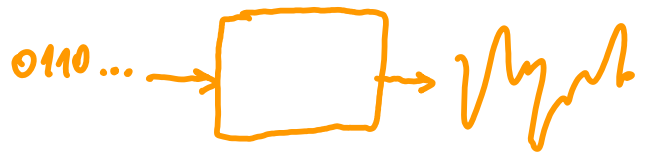
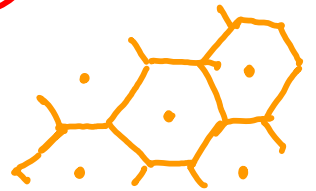

Multi-level Coded Modulation

and



Lattice Construction D



Ram Zamir

Joint work with Uri Erez & Or Ordentlich

Multi-level Coded Modulation
and
Lattice Construction \mathcal{D}

Are lattice codes better than
non-lattice codes?

(question raised while teaching a graduate
class on digital communication...)

Lattices are everywhere!



* picture editing
by Kesseem Zamir

Lattice: Definition

Lattice = discrete subgroup of Euclidean space

$$\Lambda = \{ \underline{G} \cdot \underline{i} : \underline{i} = \text{vector of integers} \}$$

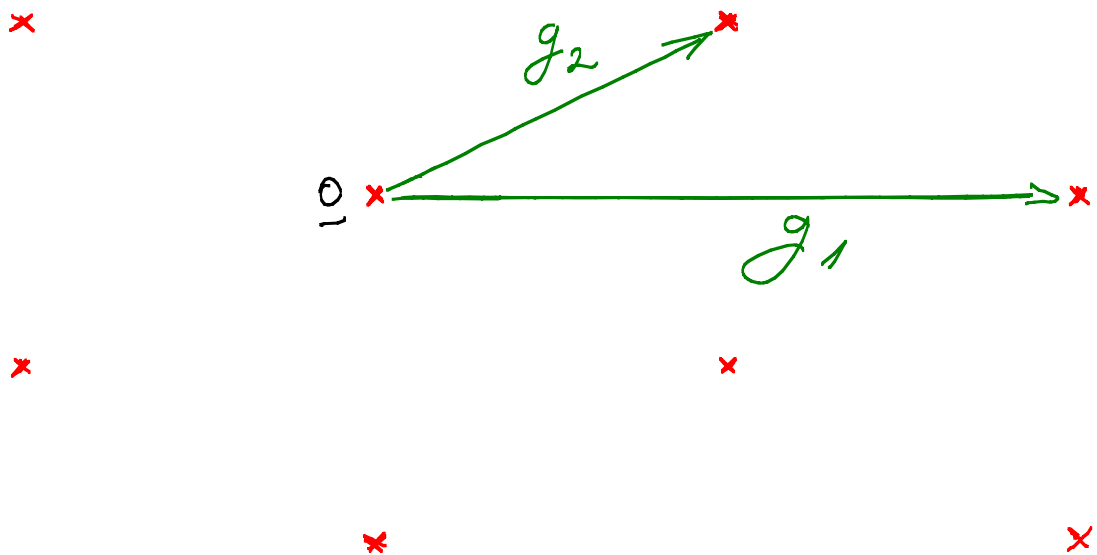
Λ is Lattice in \mathbb{R}^n

\underline{G} is Generator Matrix $n \times n$

$\underline{i} = (0, \pm 1, \pm 2, \dots)$

Closed under reflection & addition:

$$\text{linearity: } \lambda_1, \lambda_2 \in \Lambda \Rightarrow \lambda_1 + \lambda_2 \in \Lambda$$
$$\pm i \cdot \lambda \in \Lambda$$



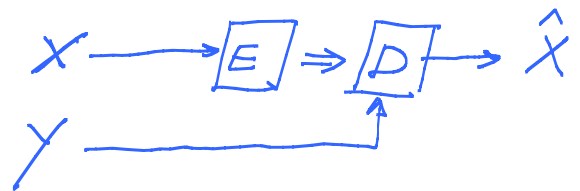
Lattice codes in information theory

* dithered quantization \rightarrow ECDO achieves $\frac{1}{2} \log(S/D)$

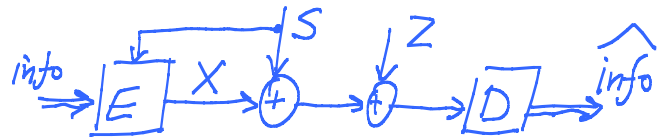
* Voronoi modulation ("shaping") \rightarrow achieves $\frac{1}{2} \log(1+SNR)$
as $n \rightarrow \infty$

* side information settings ("lattice binning")

