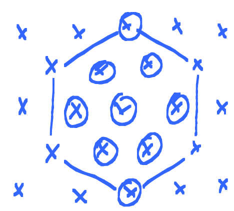
Tutorial - Part A Outline

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



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

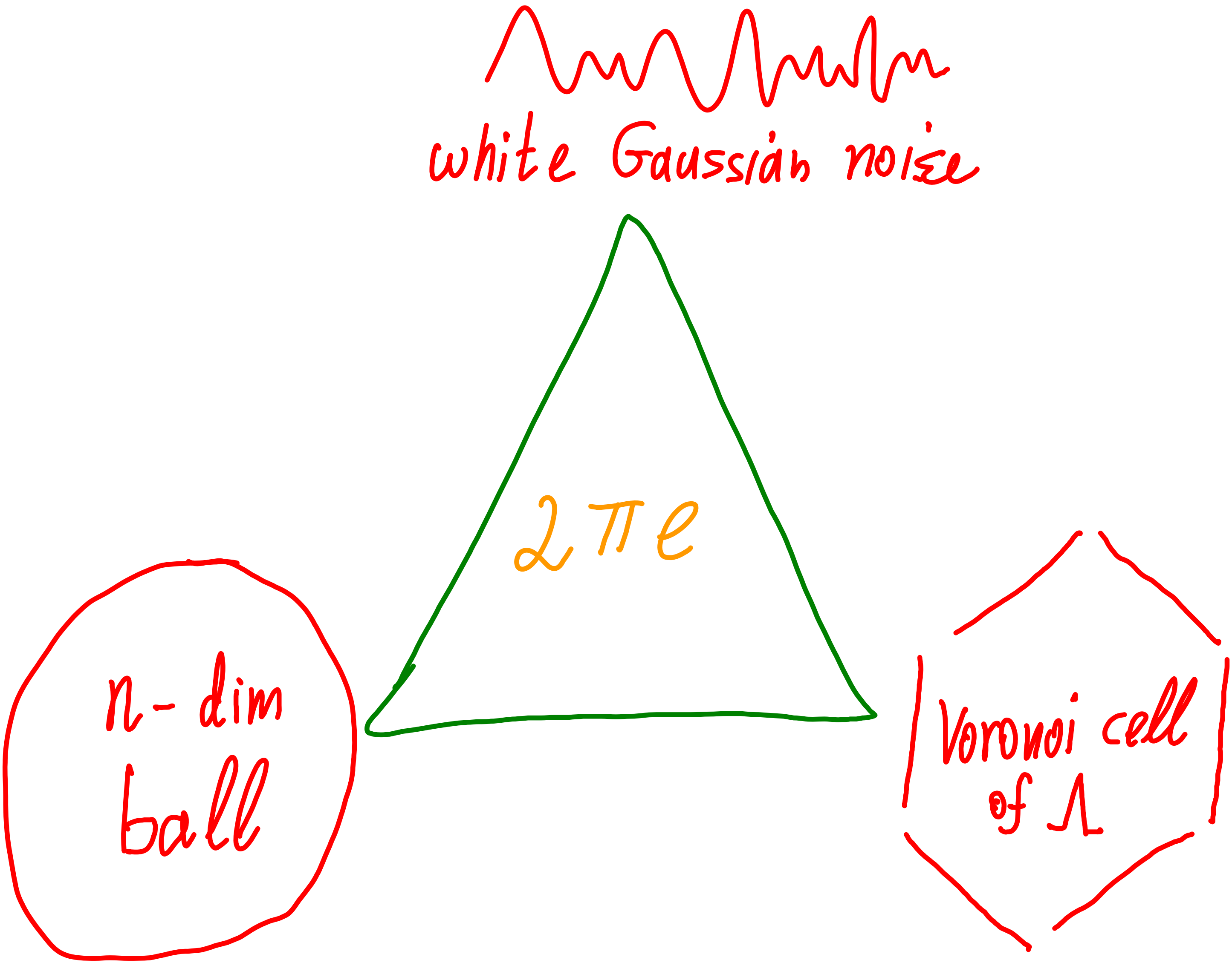
Tutorial - Part A Outline

6. Asymptotic goodness

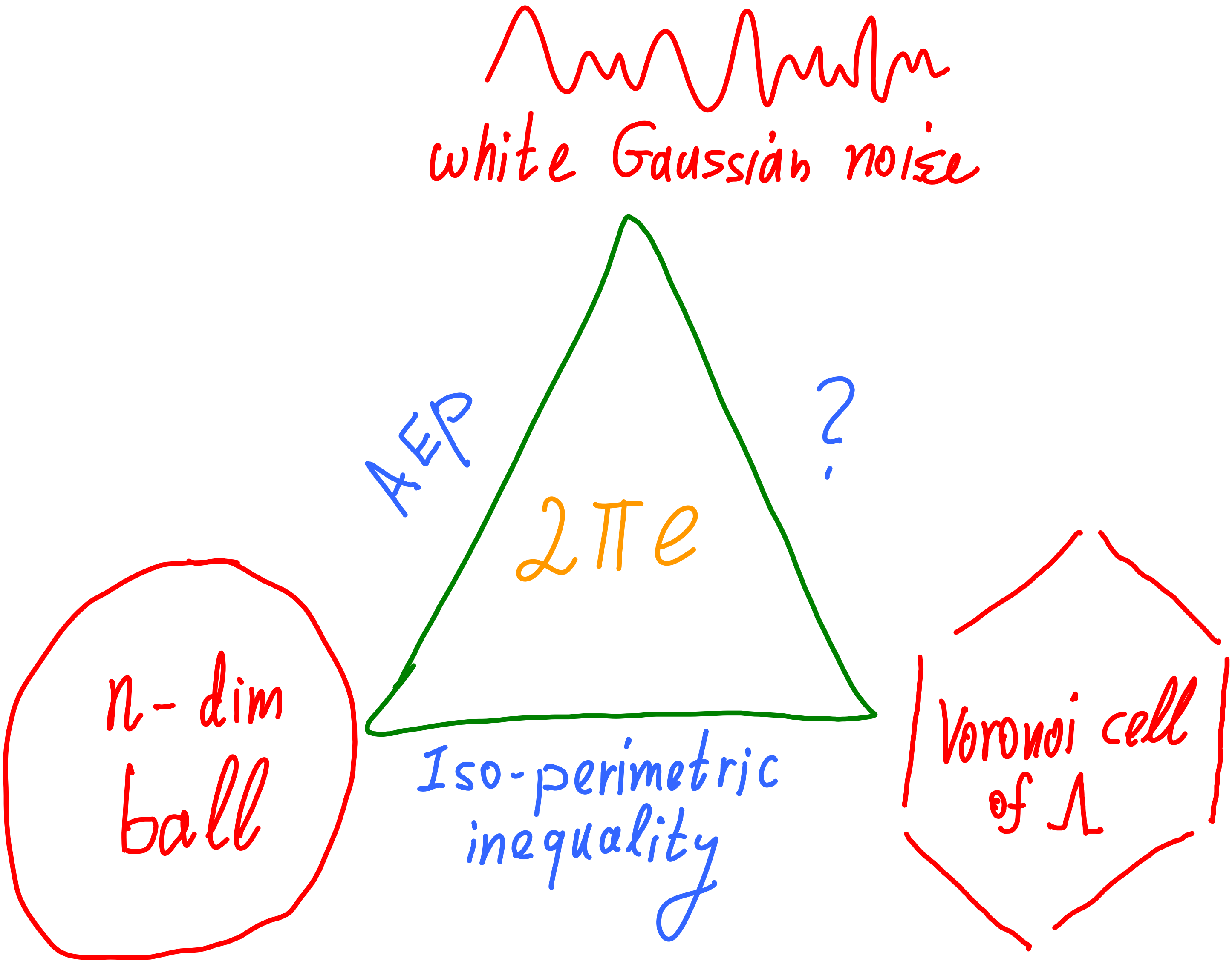
$$G(\Lambda_n) \xrightarrow{?} \frac{1}{2\pi e}, \text{ as } n \to \infty$$

