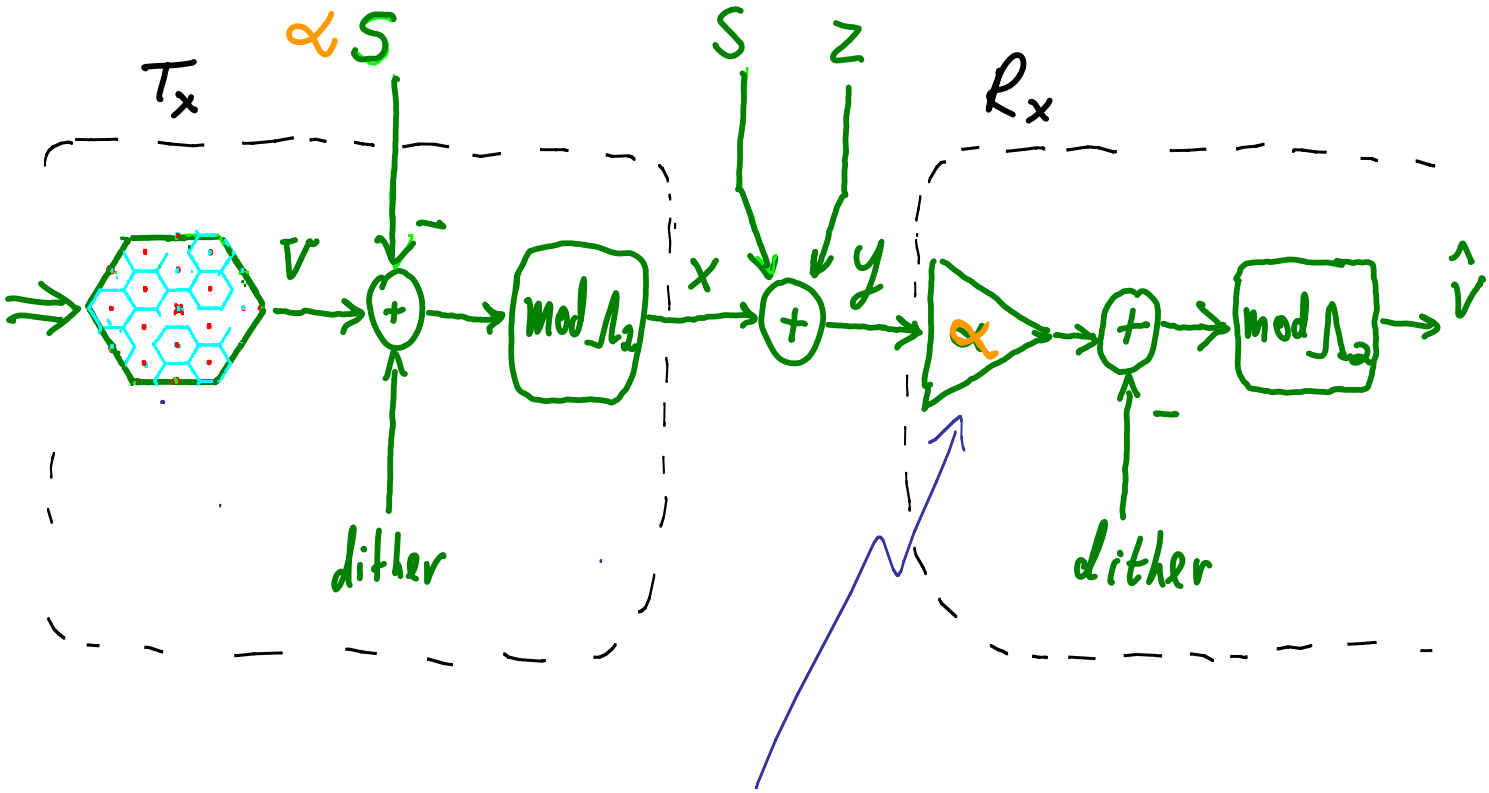
From the

Dirty Paper Channel

to the plain old

AWGN Channel ...

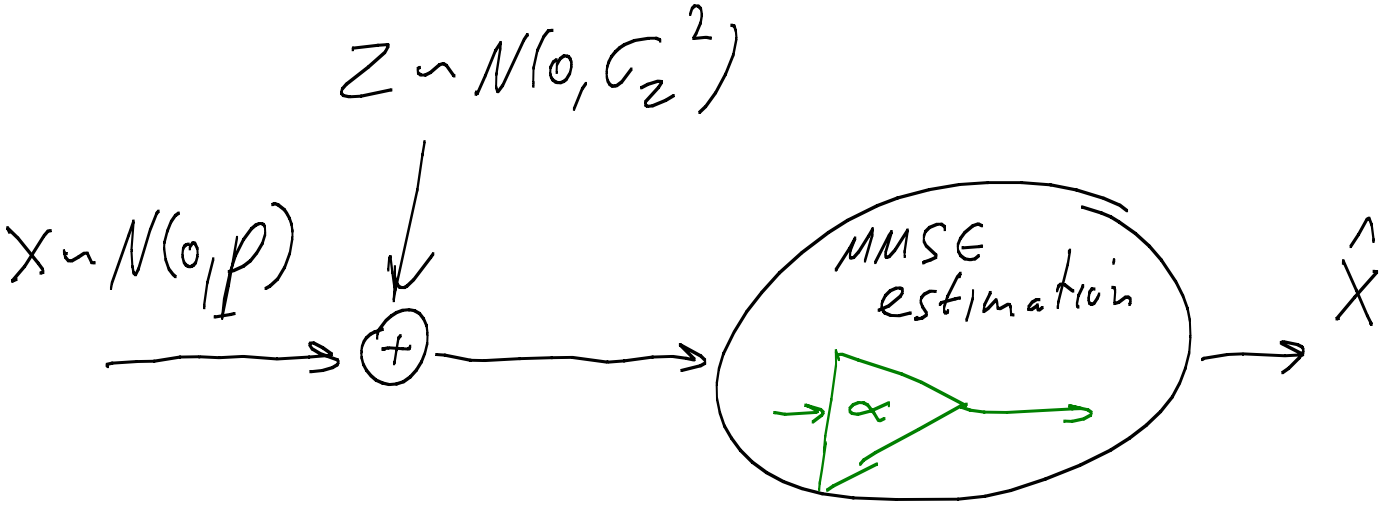
Achieving $\frac{1}{2}\log(1+SNR)$ @ general SNR



α = MMSE (Wiener) Coefficient

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

Wiener Estimation



$$\min E\left(\hat{X} - X\right)^2 \Rightarrow \alpha^{opt} = \frac{P}{P + \sigma_z^2}$$