Lattice Wyner-Ziv coding

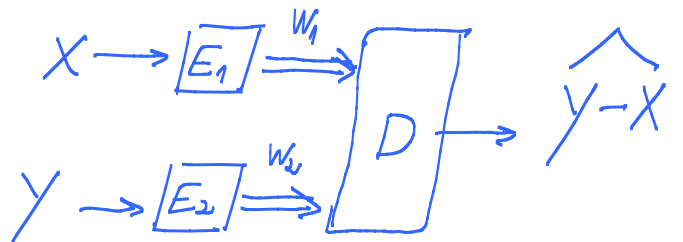


Lattice "dirty paper" coding

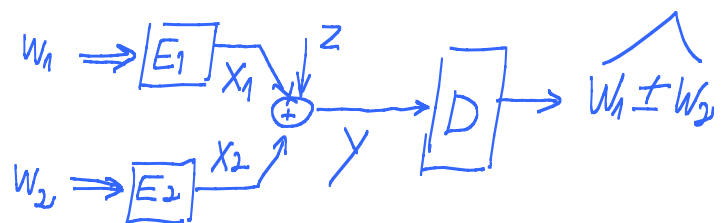


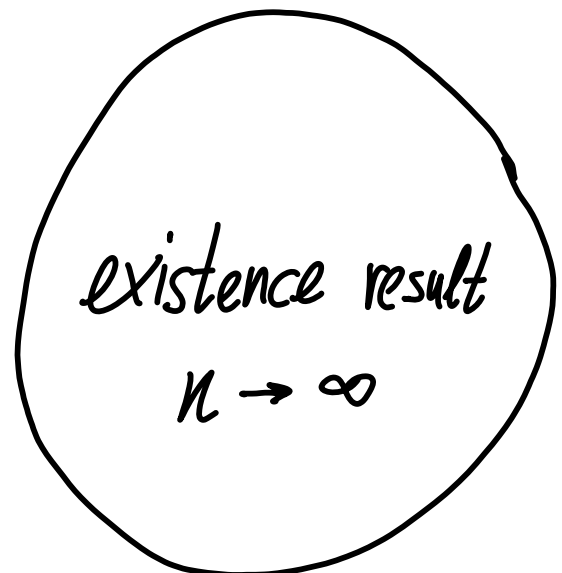
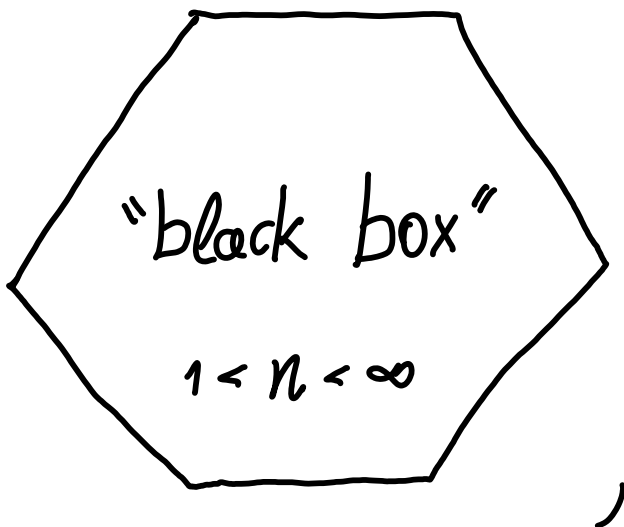
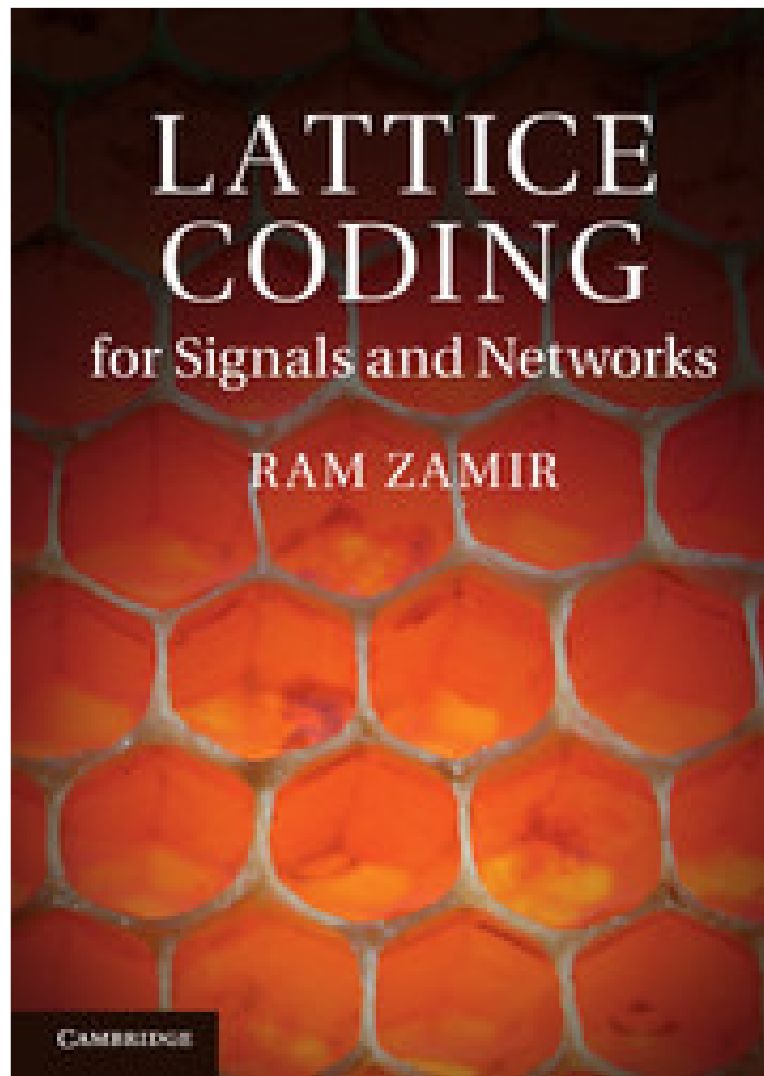
* structure beats random (distributed settings)

Lattice Kerner-Marton
(distributed computation):



Lattice network coding
(distributed relaying):





Goodness as $n \rightarrow \infty$



Random lattice ensemble + AEP

Minkowski-Hlawka-Siegel

Construction A with
random linear codes
[Loeliger 1997]

⇒ Sphere packing:

$$\rho_{\text{pack}}(\Lambda_n) \rightarrow \frac{1}{2}$$

Sphere covering:

$$\rho_{\text{cov}}(\Lambda_n) \rightarrow 1$$

Normalized second moment:

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

Normalized volume-to-noise ratio:

$$\mu(\Lambda_n, p_e) \rightarrow 2\pi e$$

$0 < p_e < 1$

as lattice dimension $n \rightarrow \infty$.

Back from infinity...



Algebraic constructions in finite dimensions
 $n < \infty$

Constructions A, B, C, D, E

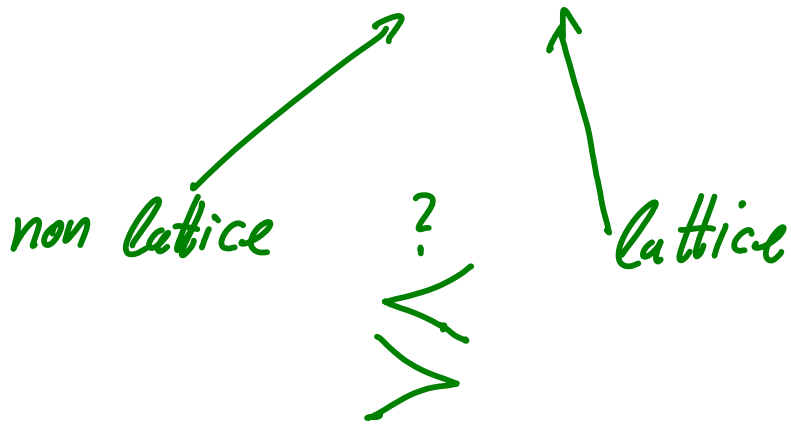
See [Conway & Sloane Book 1988].

Back from infinity...



