Lattice Codes in Information Theory

Rami Zamir

School of EE, Tel Aviv University

Talk in London, Sept. 2017

What a Lattice Means?...

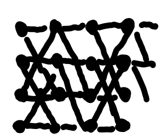
For my kid: 

For a physicist/crystallographer: 

For a mathematician: 

For a Computer Scientist: 

For a coding theorist: $\Lambda_8, \Lambda_{24}, \dots$

 ...

For an Information Theorist:

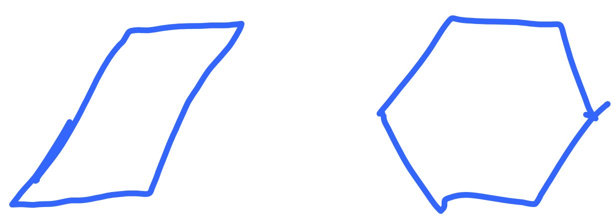
$$n \to \infty$$

We'll talk about ...

1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

1. Representation & Partition

$\mathrm{Vol}(\Lambda)$



modulo Λ

Lattice: Definition

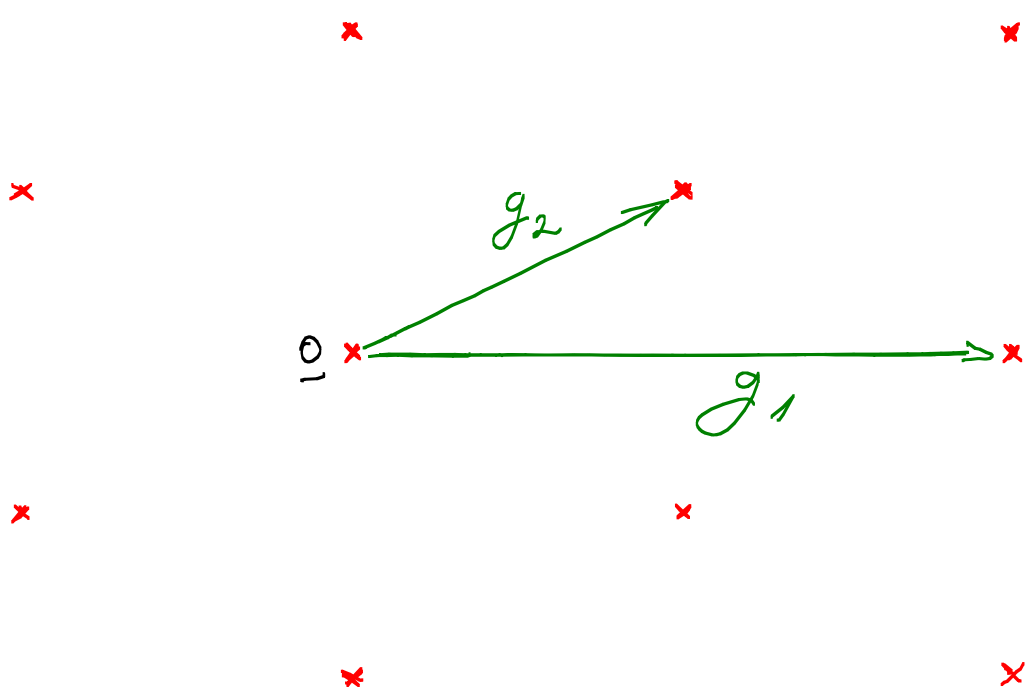
Let $\underline{g}_1, \dots, \underline{g}_n$ – linearly independent vectors in $\mathbb{R}^n$

$$\underline{\underline{G}} = \left(\underline{g}_1 \,\vdots\, \dots \,\vdots\, \underline{g}_n \right) = \text{generator matrix}$$

$$\Lambda(G) = \{ i_1 \cdot \underline{g}_1 + \dots + i_n \cdot \underline{g}_n : i_1 \dots i_n \in \mathbb{Z} \}$$

$$= \{ \underline{\underline{G}} \cdot \underline{i} : \underline{i} \in \mathbb{Z}^n \}$$

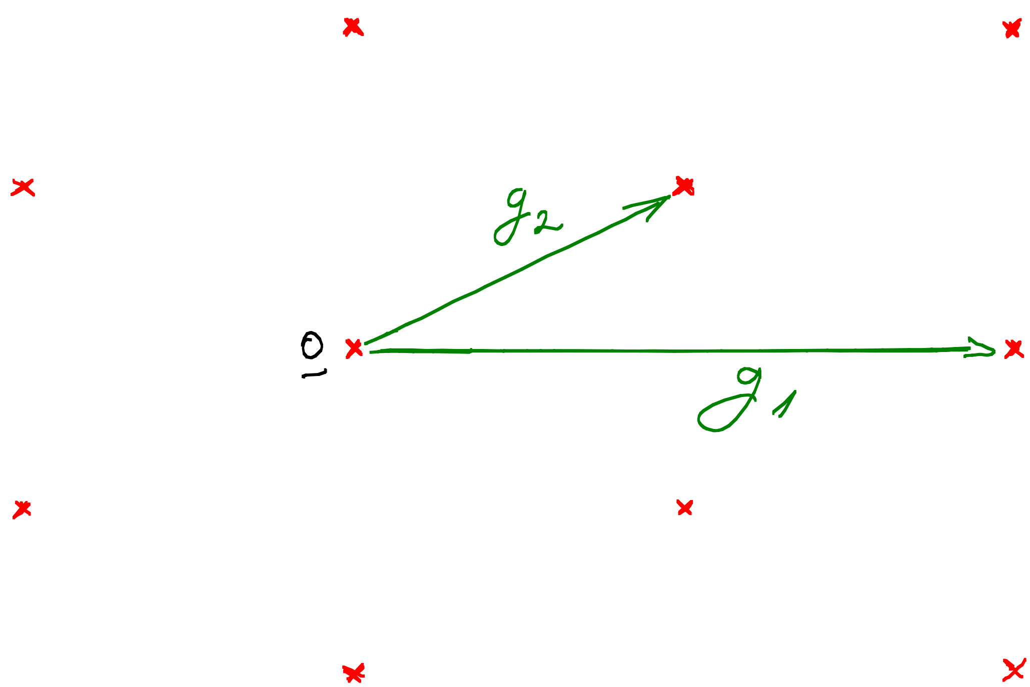
$$= \underline{\underline{G}} \cdot \mathbb{Z}^n$$



n-dimensional lattice: Definition

Let $\underline{g}_1, \dots, \underline{g}_n$ – linearly independent vectors in $\mathbb{R}^n$

$$\underline{\underline{G}} = \left(\underline{g}_1 \,\vdots\, \cdots \,\vdots\, \underline{g}_n \right) = \text{generator matrix}$$



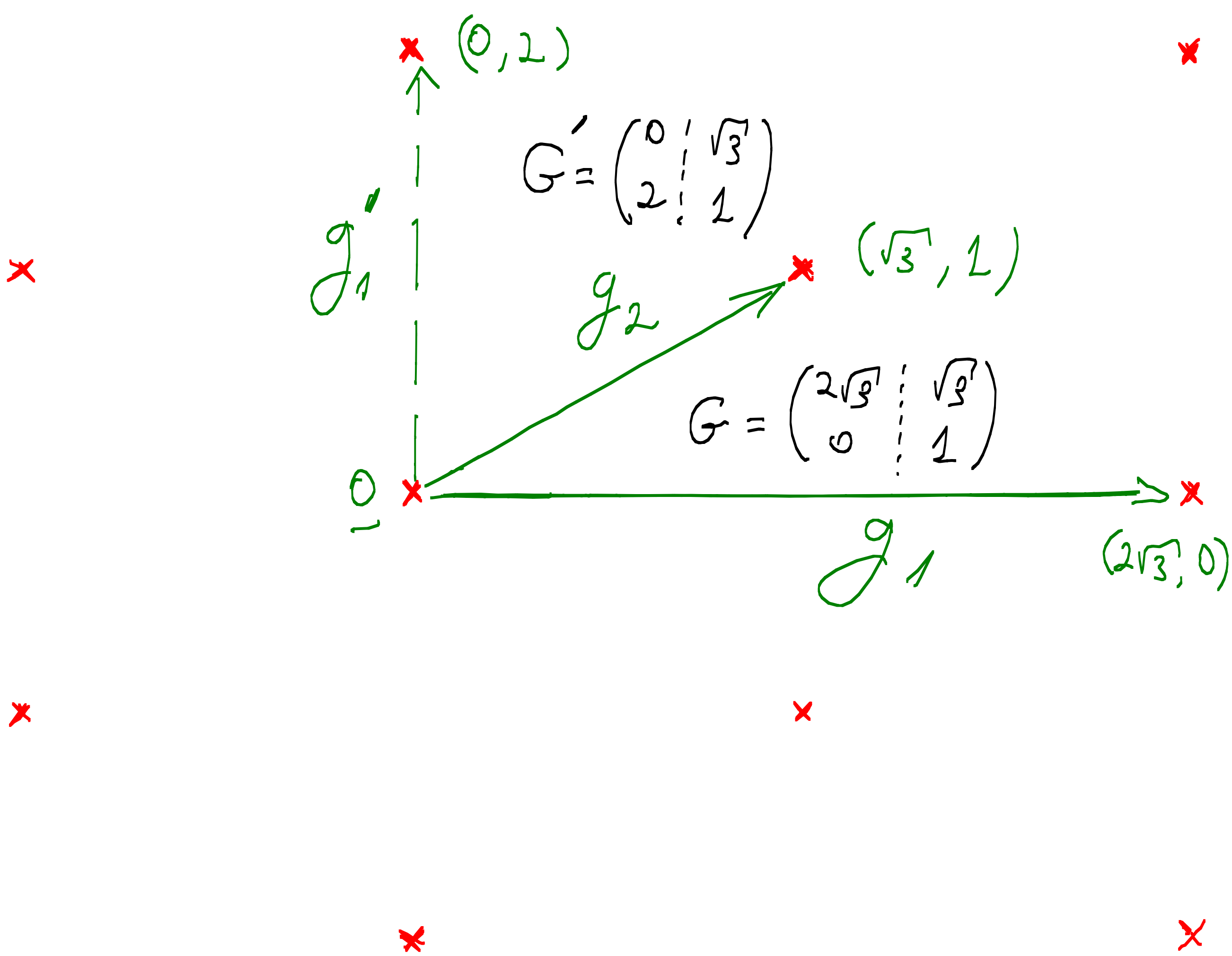
Linearity:

$$\lambda_1, \lambda_2 \in \Lambda \Rightarrow \lambda_1 \pm \lambda_2 \in \Lambda$$

Lattice : Equivalent Representations

T = unimodular matrix
(integer elements, $\det(T) = \pm 1$)

$$\Longrightarrow \quad \Lambda(G \cdot T) = \Lambda(G)$$

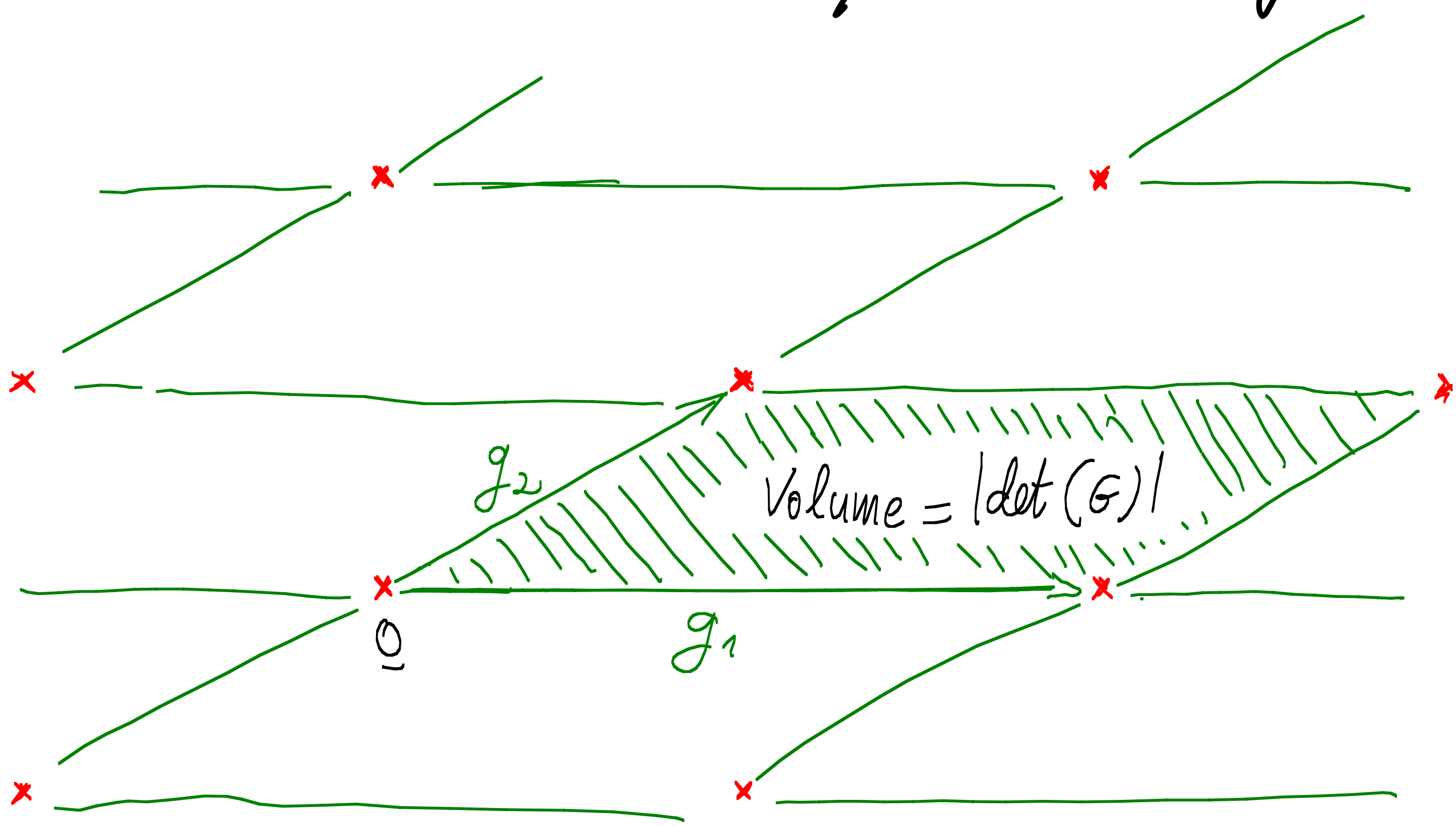


On-Board Calculation...

$$\therefore \quad \det(\Lambda) \triangleq |\det(G)| = \text{basis invariant}$$

Lattice Partition:

Quantization / Decision Regions

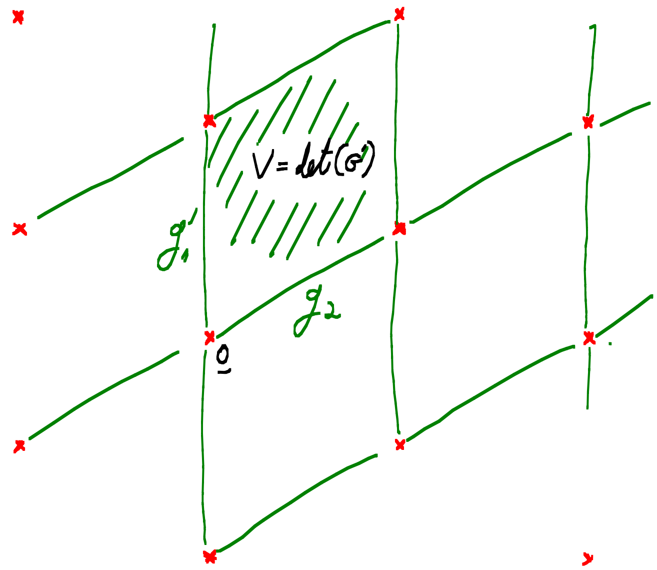


parallelopipeds

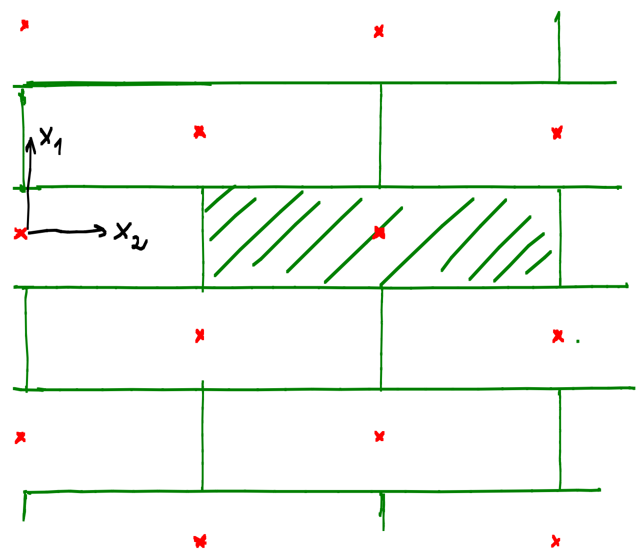
$$P_0 = \{ \alpha_1 g_1 + \alpha_2 g_2 : \quad 0 \leq \alpha_1, \alpha_2 \leq 1 \}$$

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

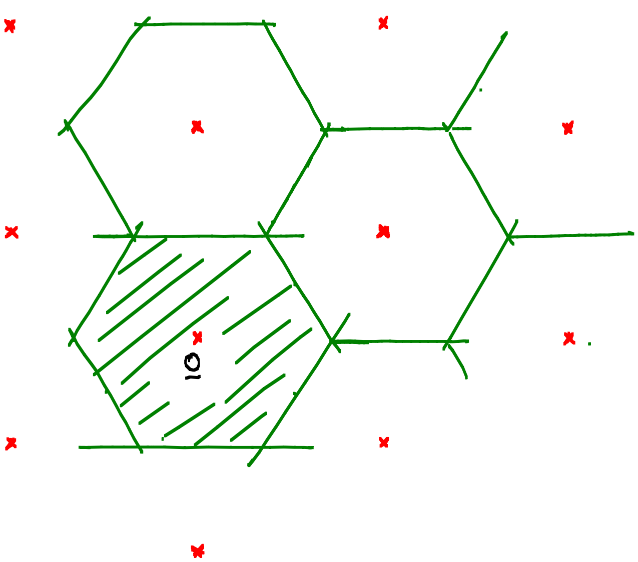
Partitions, Fundamental Cells



Other Basis $\Rightarrow$
other Parallelepiped
$\Rightarrow$ Cell Volume V is
invariant of partition



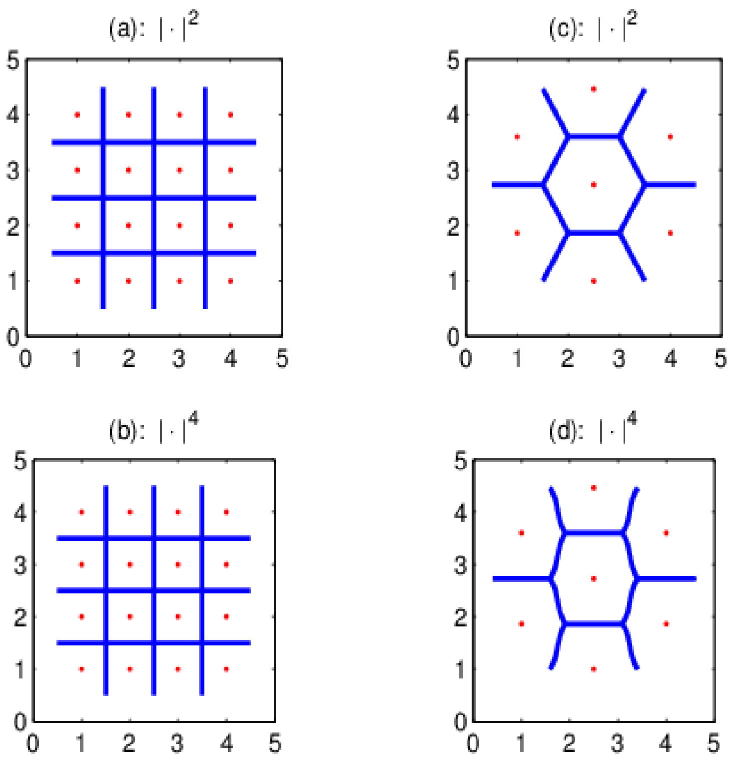
Sequential Quantization



Voronoi Partition

$$P_0 = \left\{ x : \|x\| \le \|x - l_i\| \quad \forall l_i \in \Lambda \right\}$$

Non-Euclidean Voronoi partition



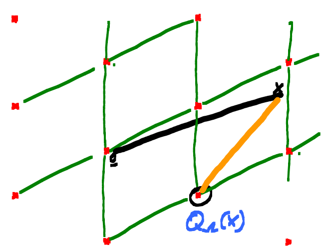
Lattice Quantization, Modulo Lattice

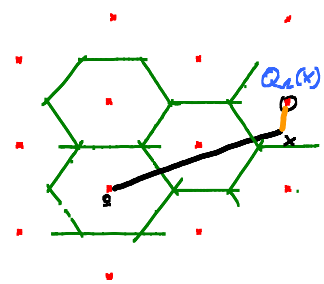
Given lattice Λ and fund. cell $\mathcal{P}_0$:

$$Q(x) = \lambda \quad \text{if} \quad x \in (\lambda + \mathcal{P}_0)$$

$$x \bmod \Lambda = x - Q(x)$$

$\Rightarrow$ $x \in \mathbb{R}^n$ uniquely written as $\underbrace{Q_\Lambda(x)}_{\text{quantization}} + \underbrace{(x \text{ modulo } \Lambda)}_{\text{error}}$





Modulo Laws:

* $a \bmod \Lambda = a + \lambda(a), \quad \lambda(a) \in \Lambda$
* $(a + \lambda) \bmod \Lambda = a \bmod \Lambda, \quad \forall \lambda \in \Lambda$
* $[(a \bmod \Lambda) + b] \bmod \Lambda = (a+b) \bmod \Lambda$
* $(a \bmod_{\mathcal{P}_0} \Lambda) \bmod_{Q_0} \Lambda = a \bmod_{Q_0} \Lambda$

On-Board Calculation...

$$\therefore \quad V(\Lambda) \triangleq \text{cell volume} = \det(\Lambda)$$

$$= \text{invariant of partition}$$

Similarity

$\Lambda(G')$ is similar to $\Lambda(G)$ if

$$G' = \underbrace{\alpha}_{\text{scaling}} \cdot \underbrace{A}_{\text{orthonormal transformation (rotation)}} \cdot G \cdot \underbrace{T}_{\text{unimodular transformation (basis change)}}$$

Example: E8 lattice

Definition 1: all all-integer or all half-integer vectors in $\mathbb{R}^8$ whose coordinate sum is even.

Definition 2 (construction A): $\{ \underline{x} \in \mathbb{R}^8 : \underline{x} \bmod 2 \in \mathcal{C}_H \}$

$\mathcal{C}_H = (8,4,4)$ extended Hamming code $= \ldots$

Nested Lattices

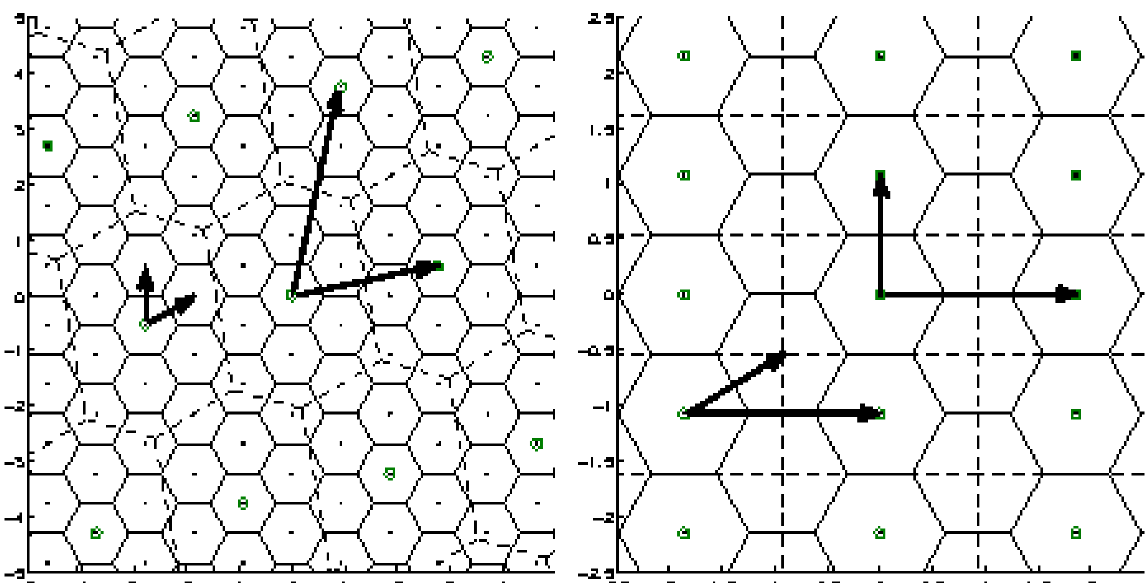
$$\Lambda_2 \subset \Lambda_1 \implies \underline{\underline{G_2}} = \underline{\underline{G_1}} \cdot \underline{\underline{J}}$$

course lattice

fine lattice

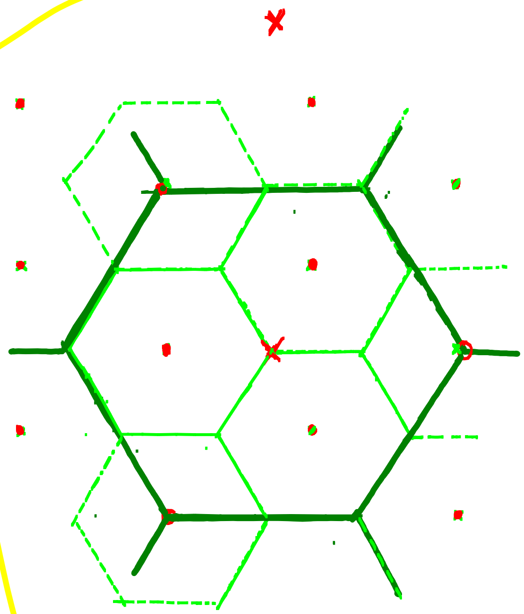
integer matrix

$$\text{Nesting Ratio} = \left(\frac{V(\Lambda_2)}{V(\Lambda_1)}\right)^{1/n} = \left|\det(J)\right|^{1/n}$$



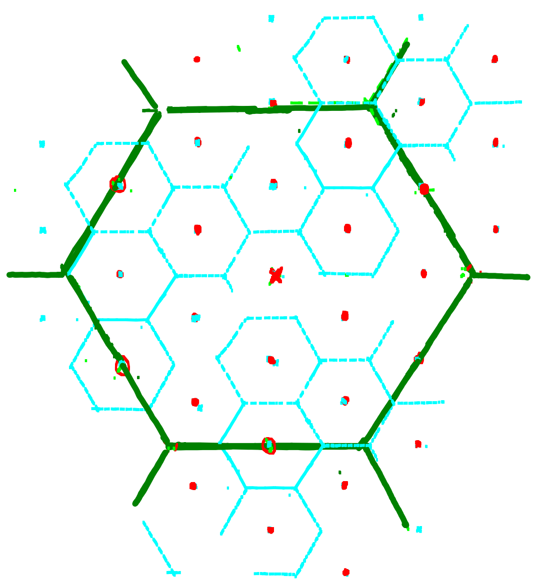
Not necessarily "Self Similar"!

$\Rightarrow V_{02} \not\subset V_{01}$



Relatively Periodic (non nested)

Nested & Self Similar



Diagonal Form

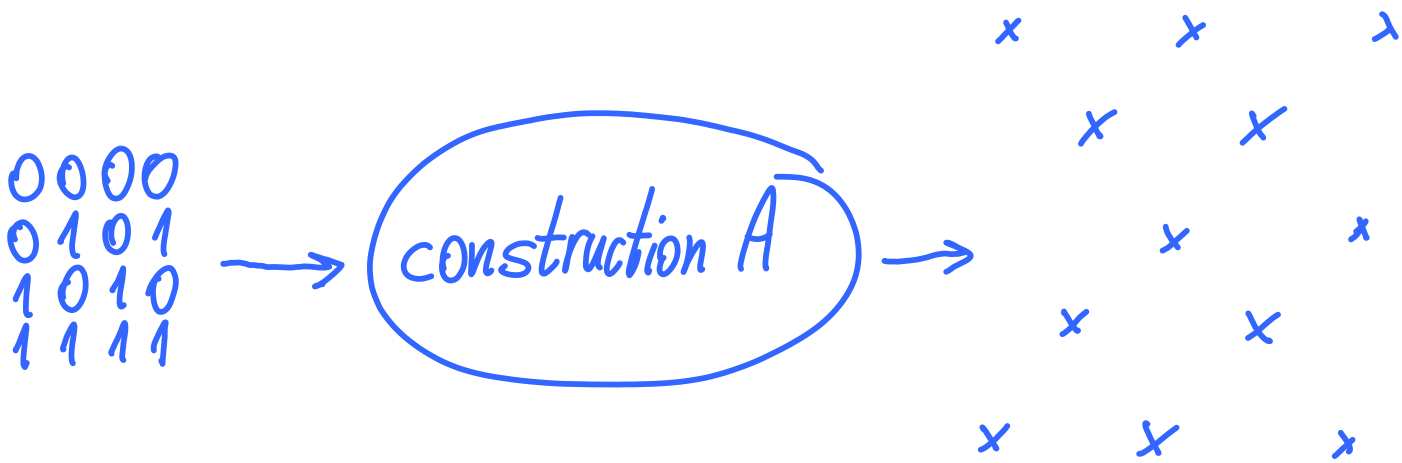
If $\Lambda_2 \subset \Lambda_1$, then $\exists$ generator matrices G_1, G_2 s.t. the nesting matrix J is diagonal

$$\underline{\underline{J}} = \begin{pmatrix} j_1 & & 0 \\ & \ddots & \\ 0 & & j_n \end{pmatrix}$$

We'll talk about ...

1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

2. Construction from Linear Codes



Construction A

Let $\mathcal{C}$ be an (n, M, d) binary code:

$\mathcal{C} = \{\underline{c}_i\}_{i=1}^{M}$, $\underline{c}_i \in \{0,1\}^n$, d = minimum Hamming distance.