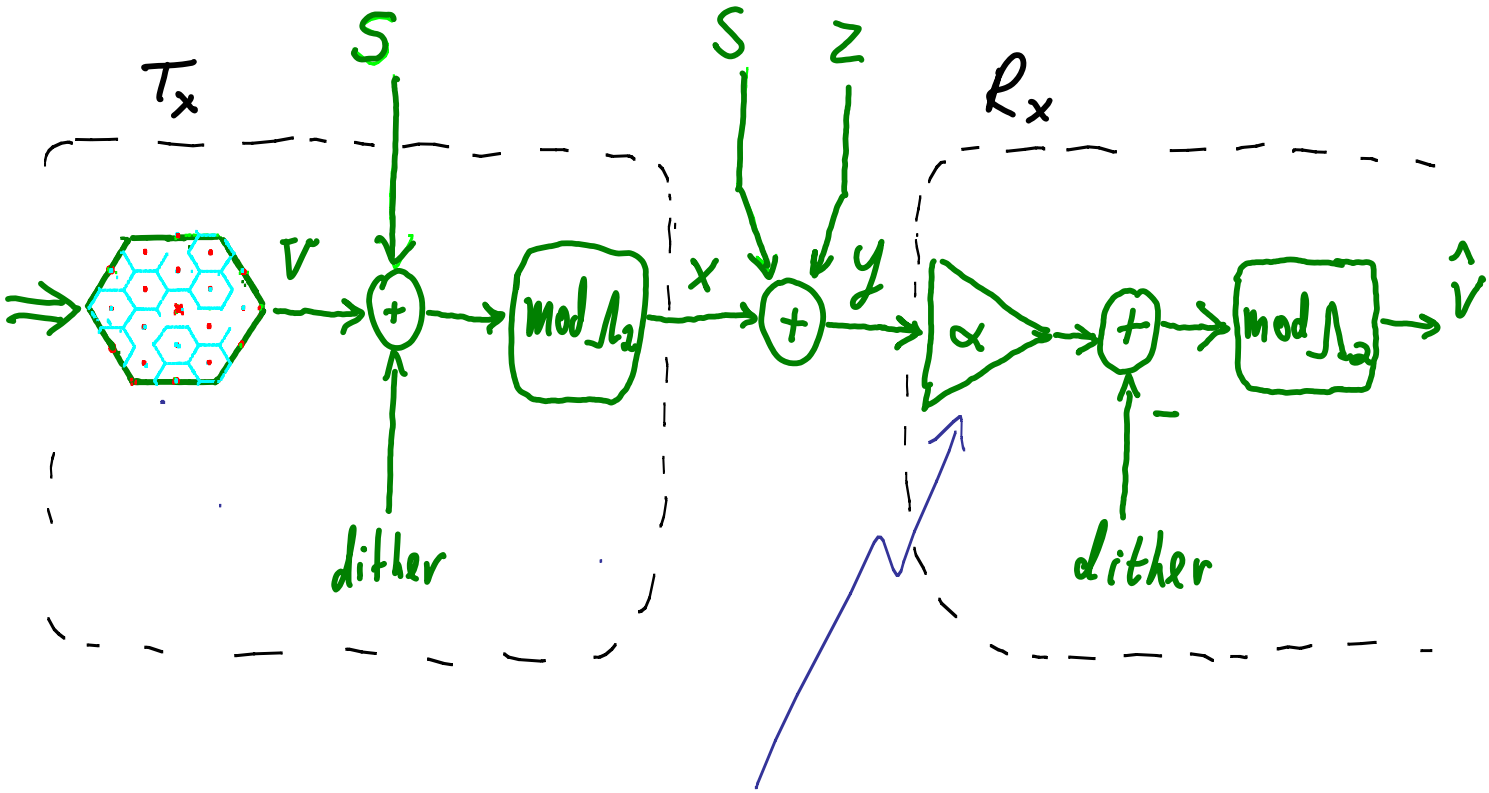
$$\Rightarrow MSE = \frac{P \cdot \sigma_z^2}{P + \sigma_z^2}$$

$$error = (\alpha - 1) \cdot X + \alpha \cdot Z$$

"self noise"