Algebraic constructions in finite dimensions
 $n < \infty$

Constructions A, B, C, D, E



Classification of "almost"-lattice codes
(infinite constellations)

Lattice Λ



Geometrically Uniform



Equi-Distance Spectrum



Equi-Minimum distance
(& Equi-kissing number)



Random, $n \rightarrow \infty$

Classification of "almost"-lattice codes

(infinite constellations in AWGN channel)

Lattice Λ

$$\Rightarrow P_{e \max} = \overline{P_e}$$



Geometrically Uniform

$$\Rightarrow \text{---} \text{---}$$



Equi-Distance Spectrum

$$\Rightarrow \text{Union (\& Gallager's) Bound-identical for all codewords}$$



Equi-Minimum distance
(\& Equi-kissing number)

$$\Rightarrow \text{Union Bound Estimate --- (exponential UBE)}$$

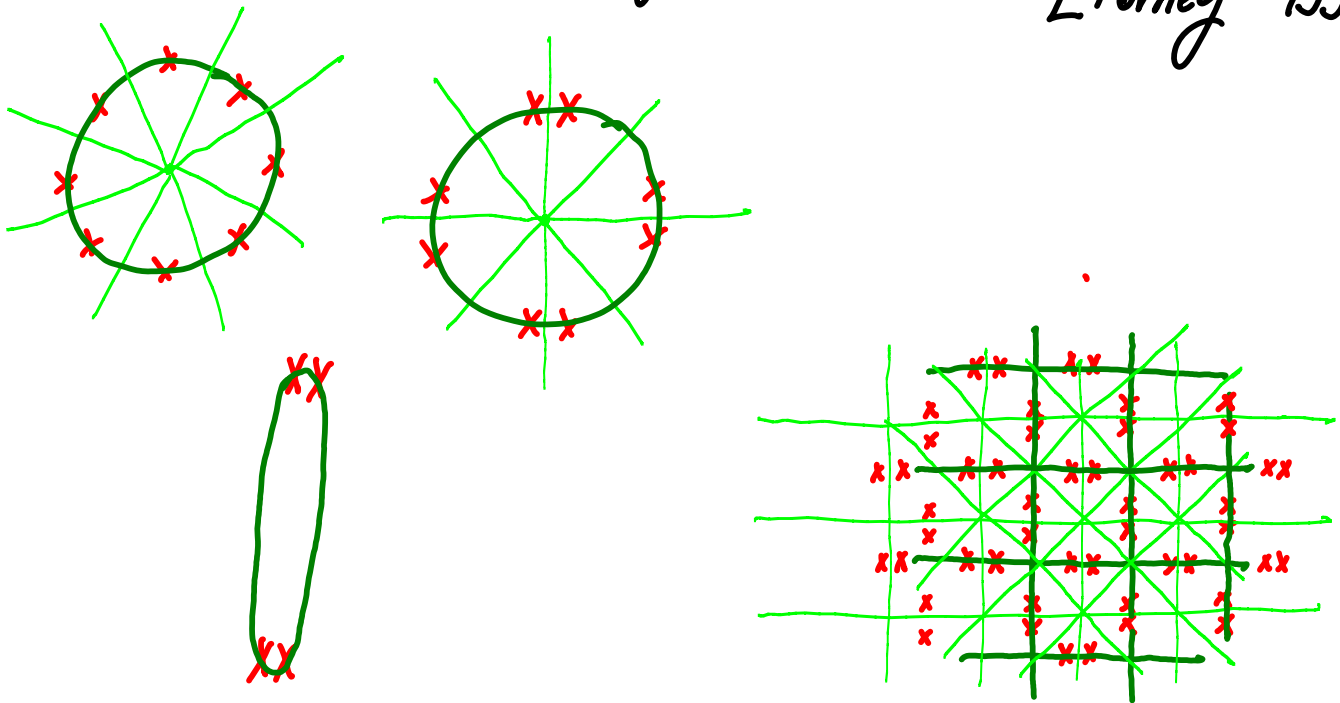


Random, $n \rightarrow \infty$

$$\Rightarrow C, E(R)$$

(most codewords are "good" as $n \rightarrow \infty$)

Reminder : Geometrically Uniform Constellation [Forney 1991]



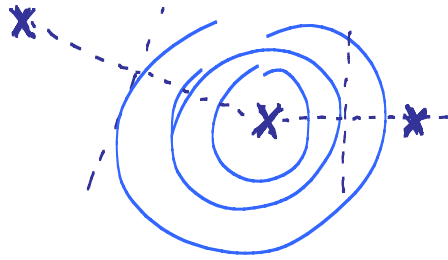
Definition: \mathcal{C} is GU if for any two codewords $c, c' \in \mathcal{C}$, there exists a distance-preserving transformation T (translation, reflection, rotation) such that $c' = T(c)$ and $T(\mathcal{C}) = \mathcal{C}$.

\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).

Reminder : Union Bound

Channel : $y = c + z$, $c \in \mathcal{C}$, $z \sim \text{AWGN}(\sigma)$



$$P_e(c) \leq \sum_{d \geq d_{\min}(c)} N(c, d) \cdot Q\left(\frac{d/2}{\sigma}\right)$$

where $N(c, d)$ = number of codewords in \mathcal{C} at distance d
from $c \in \mathcal{C}$,

and

$$d_{\min}(c) = \min \{d : N(c, d) > 0\}.$$

UBE: $P_e(c) \approx N_{\min}(c) \cdot Q\left(\frac{d_{\min}(c)/2}{\sigma}\right)$

where $N_{\min}(c)$ = "kissing number" = $N(c, d = d_{\min}(c))$

(For a lattice = number of spheres at radius $\frac{d_{\min}}{2}$ touching sphere @ origin.)

Equi-Distance Spectrum Definition:

$$N(c, d) = N(d) \quad \forall c \in \mathcal{C}$$

⇒ UB is identical for all codewords.
(as well as the Gallager bounds)

Equi-minimum distance definition:

$$d_{\min}(c) = d_{\min} = \text{constant} \quad \forall c \in \mathcal{C}$$

⇒ (Since $Q(x) \sim e^{-x^2/2}$)

UBE is exponentially (in SNR)
identical for all codewords.

Construction A

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

$$\mathcal{C} = \{c_i\}_{i=1}^M, \quad c_i \in \{0, 1\}^n, \quad d = \text{minimum Hamming distance.}$$

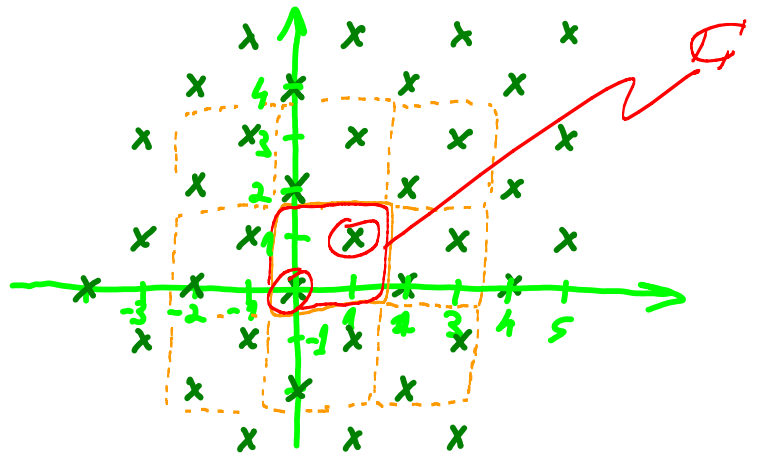
Construction A lifts \mathcal{C} to \mathbb{R}^n periodically:

Def. I

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

integer vectors

modulo 2 per each component



Equivalent definitions:

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

Def. II

2) Let $z = (\text{LSB}(z), \text{MSB}_1(z), \text{MSB}_2(z), \dots)$ = binary expansion of z

$$\Gamma_{\mathcal{C}} = \{x \in \mathbb{Z}^n : \text{LSB}(x) \in \mathcal{C}\}$$

Def. III

Construction A : Properties

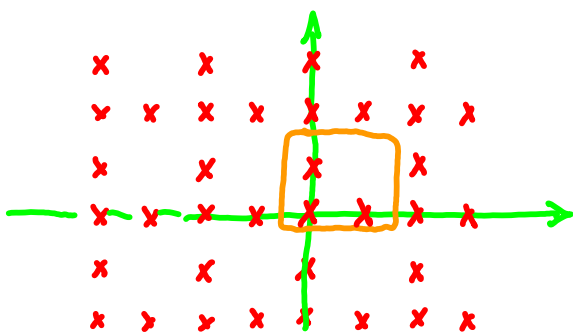
1) $d_{\min}^E(\Gamma) \triangleq \min \text{Euclidean distance} \triangleq \min_{\substack{x, y \in \Gamma \\ x \neq y}} \|x - y\|$
 $= \min \{2, \sqrt{d}\}$

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

$d_H(\xi_1, \xi_2) = d$
 $\Rightarrow \|\xi_1 - \xi_2\| = \sqrt{d}$ (Pythagoras)

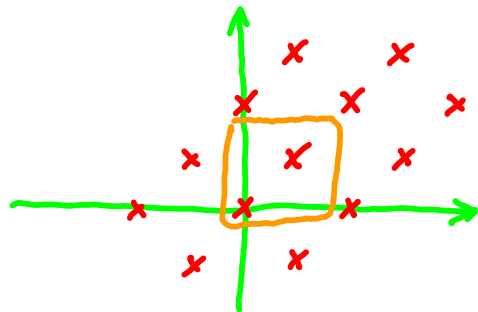
2) If \mathcal{C} is a linear (n, k, d) code ($M = 2^k$)

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



non lattice

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



lattice

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

Construction A : Properties

$$1) d_{\min}^E(\Gamma) \triangleq \min \text{Euclidean distance} \triangleq \min_{\substack{x, y \in \Gamma \\ x \neq y}} \|x - y\|$$

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

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.

Def. IV

$$\Rightarrow \Gamma_{\mathcal{C}} = \left\{ \underline{w} \cdot \underline{G} + 2\mathbb{Z}^n : \underline{w} \in \{0, 1\}^k, \mathbb{Z} \in \mathbb{Z}^n \right\}$$

mod-2 or real multiplication (due to $2\mathbb{Z}^n$ term)

where $\underline{G} = \begin{bmatrix} \underline{g}_1 \\ \vdots \\ \underline{g}_k \end{bmatrix} = (k \times n)$ generator matrix for \mathcal{C} .

Construction A : Properties

$$1) d_{\min}^E(\Gamma) \triangleq \min \text{Euclidean distance} \triangleq \min_{\substack{x, y \in \Gamma \\ x \neq y}} \|x - y\|$$
$$= \min \{2, \sqrt{d}\}$$

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

$$d_H(\xi_1, \xi_2) = d$$
$$\Rightarrow \|\xi_1 - \xi_2\| = \sqrt{d} \text{ (Pythagoras)}$$

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.

Example 1: Construction A of Gosset lattice E8
via extended $(8, 4, 4)$ Hamming code.

Example 2: Trellis-Coded Modulation (\mathcal{C} = convolutional code)
[Ungerboeck 1982]

3) Extension to p -ary (linear) codes ("mod- p lattices")

Construction C

- * "Multi-level coded modulation"
- * Natural extension (?) of construction A to L levels
- * Bound on minimum distance $2 \rightarrow 2^{L-1}$
- * Super-position of L binary codes: C_1, \dots, C_L

$$\Gamma = C_1 + 2 \cdot C_2 + 4 \cdot C_3 + \dots + 2^{L-1} \cdot C_L + 2^L \cdot \mathbb{Z}^n$$

- * Equivalent definitions:

binary expansion

$$\{ \underline{x} \in \mathbb{Z}^n : \text{LSB}(\underline{x}) \in C_1, \text{MSB}_1(\underline{x}) \in C_2, \dots, \text{MSB}_{L-1}(\underline{x}) \in C_{L-1} \}$$



recursive law

$$\left\{ \underline{x} \in \mathbb{Z}^n : \begin{aligned} \hat{c}_1 &\triangleq \underline{x} \bmod 2 \in C_1 \\ \hat{c}_2 &\triangleq \frac{1}{2}(\underline{x} - \hat{c}_1) \bmod 2 \in C_2 \\ \hat{c}_3 &\triangleq \frac{1}{4}(\underline{x} - \hat{c}_1 - 2\hat{c}_2) \bmod 2 \in C_3 \\ &\vdots \\ \hat{c}_L &\triangleq \frac{1}{2^{L-1}}(\underline{x} - \hat{c}_1 - 2\hat{c}_2 - 4\hat{c}_3 - \dots) \bmod 2 \in C_L \end{aligned} \right\}$$