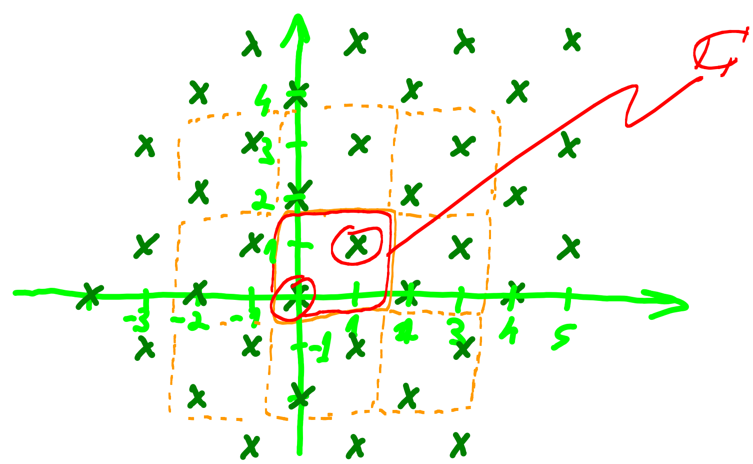
Construction A lifts $\mathcal{C}$ to $\mathbb{R}^n$ periodically:

Def. I

$$\Gamma_{\mathcal{C}} = \{\underline{x} \in \mathbb{Z}^n : \underline{x} \bmod 2 \in \mathcal{C}\}$$

integer vectors

modulo 2 per each component



Equivalent definitions:

1) $\Gamma_{\mathcal{C}} = \mathcal{C} + 2 \cdot \mathbb{Z}^n$ Def. II

2) Let $z = (LSB(z), MSB_1(z), MSB_2(z), \ldots)$ = binary expansion of z

$$\Gamma_{\mathcal{C}} = \{\underline{x} \in \mathbb{Z}^n : LSB(\underline{x}) \in \mathcal{C}\}$$ Def. III

Construction A : Properties

1) $d^E_{min}(\Gamma) \triangleq$ min Euclidean distance $\triangleq \min\limits_{\substack{x,y\in\Gamma \\ x\neq y}} \|x-y\|$

$$= \min\left\{2 , \sqrt{d}\right\}$$

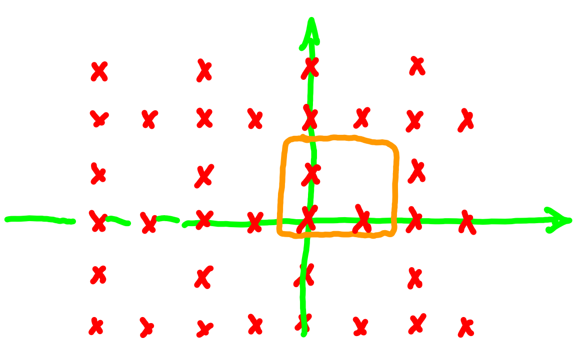
min Euclidean dist in coset $\underline{c} + 2\mathbb{Z}^n$ for $\underline{c} \in \mathcal{C}$

$d_H(\underline{c}_1, \underline{c}_2) = d$

$\Rightarrow \|\underline{c}_1 - \underline{c}_2\| = \sqrt{d}$ (Pythagoras)

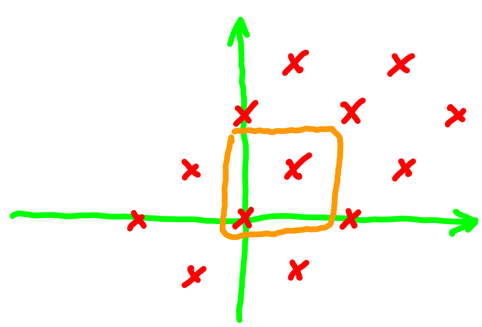
2) If $\mathcal{C}$ is a linear (n,k,d) code ($M = 2^k$)

$\Rightarrow \Gamma_{\mathcal{C}} = \Lambda_{\mathcal{C}}$ is a modulo-2 lattice.



non lattice

$\mathcal{C} = \{(00), (01), (10)\}$



lattice

$\mathcal{C} = \{(00), (11)\}$

We'll talk about ...

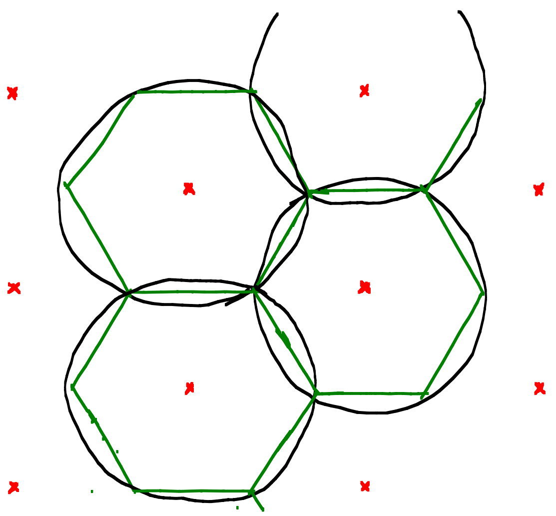
1. lattices: representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

3. Figures of merit

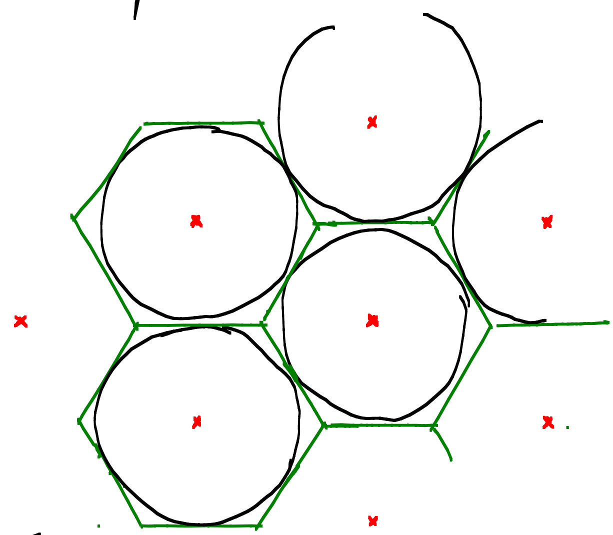
$G(\Lambda)$, $\mu(\Lambda, p_e)$

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

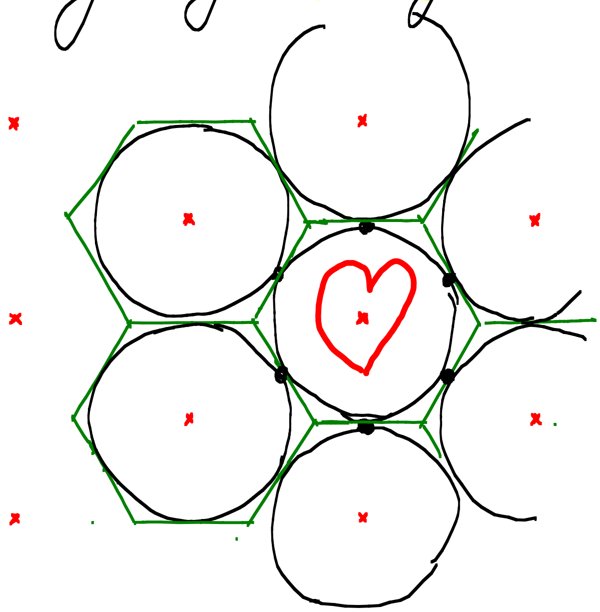
Covering $\mathbb{R}^n$ with (few) Spheres



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



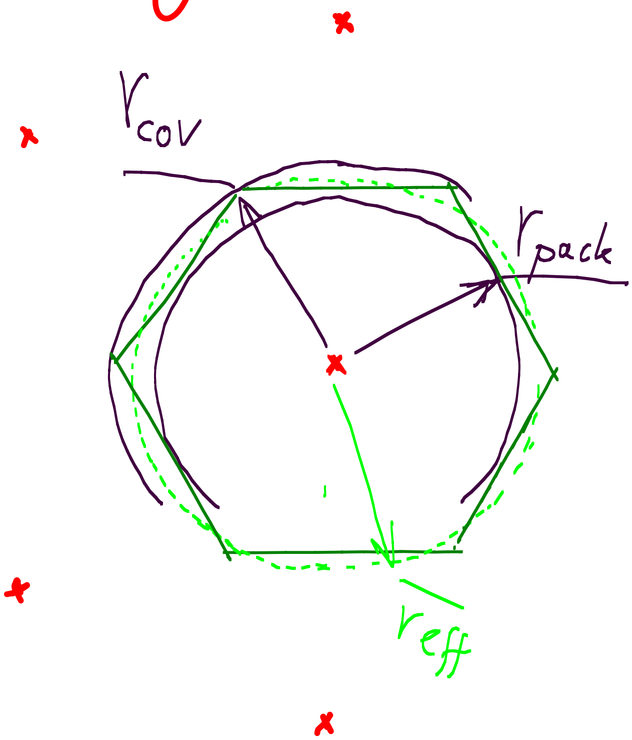
Kissing by (many) Spheres



&

good arrangements for quantization and AWGN channel coding

Figures of Merit



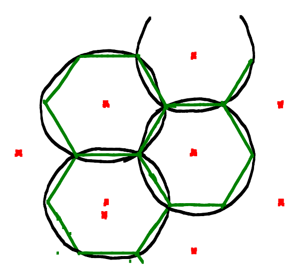
Radiuses:

r_{cov} = min sphere containing V_0

r_{pack} = max sphere contained in V_0
$= d_{min} / 2$

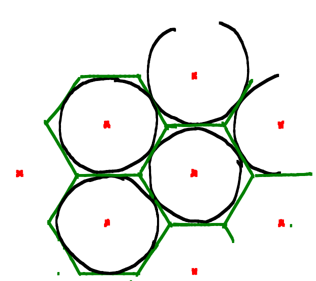
r_{eff} = Sphere with same volume

- Covering efficiency:



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

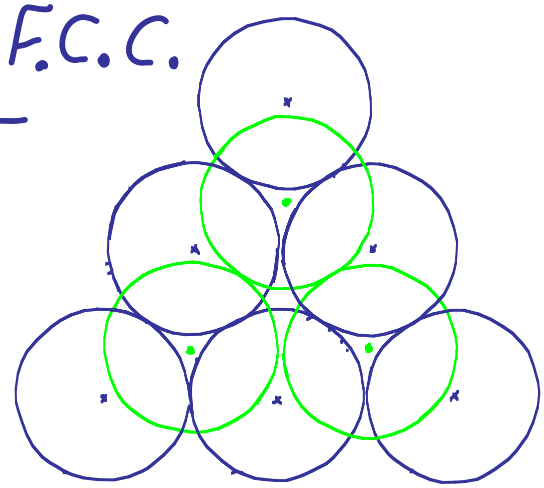
- Packing efficiency:



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

Not an "All-Purpose" Lattice!

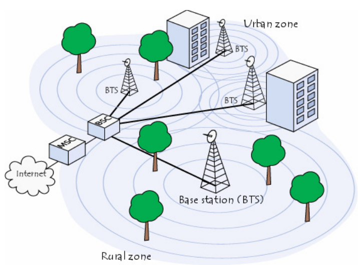
* <u>Best 3-dim Packing: F.C.C.</u>

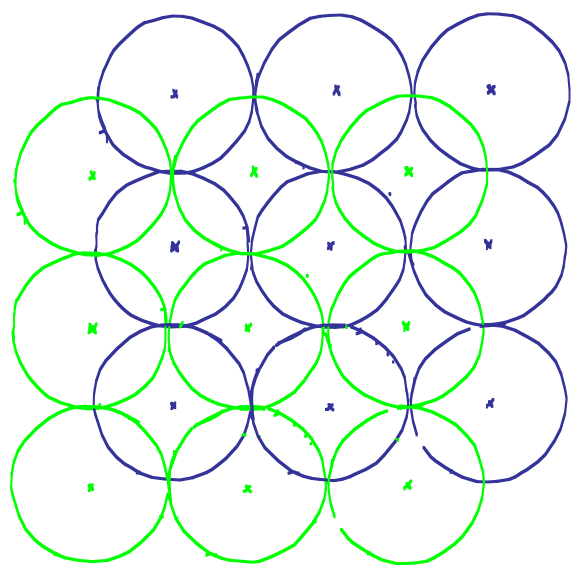


each layer = hexagonal Λ
layers are staggered

* <u>Best 3-dim Covering: B.C.C.</u>

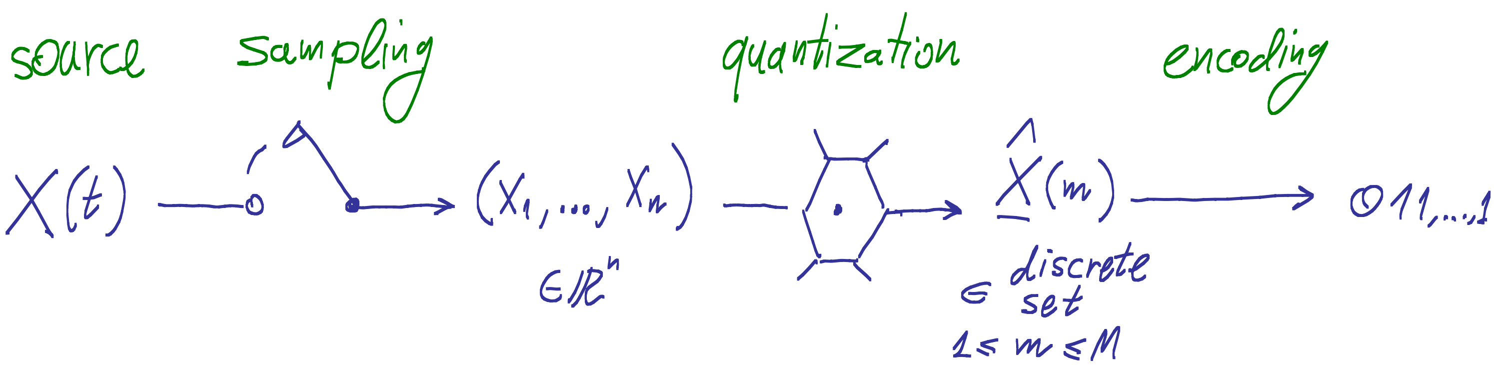
each layer = cubic Λ
layers are staggered

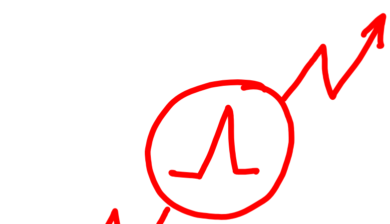




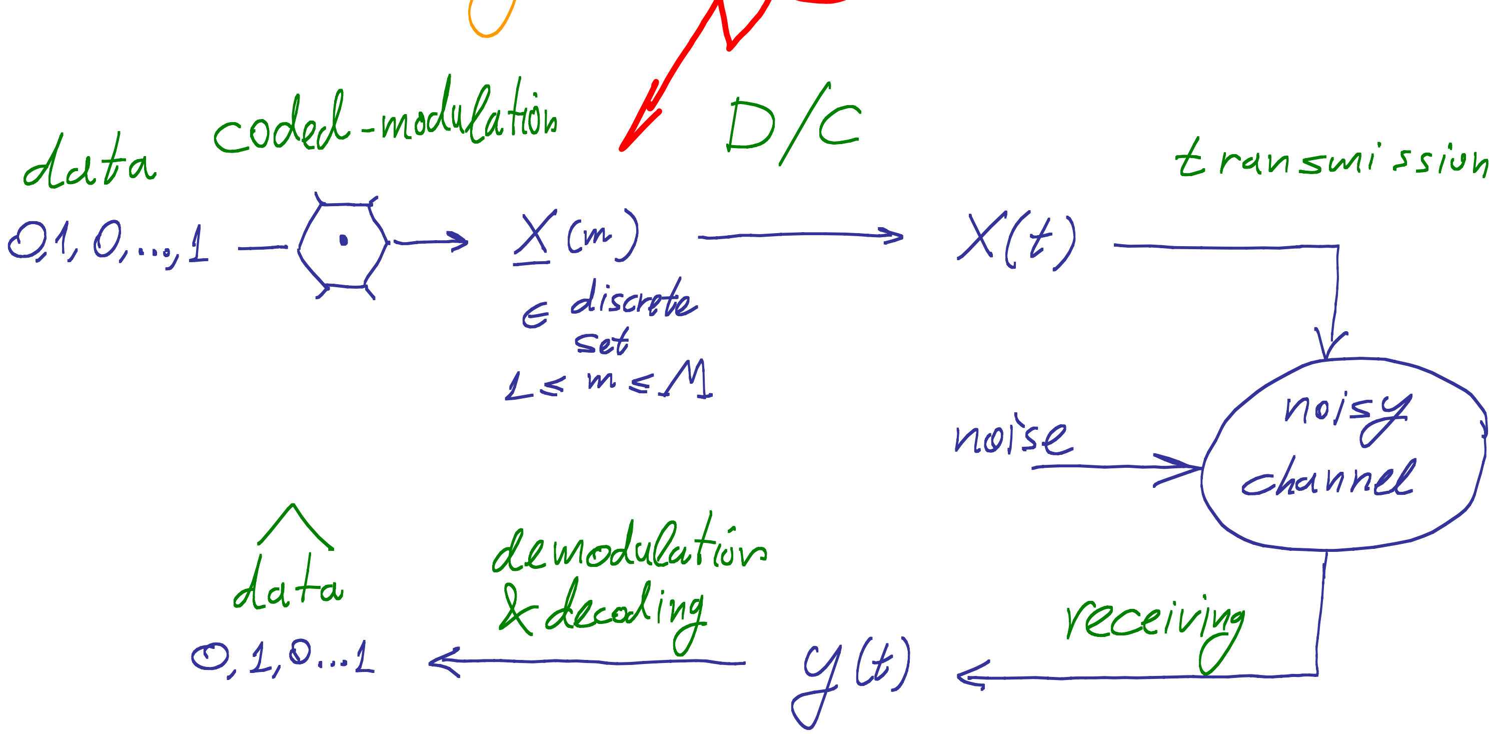
Source coding (quantization) & Channel coding (modulation)

Source coding:



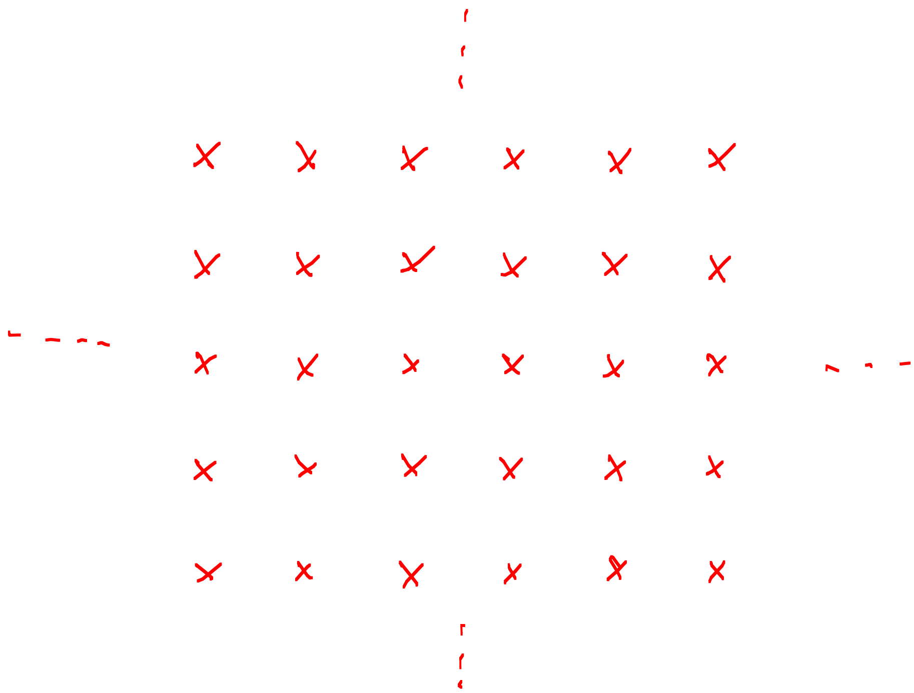


channel coding:

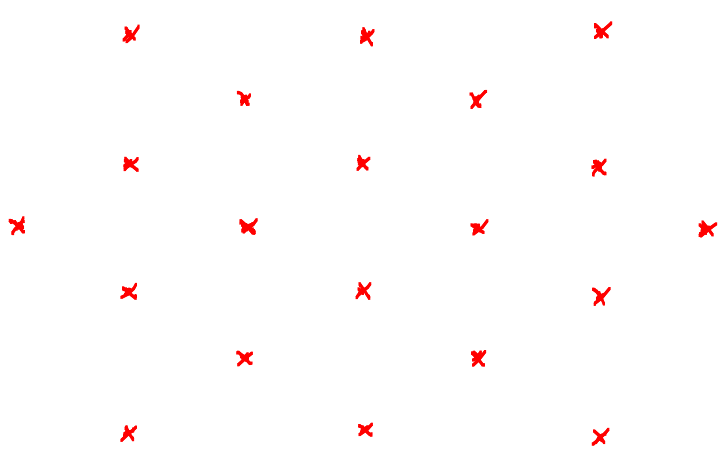


Lattice Codes in Signal Space

square ($\mathbb{Z}$)-lattice $\Rightarrow$ uncoded constellation



More "interesting" lattice $\Rightarrow$ coded constellation



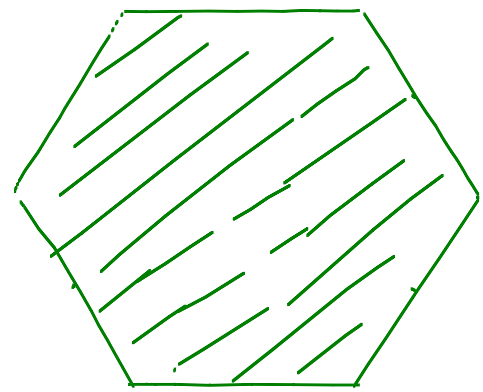
Figures of Merit (Continued)

- Quantization efficiency:

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

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

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

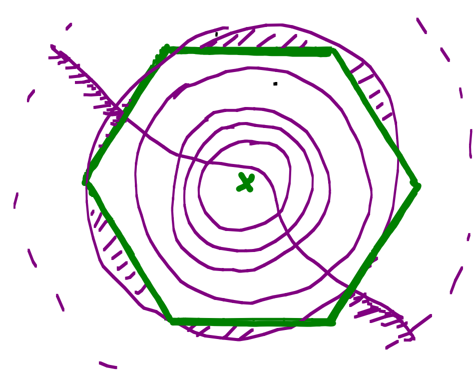


Figures of Merit (Continued)

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

$$\mu(\Lambda, \sigma^2) \triangleq \frac{V^{2/n}}{\sigma_z^{\,2}} \quad = \text{Volume-to-Noise Ratio}$$

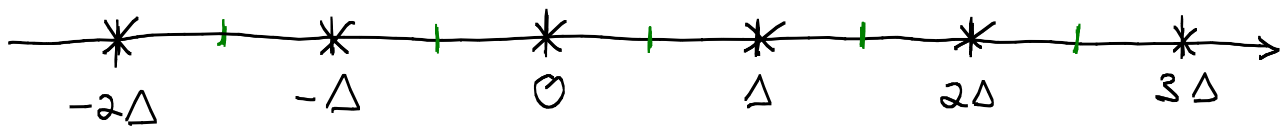
$$P_e \triangleq \Pr\{\underline{Z} \notin V_0\}$$



$$\mu(\Lambda, P_e) \triangleq \left.\frac{V^{2/n}}{\sigma_z^{\,2}}\right|_{@ P_e}$$

Example: One dimensional lattice

(Voronoi cell = interval)



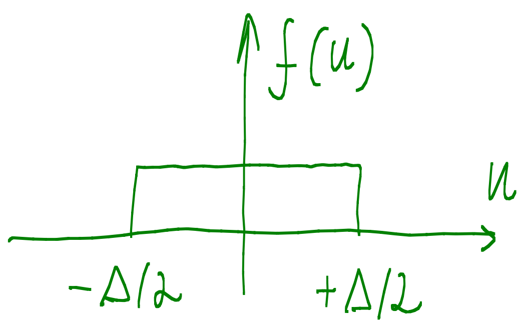
1. NSM

U = dither

~uniform

on Voronoi cell

$= (-\Delta/2, +\Delta/2)$



$V(\Lambda) = \Delta$

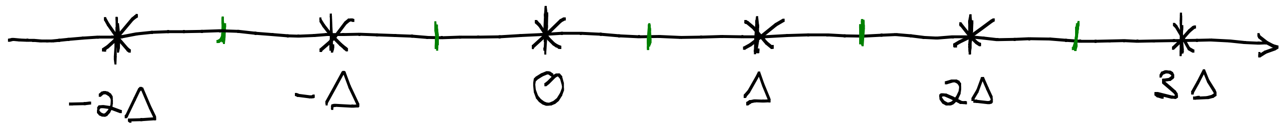
$EU^2 = \dfrac{\Delta^2}{12}$

$$\Rightarrow \quad G(\square) = \frac{EU^2}{V^2(\Lambda)} = \frac{\Delta^2/12}{\Delta^2} = \frac{1}{12}$$

<u>invariant of Δ</u>

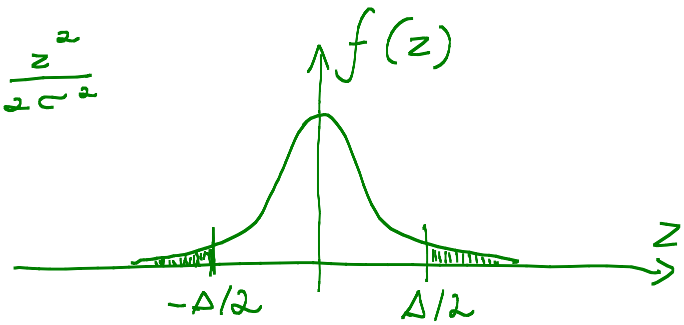
Example: One dimensional lattice

(Voronoi cell = interval)



2. NVNR

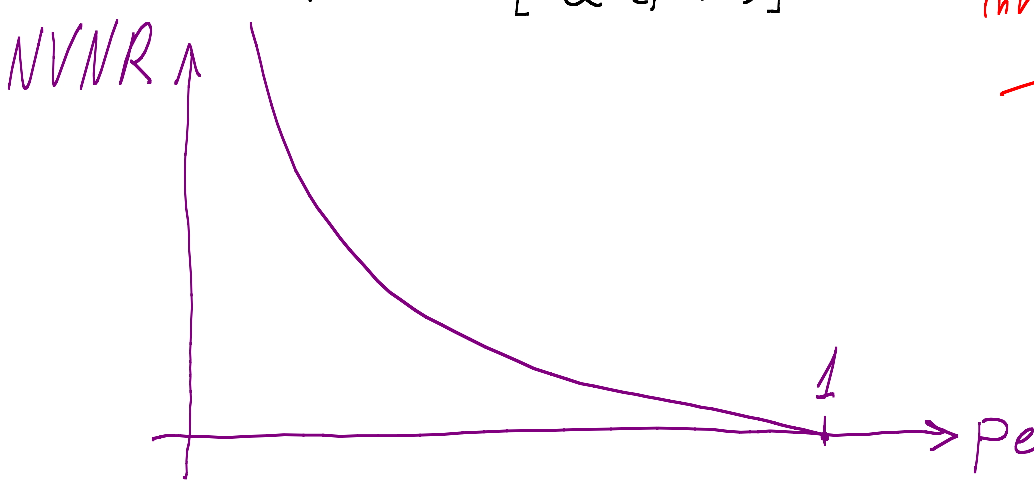
$$Z \sim \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{z^2}{2\sigma^2}}$$



$$P_e = P_r\left\{|Z| > \frac{\Delta}{2}\right\} = 2 \cdot Q\left(\frac{\Delta/2}{\sigma}\right)$$

$$\Rightarrow \mu(\Lambda, P_e) = \frac{V^2(\Lambda)}{\sigma_{P_e}^2} = \left[\frac{\Delta}{\frac{\Delta/2}{Q^{-1}(P_e/2)}}\right]^2 = \left[2 \cdot Q^{-1}\left(\frac{P_e}{2}\right)\right]^2$$

invariant of Δ



Coding Gains (w.r.t. $\mathbb{Z}$ - lattice)

* **lattice vector quantizer gain:**

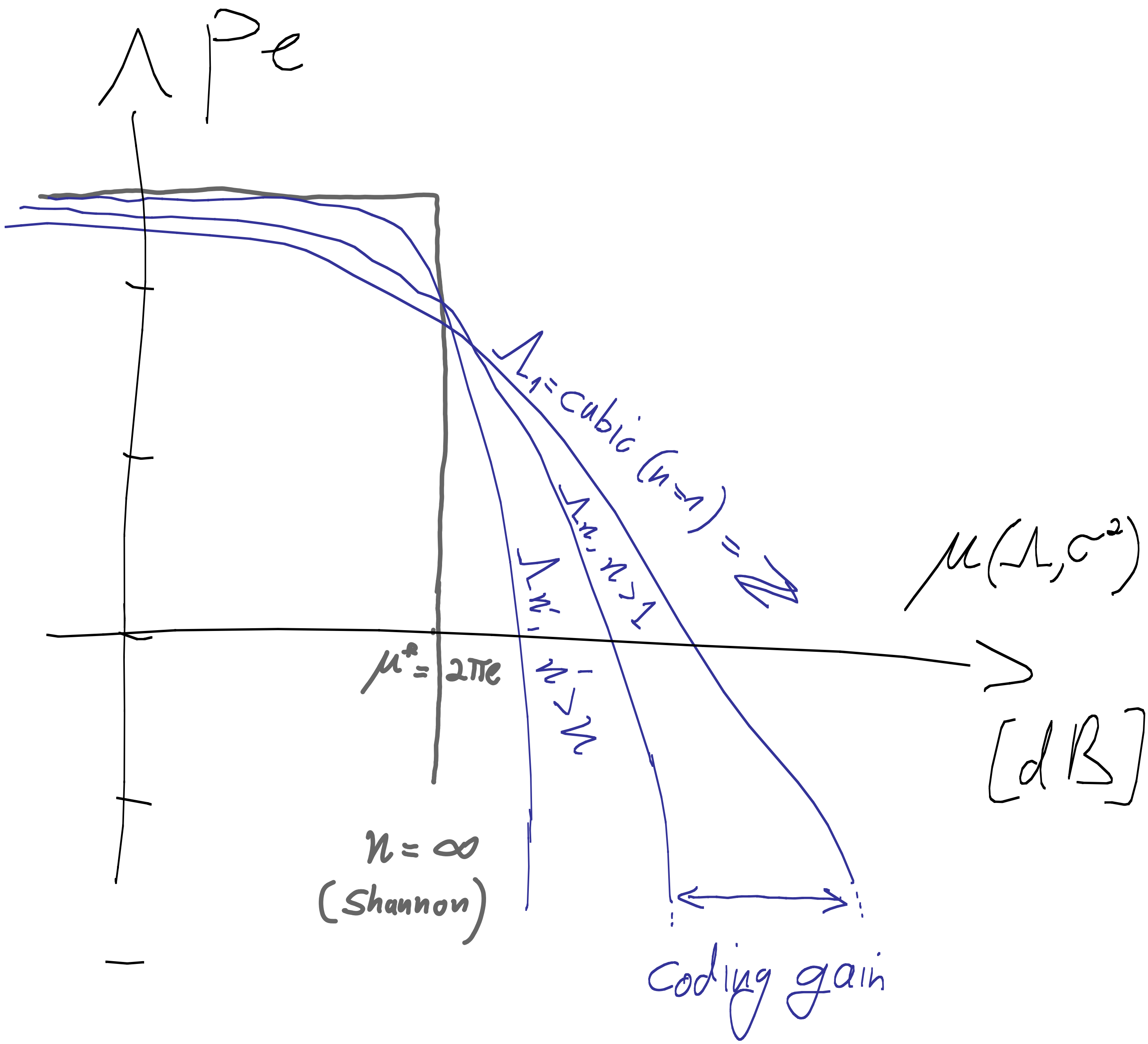
$$\triangleq \left.\frac{\sigma^2(\mathbb{Z})}{\sigma^2(\Lambda)}\right|_{@\text{ same } V} = \frac{G(\mathbb{Z})}{G(\Lambda)}$$

* **Coding gain @ AWGN channel:**

$$\triangleq \left.\frac{\sigma_z^2 @ \Lambda}{\sigma_z^2 @ \mathbb{Z}}\right|_{\substack{@\text{ same } P_e \\ \text{same } V}} = \frac{\mu(\mathbb{Z}^n, P_e)}{\mu(\Lambda, P_e)} \xrightarrow[P_e \to 0]{} \left.\frac{d_{min}^2(\Lambda)}{d_{min}^2(\mathbb{Z})}\right|_{@\text{ same } V}$$

P_e versus V.N.R. for fixed V

(~ "P_e versus SNR @ fixed Rate")



We'll talk about ...