residual "natural" noise

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



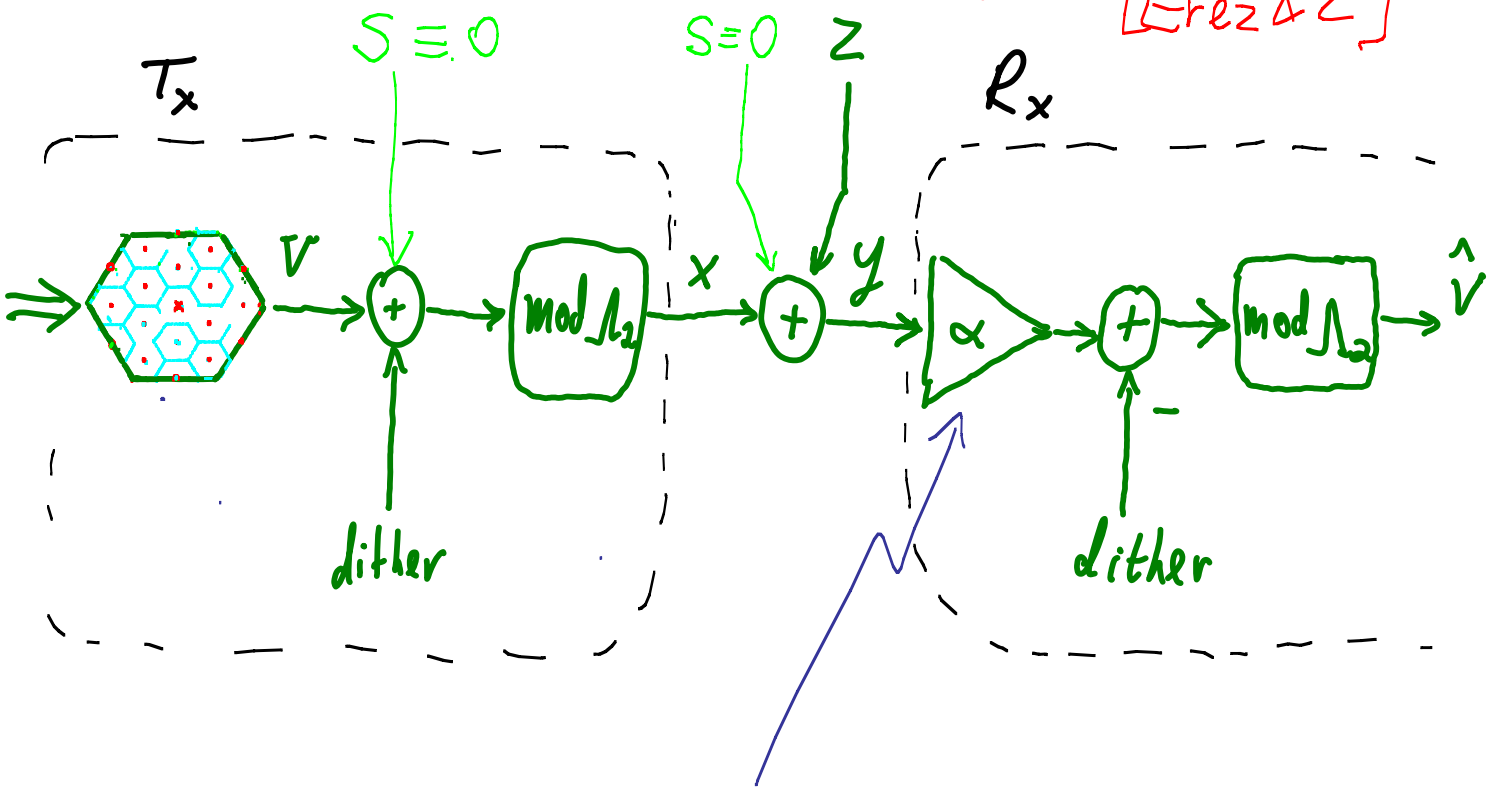
α = MMSE (Wiener) Coefficient

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

$$\Rightarrow Var(Z_{eq}) = \frac{P\cdot\sigma_z^2}{P+\sigma_z^2}$$

Achieving $\frac{1}{2}\log(1+SNR)$ over the AWGNC with Lattice Encoding & Decoding

[Erez & Z.]