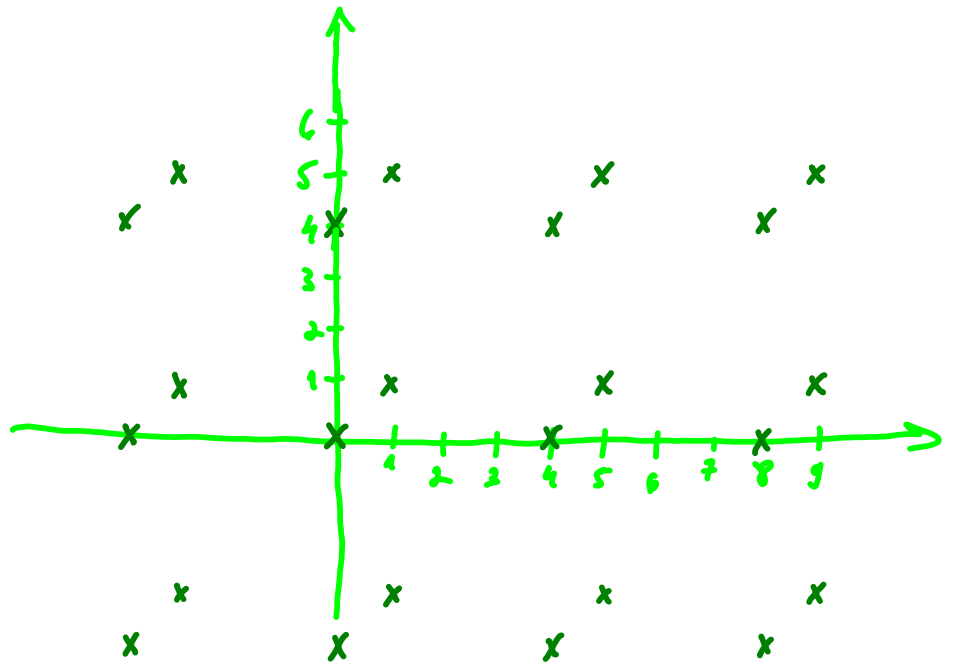
Construction C : general context

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

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

$$C_2 = \{(00)\}$$

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



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

Special case where

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

Construction C : basic properties

1) Unique decomposition for $\underline{x} \in \Gamma$:

$$\underline{x} = \underline{c}_1 + 2\underline{c}_2 + \dots + 2^{L-1}\underline{c}_L + \underline{z}, \quad c_j \in \mathcal{C}_j, \quad \underline{z} \in \mathbb{Z}^n$$

2) Distance improvement (monotonic with L):

$$\|\underline{x} - \underline{y}\| = \underbrace{\|c_{x1} - c_{y1}\|}_{\in \{-1, 0, +1\}} + 2 \cdot \underbrace{\|c_{x2} - c_{y2}\|}_{\in \{-2, 0, +2\}} + 4 \underbrace{\|z_x - z_y\|}_{\in \{0, \pm 4, \pm 8, \dots\}} \geq \|c_{x1} - c_{y1}\|$$

2 levels

⇒ Upper levels retain distance (if equal) or increase distance (if different) but never decrease it !

3) Equi - minimum distance property $\forall \underline{x} \in \Gamma$:

$$d_{\min}^E(\underline{x}) = \min \left\{ \sqrt{d_1}, \dots, 2^{L-1} \sqrt{d_L}, 2^L \right\}, \quad d_i = d_{\min}^{\text{Hamming}}(\mathcal{C}_i)$$

achieved when all levels but one are equal.

4) Balanced Hamming distances:

$$d_i = \frac{d_1}{4^{i-1}} \Rightarrow d_{\min}^E(\Gamma) = \min \left\{ \sqrt{d_1}, 2^L \right\} = 2^L$$

$d_1 = 4^L$

⇒ maximum point density per minimum distance.

Construction G: more properties

5) Point density:

$M = M_1 \cdot M_2 \cdot \dots \cdot M_L$ codewords per a $[2^L \times \dots \times 2^L]$ cube.

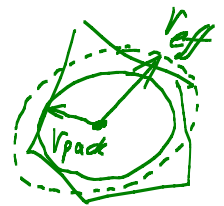
For linear component codes, $M_i = 2^{k_i} = 2^{nr_i}$, $i=1 \dots L$

$\Rightarrow \bar{V} = \text{average cell volume} = \frac{2^{nL}}{M} = 2^{n \cdot \sum_{i=1}^L (1-r_i)}$

6) Packing efficiency $\rho_{\text{pack}} \triangleq \frac{r_{\text{pack}}}{r_{\text{eff}}}$:

$r_{\text{pack}} = d_{\text{min}}/2$

$r_{\text{eff}} = \sqrt[n]{V/V_n}$



Assume balanced linear codes ($L \rightarrow \infty$),

satisfying the Varshamov-Gilbert bound $\Rightarrow r_i \lesssim 1 - H_b(d_i/n)$
 \uparrow
 $n \gg 1$

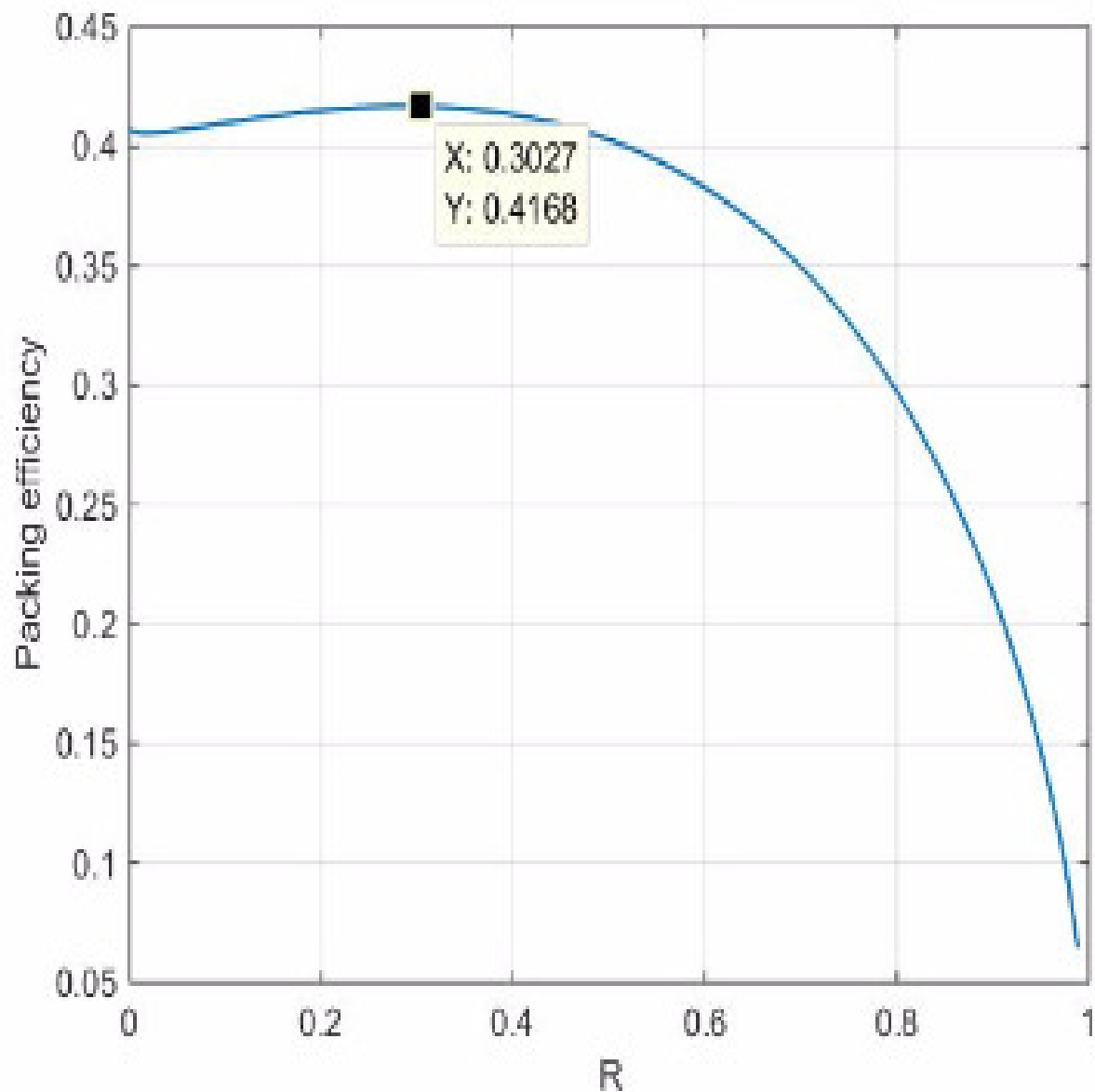
$\Rightarrow \rho_{\text{pack}}(\Gamma) \lesssim \frac{1}{2} \cdot \sqrt{2\pi e \cdot \alpha \cdot 2^{-2 \sum_{i=1}^{\infty} H_b(\alpha/4^{i-1})}} \approx 0.42$