1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

4. Asymptotic goodness

dimension $\to \infty$

$$G(\Lambda_n) \xrightarrow{?} \frac{1}{2\pi e}, \quad \text{as } n \to \infty$$

$$\mu(\Lambda_n, P_e) \xrightarrow{?} 2\pi e, \quad \text{as } n \to \infty \quad \forall P_e > 0$$

$G(\Lambda_n)$ and $\mu(\Lambda_n, P_e)$ as a function of dimension n

[Conway & Sloane Book 1988]

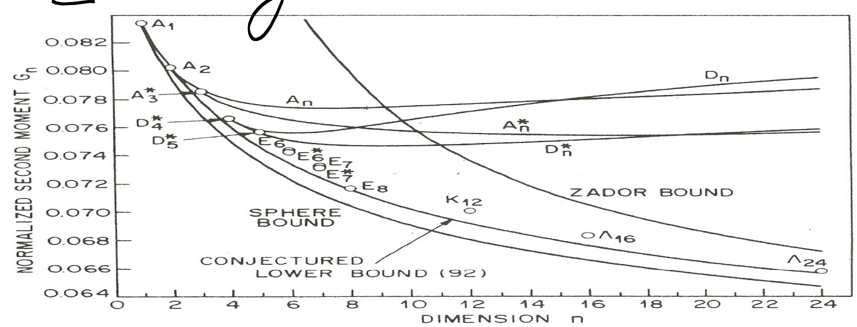
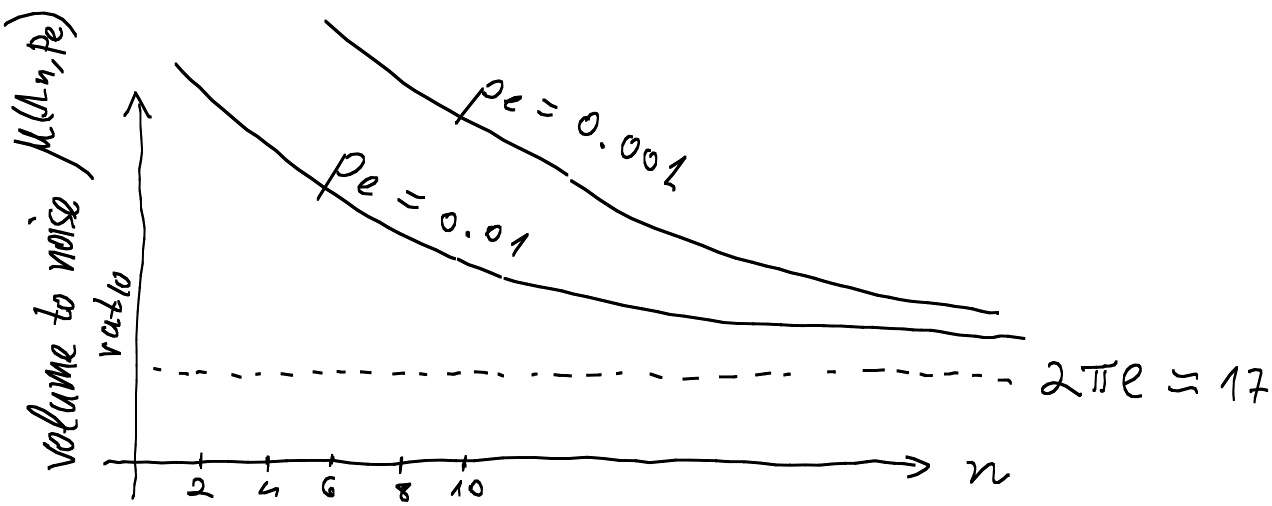


Figure 2.9. The best quantizers known in dimensions $n \leqslant 24$. - - - - - - - $\frac{1}{2\pi e} \simeq 0.058$



$\Lambda_k^{opt} \longrightarrow$

$G_k \longrightarrow$?

$\mu_k \longrightarrow$

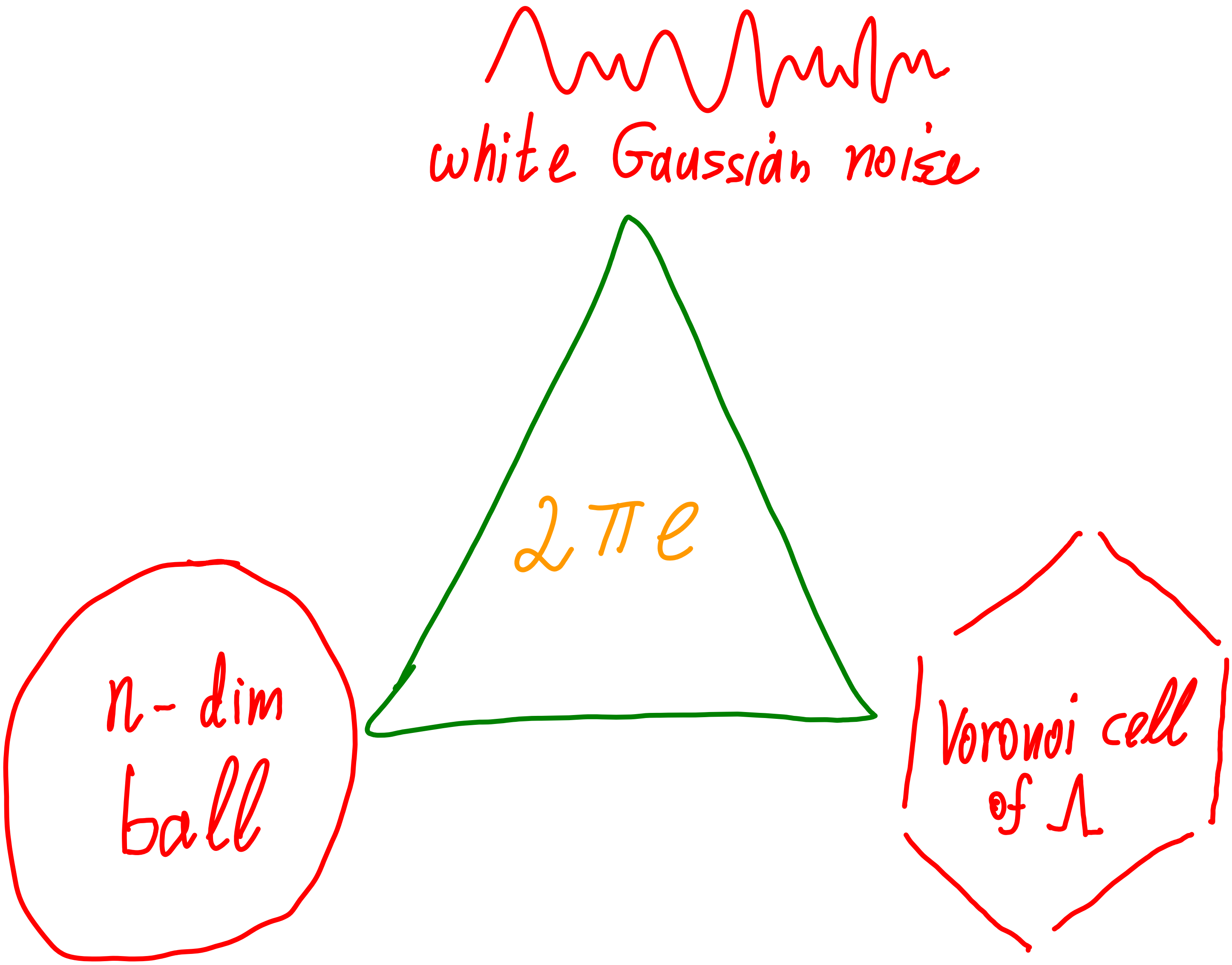
Vector Quantization Gain of Λ_n, for $n = 1, 2, 3, \ldots$

Dimension	Lattice		Γ_q [dB]	Sphere Bound
1	$\mathbb{Z}$	integer	0	0
2	A_2	hexagonal	0.17	0.20
3	A_3	FCC	0.24	0.34
3	A_3^*	BCC	0.26	0.34
4	D_4	(Example 2.4.2)	0.36	0.45
5	D_5^*		0.42	0.54
6	E_6^*		0.50	0.61
7	E_7^*		0.57	0.67
8	E_8^*	Gosset*	0.65	0.72
12	K_{12}		0.75	0.87
16	BW_{16}	Barnes-Wall	0.86	0.97
24	Λ_{24}^*	Leech*	1.03	1.10
∞	?	?	1.53	1.53

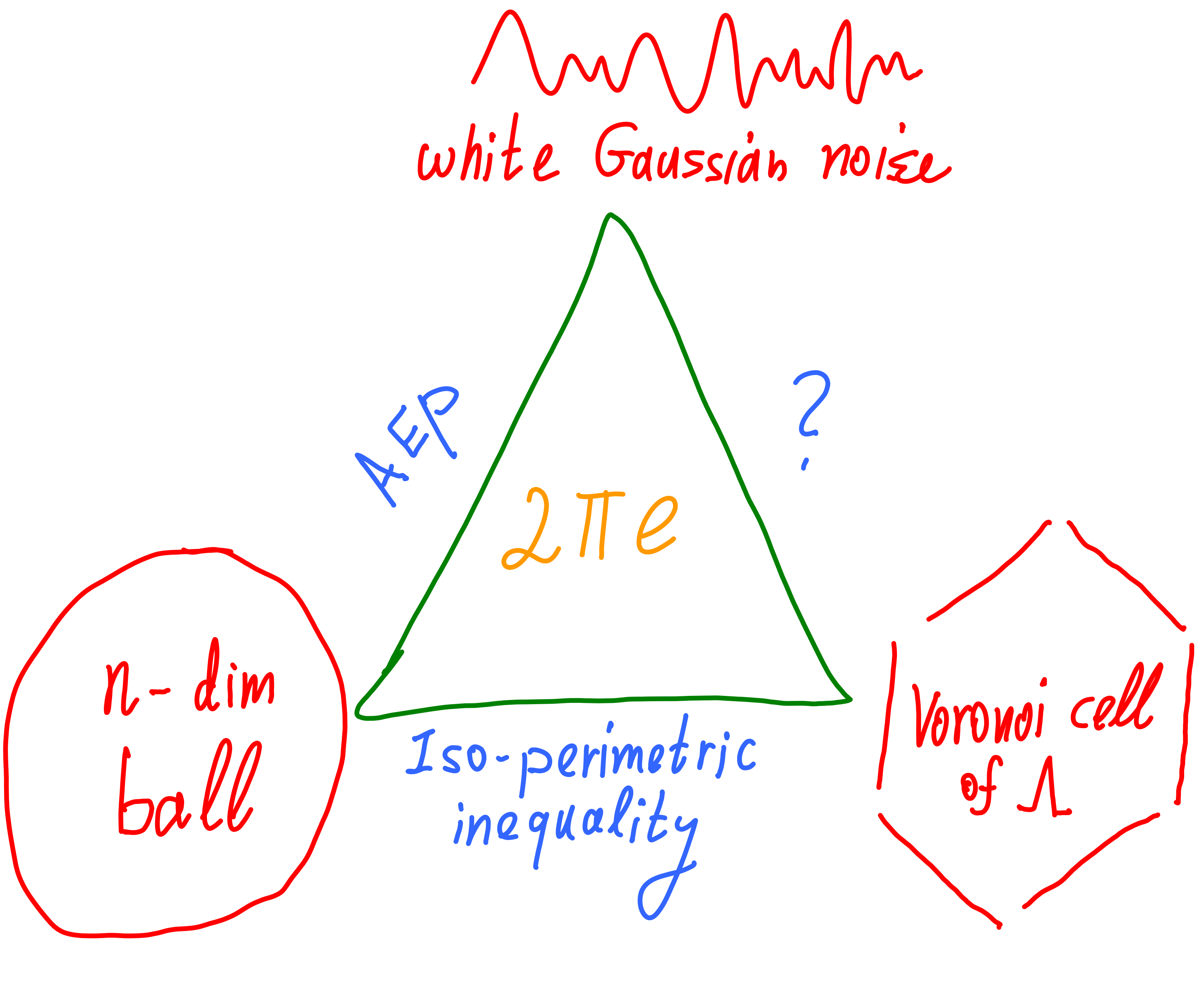
Coding Gain of Λ_n, for $n = 1, 2, 3, \ldots$

SER		10^{-1}	10^{-2}	10^{-3}	10^{-4}	10^{-5}
Dim.	Lattice					
1	$\mathbb{Z}^1$	0	0	0	0	0
2	A_2	0.14 (0.16)	0.27 (0.33)	0.33 (0.45)	0.42 (0.54)	0.46 (0.6)
3	A_3	0.20 (0.27)	0.42 (0.56)	0.55 (0.78)	0.65 (0.93)	0.72 (1.05)
	A_3^*	0.20 (0.27)	0.40 (0.56)	0.52 (0.78)	0.59 (0.93)	0.61 (1.05)
4	D_4	0.29 (0.36)	0.60 (0.75)	0.82 (1.03)	0.95 (1.24)	1.00 (1.40)
8	E_8	0.50 (0.56)	1.08 (1.2)	1.49 (1.68)	1.80 (2.04)	2.00 (2.30)
16	BW_{16}	0.63 (0.75)	1.47 (1.63)	2.09 (2.32)	2.52 (2.83)	2.80 (3.22)
24	Λ_{24}	0.75 (0.84)	1.76 (1.85)	2.51 (2.65)	3.08 (3.25)	3.50 (3.71)
∞	?	-2.0	1.9	4.0	5.5	6.6

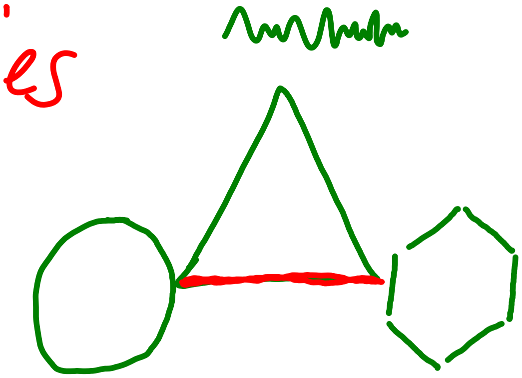
W.G.N. $\longleftrightarrow$ Ball $\longleftrightarrow$ Λ

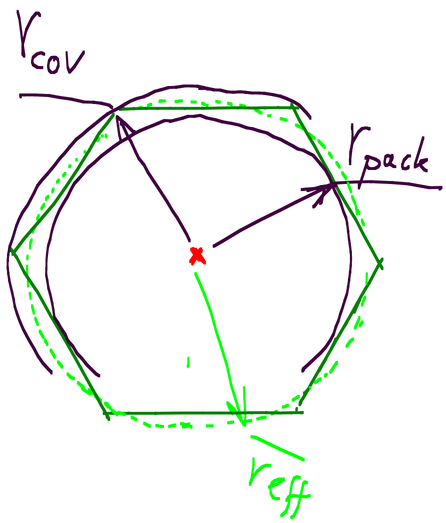


$W.G.N. \longleftrightarrow \text{Ball} \longleftrightarrow \Lambda$



Iso-perimetric Inequalities (Sphere bounds)





Ball minimizes

* * *

over all bodies of a fixed volume!

$$\sigma^2(\Lambda) \geq \sigma^2(\text{ball with radius } r_{eff})$$

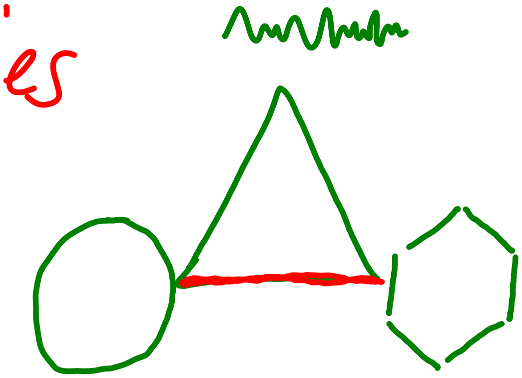
$$P_e(\Lambda) \geq P_e(\;\text{"}\quad\text{"}\quad\text{"}\quad\text{"}\;)$$

$\Longrightarrow$

$$G(\Lambda) \geq \text{N.S.M. of } n\text{-dim ball}$$

$$\mu(\Lambda, p_e) \geq \text{V.N.R.}\;\text{"}\quad\text{"}\quad\text{"}$$

Iso-perimetric Inequalities



$$G(\Omega) \geq G_n(\text{Ball})$$

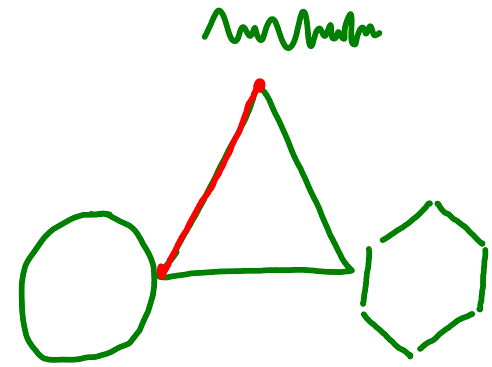
$$\mu(\Omega, p_e) \geq \mu_n(\text{Ball}, p_e)$$

Sphere limits:

$$G_n(\text{Ball}) \longrightarrow \frac{1}{2\pi e} \quad \text{as} \quad n \to \infty$$

$$\mu_n(\text{Ball}, p_e) \longrightarrow 2\pi e \quad \text{as} \quad n \to \infty$$

Shannon's AEP:



W.G.N. $\longrightarrow$ ball

$$Z_1 \dots Z_n \sim \text{AWGN} \quad N(0, \sigma^2)$$

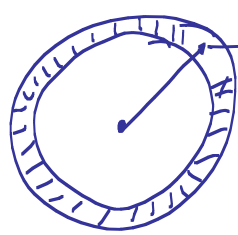
$$A_\varepsilon = \left\{ \underline{z} : \frac{1}{n}\log f_Z(\underline{z}) = h \pm \varepsilon \right\}$$

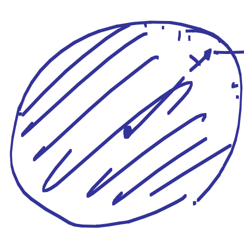
AWGN

$f_Z \sim e^{-\frac{\|z\|^2}{2\sigma^2}}$

$h = \frac{1}{2}\log 2\pi e \sigma^2$

$$= \left\{ \underline{z} : \|\underline{z}\| = \sqrt{n(\sigma^2 \pm \varepsilon')} \right\}$$

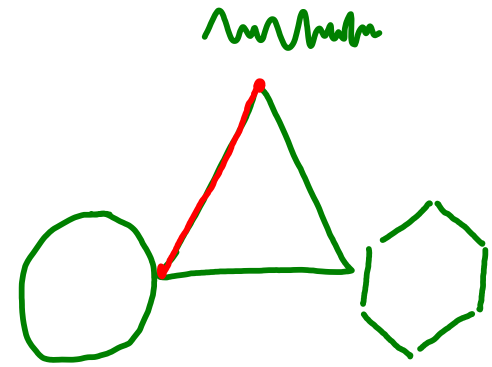
$=$  $\sqrt{n\sigma^2}$

$\cong$  $\sqrt{n\sigma^2}$

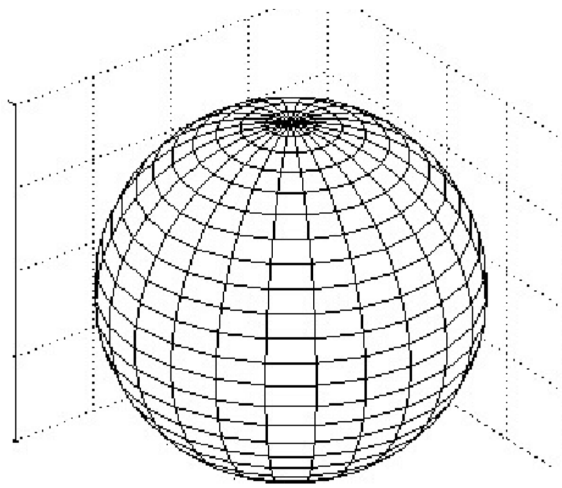
$\triangleq r_{noise}$

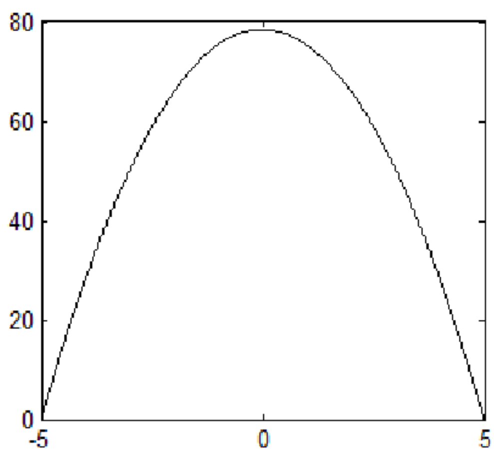
Thm. [AEP]: AWGN $\approx$ Unif$\left(B(\underline{0}, \sqrt{n\sigma^2})\right)$

"Reverse" AEP:



W.G.N. $\leftarrow$ ball



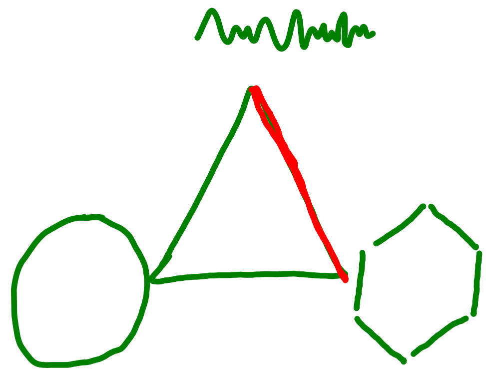


Thm. [Reverse AEP]:

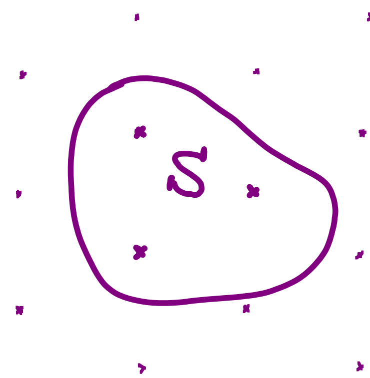
If $(Z_1, \dots, Z_n) \sim \text{Unif}\left(\text{Ball}\left(0, \sqrt{n\sigma^2}\right)\right)$,

then $Z_1 \xrightarrow{\text{dist}} N(0, \sigma^2)$ as $n \to \infty$

A Random Lattice Ensemble: Minkowski - Hlawka - Siegel



$N_\Lambda(S) \triangleq$ number of nonzero points of Λ inside a body S



Theorem: For every dimension n, there exists an ensemble $\{\Lambda\}$ of lattices with a constant point density $\boxed{\gamma = \frac{1}{V_\Lambda}}$ (= a prob. measure over all generator matrices G with determinant $1/\gamma$) such that for every bounded body S

$$E_{MHS}\{N_\Lambda(S)\} = \gamma \cdot Vol(S)$$

Just like a uniformly distributed random code!

Simultaneous Goodness

Thm. [Erez - Litsyn - Z 2004]

There exists a sequence of lattices Λ_n in dim. $n = 1, 2, \ldots$, such that as $n \to \infty$

$$\rho_{cov}(\Lambda_n) \longrightarrow 1$$

$$\underline{\lim}\ \rho_{pack}(\Lambda_n) \geq \frac{1}{2}$$

$$G(\Lambda_n) \longrightarrow \frac{1}{2\pi e}$$

$$\mu(\Lambda_n, p_e) \longrightarrow 2\pi e \qquad \forall\ p_e > 0$$

Error Exponents

[Gallager 1962]

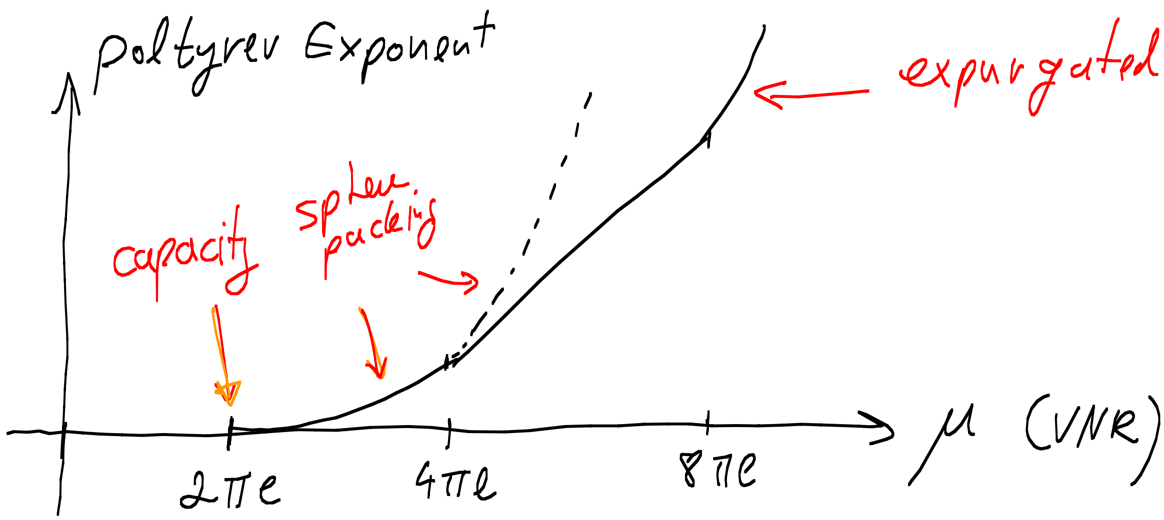
$$P_e^{ML}(\Lambda) = \int_0^\infty p(\|\underline{Z}\|=r)\cdot p\begin{pmatrix}\text{nonzero codeword}\\ \text{in Ball}(\underline{Z},r)\end{pmatrix} dr$$

$$\wedge\!\!\wedge$$

$$N_\Lambda(\text{Ball}(\underline{Z},r))$$

$$\|$$

$$E_{MHS}\{\quad\} \Longrightarrow \gamma\cdot V_n\cdot r^n$$



$$\therefore\ \exists \Lambda_n : \mu(\Lambda_n, P_e) \xrightarrow[n\to\infty]{} 2\pi e \quad \forall P_e>0$$

We'll talk about ...

1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

5. Multi-level Constructions

x^x x^x x^x

x^x x^x x^x

Construction C

* "Multi-level coded modulation"
* Natural extension (?) of construction A to L levels
* Bound on minimum distance $2 \to 2^{L-1}$
* Super-position of L binary codes : $\mathcal{C}_1, \dots, \mathcal{C}_L$

$$\Gamma = \underbrace{\mathcal{C}_1 + 2\cdot\mathcal{C}_2 + 4\cdot\mathcal{C}_3 + \dots + 2^{L-1}\cdot\mathcal{C}_L}_{\text{coded levels}} + \underbrace{2^L\cdot\mathbb{Z}^n}_{\text{uncoded levels}}$$

* Equivalent definitions:

binary expansion

$$\left\{ \underline{x} \in \mathbb{Z}^n : \; LSB(\underline{x}) \in \mathcal{C}_1, \; MSB_1(\underline{x}) \in \mathcal{C}_2, \; \dots, \; MSB_{L-1}(\underline{x}) \in \mathcal{C}_{L-1} \right\}$$

$\Longleftrightarrow$

recursive law

$$\left\{ \underline{x} \in \mathbb{Z}^n : \; \begin{array}{l} \hat{c}_1 \triangleq \underline{x} \bmod 2 \in \mathcal{C}_1 \\ \hat{c}_2 \triangleq \frac{1}{2}\cdot(\underline{x} - \hat{c}_1) \bmod 2 \in \mathcal{C}_2 \\ \hat{c}_3 \triangleq \frac{1}{4}(\underline{x} - \hat{c}_1 - 2\hat{c}_2) \bmod 2 \in \mathcal{C}_3 \\ \vdots \\ \hat{c}_L \triangleq \frac{1}{2^{L-1}}(\underline{x} - \hat{c}_1 - 2\hat{c}_2 - 4\hat{c}_3 - \dots) \bmod 2 \in \mathcal{C}_L \end{array} \right\}$$

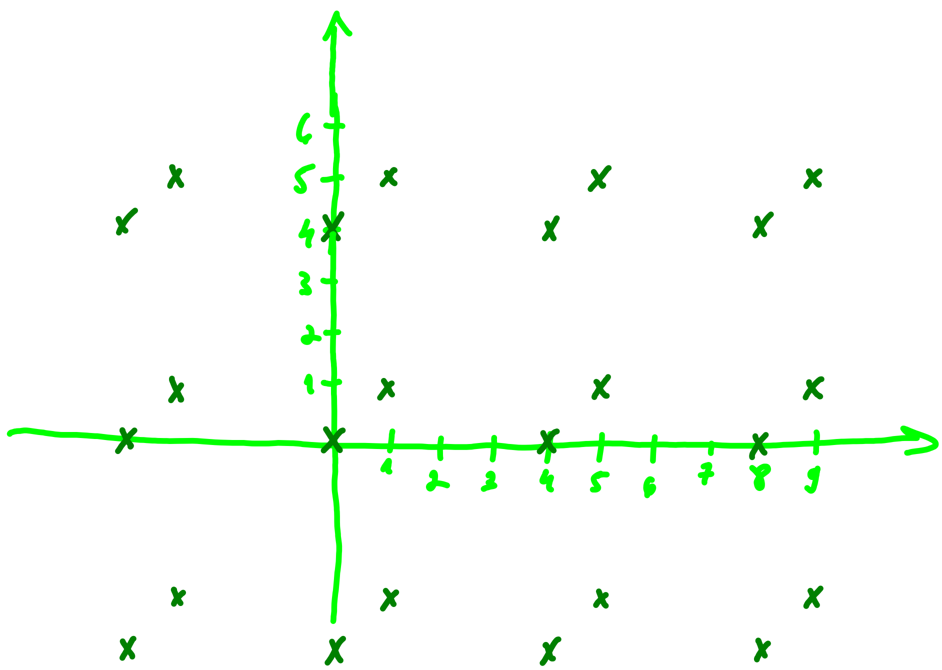
Construction C : general context

* Single level ($L=1$) $\Rightarrow$ Construction A
* Multiple levels ($L>1$) $\Rightarrow$ not necessarily a lattice even if all component codes are linear !