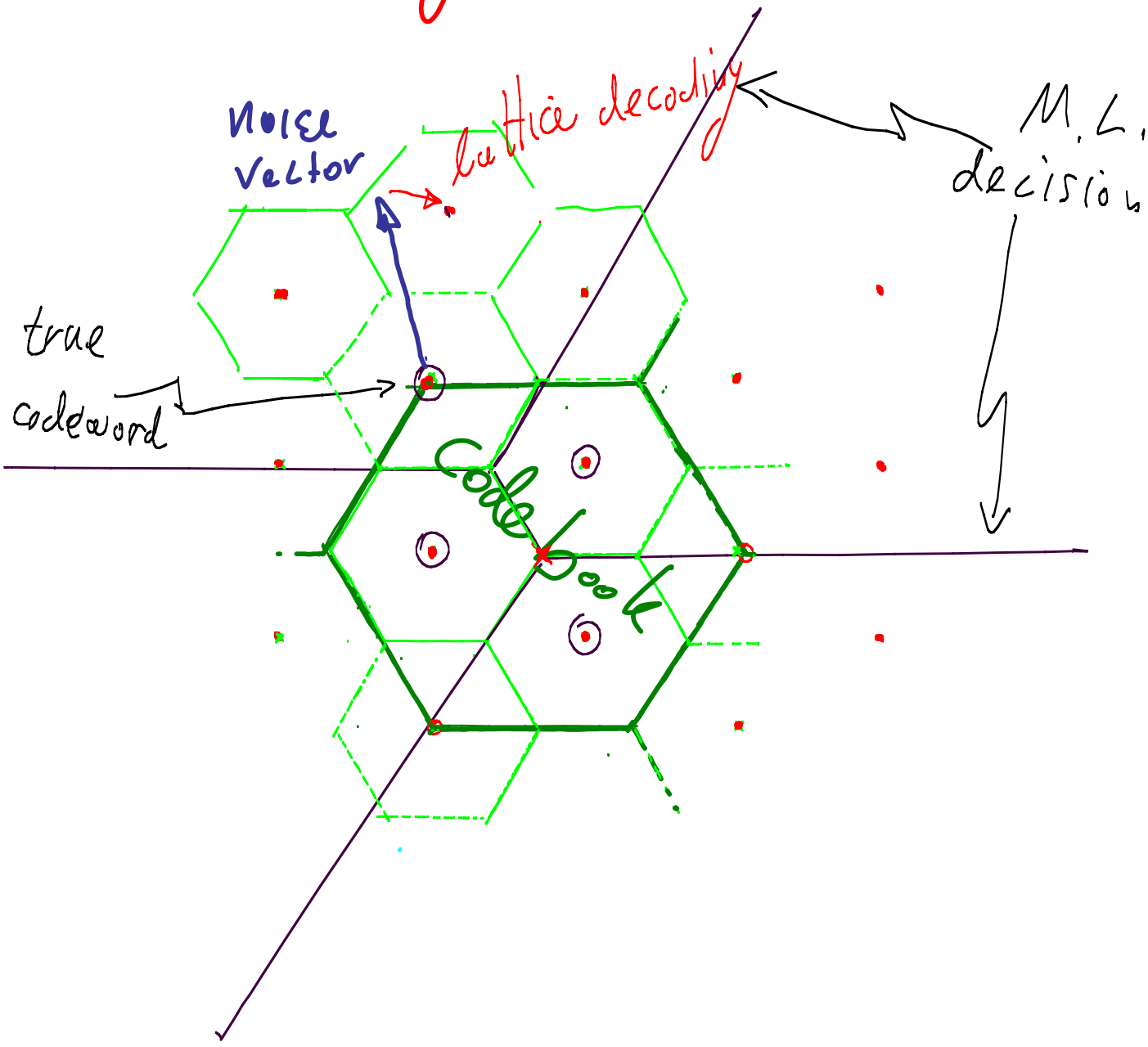


α = MMSE (Wiener) Coefficient

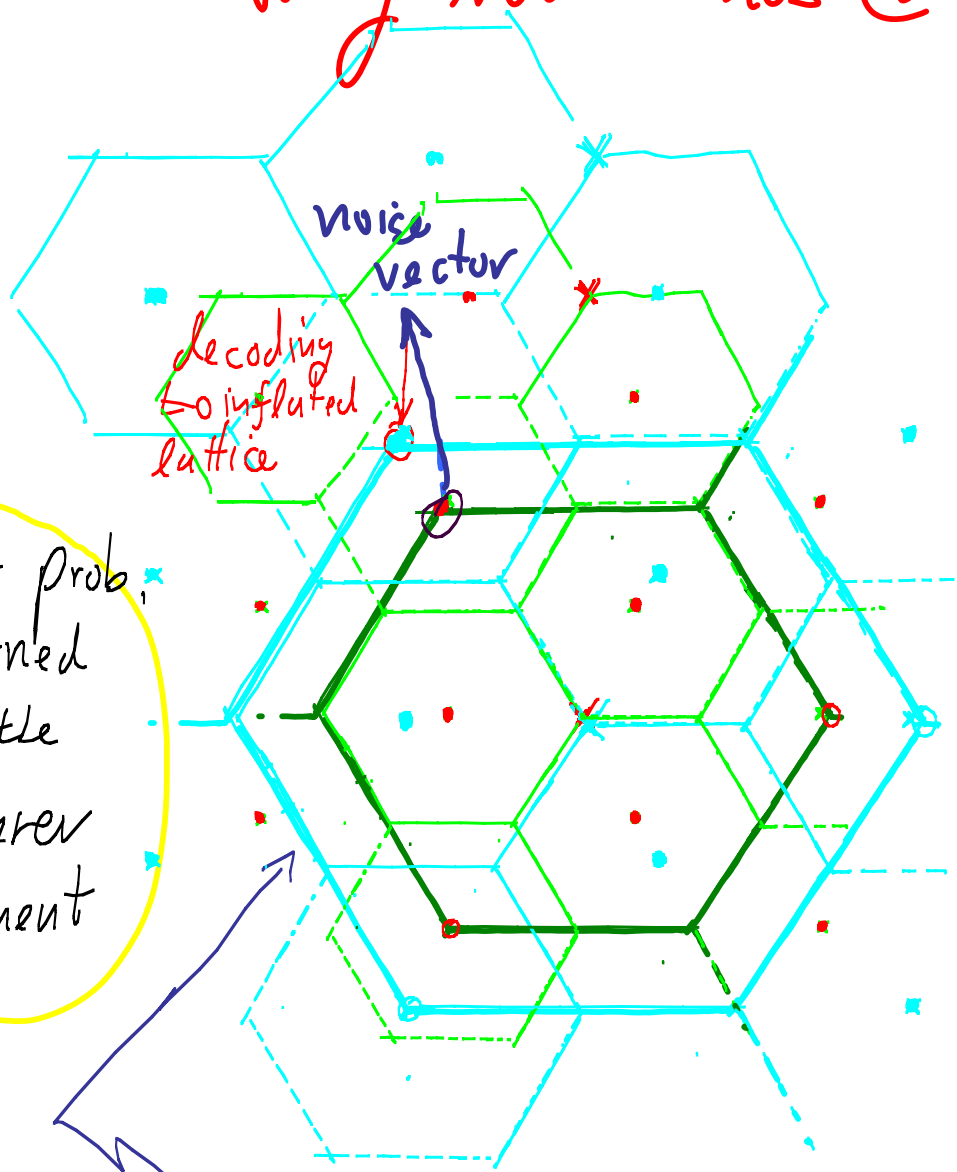
$$= \frac{P}{P+\sigma_Z^2} \approx 1 \quad @\ HSNR$$

$$\Rightarrow \mathrm{Var}(Z_{eq}) = \frac{P\cdot\sigma_Z^2}{P+\sigma_Z^2}$$

Achieving $\frac{1}{2}\log(1+SNR)$ over the AWGNC with Lattice Encoding & Decoding: Why Not Obvious @ Low SNR...



Achieving $\frac{1}{2}\log(1+SNR)$ over the AWGNC with Lattice Encoding & Decoding: Why Not Obvious @ Low SNR...



error prob. governed by the Poltyrev exponent

Lattice @ Decoder Inflated by $\frac{1}{2}$

Why Lattices in Communication?

1. a bridge from $n=1$ to $n=\infty$
   = non-asymptotic analysis per dimension

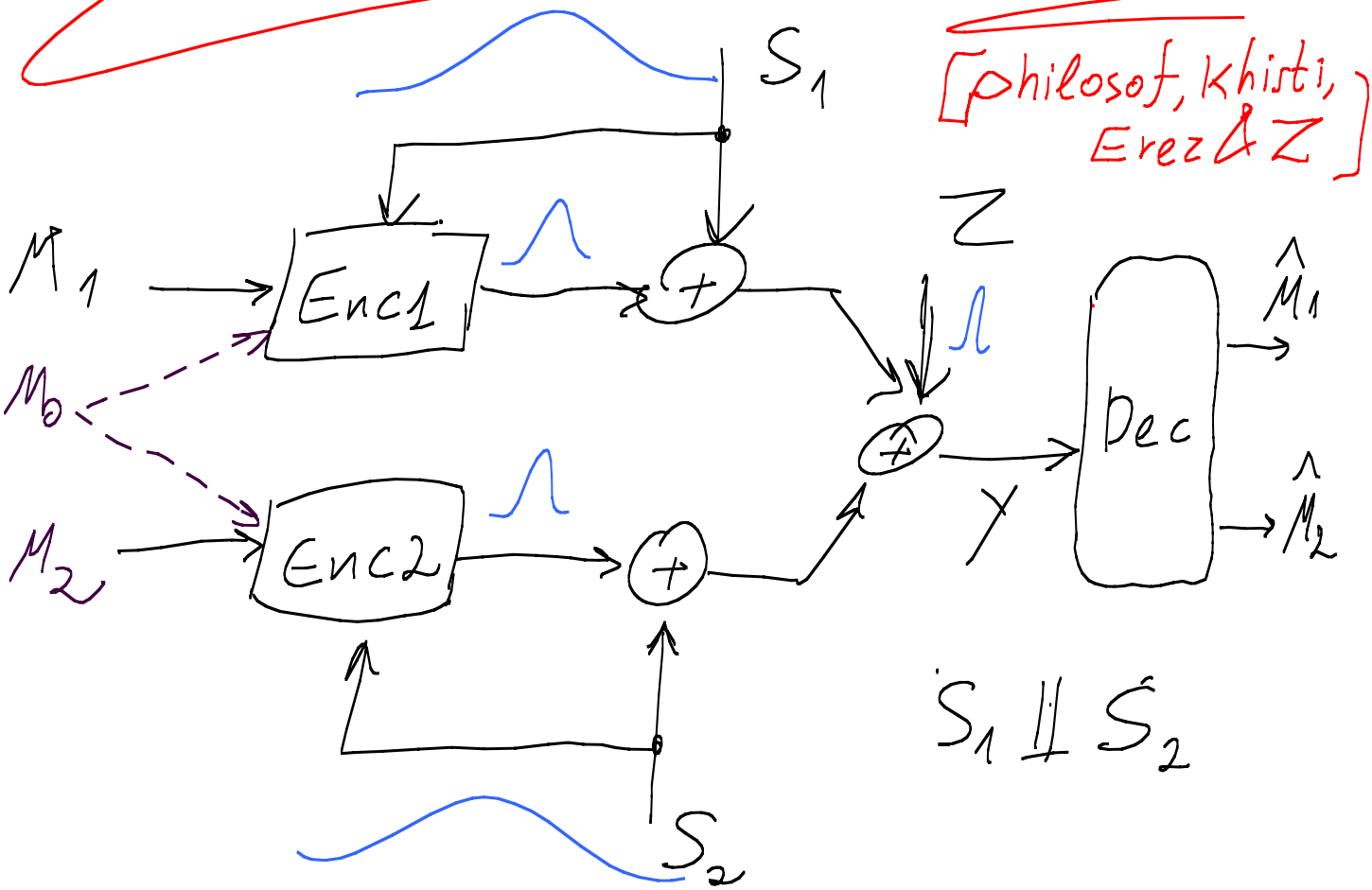
2. Algebraic (low complexity) Binning
   = structured coding schemes for networks

3. Better than Random-Coding!
   in distributed side-information problems

4.