$n \gg 1$
 $L \rightarrow \infty$
 $d_n = \alpha \cdot n$
 $r_i \approx 1 - H_b\left(\frac{\alpha}{4^{i-1}}\right)$

$\alpha = 0.11$
 $(r_1 = 1/2)$

\Rightarrow close to maximum known packing efficiency for large n (Minkowski bound) !

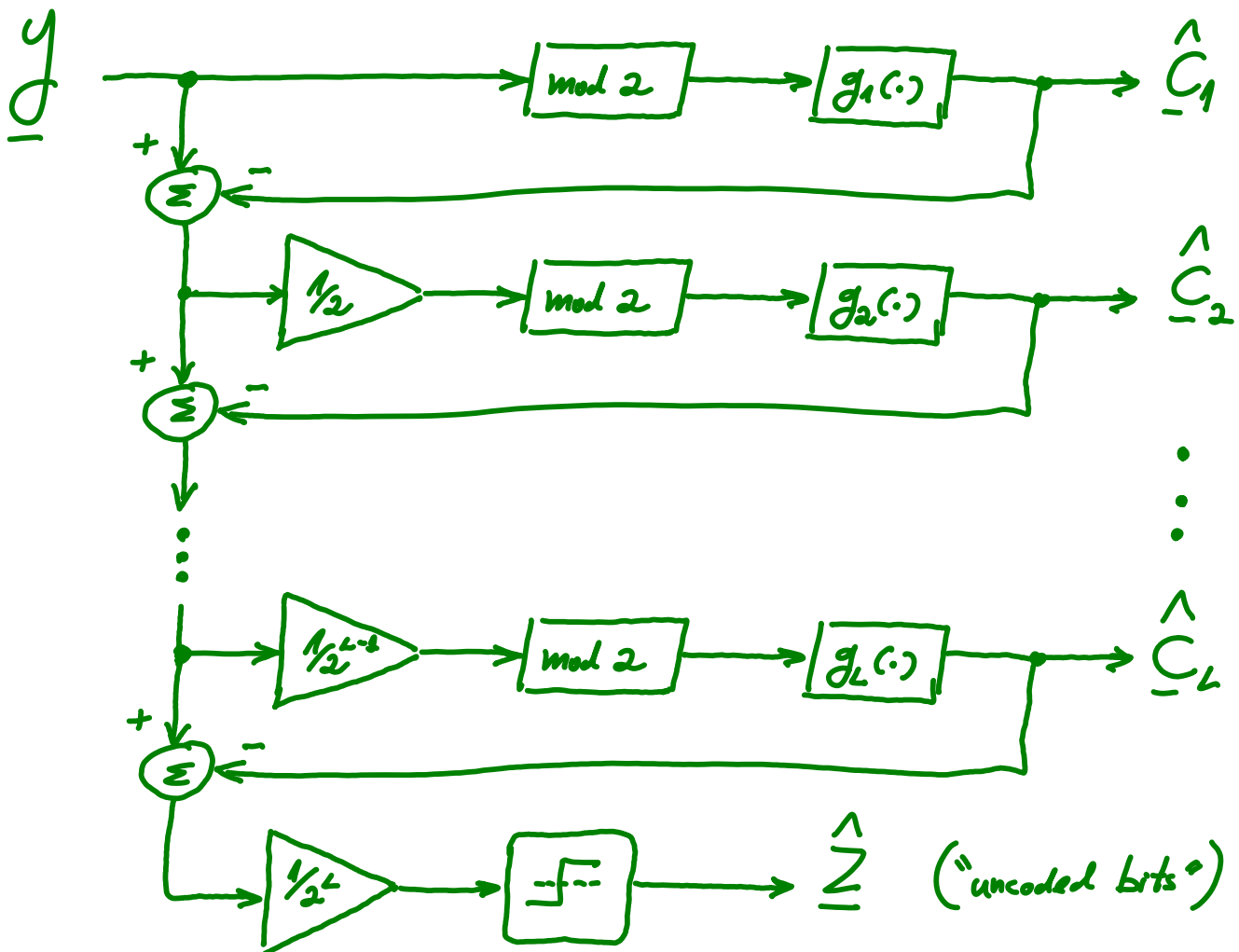
$\rho_{\text{pack}}(r_c)$ as a function of $r_1 = 1 - H_2(\alpha)$