$C_1 = \{(00), (11)\}$

$C_2 = \{(00)\}$

$\Gamma = C_1 + 2C_2 + 4\cdot\mathbb{Z}^2$



* Multi-level coset codes [Forney - Trott - Chang 2000] :

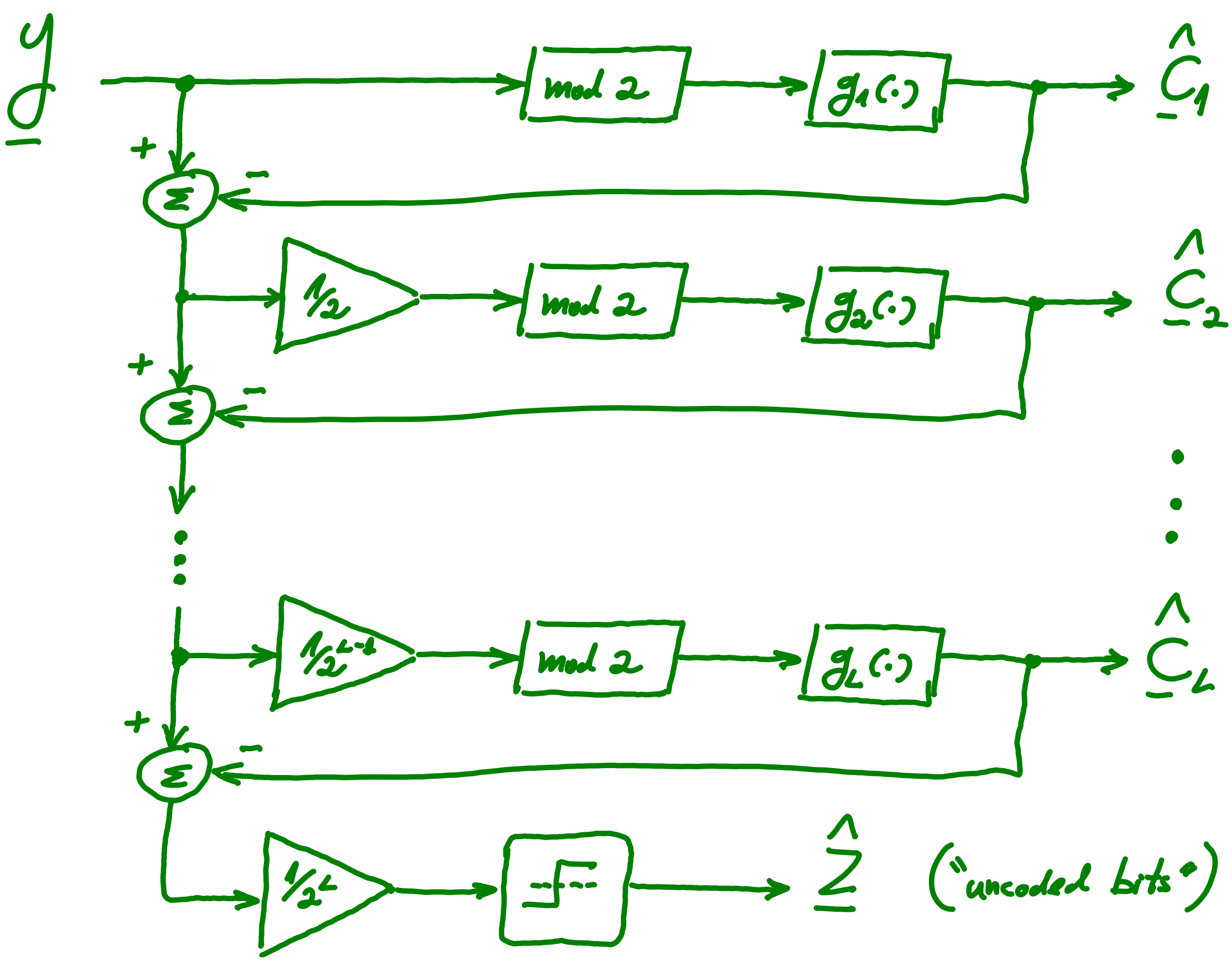
Special case where

$$\Lambda_1/\Lambda_2/\dots/\Lambda_L = \mathbb{Z}/2\mathbb{Z}/\dots/2^{L-1}\mathbb{Z}$$

Multi-Stage Decoding

$$\underline{Y} = \underline{X} + \underline{N} \quad , \quad \underline{X} \in \Gamma$$

Let $g_i(\cdot)$ = "soft-decision" decoder for $\underline{c} \in C_i$ in a modulo-2 channel: $\underline{\tilde{y}} = \left[\underline{c} + \underline{N}/2^{i-1}\right] \bmod 2$.



Construction D

* Multi-level lattice construction
* Natural extension (?) of construction A (Def. IV)
* Similar to (non-lattice) construction C
  (same d_{min}, allows MSD)
* Based on a chain of nested linear binary codes:

  $\mathcal{C}_1 \subset \cdots \subset \mathcal{C}_L$, where $\mathcal{C}_j = (n, k_j, d_j)$ code, $k_1 \le \cdots \le k_L$
* Super-position of basis vectors (rather than of the codes)
* Let $\underline{g}_1 \ldots \underline{g}_n$ be a basis for $\{0,1\}^n$, such that the $k_j \times n$ matrix $\underline{\underline{G}}_j = \begin{bmatrix} - \underline{g}_1 - \\ \vdots \\ - \underline{g}_{k_j} - \end{bmatrix}$ is a generator matrix for $\mathcal{C}_j$, $j = 1 \ldots L$.

real (not modulo 2) multiplication

$$\Lambda_D = \left\{ \underbrace{\sum_{j=1}^{L} \overbrace{2^{j-1} \cdot \underline{w}_j \cdot \underline{\underline{G}}_j}^{\text{real (not modulo 2) multiplication}}}_{} + 2^L \cdot \underline{z} : \quad \underset{j=1\ldots L}{\underline{w}_j \in \{0,1\}^{k_j}}, \ \underline{z} \in \mathbb{Z}^n \right\}$$

code nesting $\Rightarrow$ closed under mod-2^L addition $\Rightarrow$ Λ_D is a lattice

Uniformity Properties of Construction C

Maiara Bollauf & RZ

* ISIT 2016 *

Classification of "almost"-lattice codes

(infinite constellations)

Lattice Λ

$\downarrow$

Geometrically Uniform

$\downarrow$

Equi-Distance Spectrum

$\downarrow$

Equi-Minimum distance

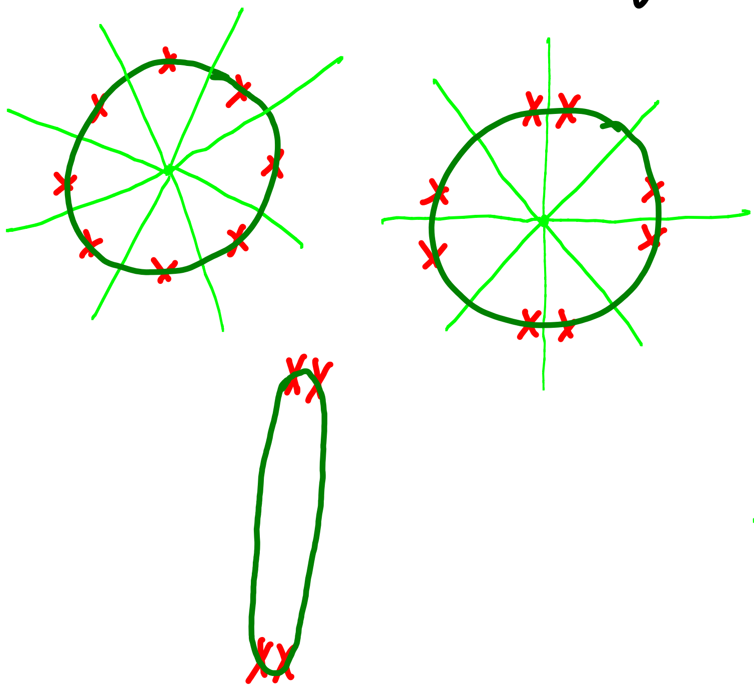
(& Equi-kissing number)

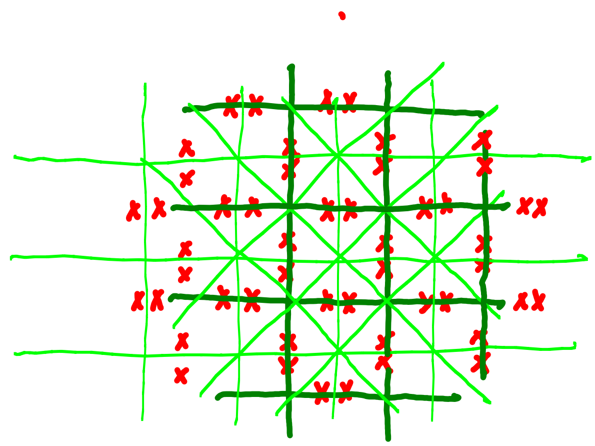
$\vdots$

Random, $n \to \infty$

Reminder: Geometrically Uniform Constellation

[Forney 1991]





Definition: Γ is GU if for any two codewords $c, c' \in \Gamma$, there exists a distance-preserving transformation T (translation, reflection, rotation) such that

$$c' = T(c) \quad \text{and} \quad T(\Gamma) = \Gamma.$$

$\Rightarrow$ The world seen by any codeword is the same, up to rotation and reflection.

$\Rightarrow$ Same Voronoi cells (Euclidean distance)
Same $p_e(c)$ (under AWGN).

Assume that $\mathcal{C}_1, \ldots, \mathcal{C}_L$ are linear,

then ...

Construction $\mathcal{C}$ is always geometrically uniform

for $L \leq 2$

Construction $\mathcal{C}$ is not always geometrically uniform

for $L \geq 3$

We'll talk about ...

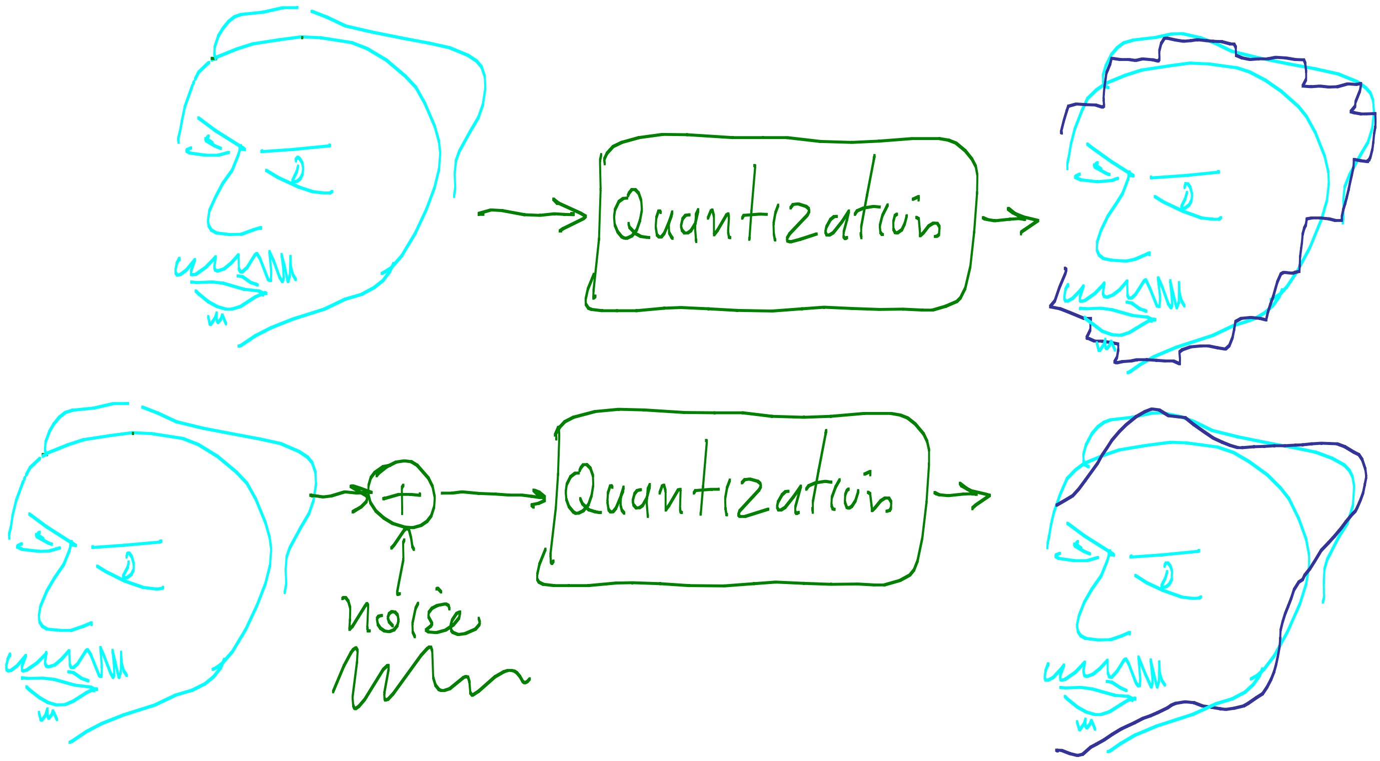
1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

6. Dither & estimation

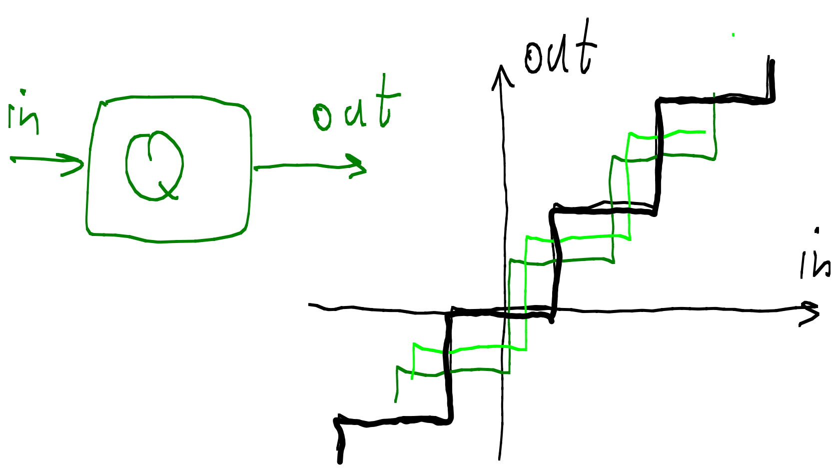
noise (Λ)

Dithered Quantization

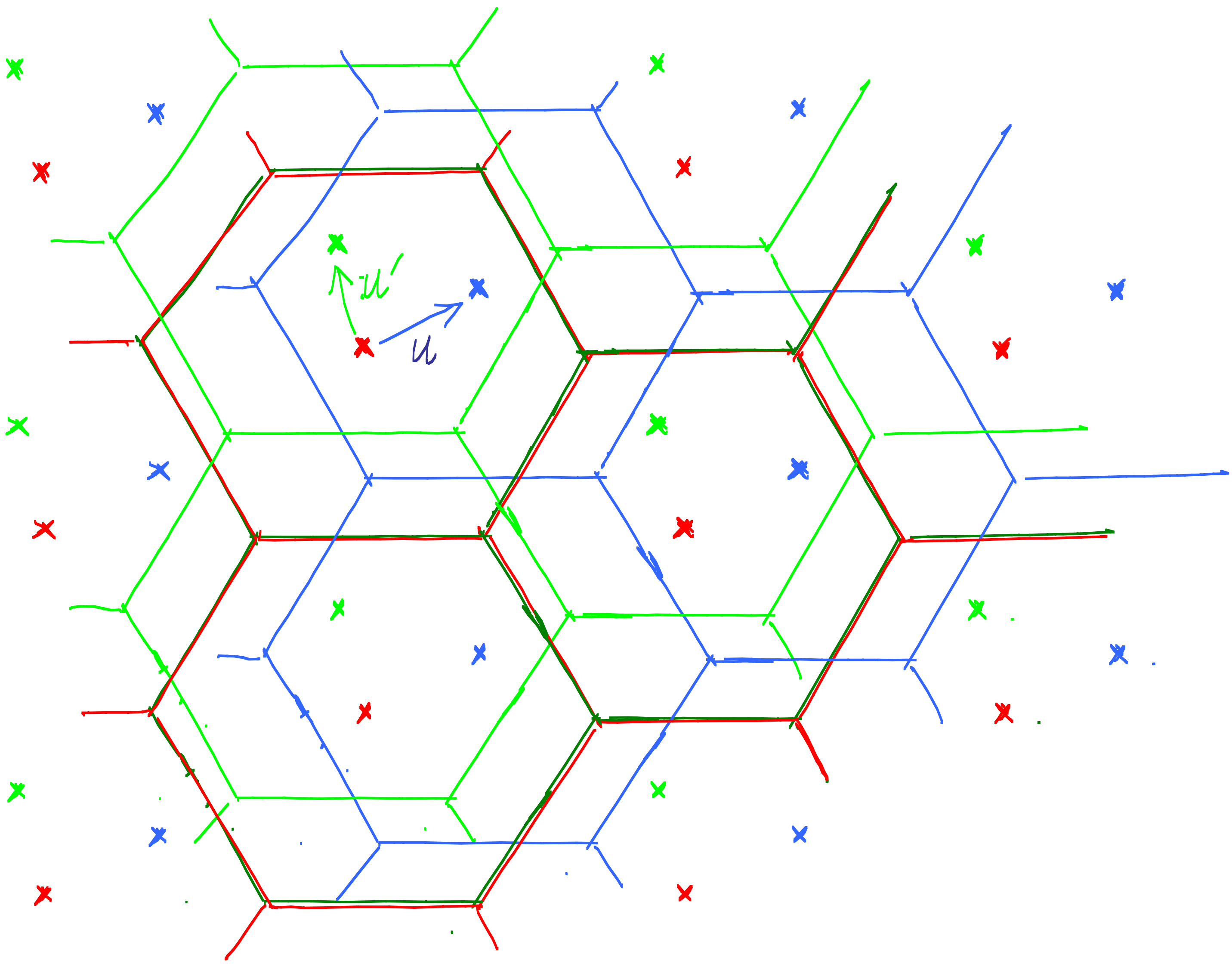
- dither for perceptual reasons:



- dither for analytical reasons:



$$Q_\Lambda(x+u)-u$$



$\Longrightarrow$ Random shift of the lattice quantizer

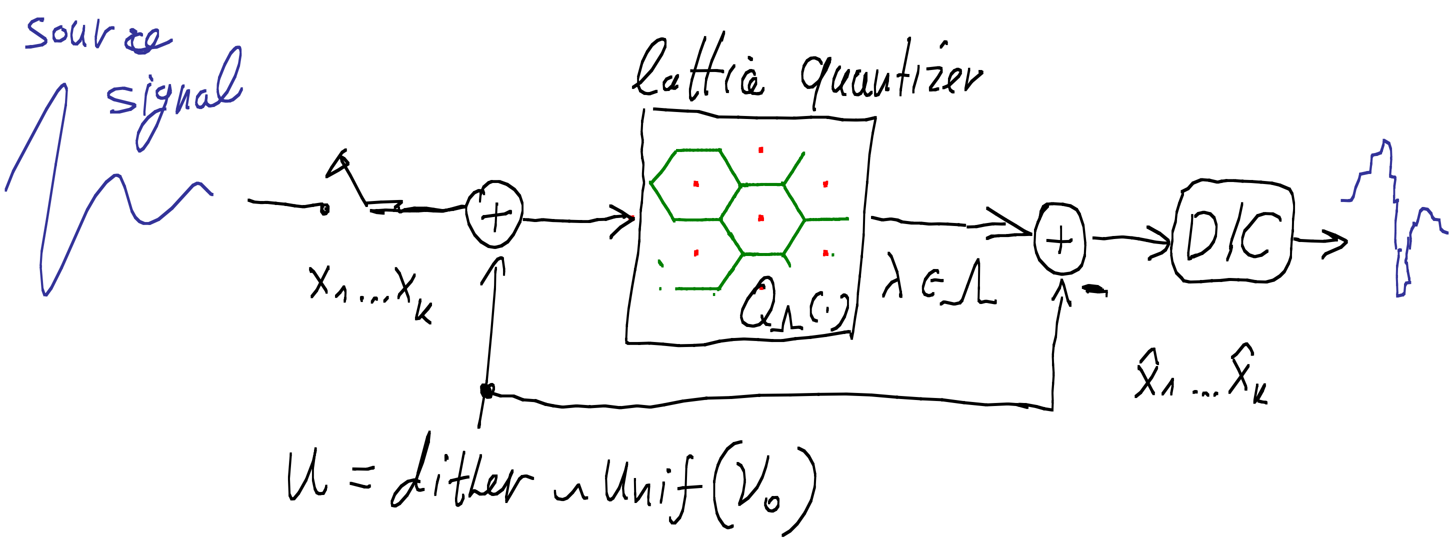
The Crypto-Lemma

Let $\boxed{x \bmod \Lambda \triangleq x - Q_\Lambda(x)}$

$$\boxed{\text{If } U \sim \text{unif}(\mathcal{P}_0), \text{ then } (x+U) \bmod \Lambda \sim \text{unif}(\mathcal{P}_0), \ \forall x}$$

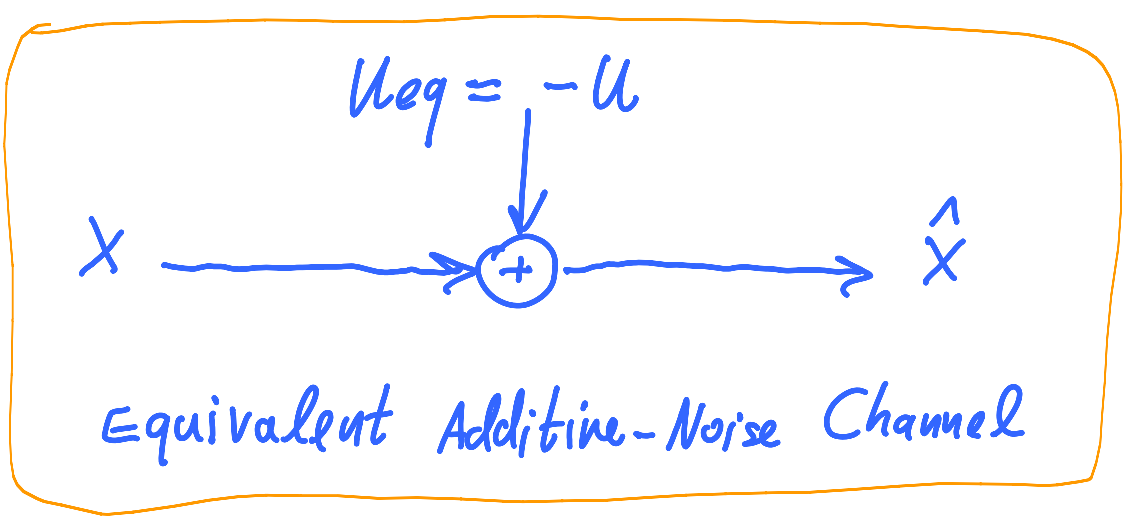
Proof: View as a modulo-additive noise channel, with a uniform noise.

Dithered Quantization Error



Crypto Lemma ⇒

Thm. 1: quantization error $Q(x+U) - x - U$ is independent of input x, and uniform over (reflection of) lattice cell:



Generalized Dither

Def. $\mathcal{U}$ is G.D. if $\boxed{(s+\mathcal{U}) \bmod \Lambda \sim \text{Unif}(\mathcal{P}_0)}$ $\forall s$

Necessary condition on $f_{\mathcal{U}}(\cdot)$ for G.D. ?

Generalized Dither

Def. $\mathcal{U}$ is G.D. if $\boxed{(s+\mathcal{U}) \bmod \Lambda \sim \mathrm{Unif}(\mathcal{P}_0)}$ $\forall s$

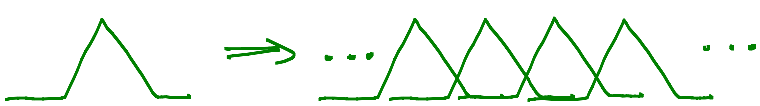
Necessary condition for G.D. ?

1. $\mathcal{U}$ is G.D. iff $\mathcal{U} \bmod \Lambda \sim \mathrm{Unif}(\mathcal{P}_0)$

2. $\mathcal{U}$ is G.D. iff $f_{\mathcal{U}_{rep}}(x) = \text{constant}$

   where,

   $f_{rep}(x) \triangleq$ periodic replication $f(x) \triangleq \sum_{\lambda \in \Lambda} f(x-\lambda)$



3. $\mathcal{U}$ is G.D. iff its characteristic function is zero on the dual lattice:

$$\mathcal{F}\{f_{\mathcal{U}}(\cdot)\} = 0 \quad \text{on } \Lambda^* \setminus \underline{0}$$

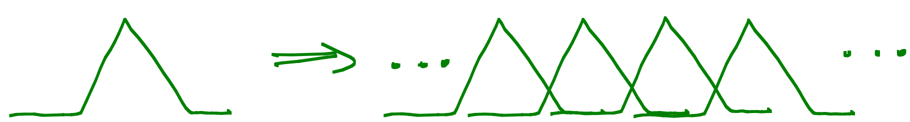
where $\Lambda^* =$ dual lattice $= \Lambda(G^{-t})$

Generalized Dither

Def. $\mathcal{U}$ is G.D. if $\boxed{(s+\mathcal{U}) \bmod \Lambda \sim \mathrm{Unif}(\mathcal{P}_0)}$ $\forall s$

Necessary condition for G.D.?

$f_{rep}(x) \triangleq$ periodic replication $f(x) \triangleq \sum_{\lambda\in\Lambda} f(x-\lambda)$



Claims

1. $f_{rep}(x)$ is periodic-Λ in space
2. If $X \sim f(x)$, and $\mathcal{P}_0$ = fundmental cell of Λ, then

$$f_{X \bmod \Lambda}(x) = \begin{cases} f_{rep}(x), & x \in \mathcal{P}_0 \\ 0, & o.w. \end{cases}$$

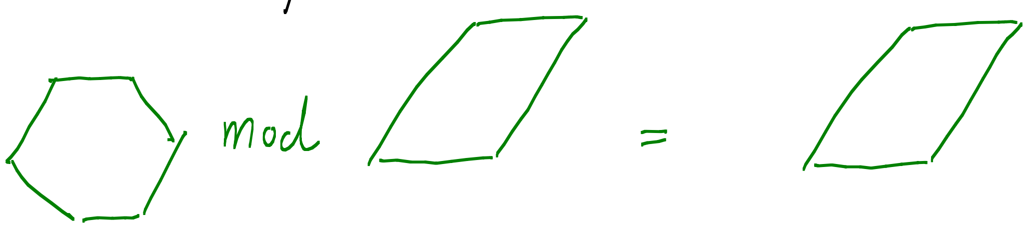
3. $X \bmod \Lambda \sim \mathrm{Unif}(\mathcal{P}_0)$ iff $f_{rep}(x) = \text{constant}$
4. $\mathcal{U}$ is generalized dither iff $f_{\mathcal{U}rep}(x) = \text{constant}$

Generalized Dither: Examples

1. Uniform over <u>any</u> fundamental cell

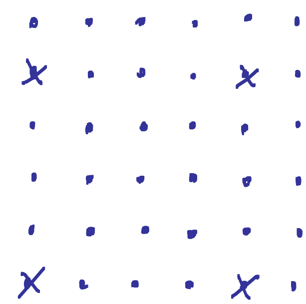
$$Unif(Q_0) \bmod_{P_0} \Lambda \sim Unif(P_0)$$

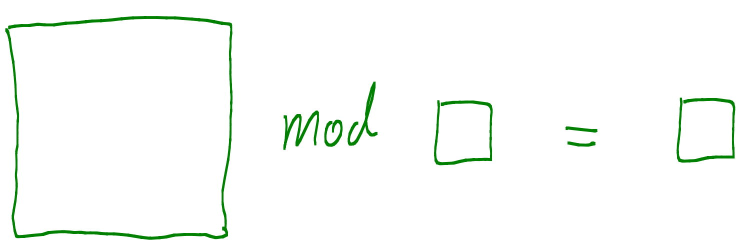
where Q_0, P_0 = fundamental cells of Λ.