The Doubly-Dirty Multiple Access Channel

[philosof, khisti, Erez & Z]



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

Results

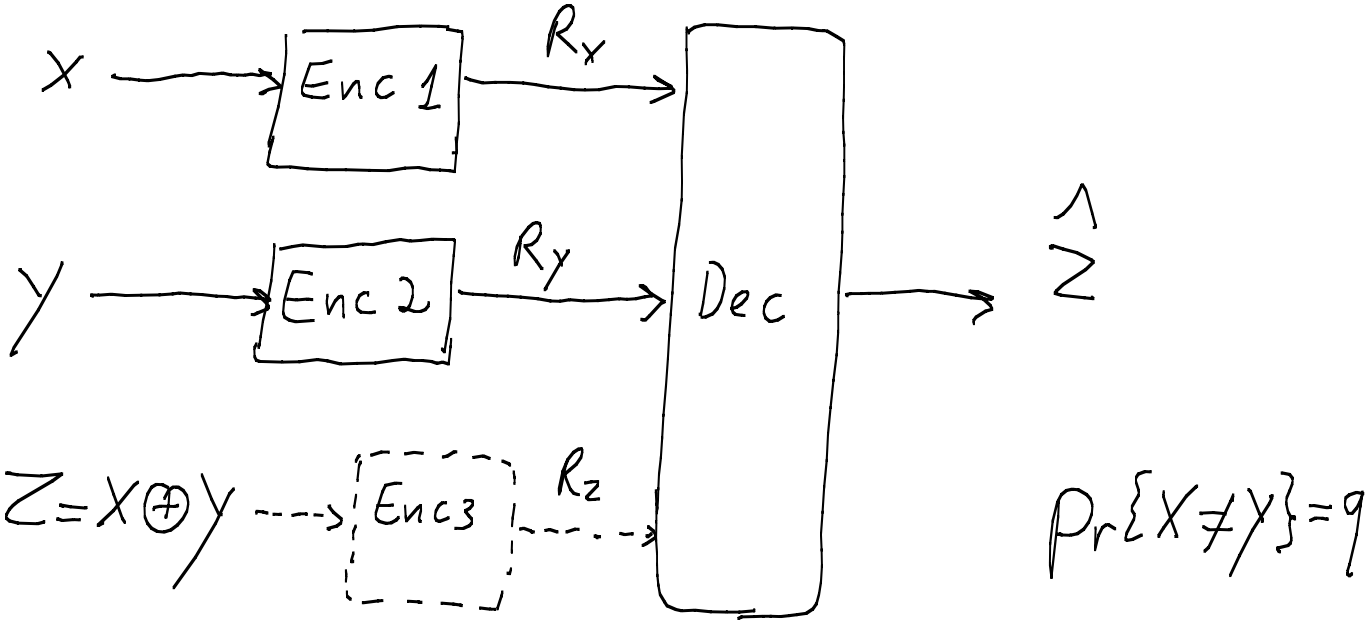
Costa (Random Binning) $\Rightarrow$ $C \simeq 0$

(for strong interference)

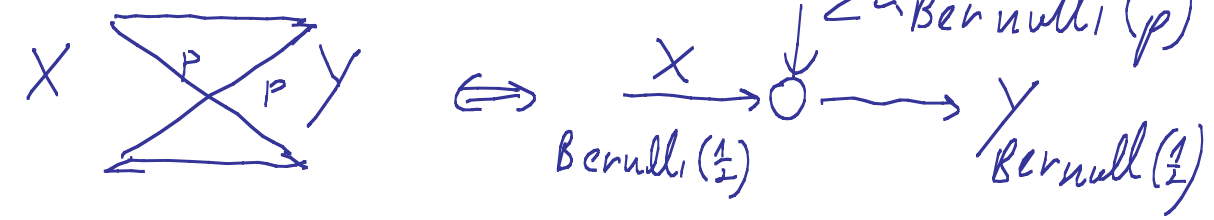
Lattice Strategies $\Rightarrow$ $C \simeq C_{\text{clean-MAC}}$

!