Multi-Stage Decoding

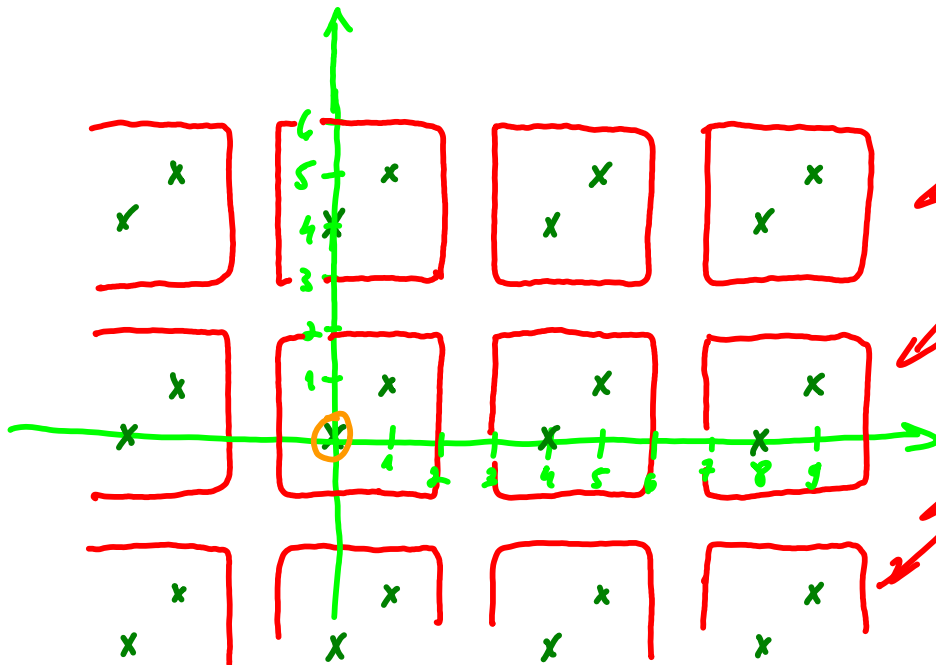
$$\underline{y} = \underline{x} + \underline{N}, \quad \underline{x} \in \mathcal{V}$$

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



Multi-Stage Decoding

$$\underline{Y} = \underline{X} + \underline{N}, \quad \underline{x} \in \mathcal{V}$$



regions where
 $\hat{X}_{-NN} = \hat{X}_{-MSD}$,
 given $\underline{X} = \underline{0}$.

Not optimal, nevertheless...

* Forney-Trott-Chung 2000:

Construction G with MSD can achieve the high-SNR AWGN channel capacity as $n \rightarrow \infty$.
 (L is tuned to SNR level)

When Construction G is a lattice?

* Binary addition: $a, b \in \{0,1\} \Rightarrow a+b = (a+b) \bmod 2 + \underbrace{2a \cdot b}_{\text{"carry"}}$

* Linearity of construction A:

$\underline{x}, \underline{y} \in \Lambda_C \triangleq C + 2\mathbb{Z}^n$, where C is a linear code.

$$\Rightarrow \underline{x} + \underline{y} = (c_x + 2z_x) + (c_y + 2z_y) = \underbrace{(c_x + c_y) \bmod 2}_{\in C} + \underbrace{2(c_x \odot c_y + z_x + z_y)}_{\in 2\mathbb{Z}^n} \in \Lambda_C$$

* Const. C is not always linear (even if component codes are):

$\underline{x}, \underline{y} \in \Gamma \triangleq C_1 + 2C_2 + 4\mathbb{Z}^n$ (2 levels)

$$\begin{aligned} \Rightarrow \underline{x} + \underline{y} &= (c_{x1} + 2c_{x2} + 4z_x) + (c_{y1} + 2c_{y2} + 4z_y) \\ &= \underbrace{(c_{x1} + c_{y1}) \bmod 2}_{\in C_1} + \underbrace{2c_x \odot c_y}_{\text{"problem"}} + \underbrace{2(c_{x2} + c_{y2}) \bmod 2}_{\in 2C_2} + \underbrace{4c_{x2} \odot c_{y2} + 4(z_x + z_y)}_{\in 4\mathbb{Z}^n} \end{aligned}$$

$\therefore \underline{x} + \underline{y} \notin \Gamma$, unless C_2 is closed under products in C_1 :
 $c_x \odot c_y \in C_2 \quad \forall c_x, c_y \in C_1$ [Kositwattanakorn-Oggier 14].

* Example: If $C_1 \subset \dots \subset C_L$ is a chain of Reed-Muller codes, then $\Gamma = \Lambda_{BW}$ is the Barnes-Wall lattice.

So ... what can we say when
construction C is not a lattice? ...

\wedge X

GU ?

EDS ?

EMD ✓

EKN ?



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:
 $C_1 \subset \dots \subset C_L$, where $C_j = (n, k_j, d_j)$ code, $k_1 \leq \dots \leq k_L$
- * Super-position of basis vectors (rather than of the codes)
- * Let $\underline{g}_1 \dots \underline{g}_n$ be a basis for $\{0, 1\}^n$, such that the $k_j \times n$ matrix $\underline{G}_j = \begin{bmatrix} -\underline{g}_1 \\ \vdots \\ -\underline{g}_{k_j} \end{bmatrix}$ is a generator matrix for C_j , $j=1 \dots L$.

real (not modulo 2) multiplication

$$\Lambda_D = \left\{ \sum_{j=1}^L 2^{j-1} \cdot \underline{w}_j \cdot \underline{G}_j + 2^L \underline{z} : \begin{array}{l} \underline{w}_j \in \{0, 1\}^{k_j} \\ j=1 \dots L \end{array}, \underline{z} \in \mathbb{Z}^n \right\}$$

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

Construction D versus C

* Similar form: replication by $2^L \mathbb{Z}^n$ of

$$\left[\sum_{j=1}^L 2^{j-1} \left(\frac{w_j}{\underline{g}_j} \cdot \underline{g}_j \pmod{*} \right) \right] \pmod{2^L}$$

mod 2 for Γ
no modulo (real multiplication) for Λ_D

* Similar features:

* upper levels can only increase distance

$$\Rightarrow d_{\min}^E(\Lambda_D) = \min\{\sqrt{d_1}, \dots, 2^{L-1}\sqrt{d_L}, 2^L\} \equiv d_{\min}^E(\Gamma)$$

* Unique decomposition: $x = w_1 \underline{g}_1 + \dots + 2^{L-1} w_L \underline{g}_L + 2^L z$

$$\Rightarrow V(\Lambda_D) = \text{cell volume} = 2^n \prod_{j=1}^L (1 - r_j) \equiv V(\Gamma)$$

* achieves AWGN capacity w MSD, as $n \rightarrow \infty$.

* Λ_D is always a lattice

* Given $\underline{c}_1, \dots, \underline{c}_L$, Λ_D may depend on the selected basis
 $\underline{g}_1, \dots, \underline{g}_L$

* If code chain is closed under products, then
 Λ_D is unique = Γ [Kositumtanavek-Oggier 14].

So ... how close to a lattice can
construction G get ? ...