2. Uniform over a <u>nested</u> coarse lattice cell

Q_0 = fundamental cell of $\Lambda_c \subset \Lambda$





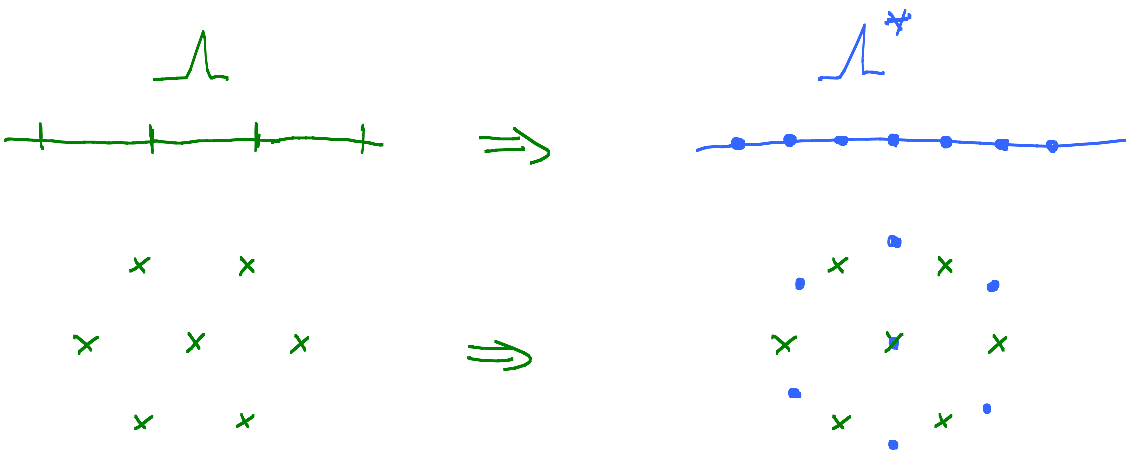
3. Spreading

$$\{f_U(\cdot)\}_{rep} = \text{constant} \Rightarrow \{f_U(\cdot) * \tilde{f}(\cdot)\}_{rep} = \text{constant}$$

Generalized Dither $\Rightarrow$ Zeroes on Dual Lattice

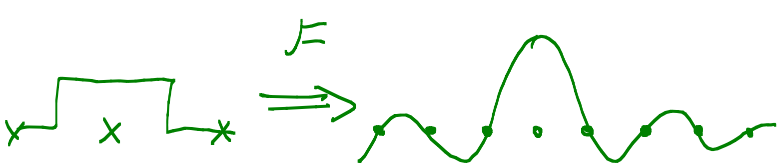
Def. $\Lambda^* = \text{dual lattice of } \Lambda(G)$

$$= \Lambda(G^{-t})$$



Claim: U is G.D. *iff* its characteristic function is zero on the dual lattice:

$$\mathcal{F}\{f_U(\cdot)\} = 0 \quad \text{on } \Lambda^* \setminus \underline{0}$$



Good lattice $\Rightarrow$ white dither

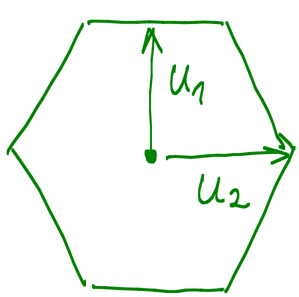
$\underline{\underline{R}}_Q \triangleq$ dither auto-correlation matrix $= E\{\underline{U} \cdot \underline{U}^t\}$

$M_U \triangleq \frac{1}{n} \text{trace}\{\underline{R}_Q\} \geq \sigma^2(\Lambda)$

equality if Voronoi cells

Thm.: If Λ is an optimal lattice quantizer in $\mathbb{R}^n$ (minimizes N.S.M. $G(\Lambda)$), then $\underline{U}$ is white:

$$\underline{R}_Q = \sigma^2(\Lambda) \cdot \underline{\underline{I}}_n$$



U_1 and U_2 are dependent

but $Var(U_1) = Var(U_2)$

$E\{U_1 \cdot U_2\} = 0$

Proof:

1. $\Lambda, V_0 \longrightarrow$ whitenning (orthonormal) transformation $\longrightarrow \Lambda', P_0'$

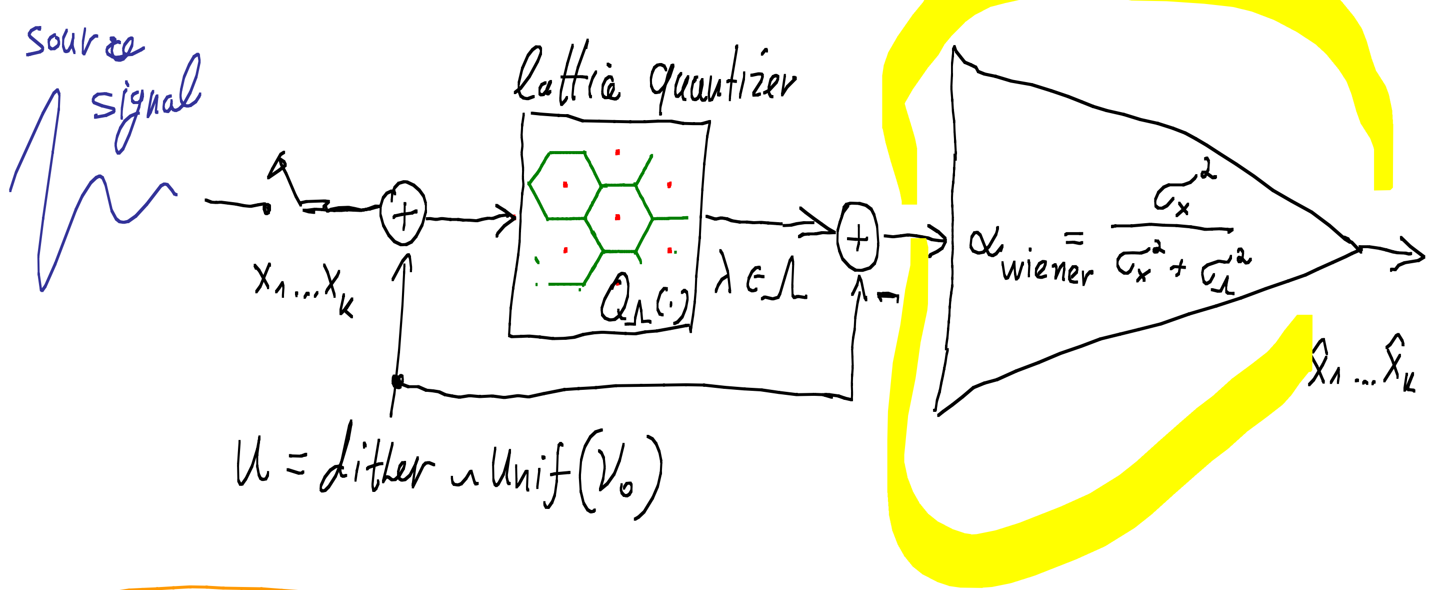
2. $\Lambda', P_0' \longrightarrow$ Voronoi Partition $\longrightarrow \Lambda', V_0'$

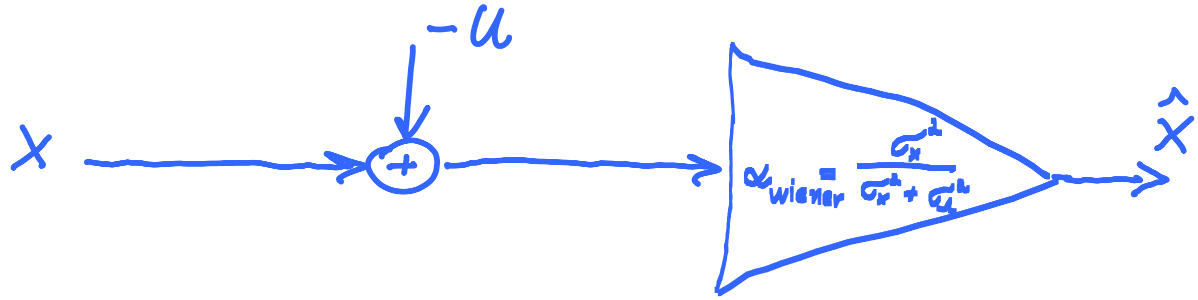
and repeat ...

$\Rightarrow \quad G(\Lambda) \geq G(\Lambda') \geq G(\Lambda'') \geq \ldots$

w. equality iff Λ is white !

Wiener Estimation





Equivalent Additive-Noise Wiener-Estimated Channel

$\Rightarrow$ distortion : $\sigma_\Lambda^2 \longrightarrow \dfrac{\sigma_x^2\,\sigma_\Lambda^2}{\sigma_x^2 + \sigma_\Lambda^2}$

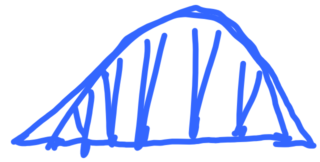
We'll talk about ...

1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

7. Side-information problems

Modulo (Λ)

Why Lattices in Communication?

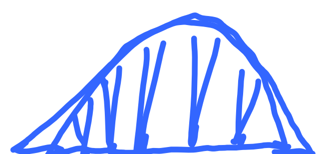


1. a bridge from $n=1$ to $n=\infty$

   = non-asymptotic analysis per dimension

2. Algebraic (low complexity) Binning

   = structured coding schemes for networks



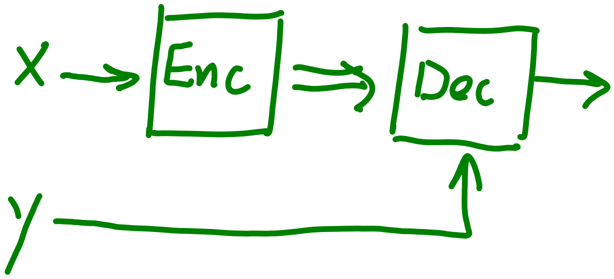
3. bridge from Analog-to-Digital

   = Robust joint source-channel coding

4. Better than Random-Coding!

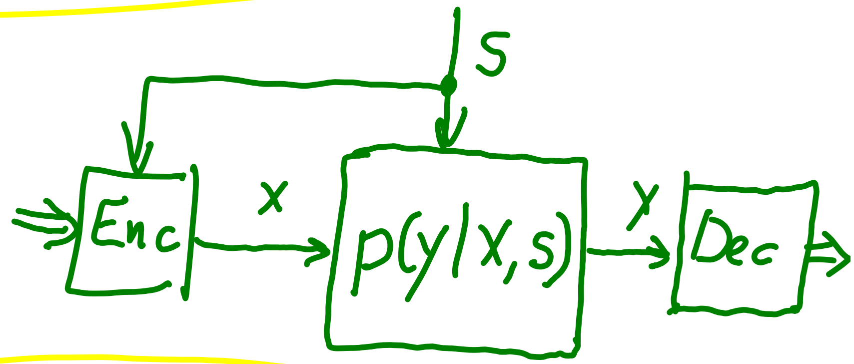
   in distributed side-information problems

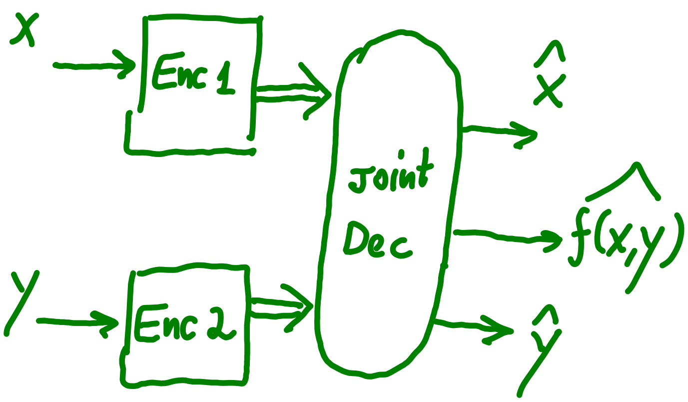
Lattices in Multi-Terminal Problems



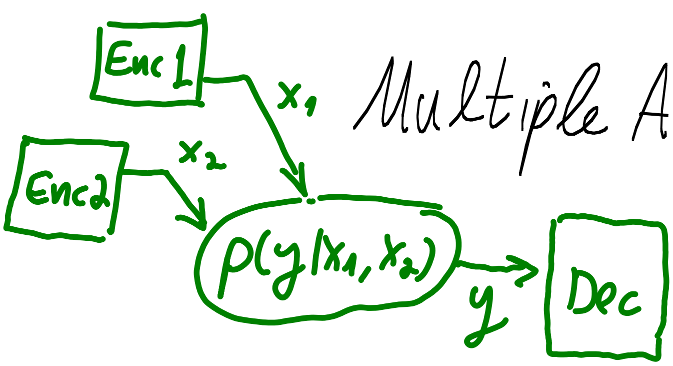
Source coding with Side Information

Channel Coding with Side Information

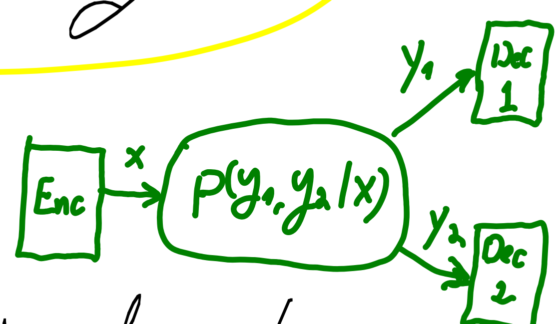




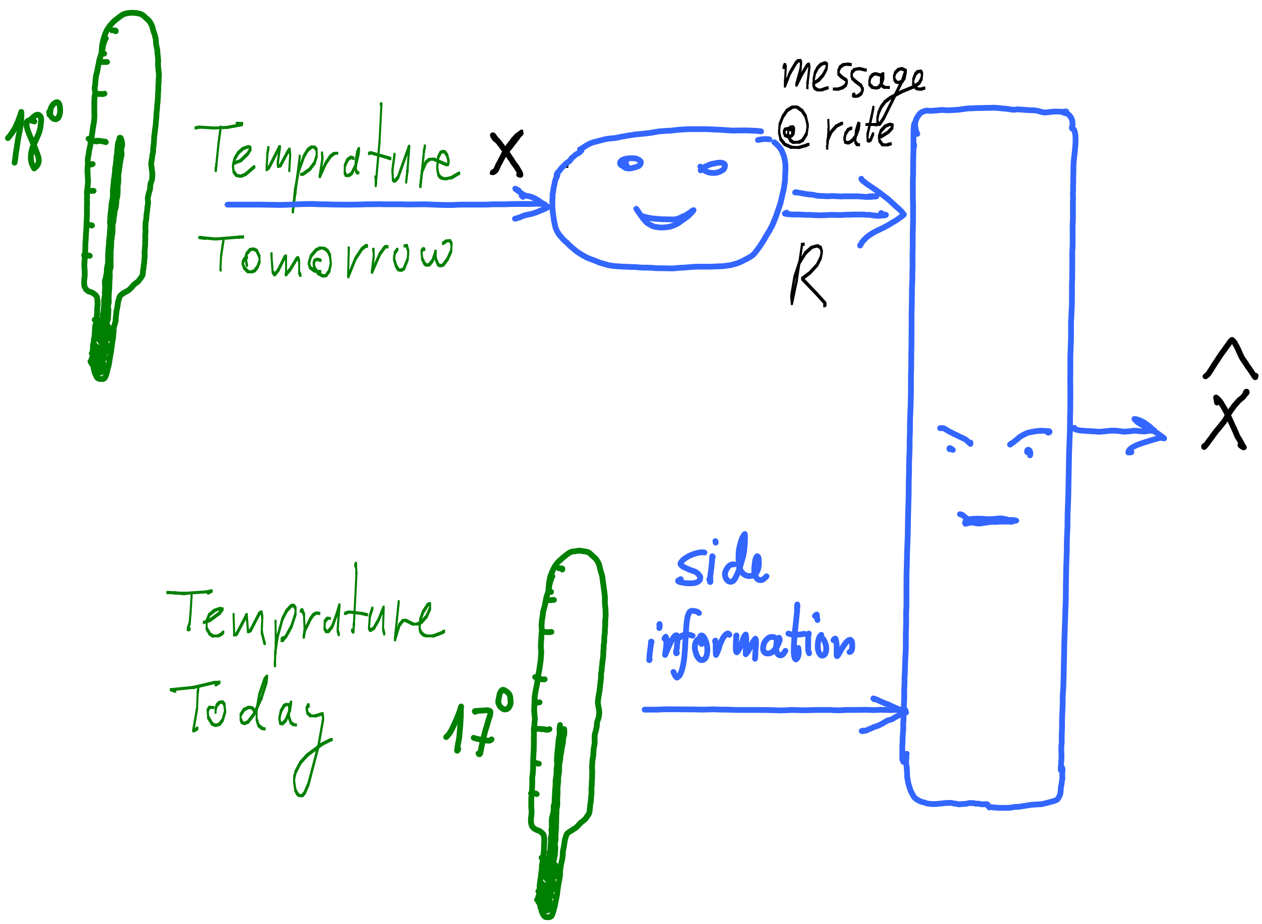
Multi-terminal Source coding



Multiple Access & Broadcast Channels



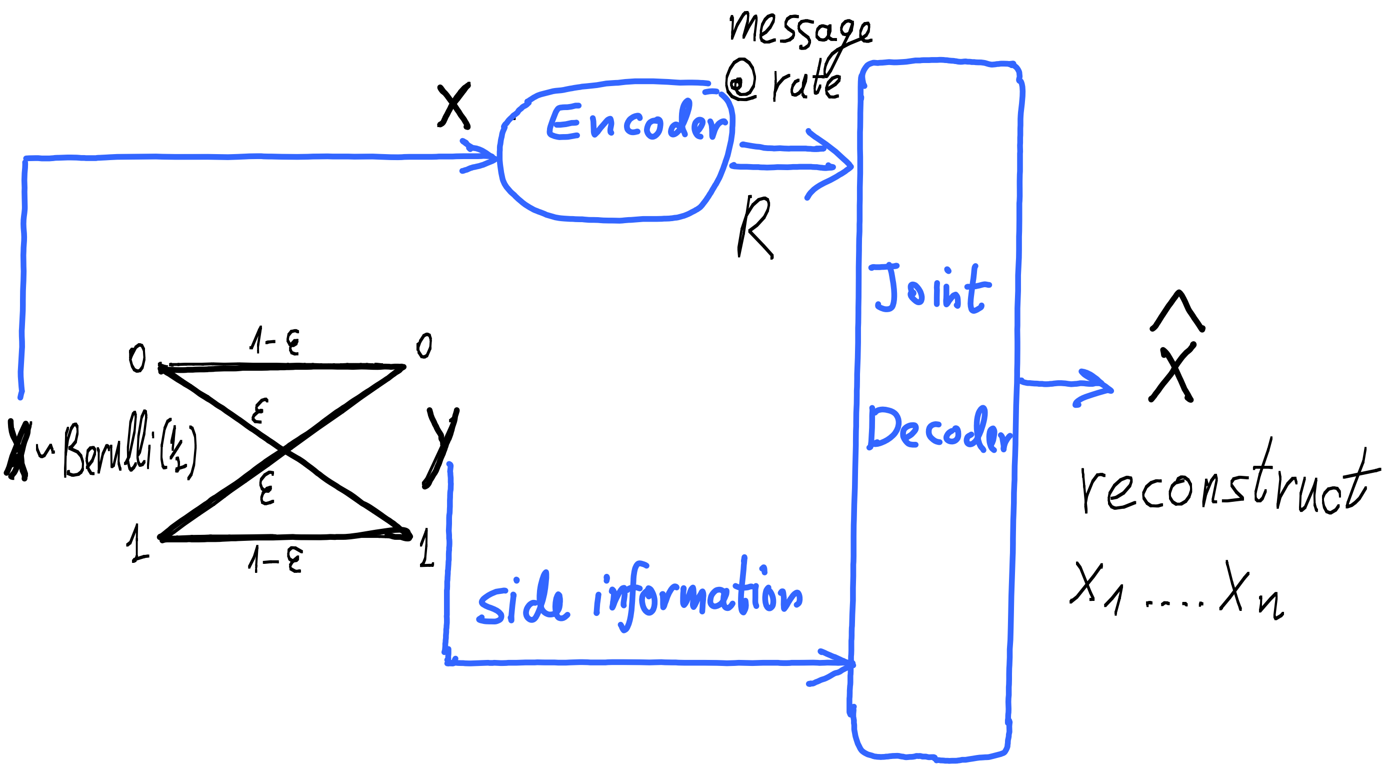
The Slepian-Wolf Problem



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

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

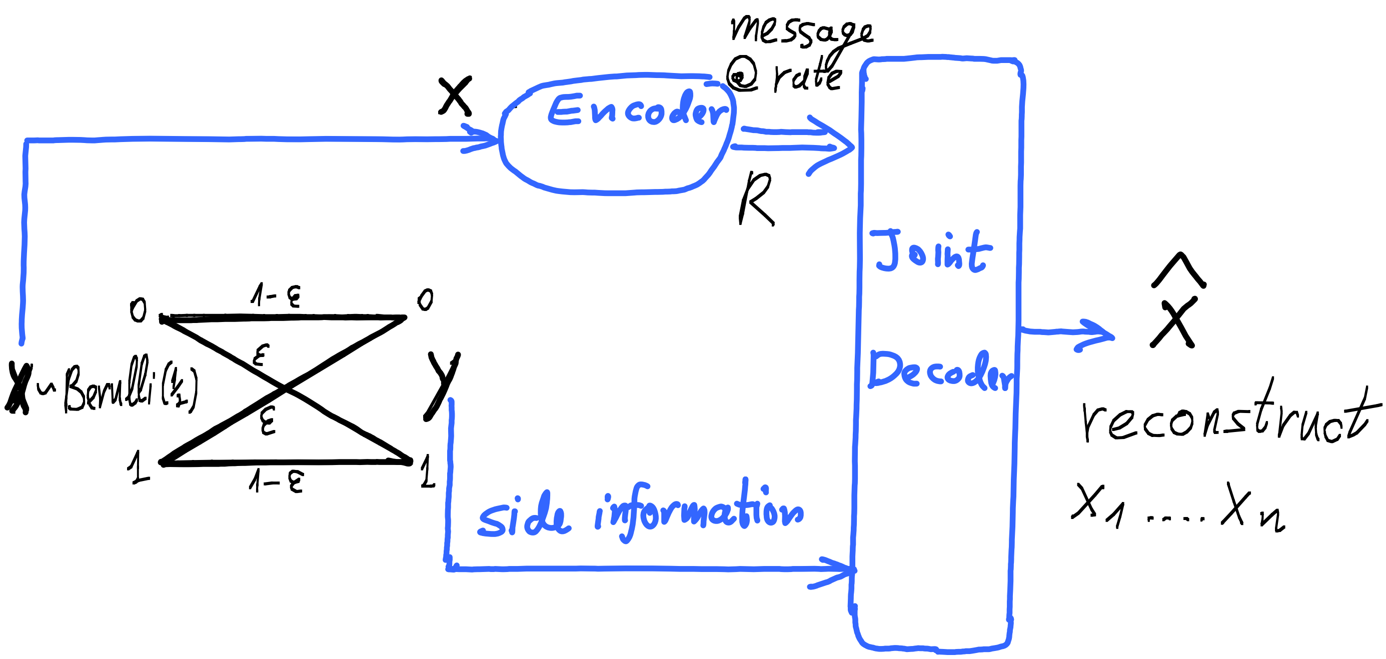
The Slepian-Wolf Problem



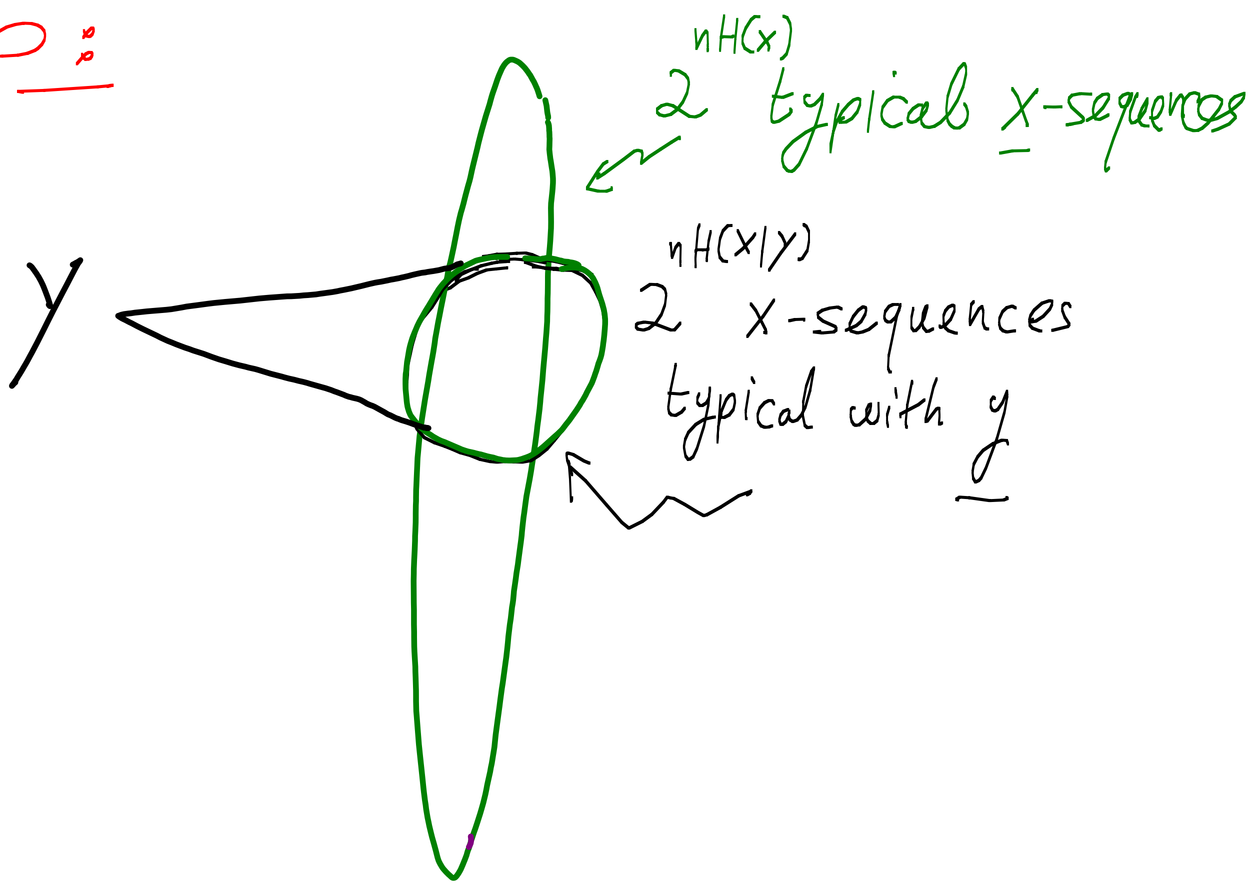
$$R = H(X|Y) = H(Z) = H_B(\varepsilon) = 0.1 \text{ Bit}$$

as if Y were available @ both encoder + decoder!

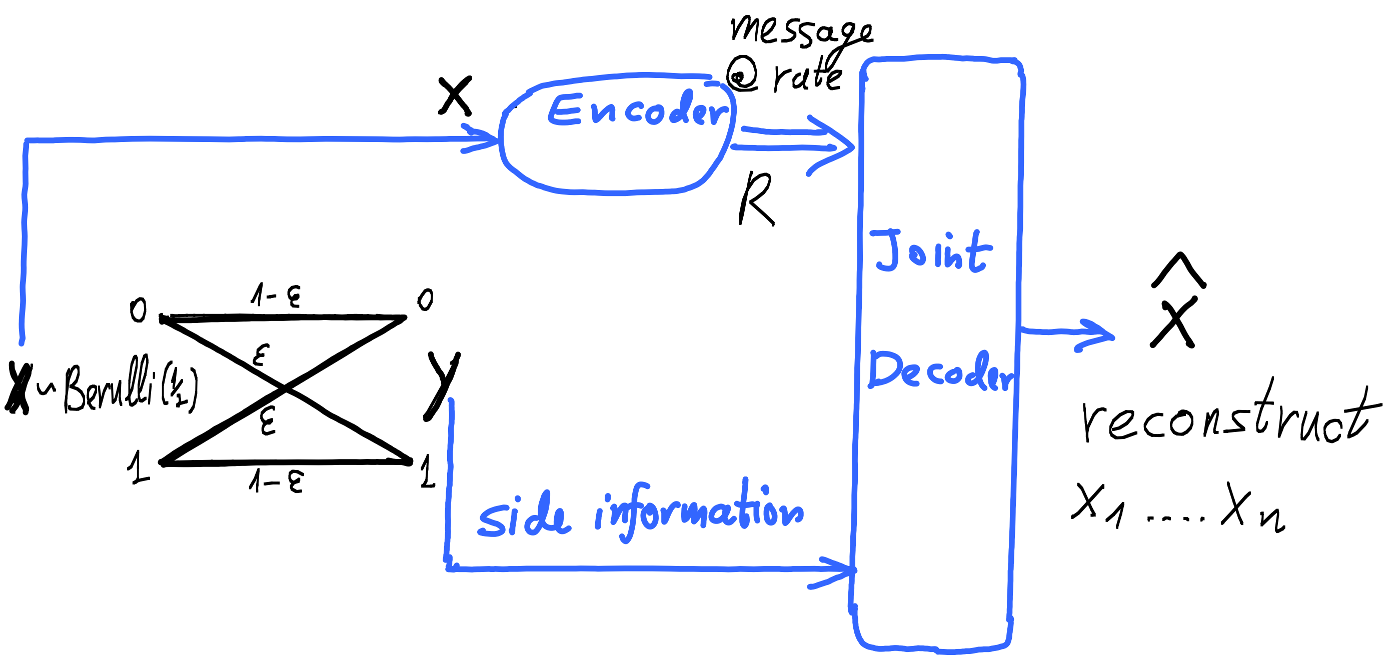
The SW Problem: Random Binning

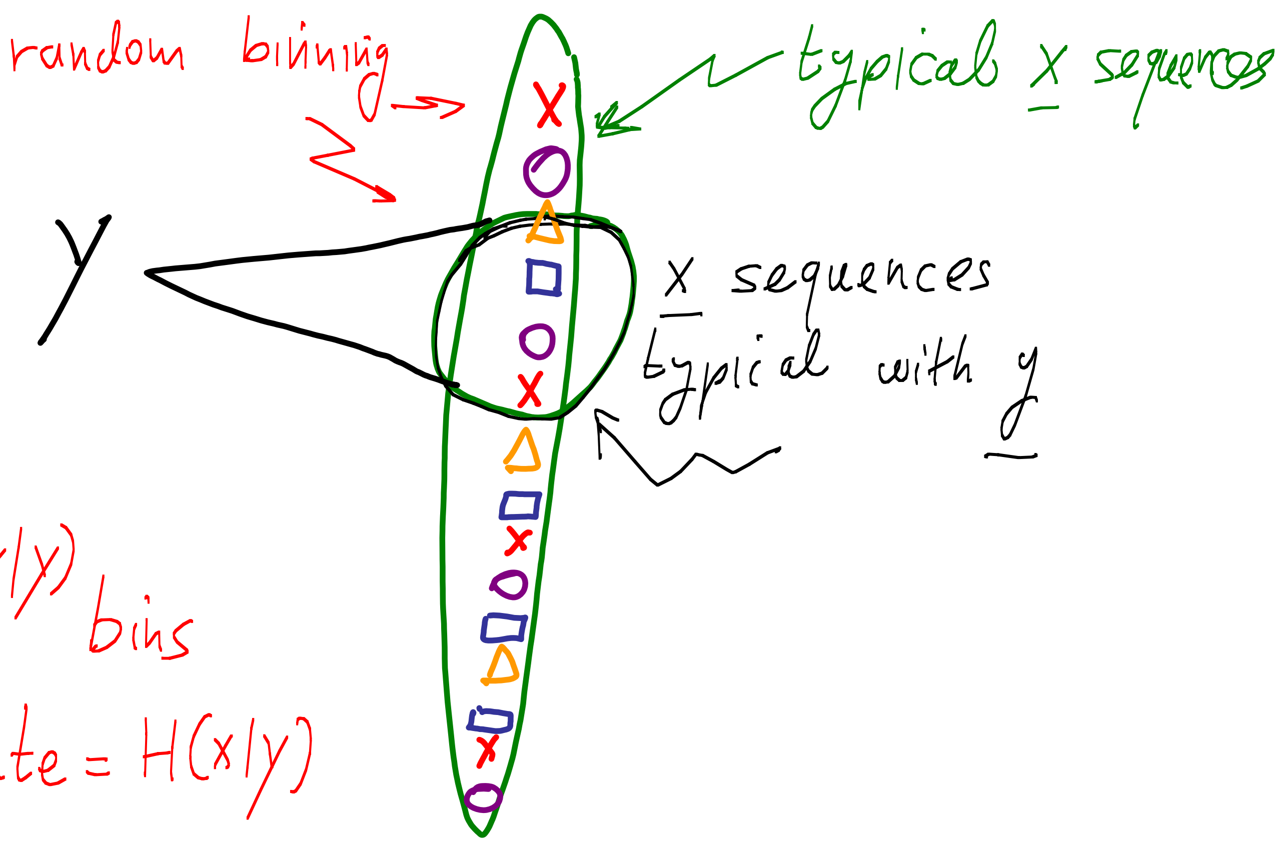


AEP:



The SW Problem: Random Binning





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

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

From "random"
back to "Structure"...