Korner-Marton [1979]: How to Encode the Modulo-Two Sum of Binary Sources

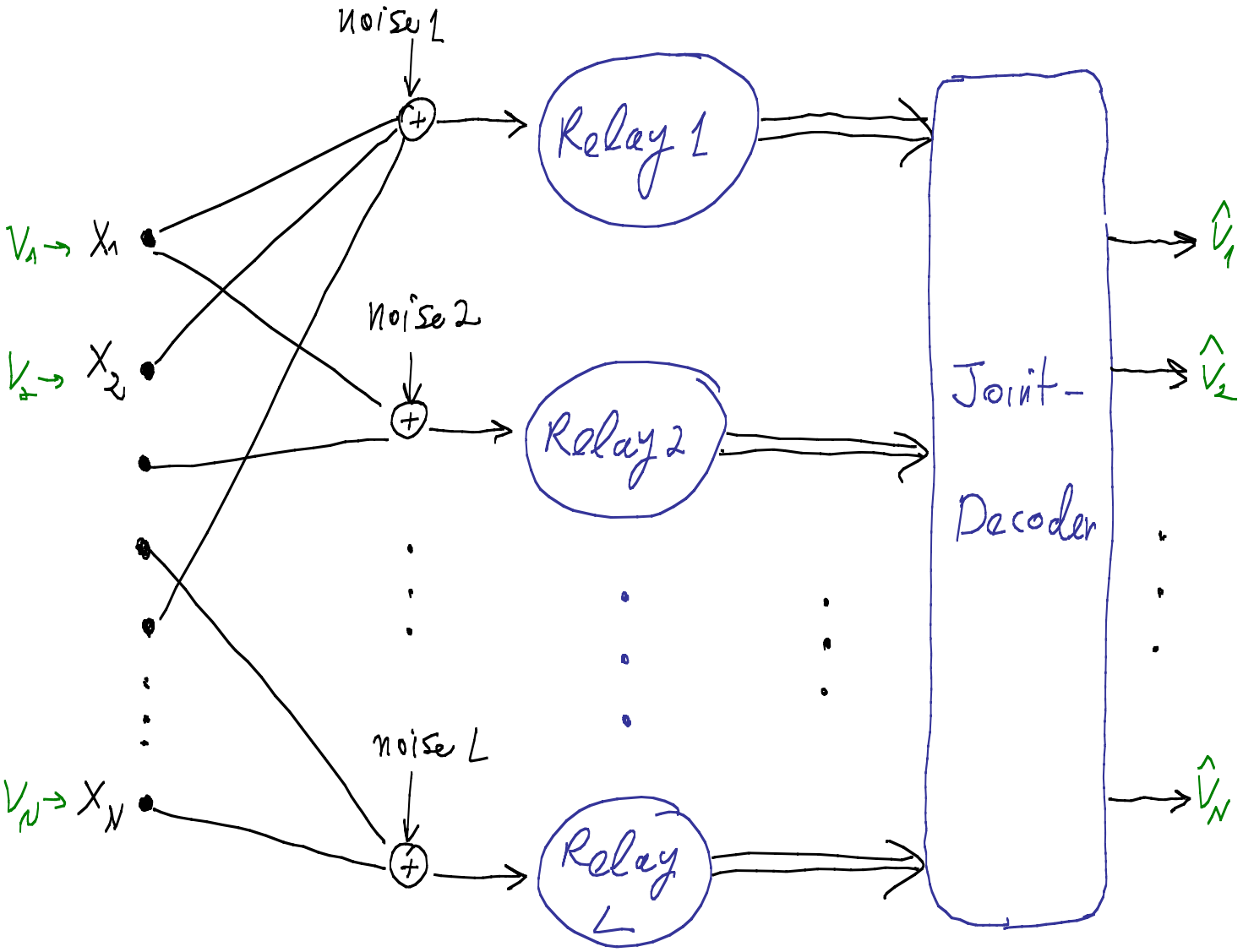


(1) "Two help one": No need to reconstruct X, Y
(generalize Wyner-Ahlswede-Korner 1975)

(2) 

(3) How can we save rate if $p \ll \frac{1}{2}$?

Lattice Coding for Noisy-Linear-Networks

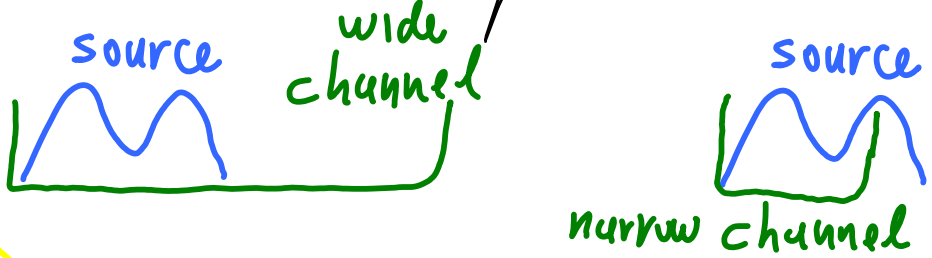


"digital" network coding : noiseless, bit pipes, random ✓ / linear ✓ code

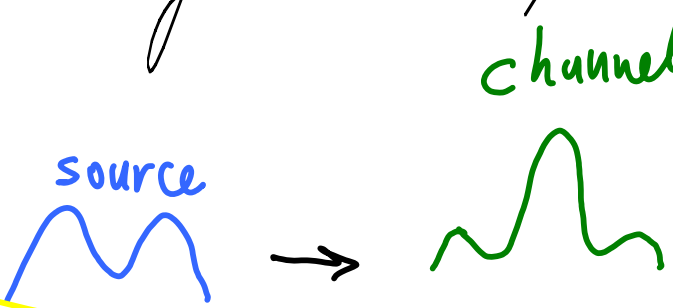
"analog" network coding : noisy, linear channels (interference), ~~random~~ / lattice ✓ code