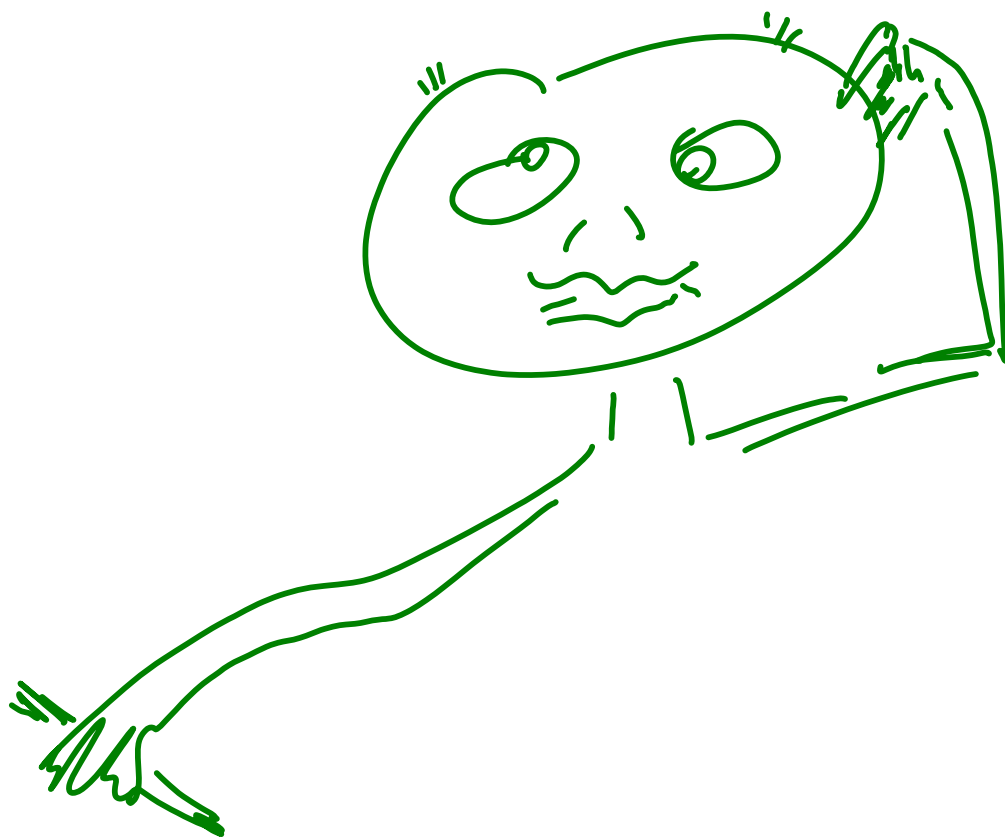
Λ \times

GU ?

EDS ?

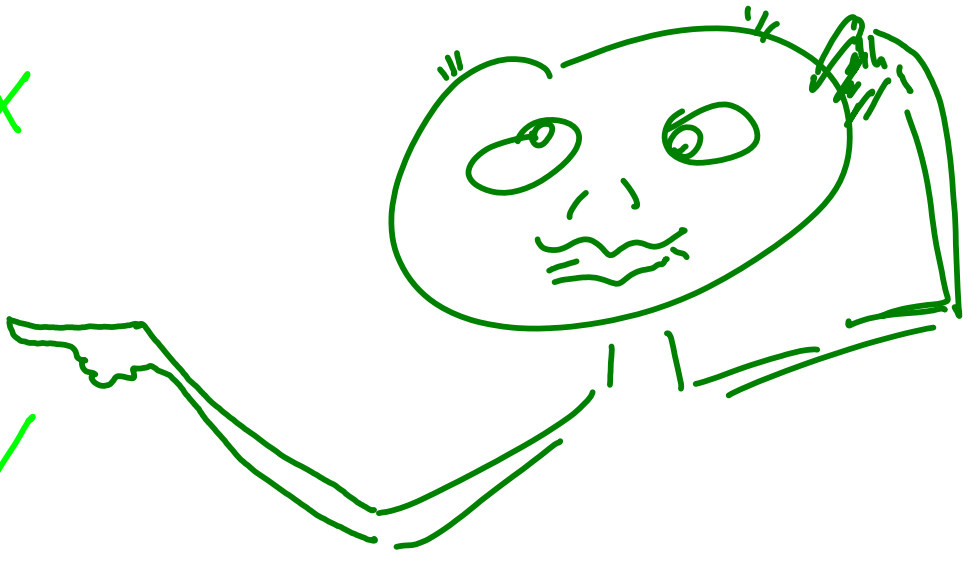
EMD \checkmark

EKN ?



So ... how close to a lattice can construction G get ? ...

- Λ X
- GU ?
- EDS
- EMD \checkmark
- EKN ?



Construction Γ is EDS for $L=2$ linear levels
 (EDS = equi distance spectrum)

Def (equal vectors up to sign of some components):

$$(a_1 \dots a_n) \stackrel{||}{=} (b_1 \dots b_n) \quad \text{if } |a_i| = |b_i| \quad i=1 \dots n.$$

Lemma: Consider $\Gamma = C_1 + 2C_2 + 4\mathbb{Z}^n$, where C_1, C_2 -linear.

Then, for any $\underline{x}, \underline{y}, \underline{x}' \in \Gamma$, there exist $\underline{y}' \in \Gamma$

s.t. the error vectors $\underline{y}' - \underline{x}'$ and $\underline{y} - \underline{x}$ are equal up to signs: $\underline{y}' - \underline{x}' \stackrel{||}{=} \underline{y} - \underline{x}$. Furthermore, for $\underline{x}, \underline{x}' \in \Gamma$

and \underline{e} , the number of \underline{y}' 's for which $\underline{y}' - \underline{x}' \stackrel{||}{=} \underline{e}$ is equal to the number of \underline{y} 's for which $\underline{y} - \underline{x} \stackrel{||}{=} \underline{e}$.

Corollary: The distance spectrum is identical for all codewords in Γ : $N(c, d) = N(d) \quad \forall c \in \Gamma$.

proof: First, choose component linear codes of \underline{y} such that:

$$C_{y_1} \oplus C_{x'_1} = C_{y_1} \oplus C_{x_1} \quad , \quad C_{y_2} \oplus C_{x'_2} = C_{y_2} \oplus C_{x_2}$$

$$\text{Note that: } \Delta C \in \{-1, 0, +1\} + \{-2, 0, +2\} \in \{-3, -2, -1, 0, +1, +2, +3\}$$

$$\Delta 4Z \in \{\dots, -8, -4, 0, +4, +8, \dots\}$$

\Rightarrow Can choose \underline{z}' such that $|\Delta C' + 4\Delta Z'| = |\Delta C + 4\Delta Z|$. ■

Summary : what we know



what we think



and what we don't



Is it true also that for $L=2$ levels...

- * Construction C is GU?
- * All possible const. D lattices have the same spectrum?
- * Spectra of const. C and D are equal?
(for the same component codes)

Is it true that for $L \geq 3$ levels ...

- * Const. C is not GU? not EDS?
(unless it is a lattice - [K-0-14] condition)
- * Average spectrum of const. C \cong const D ?
(for the same component codes)
- * If not, is const. C at least EKN?

Finally, is const. D better than C
(for the same component codes)? in what sense?

The End