(i) Hamming space ⟸

(ii) Euclidean space

Syndrome Coding

1. Good linear binary codes:

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

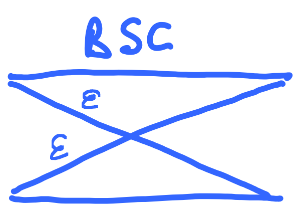
general properties:

generator matrix

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

parity-check

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

$\underline{x}$ 

$\underline{y} = \underline{x} \oplus \underline{z}$, $\underline{z} \sim \text{Bernoulli}(\varepsilon)$

$$\text{Syndrome} = \underline{\underline{H}} \cdot \underline{y} \quad (n-k \text{ dimensional})$$

$$\hat{\underline{z}}_{M.L.} = \text{error}(\underline{y}, \mathbb{C}) = f(\underline{\underline{H}} \cdot \underline{y}) \triangleq \underline{y} \bmod \mathbb{C}$$

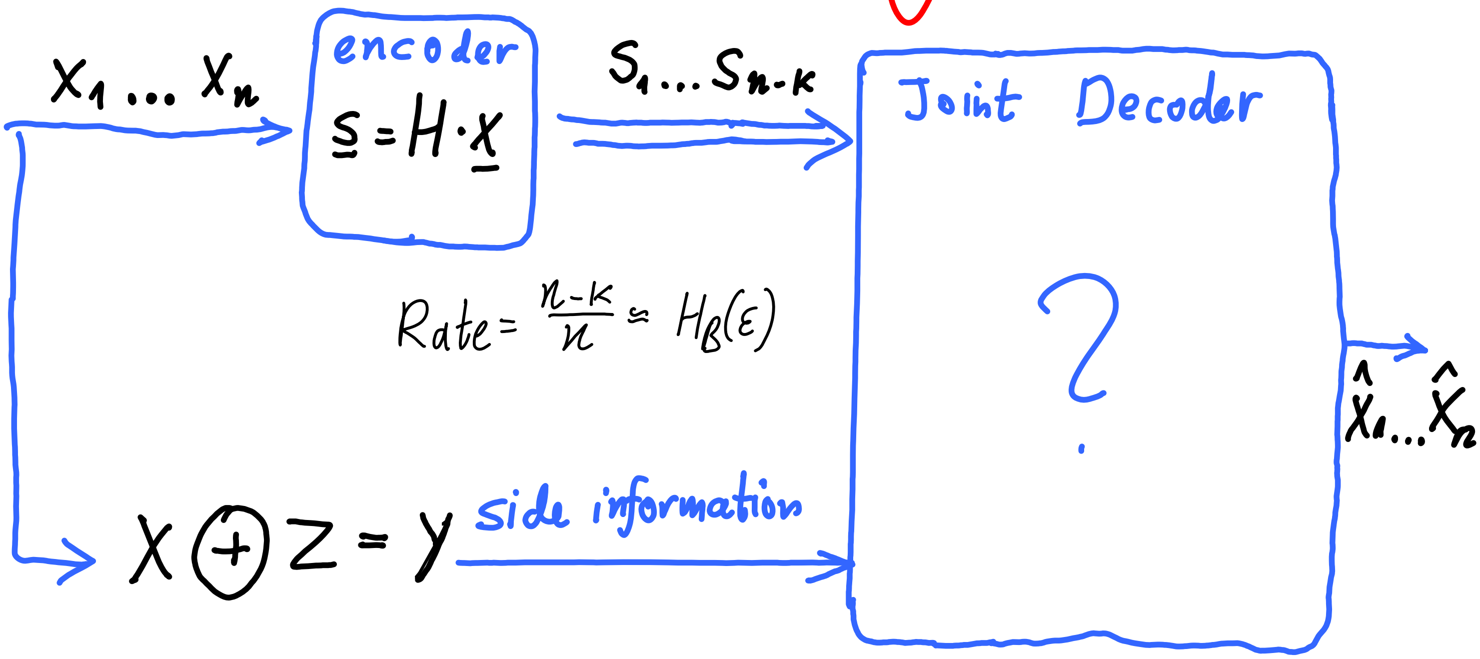
$$P_e = \Pr\{\hat{\underline{z}}_{ML} \neq \underline{z}\} \longrightarrow 0$$

for "good" codes

$n \to \infty$ @ $\frac{k}{n} \approx 1 - H_B(\varepsilon)$

Syndrome Coding

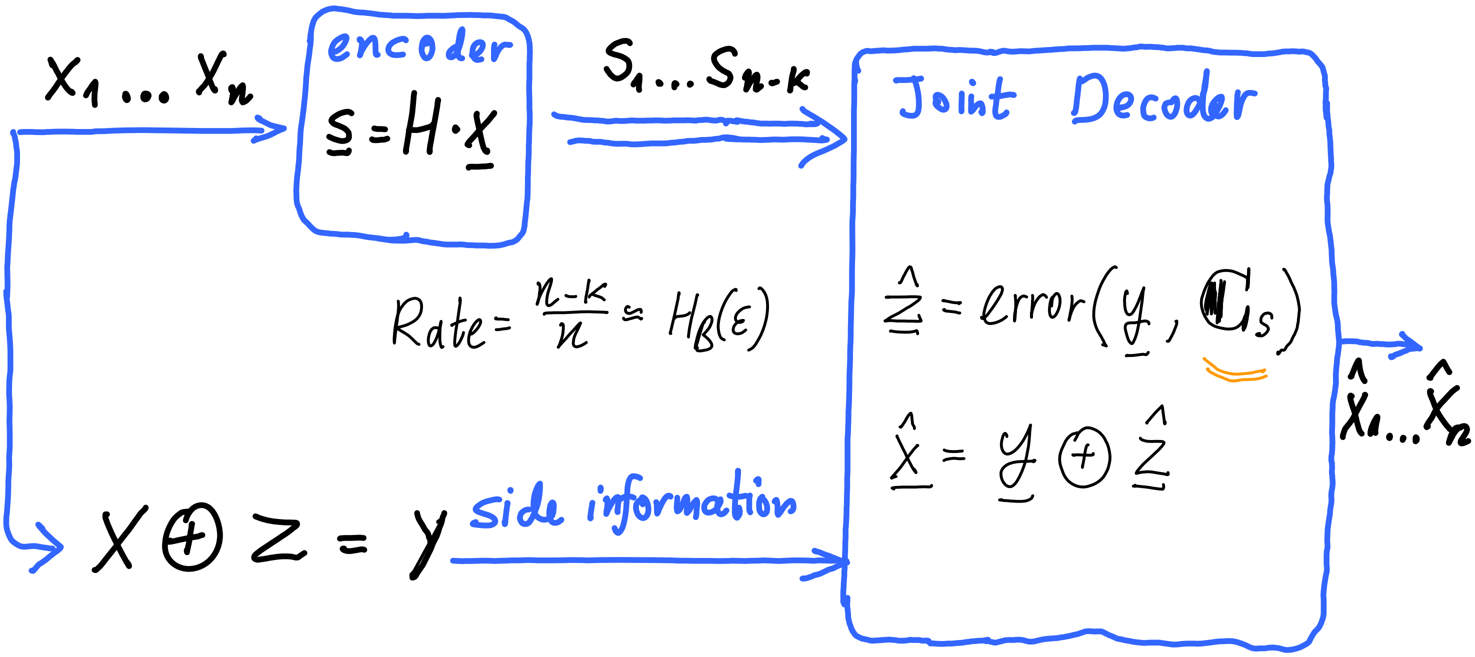
2. -"- -"- for binary Slepian-Wolf:



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

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

Syndrome Coding



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

Equivalent scheme

- **encoder:** $\quad \text{message} = \underline{s} \iff \underline{x} \bmod \mathcal{C}$

- **decoder:** $\quad \hat{\underline{z}} = \left[(\underline{x} \bmod \mathcal{C}) \oplus \underline{y} \right] \bmod \mathcal{C}$

distributive law

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

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

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

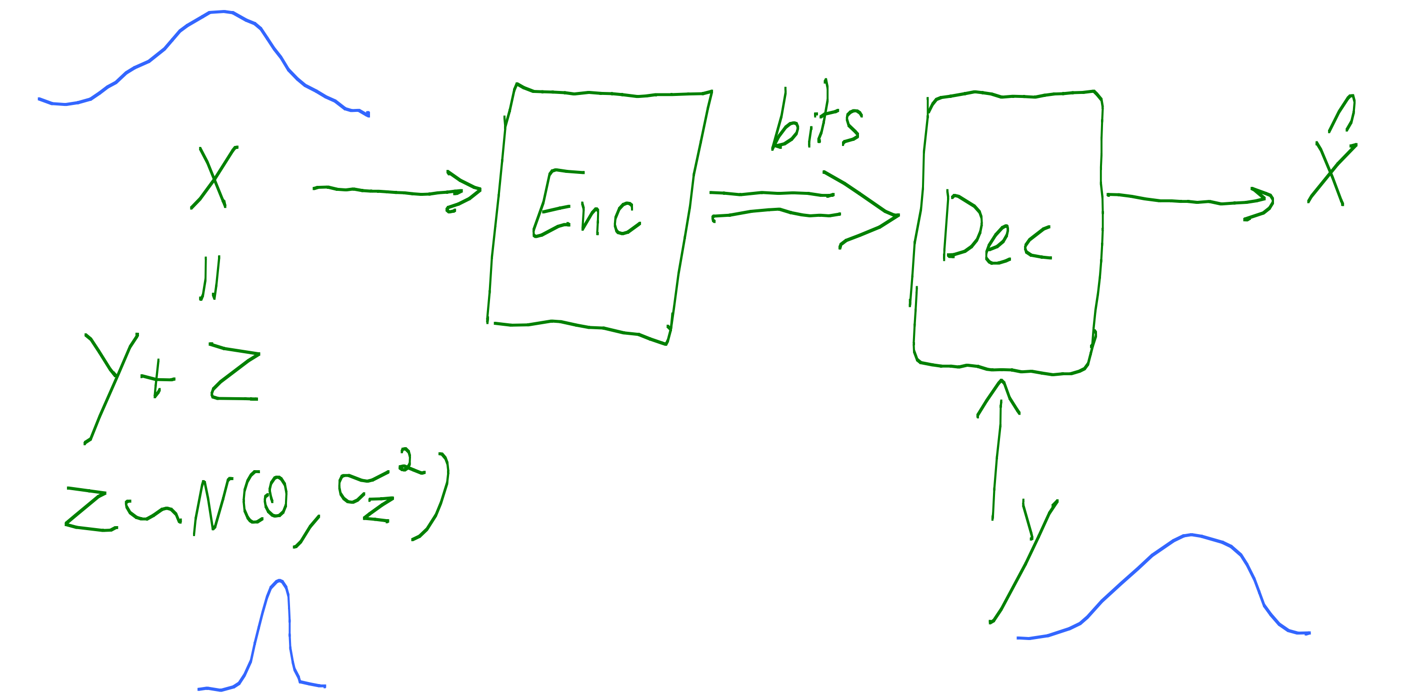
From "random" back to "Structure"...

(i) Hamming space

(ii) Euclidean space ⇐

The Wyner - Ziv Problem

(Lossy source coding with S.I. @ Decoder)



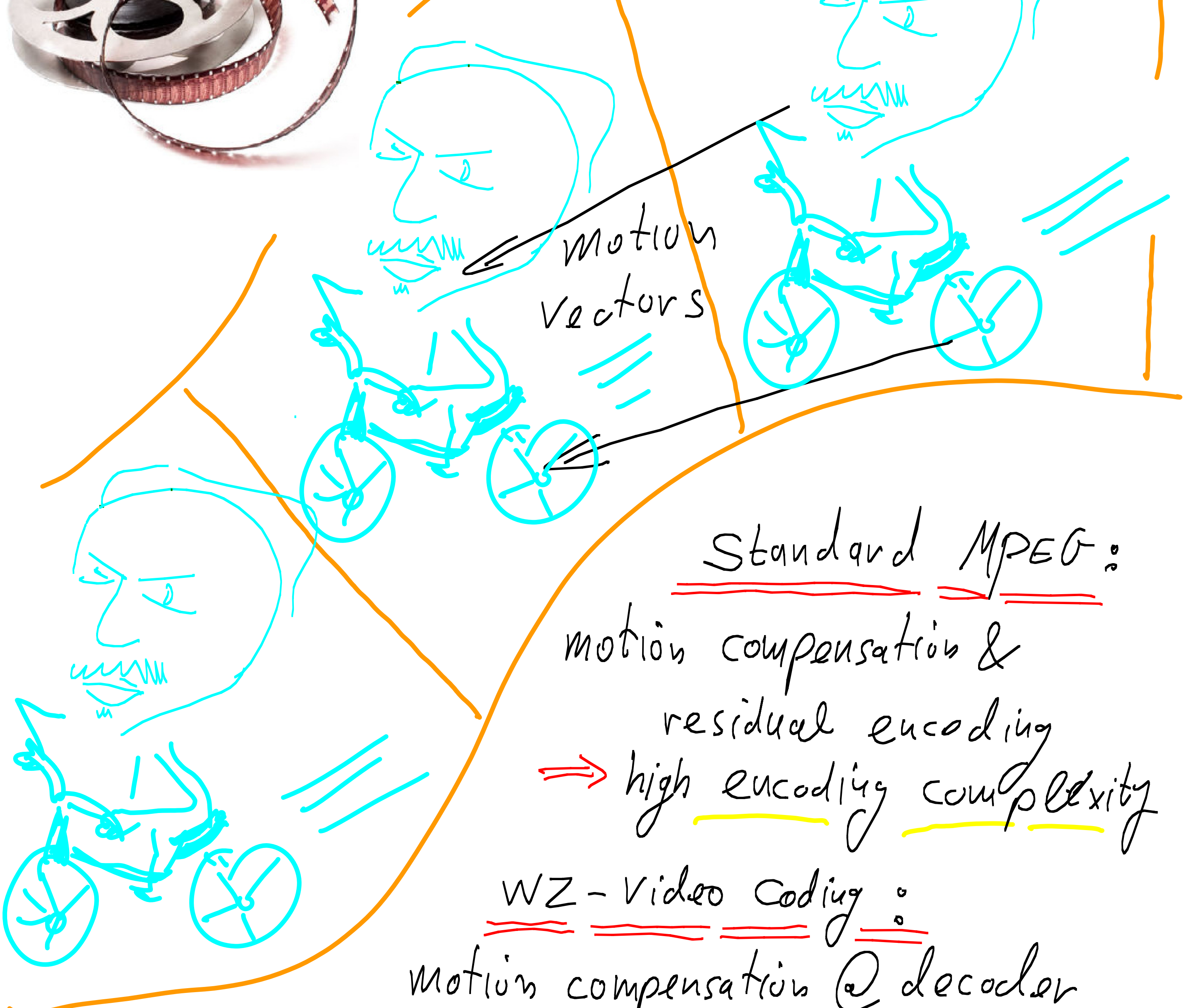
* The information - theoretic limit:

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

Wyner-Ziv 1976

Wyner 1978

Wyner-Ziv Video Coding



Standard MPEG:

motion compensation &
residual encoding

⇒ high encoding complexity

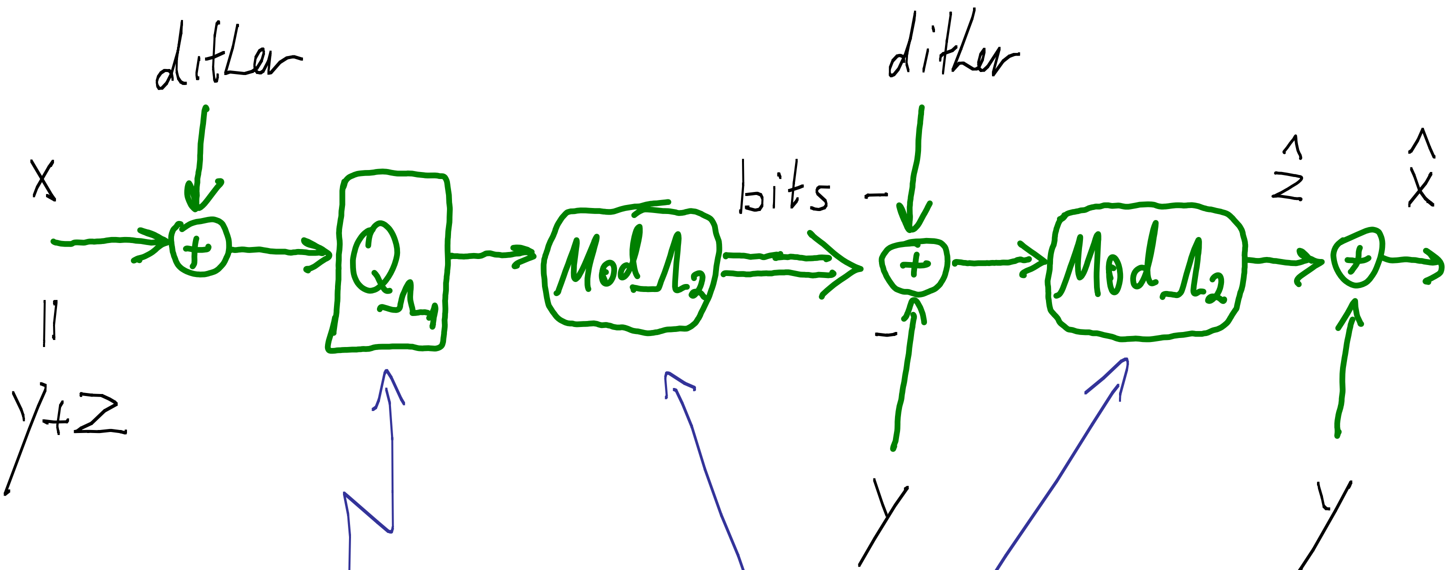
WZ-Video Coding:

motion compensation @ decoder

⇒ encoding = simple / deoding = complex

Lattice Wyner-Ziv Coding

[Z & Shamai Verdu]

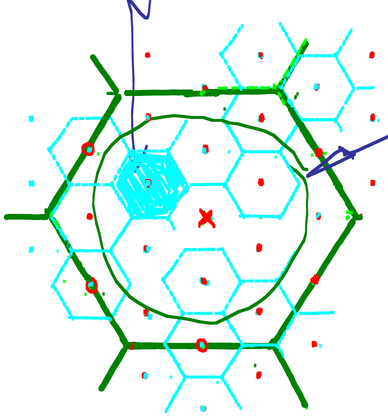


Good quantizer for desired distortion:

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

Good channel code for the noise Z:

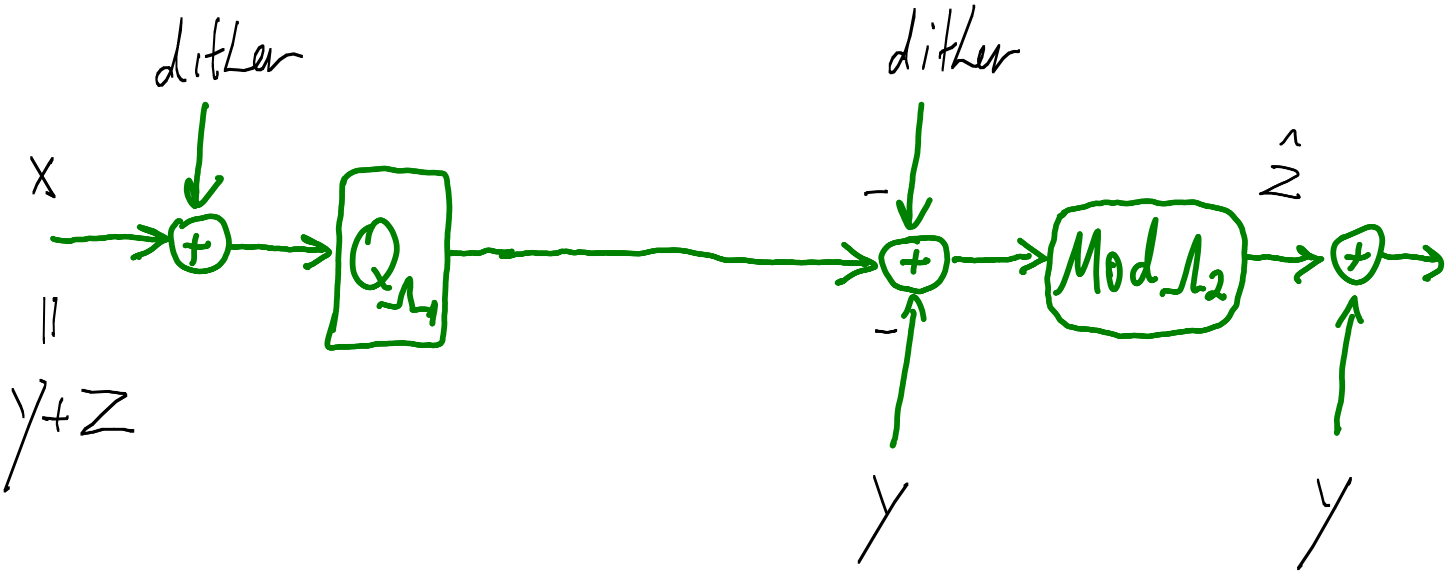
$P_e(\Lambda_2, \sigma_Z^2) < \varepsilon$



Lattice Wyner-Ziv Coding

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

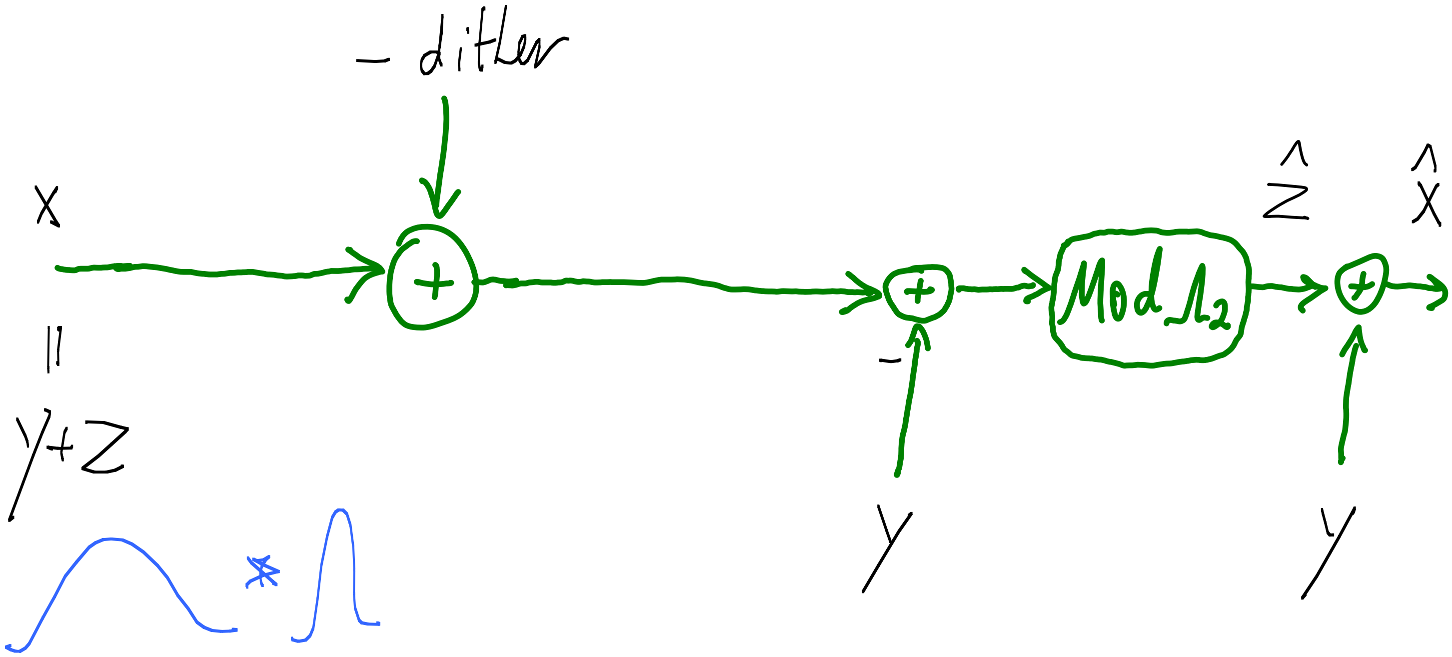
$\Longrightarrow$



Lattice Wyner-Ziv Coding

dithered quantization ≡ additive noise

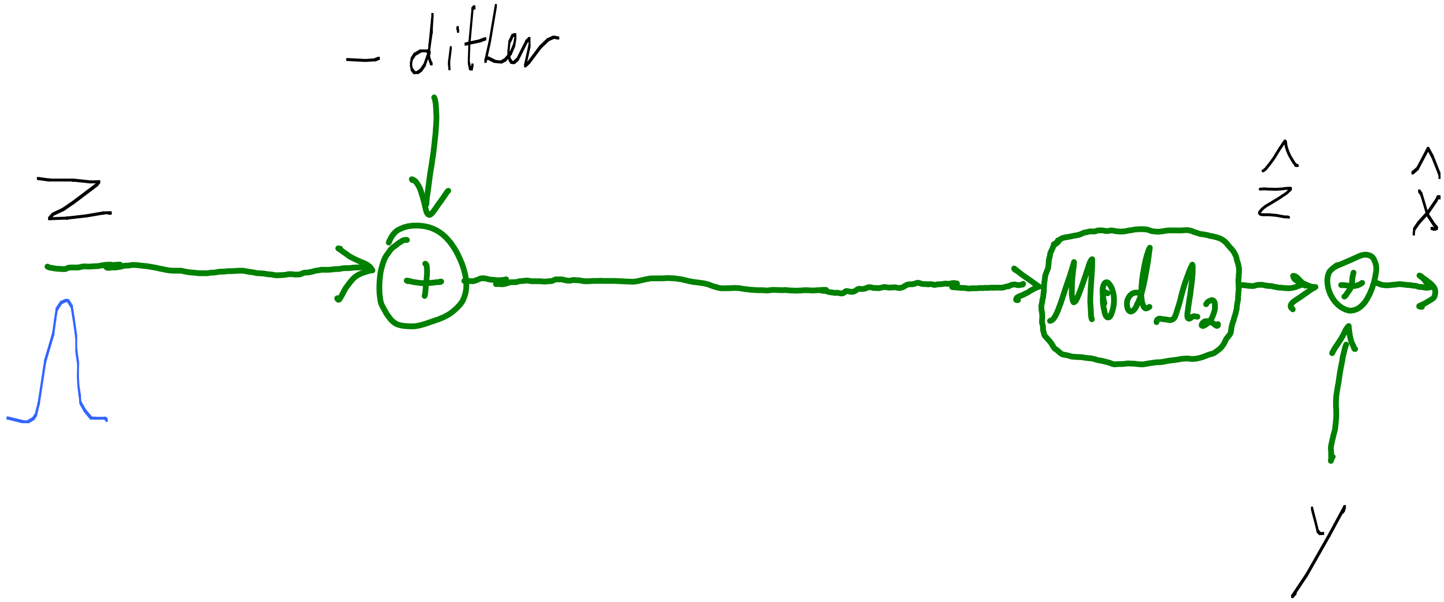
$\Rightarrow$



Lattice Wyner-Ziv Coding

dithered quantization $\equiv$ additive noise

$\Rightarrow$

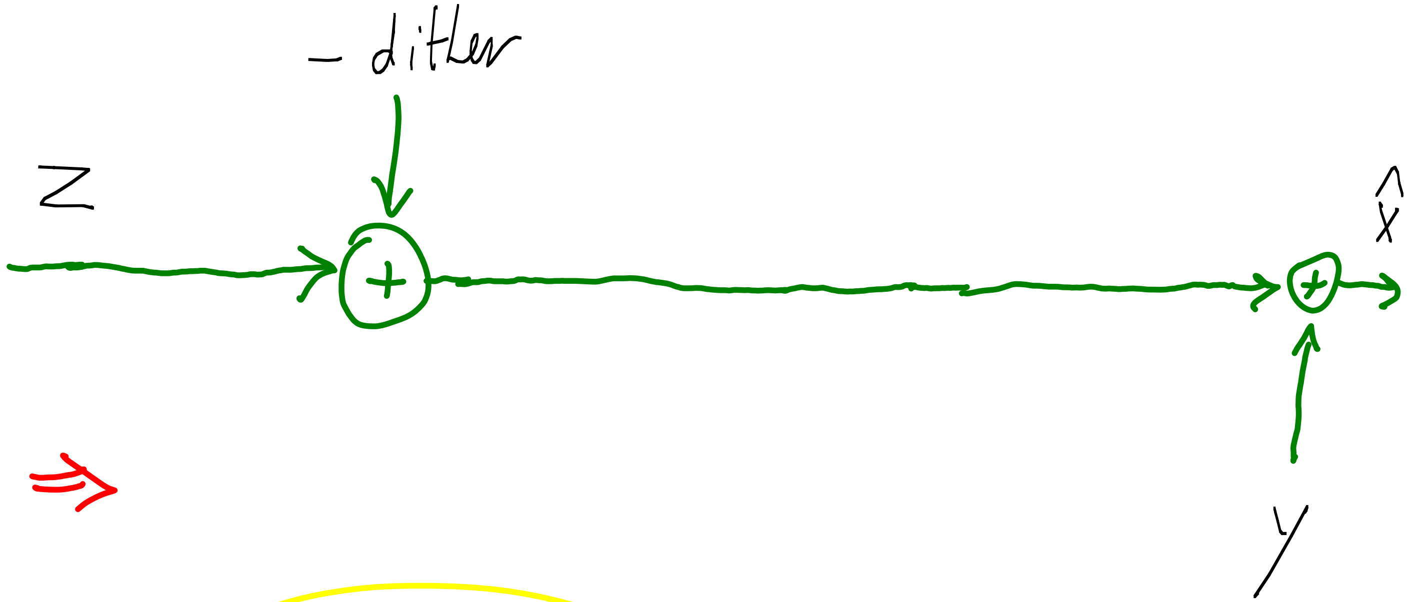


Lattice Wyner-Ziv Coding

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. $> 1 - \varepsilon$

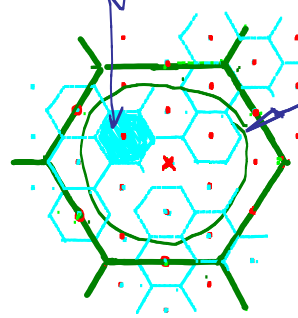
$\Rightarrow$ distortion $= \sigma^2(\Lambda_1) = D$

Lattice Wyner-Ziv Coding

Nesting Ratio:

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

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



$\Rightarrow$

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

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

NSM (Λ_1)

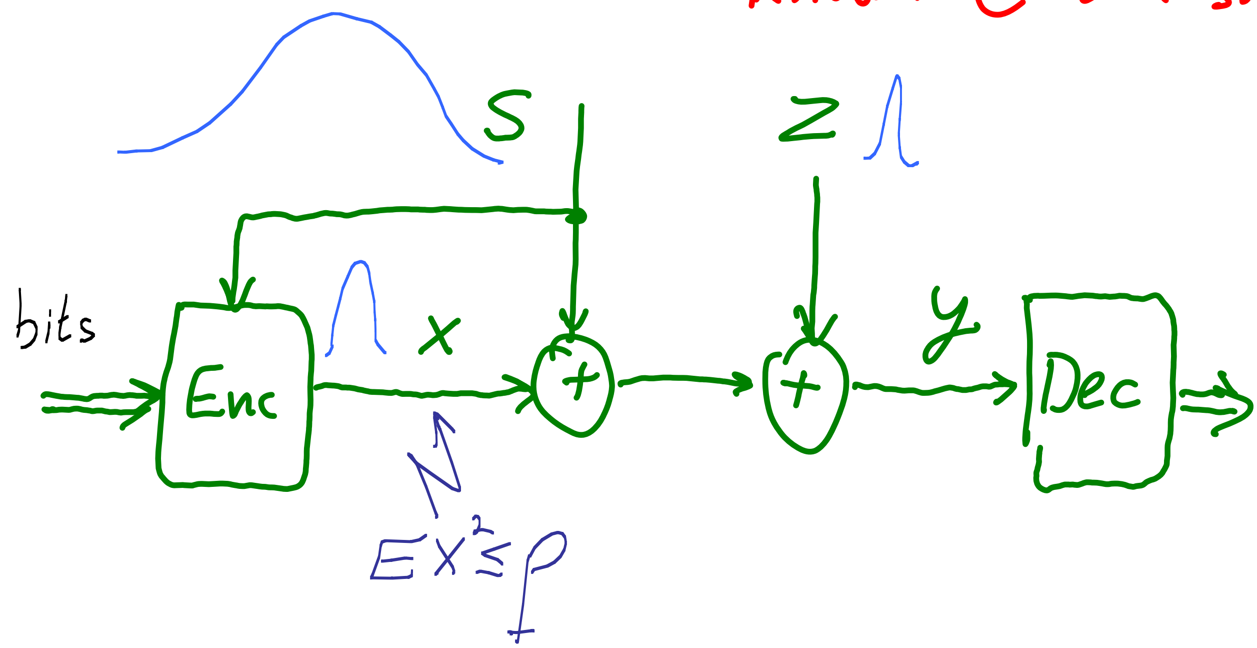
VNR (Λ_2)

$n \to \infty$

for good lattices ....