Joint Source-channel Coding

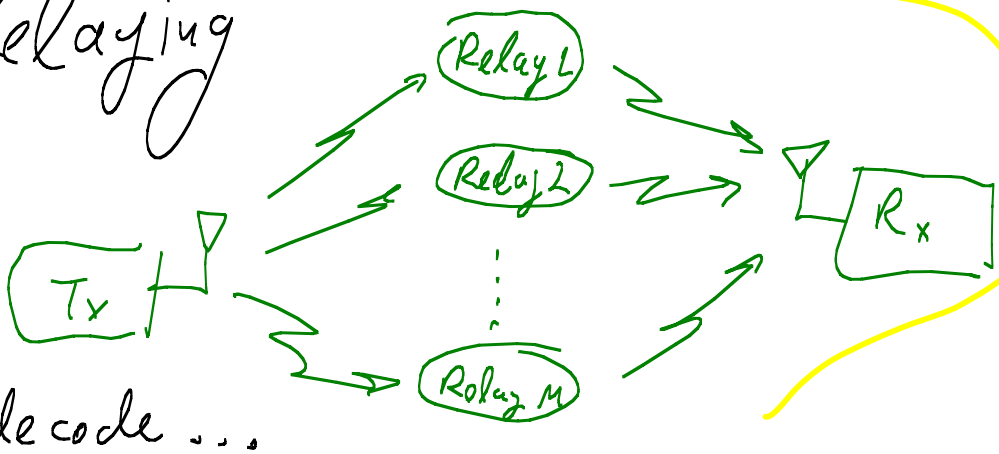
Bandwidth Expansion & Compression



Analog (colored) Matching



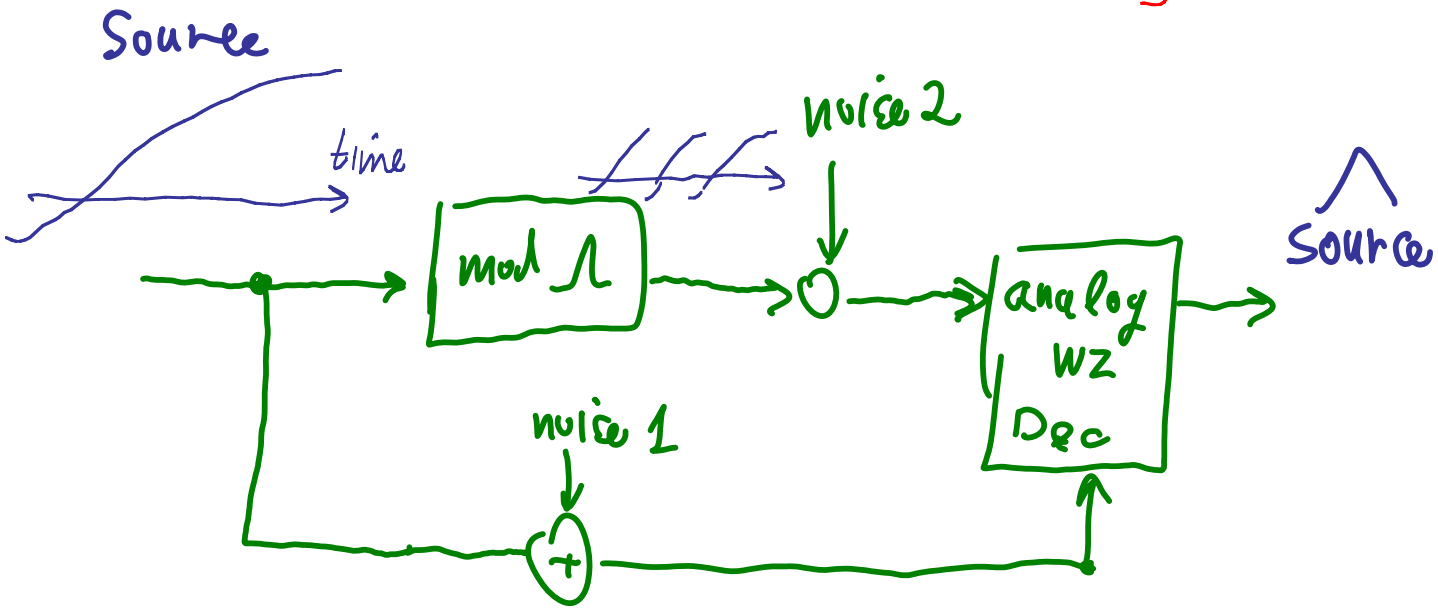
Analog Relaying



relays cannot decode ...

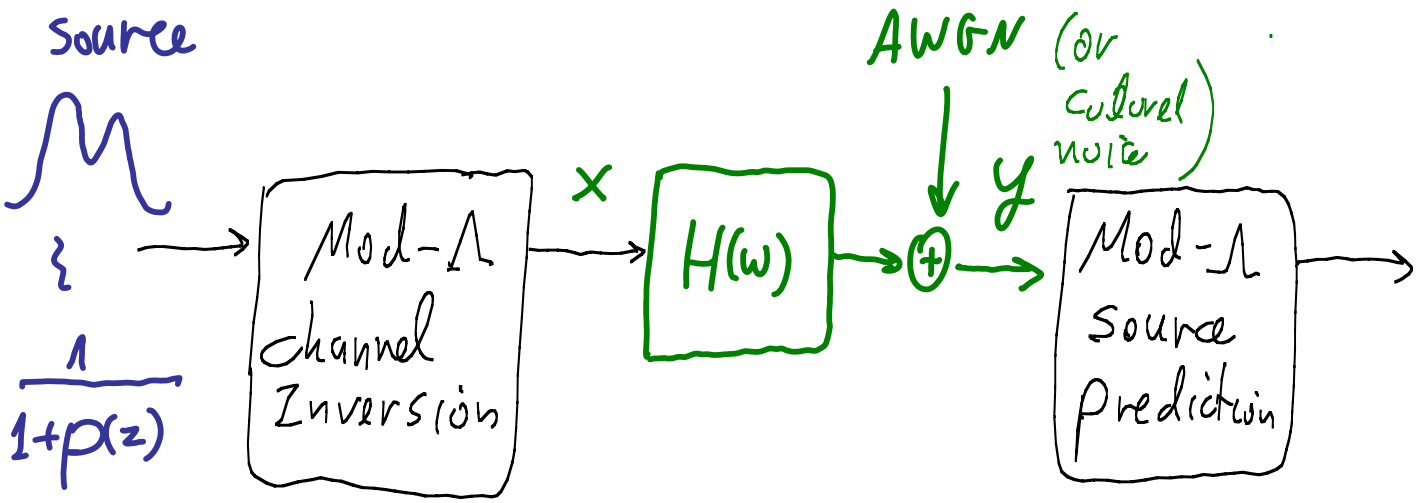
Modulo-Lattice Modulation for Bandwidth Expansion

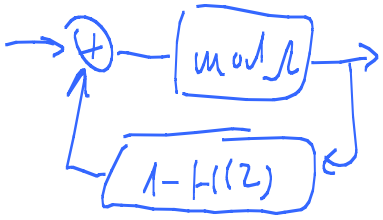
[Reznic & Z]

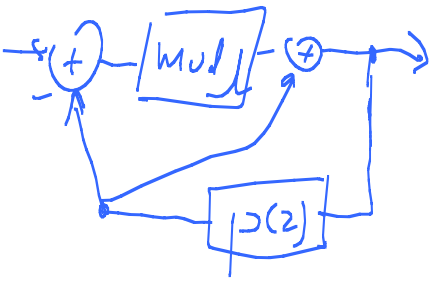


Analog Matching of Colored Sources to Colored Channels

[Kochman & Z]





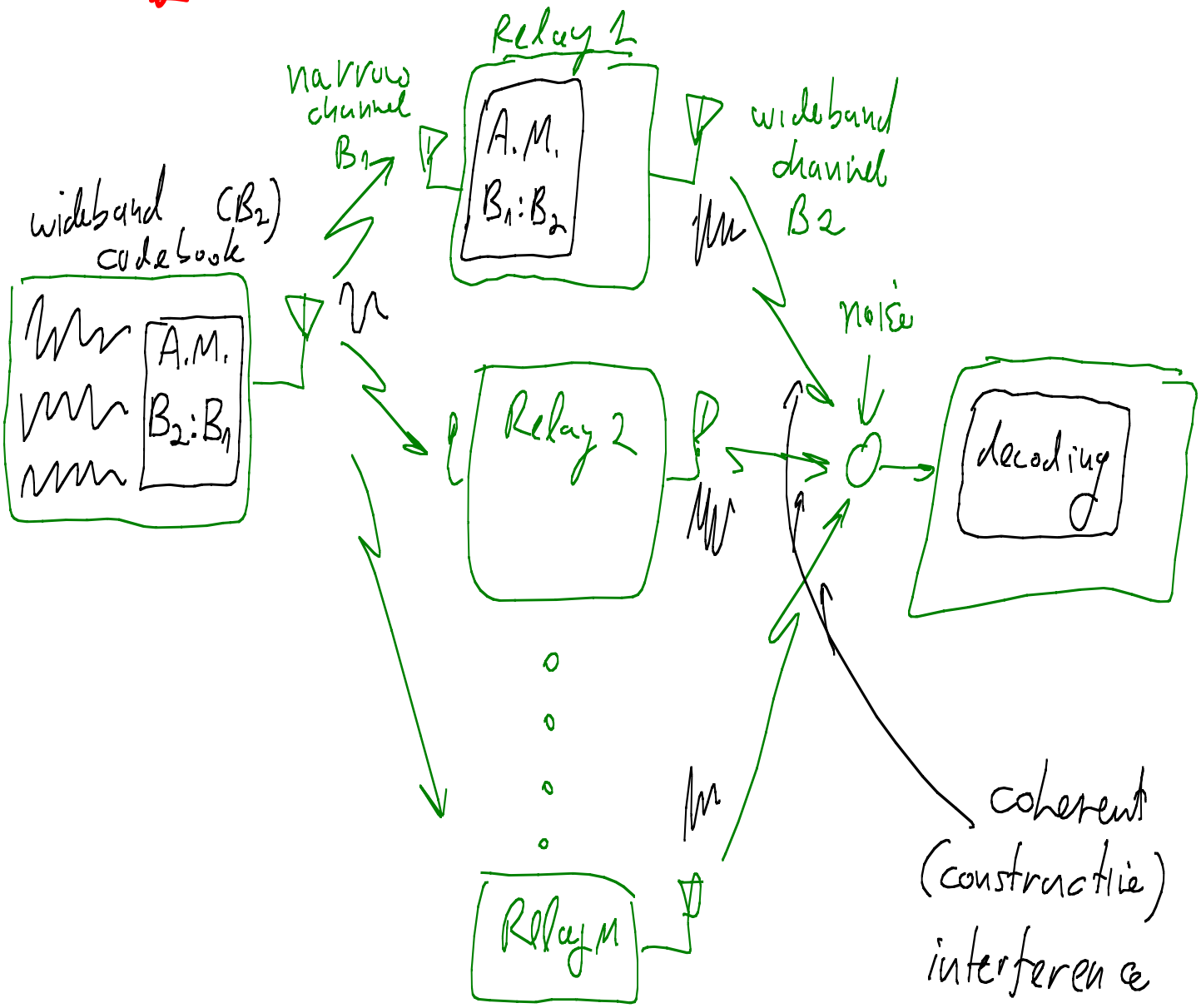


analog - DPC / Tomlinson Harashima

analog WZ

$\Rightarrow$ Achieves $R(D) = C$

Rematch & Forward for Parallel Relays [Kochman Khina Erez '12]



$\Rightarrow$ extension of Amplify & Forward for $B_2 \neq B_1$

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. Better than Random-Coding,
   in distributed side-information problems

4. a bridge from Analog-to-Digital
   = Robust joint source-channel coding

Summary

Lattices are Everywhere!

More scenarios:

- Multiple descriptions video coding
- Computation & Interference management in linear networks

More applications in practice:

- Lattice decoding for MIMO channels
- Trellis code as a "time invariant lattice"

Lectures @ ETH

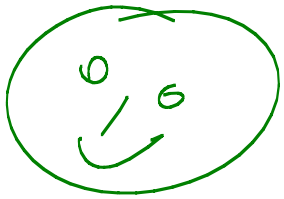
Lattices in ...

12/8/08 Side information problems

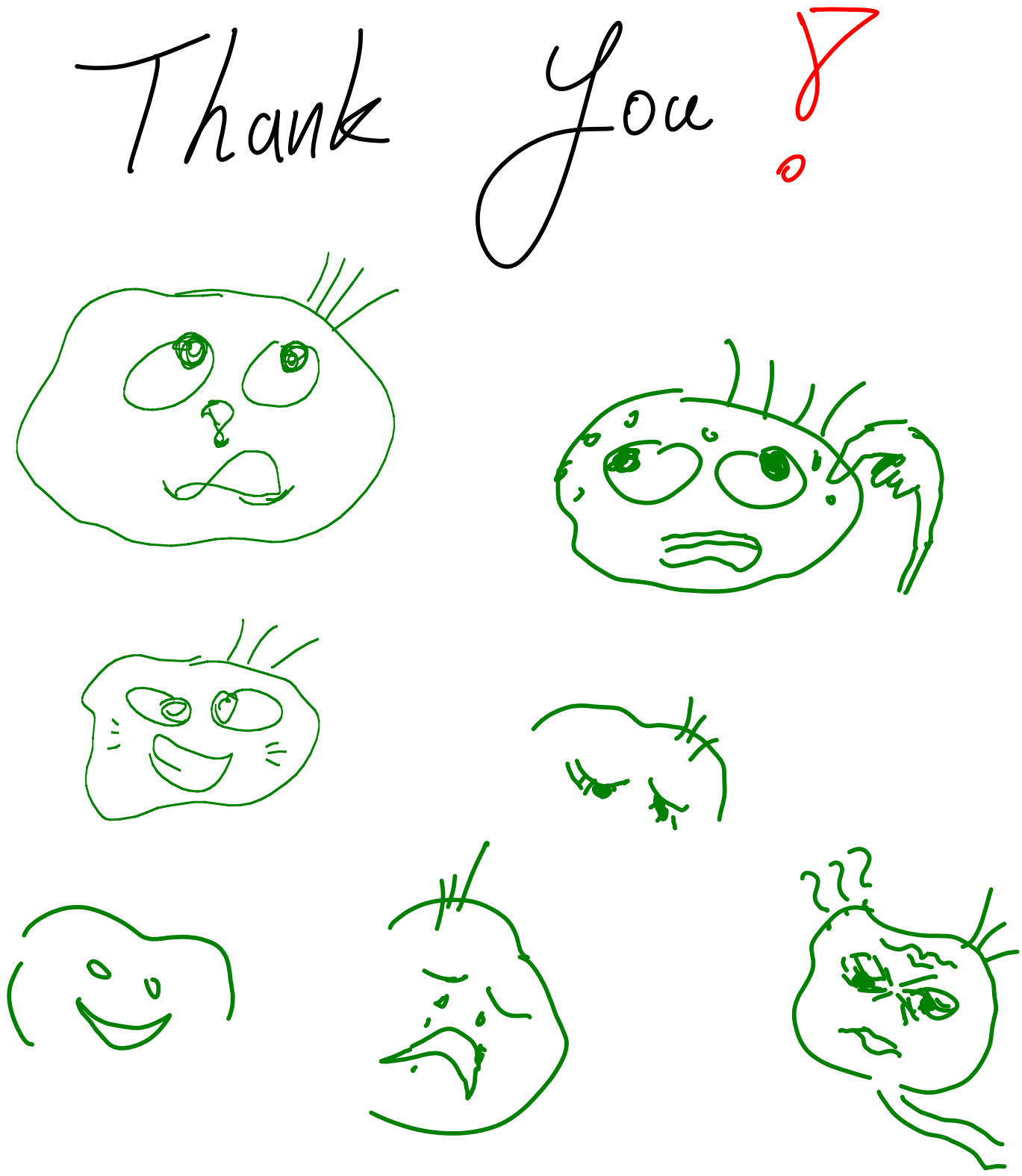
19/8/08 General networks

26/8/08 Joint Source/channel coding

See you there!



Thank You


Thank You!