"Writing on Dirty Paper"

(AWGN channel coding with Interference known @ transmitter)



* The information-theoretic limit:

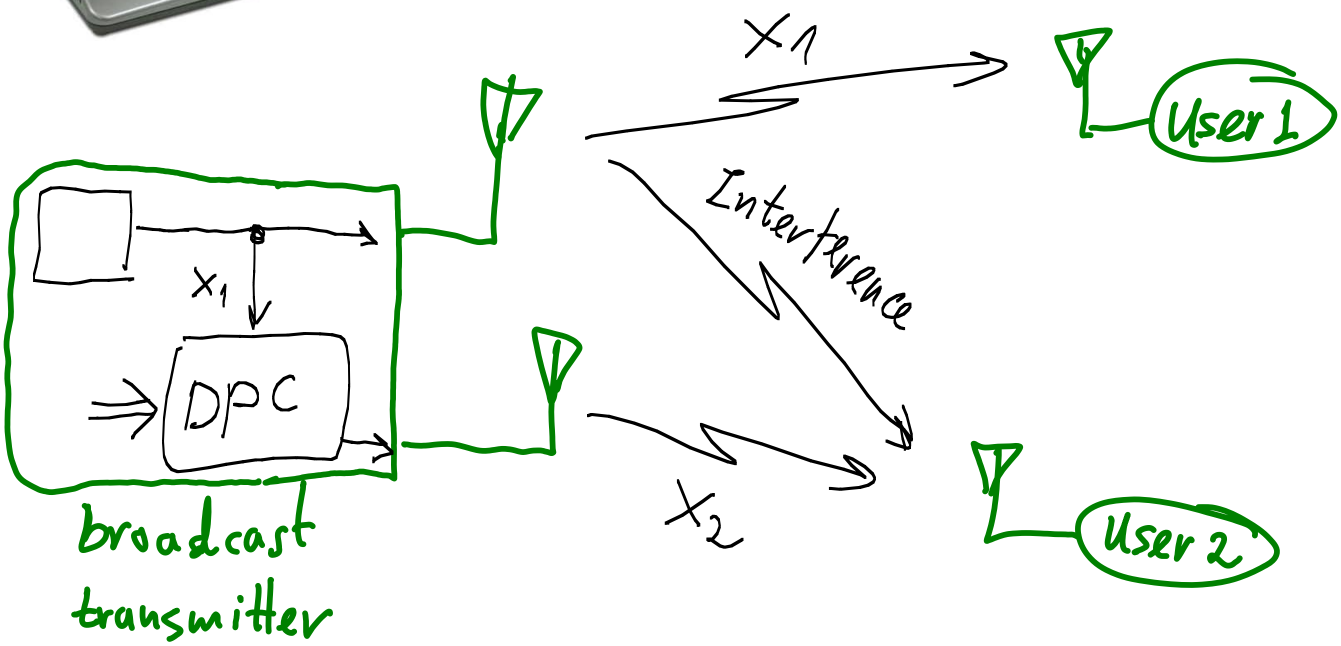
$$C_{SI@Tx} = \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right) = C_{AWGN}$$

Gelfand-Pinsker 1980

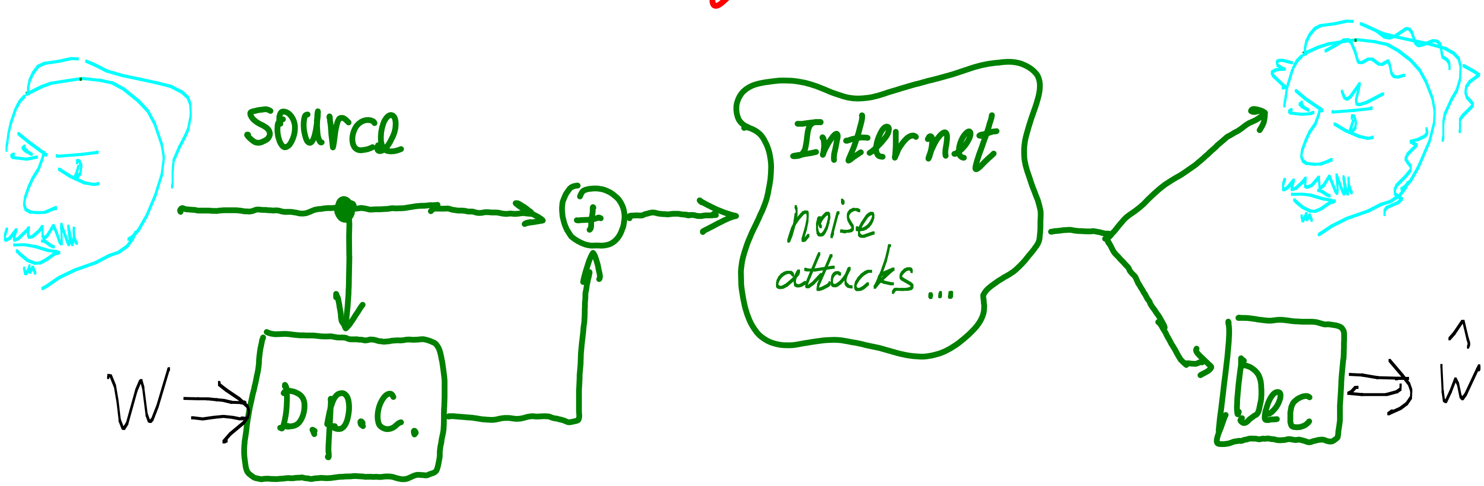
Costa 1983

Surprising: interference cancellation with no power penalty?

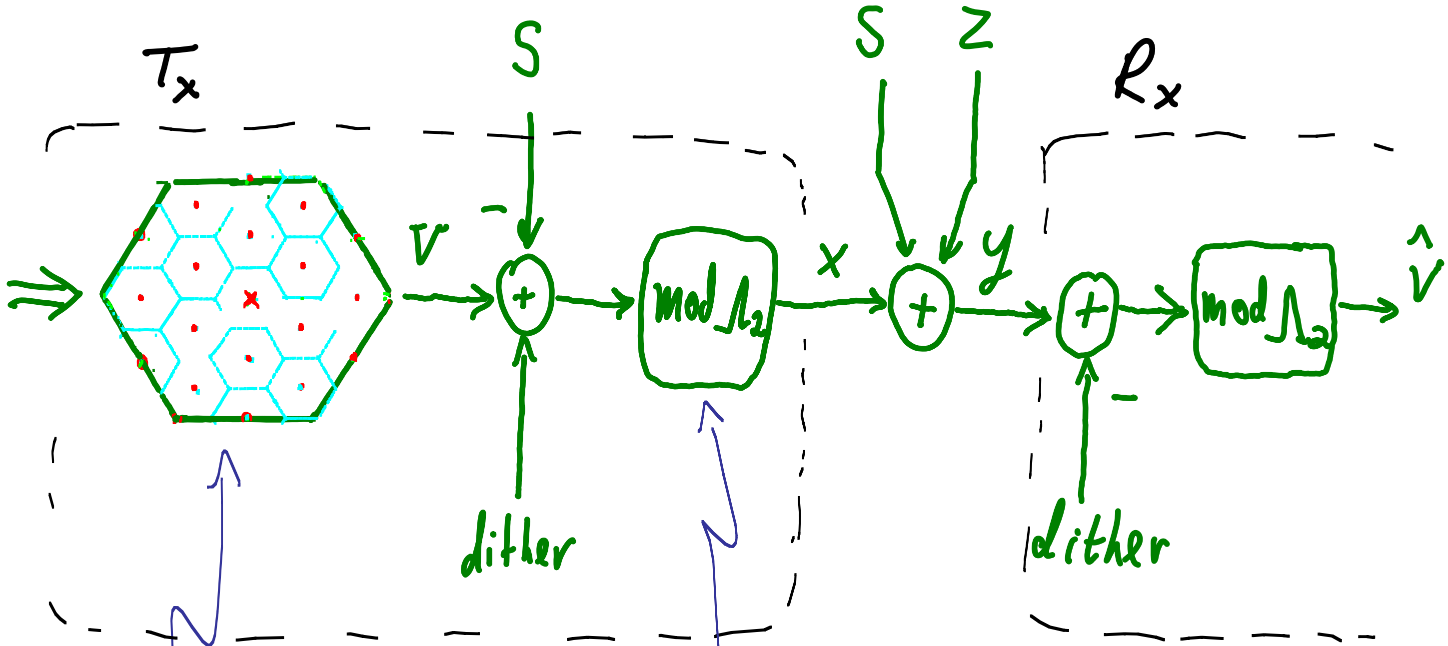
MIMO-Broadcast using D.P.C



Information Embedding ("Watermarking")



Lattice Dirty Paper Coding



Λ_1 / Λ_2
Voronoi
Constellation

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

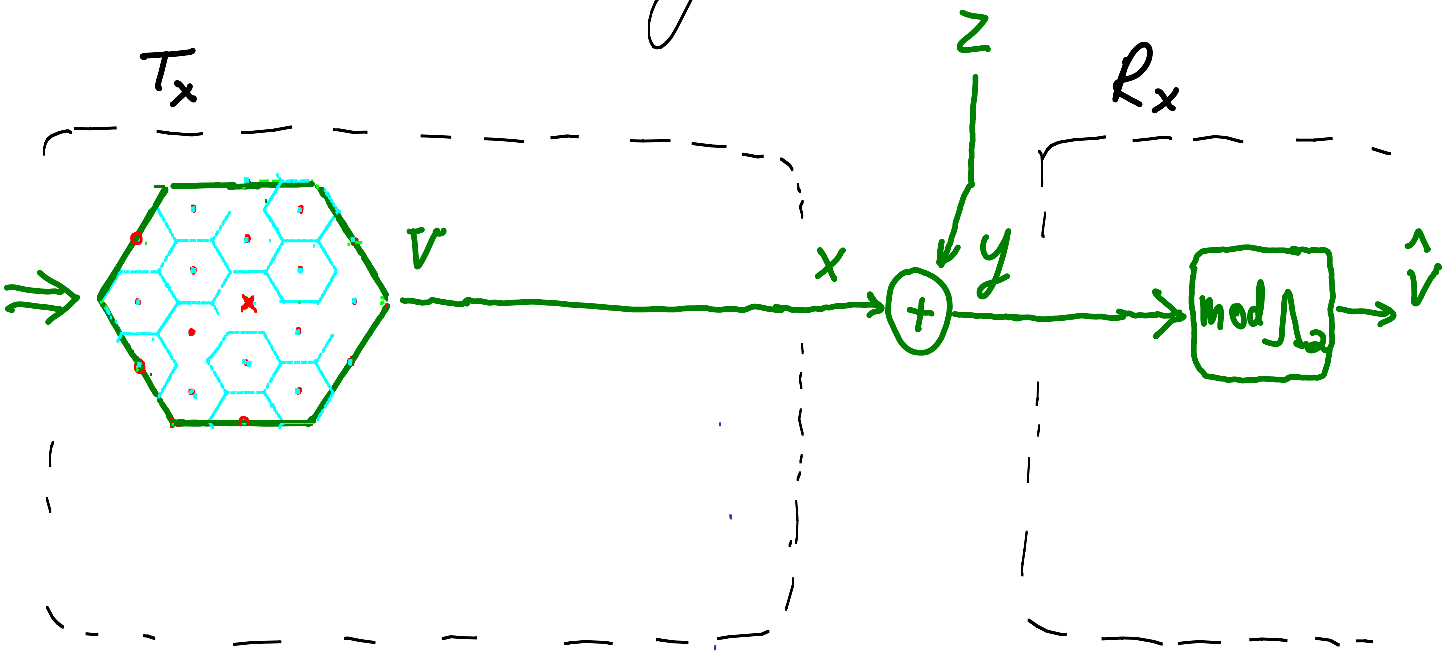
Good quantizer
$\sigma^2(\Lambda_2) = P$ + dither

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

for any codeword!

Lattice Dirty Paper Coding

Modulo property ⇒



We'll talk about ...

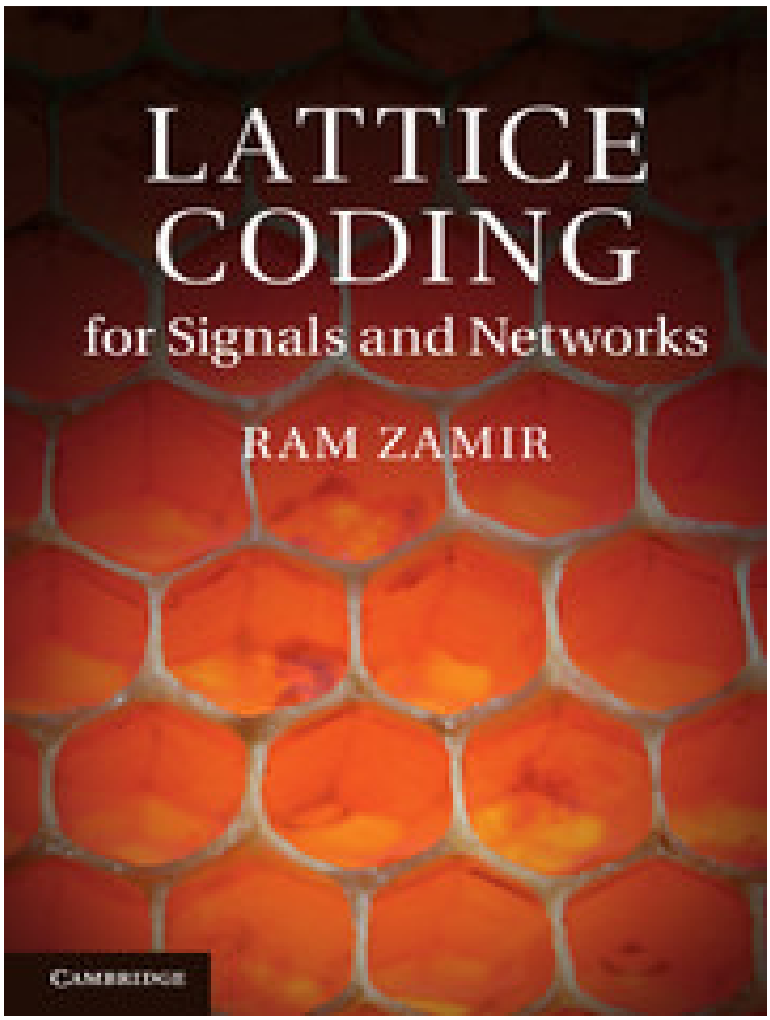
1. lattices : representation & partition
2. Construction from linear codes
3. figures of merit
4. asymptotic goodness
5. multi-level constructions
6. dithering (lattice randomization)
7. side-information problems
8. distributed lattice coding

8. Distributed lattice coding

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

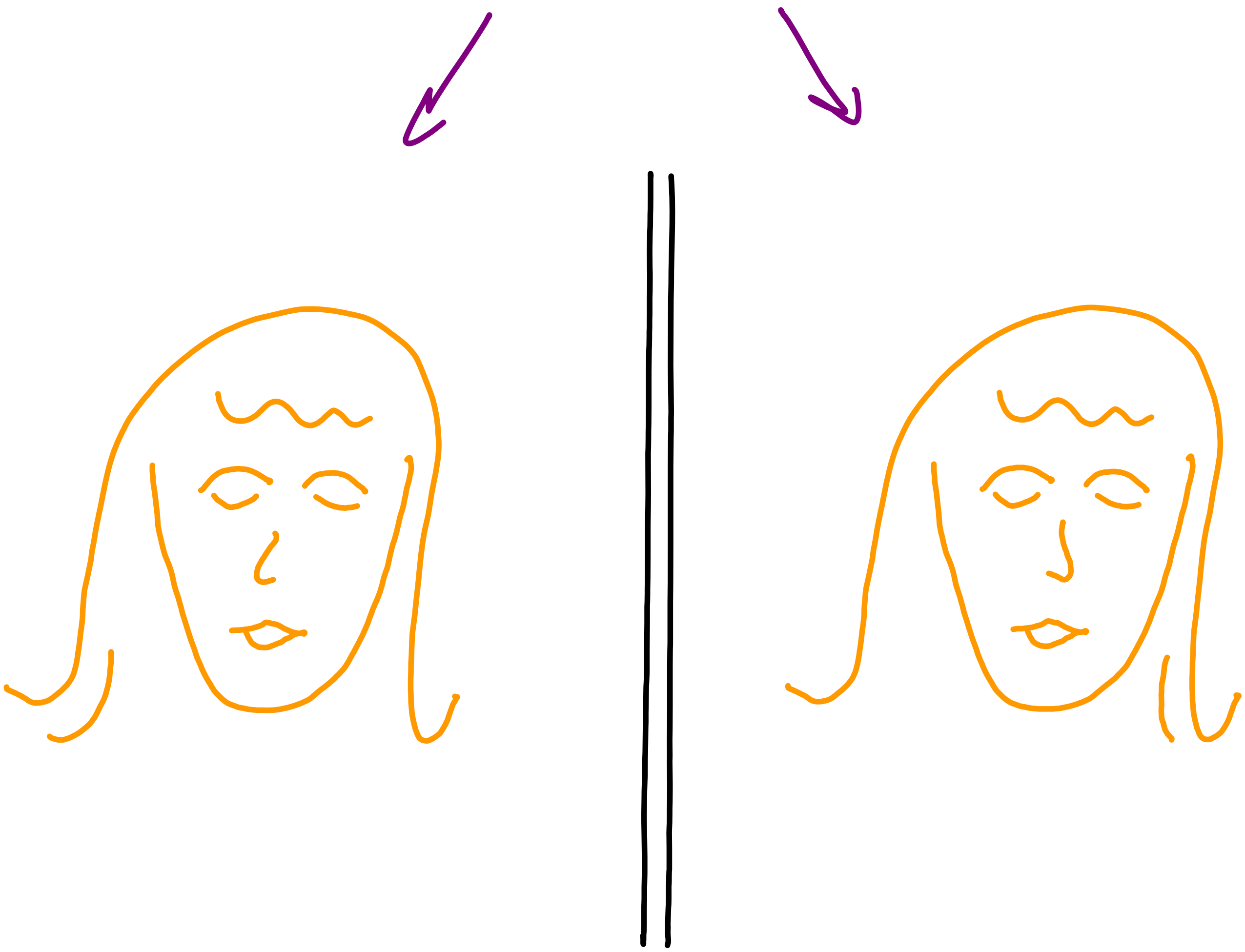
Lattices in

Network Information Theory



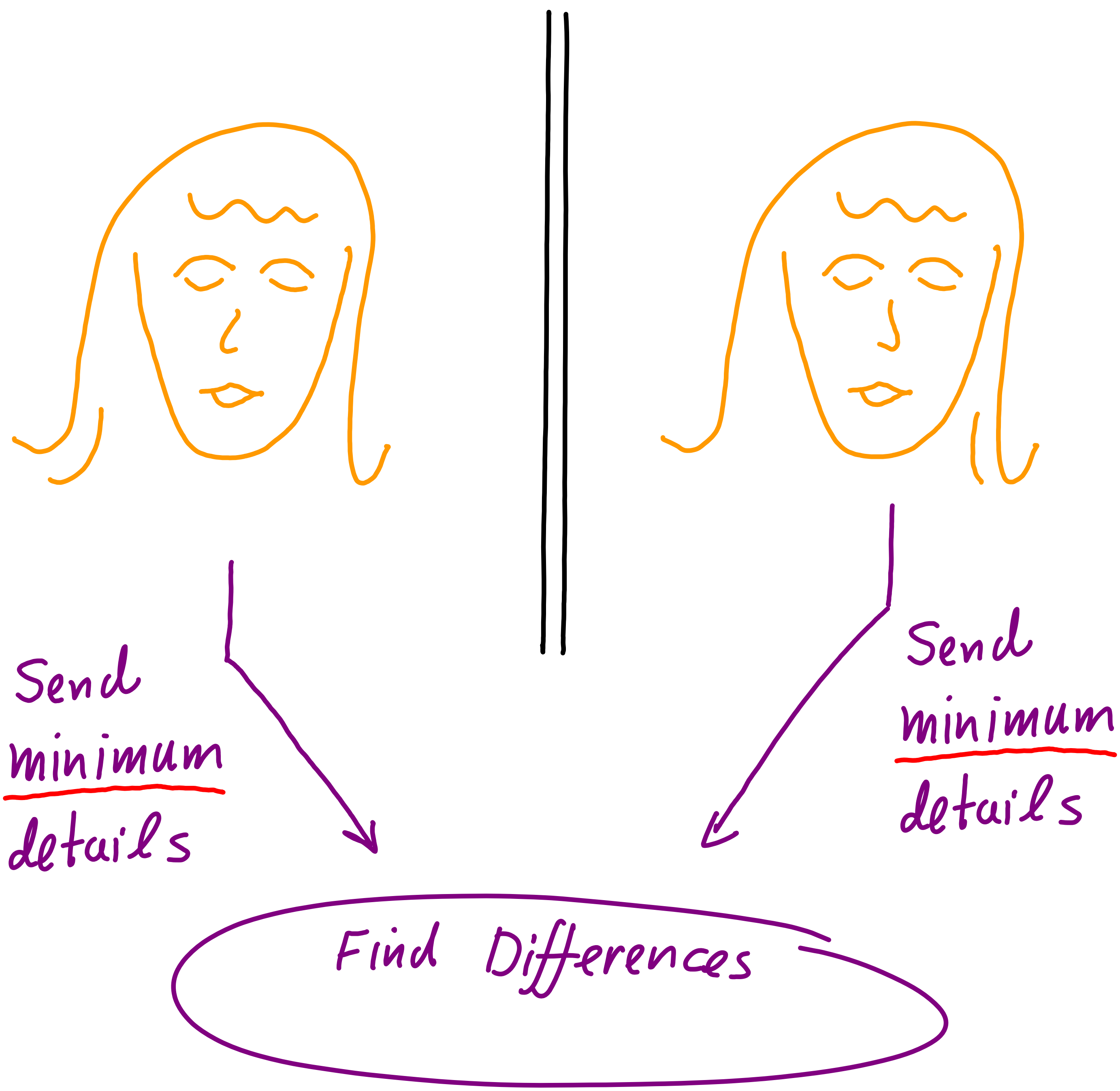
Can structure beat random ? ...

Find the Differences

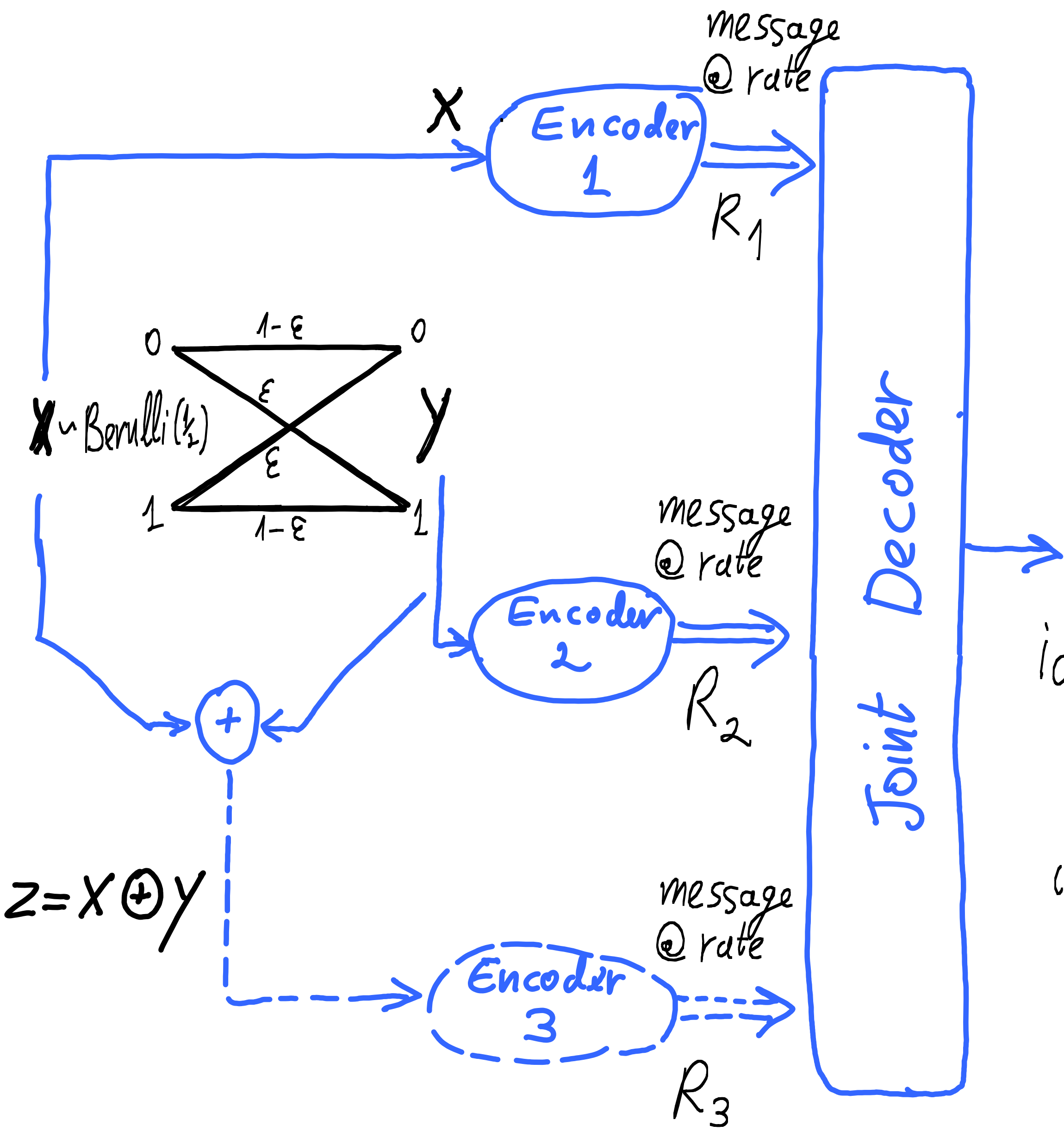


?

Communicate the Differences



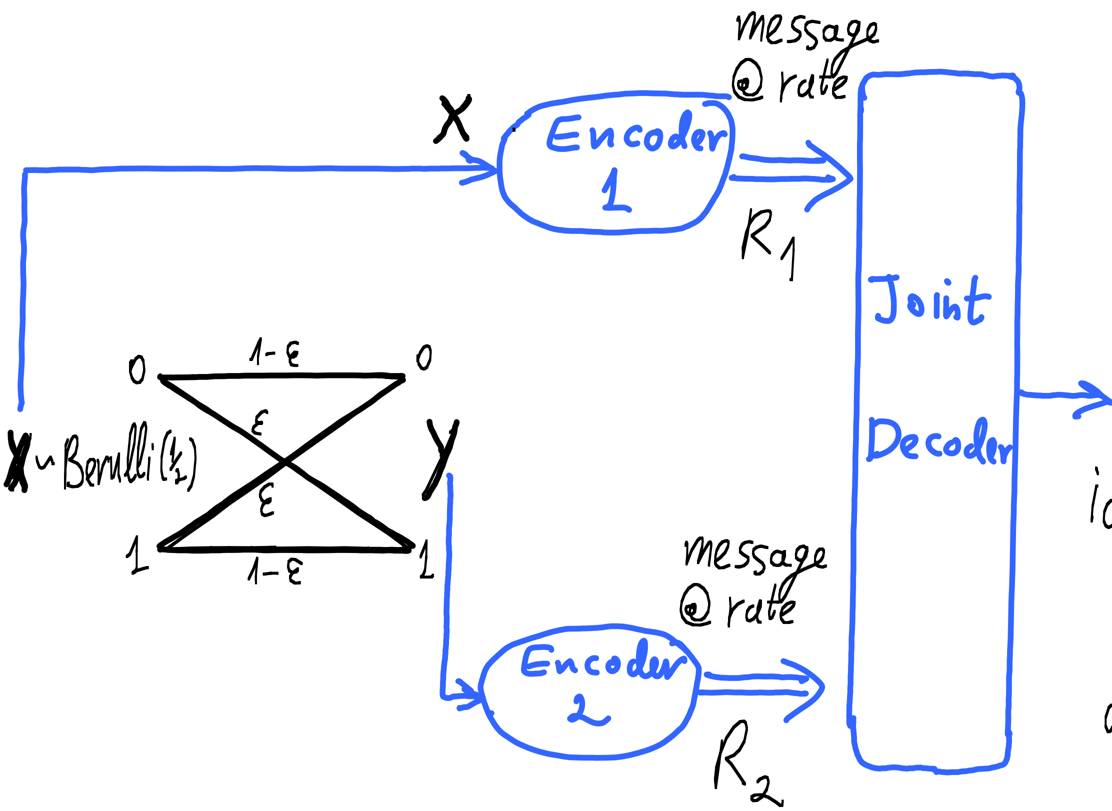
The Korner-Marton Problem



$\widehat{X \oplus Y} =$ identify where $X_i \neq Y_i$, $i = 1 \ldots n$

"Two help one" $\Rightarrow R_3 = 0$

The Korner-Marton Problem



$\widehat{X \oplus Y} =$ identify where $X_i \neq Y_i$, $i = 1 \dots n$

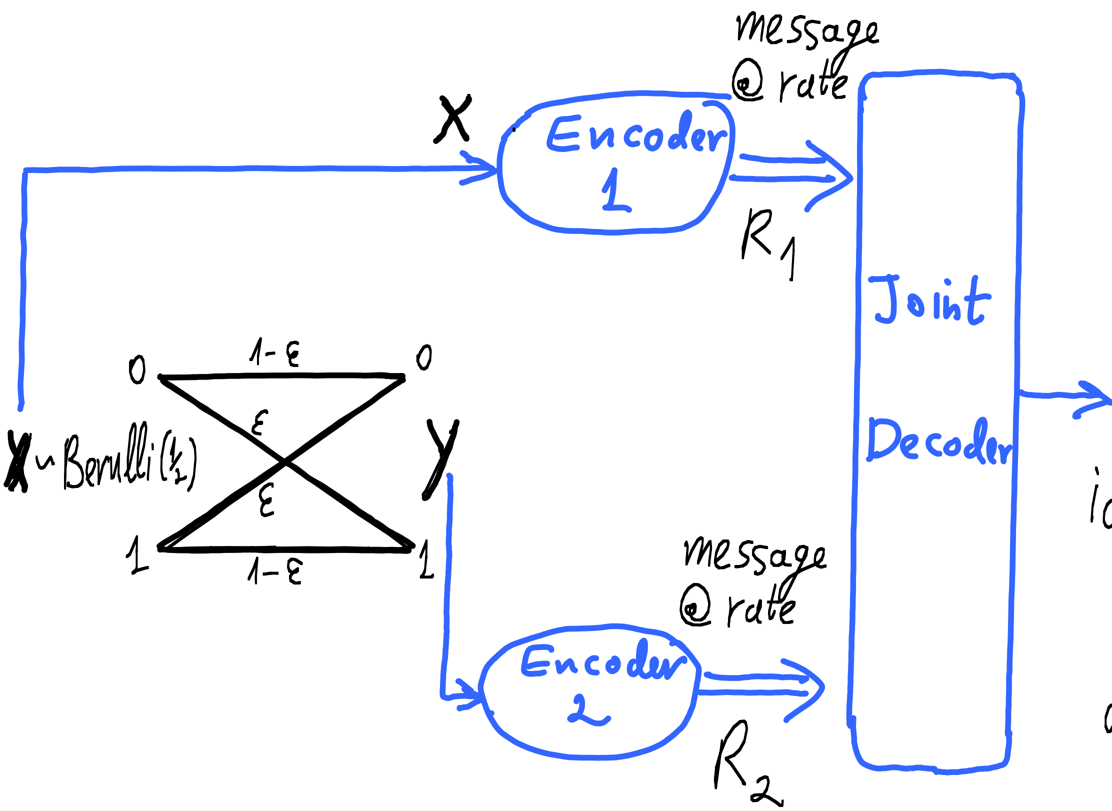
$Z = X \oplus Y$

Compress & estimate:

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

Rate $\stackrel{?}{=}$

The Korner-Marton Problem



$\widehat{X \oplus Y} =$ identify where $X_i \neq Y_i$ $i = 1 \dots n$

$Z = X \oplus Y$

compress & estimate:

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

Rate $\overset{?}{=}$

compress **well** & estimate $\Rightarrow$ Slepian-Wolf:

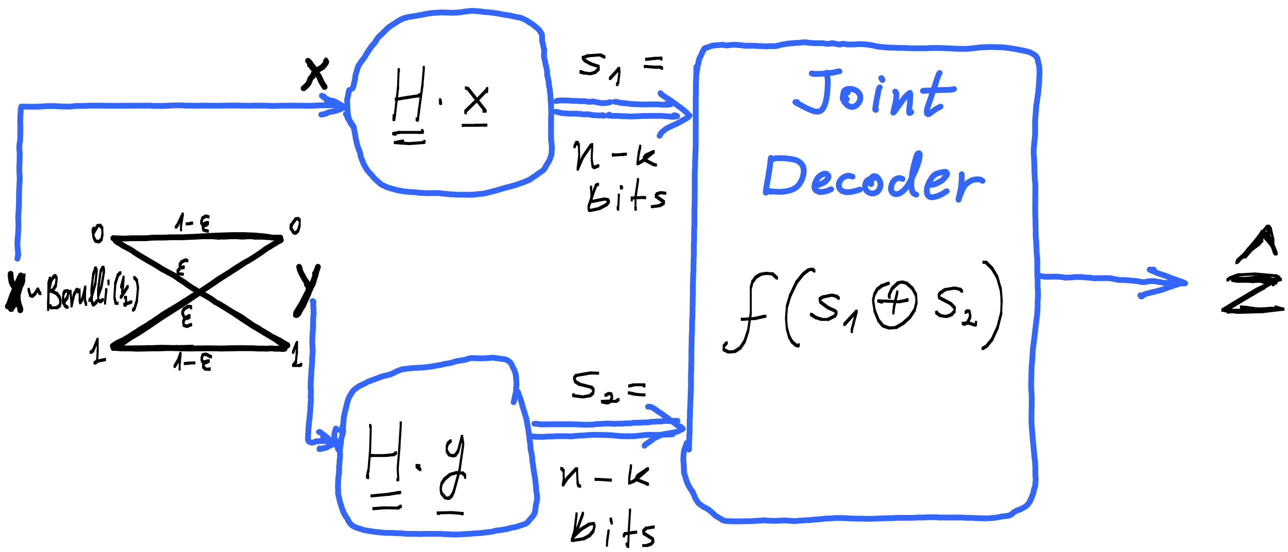
$H(X,Y) = H(X) + H(Z) = 1 + H_B(\varepsilon) = 1.1$ Bit

estimate & compress:

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

A syndrome-Coding Solution [KM 1979]:

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



$S_1 \Longleftrightarrow X \bmod \mathbb{C}$

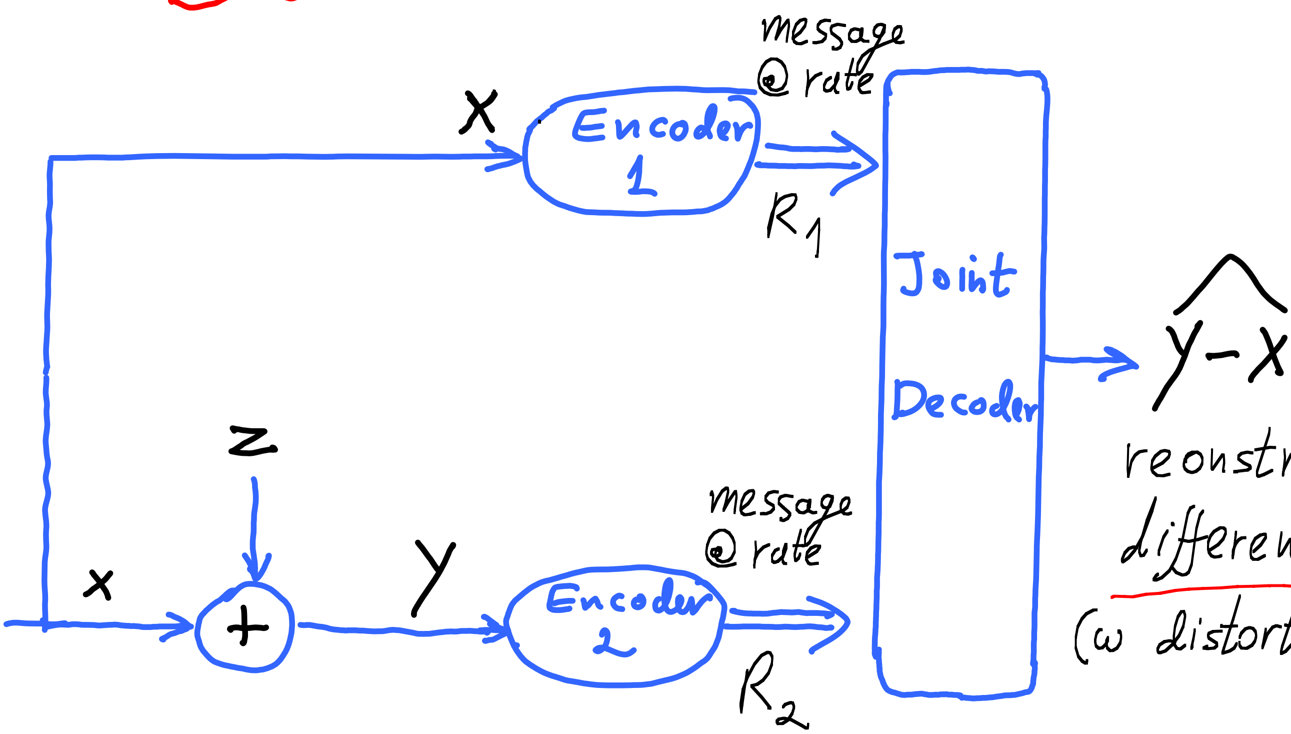
$S_2 \Longleftrightarrow Y \bmod \mathbb{C}$

$$\Longrightarrow \left\{ \begin{aligned} \hat{Z} &= (X \bmod \mathbb{C} \oplus Y \bmod \mathbb{C}) \bmod \mathbb{C} \\ &= (X \oplus Y) \bmod \mathbb{C} \\ &= Z \bmod \mathbb{C} = Z \text{ w.h.p.} \end{aligned} \right.$$

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

A comment by KM: best known random coding solution ("single letter" solution) = Slepian Wolf $\Rightarrow$ Rate $= 1.1$ bit

The Gaussian Korner-Marton Problem



reconstruct the difference Z (w distortion D)

Rate =

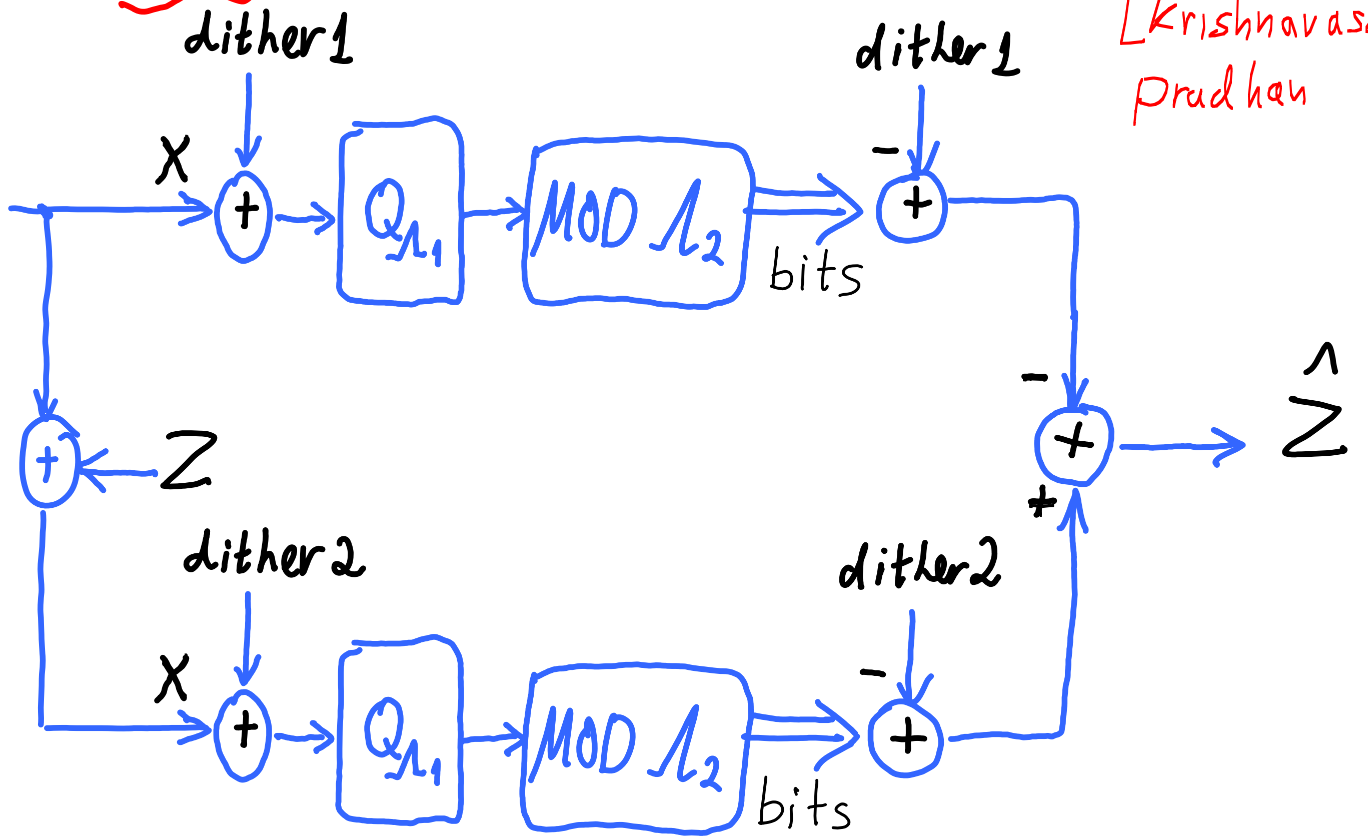
- $R_{X,Y}(D_1, D_2)$ where $D_1 + D_2 = D$ — random coding ☹
- $R_Z(D)$ — over optimistic ☺
- $> 2R_Z(D)$, $< 2 \cdot R_Z(D/2)$ — outer / inner ☹

genie aided ($> 2R_Z(D)$)

smart lattice coding ($< 2 \cdot R_Z(D/2)$)

The Gaussian Korner-Marton Problem

[Krishnavasan Pradhan]



* modulo distributive law ⟹

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

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

gap of 1/2 bit from outer bound

redundancy → 0 @ dim → ∞

Distributed Lattice Coding Problems

1. Korner-Marton (distributed computation)

2. Dirty Multiple-Access channel (distributed state @ Encoders)

3. Lattice network coding (distributed relaying)

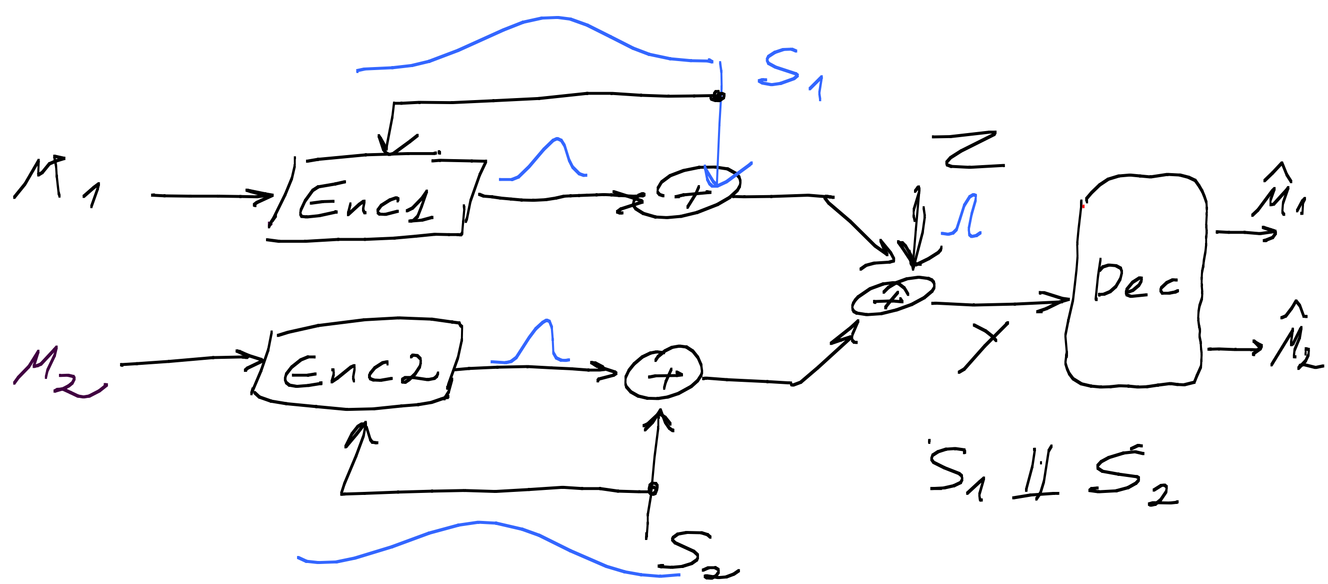
4. Lattice interference alignment

$\Longrightarrow$ Structure $\succ$ random ?

Distributed Lattice Coding Problems

1. Korner-Marton (distributed computation)

2. Dirty Multiple-Access channel (distributed state @ Encoders)



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

3. Lattice network coding (distributed relaying)

4. Lattice interference alignment

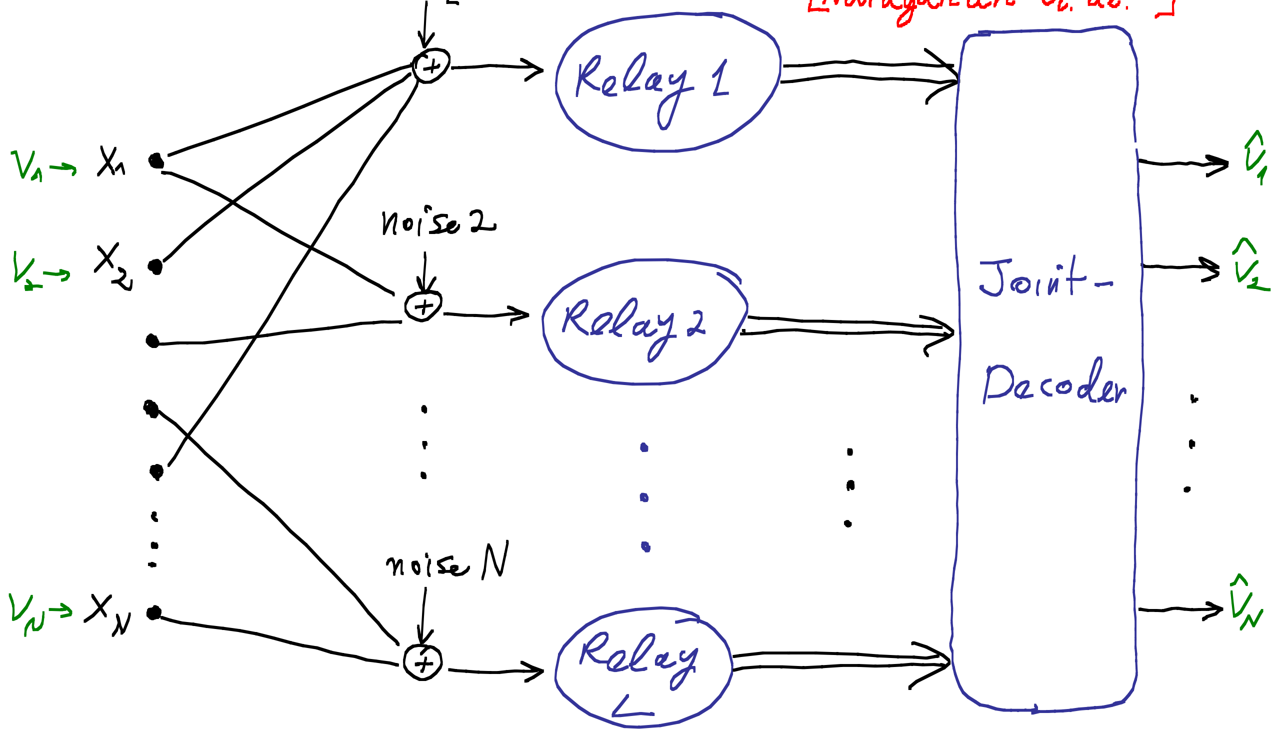
Distributed Lattice Coding Problems

1. Korner-Marton (distributed computation)

2. Dirty Multiple-Access channel (distributed state @ Encoders)

3. Lattice network coding (distributed relaying)

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



4. Lattice interference alignment

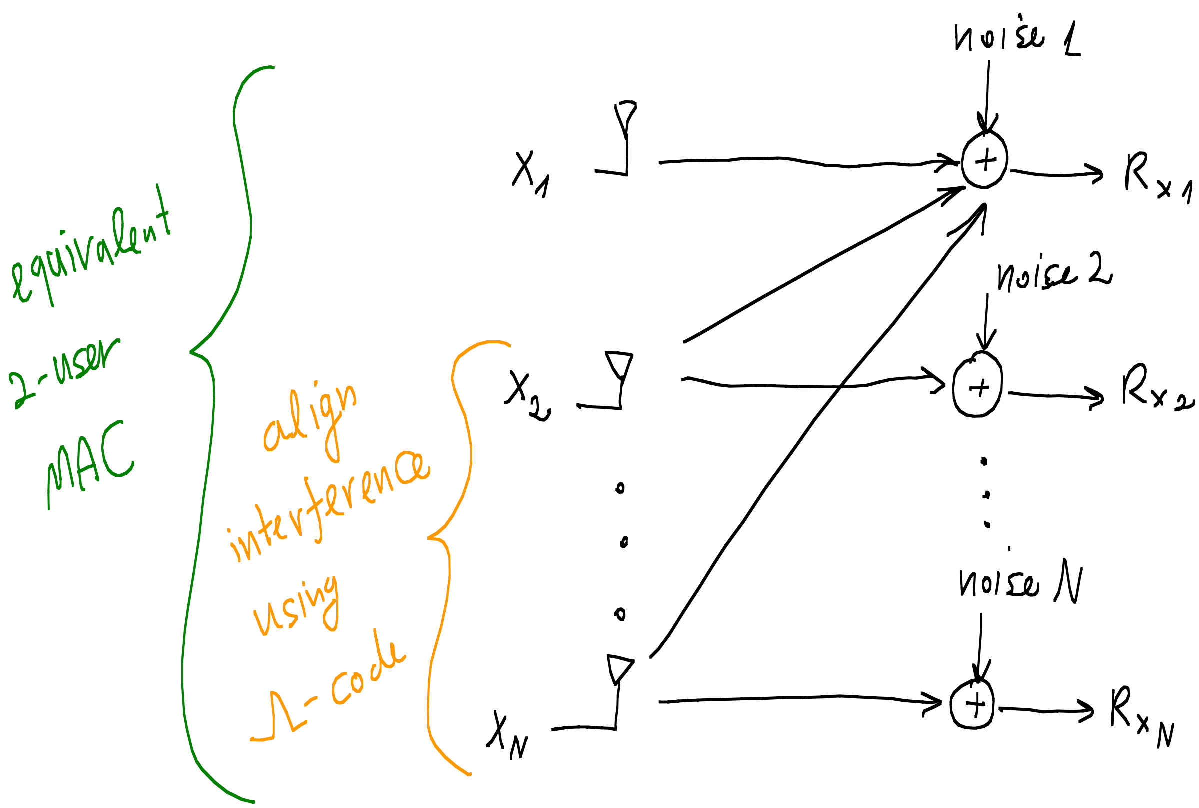
Distributed Lattice Coding Problems

1. Korner-Marton (distributed computation)

2. Dirty Multiple-Access channel (distributed state @ Encoders)

3. Lattice network coding (distributed relaying)

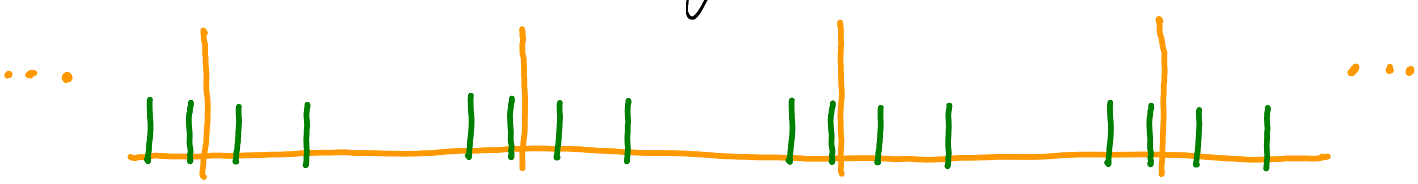
4. Lattice interference alignment



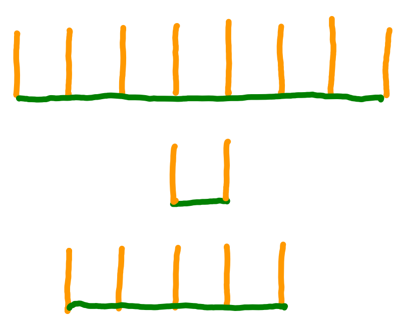
Lattice Alignment

	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

- Coarse lattice alignment:



- fine lattice alignment:

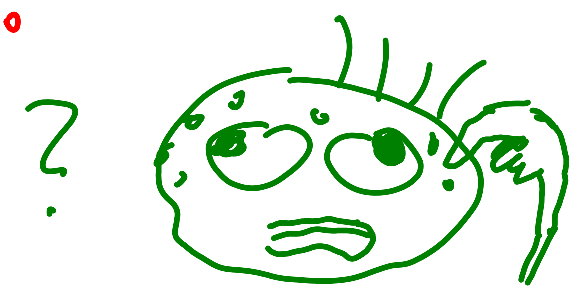


Lattice Alignment

	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:

More cases?...



Thank You!

Appendix

On-Board Calculation...

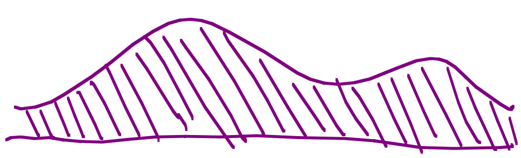
Minkowski - Hlawka - Siegel

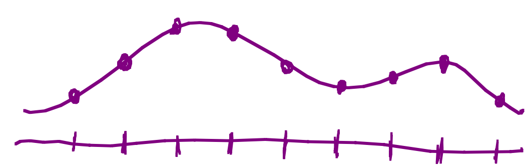
$\Longrightarrow$

1. For any Riemann integrable function $f(\cdot)$

$$\text{integral} = \frac{1}{\gamma}\cdot E_{MHS}\left\{\begin{matrix}\text{lattice - samples}\\ \text{sum}\end{matrix}\right\}$$

$$\text{integral} = \int_{\mathbb{R}^n} f(x)\,dx \qquad\qquad \text{lattice-samples sum} = \sum_{\lambda\in\Lambda} f(\lambda)$$



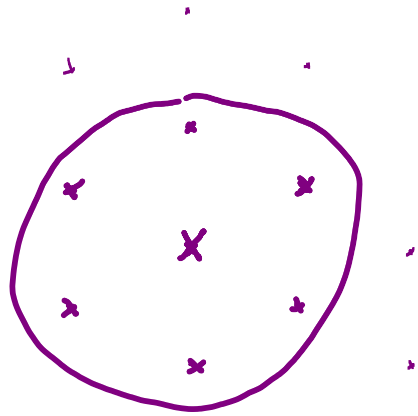


2. There exists (at least one) lattice which is (at least) as "good" as (1.)

Implication 1 : packing Goodness

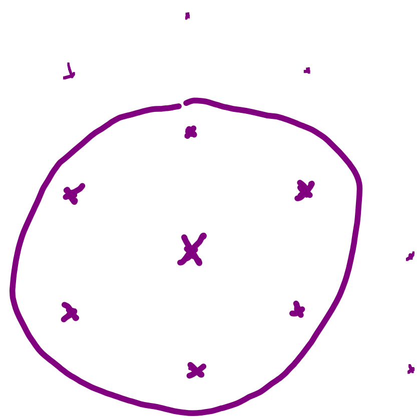
$$S = \mathrm{Ball}(0, r)$$

$$\boxed{E_{MHS}\left\{ N_{\Lambda}(\mathrm{Ball}) \right\} = \gamma \cdot V_n \cdot r^n}$$



Implication 1 : packing Goodness

$$S = \mathrm{Ball}(0, r)$$



$$\boxed{E_{MHS}\left\{ N_\Lambda(\mathrm{Ball}) \right\} = \gamma \cdot V_n \cdot r^n}$$

If $\mathrm{Vol}(\mathrm{Ball}) = V_n \cdot r^n < 1/\gamma$

$\Longleftrightarrow \quad r < r_{eff} \qquad (*)$

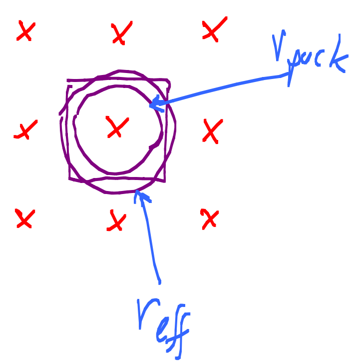
$\Longrightarrow \quad E\{N_\Lambda\} < 1$

But $\quad N_\Lambda = \text{integer}$

$\Longrightarrow \quad N_\Lambda = 0$ for some $\Lambda^* \in MHS$

$\Longrightarrow \quad d_{min} = \|\text{shortest vector}\| > r$

$\Longrightarrow \quad r_{pack} > r/2 \qquad (**)$



$(*) + (**) \Longrightarrow$ packing efficiency of $\Lambda^* = \dfrac{r_{pack}}{r_{eff}} \geq 1/2$

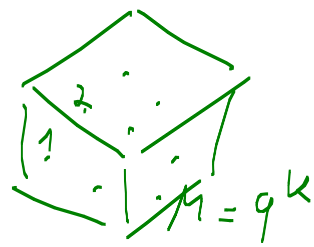
(for each dim n)

Alternative Ensemble:

Random Construction A (Loeliger 97, Erez et al 2005)

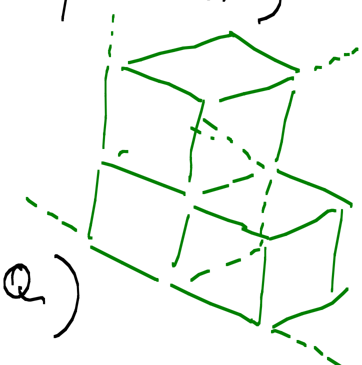
Let $\mathcal{C}$ = q-ary (n,k) liner code over $Q=\{0,\dots,q-1\}$

$$= \{ \underbrace{\underline{\underline{G}}}_{n\times k}\cdot \underline{i} \;:\; \underline{i}\in Q^k \}$$



Let $\Lambda_{\mathcal{C}}$ = modulo-q lattice

$$= \{ \lambda \in \mathbb{R}^n : \lambda \bmod q \in \mathcal{C} \}$$



G random (iid uniform on Q)

$\Rightarrow$ $\Lambda_{\mathcal{C}}$ = random lattice

$\therefore$ $G(\Lambda_{\mathcal{C}})$, $\mu(\Lambda_{\mathcal{C}}, P_e) = \text{func}\{q, k, n\}$

* $\Lambda_{\mathcal{C}} \longrightarrow$ MHS property as $q \longrightarrow \infty$!