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

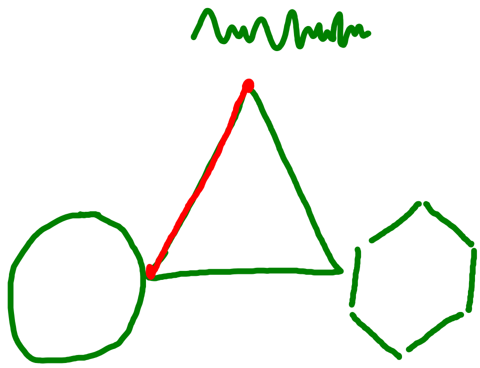
W.G.N. $\longleftrightarrow$ Ball $\longleftrightarrow$ Λ



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



Shannon's AEP:



W.G.N. $\longrightarrow$ ball

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

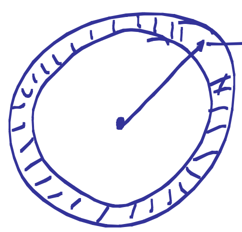
AWGN

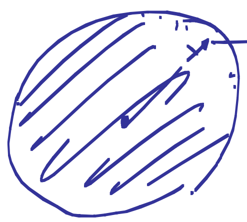
$f_Z \sim e^{-\frac{\|z\|^2}{2\sigma^2}}$

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

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

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

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

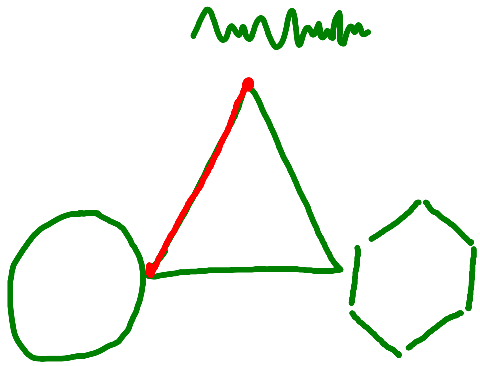
$\cong$  $\sqrt{n\sigma^2}$

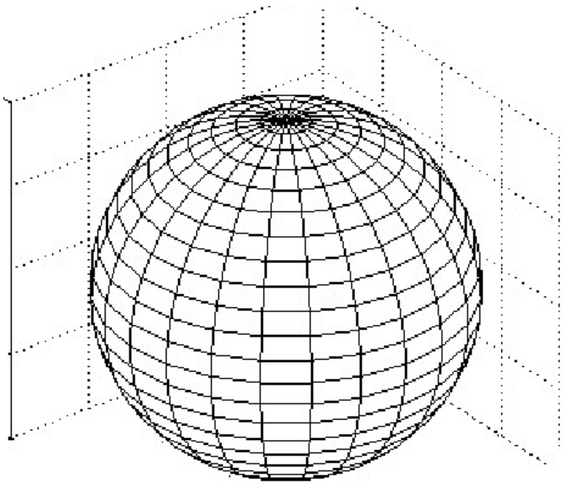
$\triangleq r_{noise}$

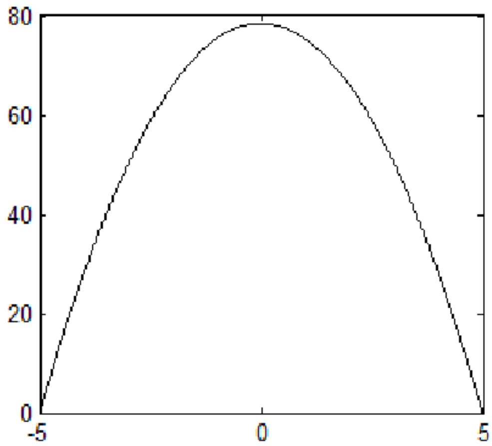
Thm. [AEP]: AWGN $\approx \mathrm{Unif}\left(B(\underline{0}, \sqrt{n\sigma^2})\right)$

"Reverse" AEP:

W.G.N. $\longleftarrow$ ball





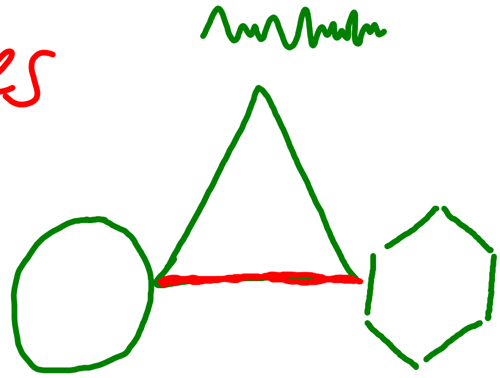


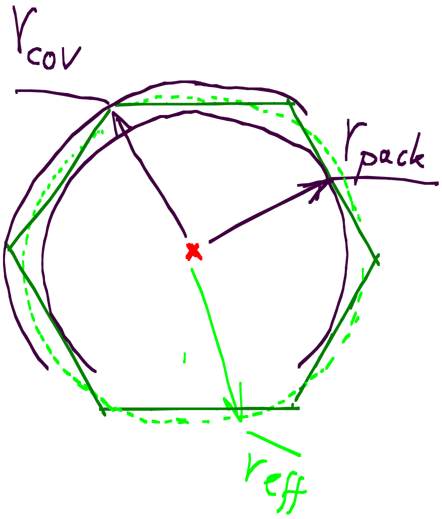
Thm. [Reverse AEP]:

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

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

Iso-perimetric Inequalities
(Sphere bounds)





Ball minimizes

* * *

over all bodies

of a fixed volume!

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

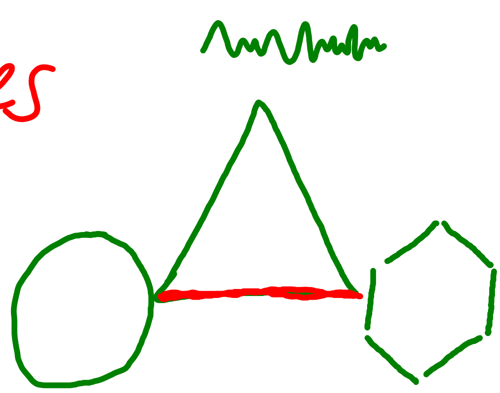
$$Pe(\Lambda) \ge Pe(\text{" " " "})$$

$\Longrightarrow$

$G(\Lambda) \ge$ N.S.M. of n-dim ball

$\mu(\Lambda, pe) \ge$ V.N.R. " " "

Iso-perimetric Inequalities



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

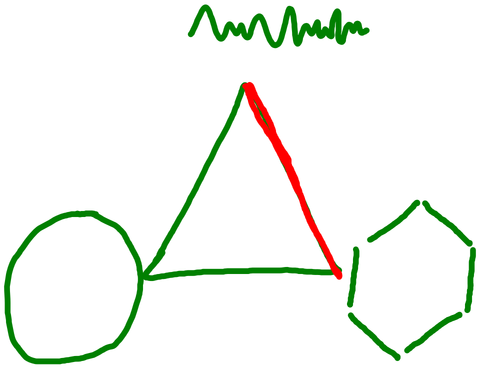
$$\mu(\Lambda, p_e) \geq \mu_n(\text{Ball}, p_e)$$

Asymptotic sphere bounds:

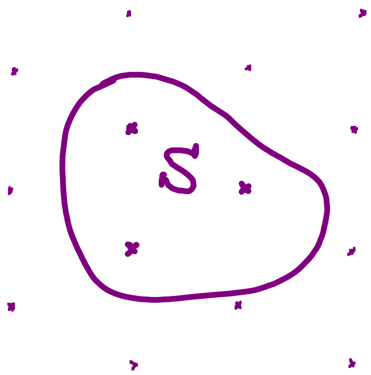
$$G_n(\text{Ball}) \longrightarrow \frac{1}{2\pi e} \quad \text{as} \quad n \to \infty$$

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

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

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

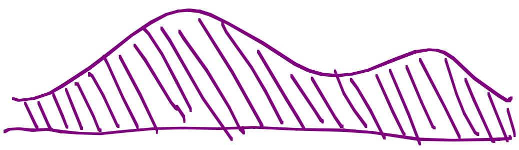
Just like a uniformly distributed random code!

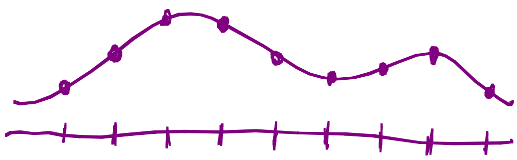
Minkowski - Hlawka - Siegel

$\Longrightarrow$

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

$$\underbrace{\text{integral}}_{\textstyle \| \atop \textstyle \int_{\mathbb{R}^n} f(x)\,dx} = \frac{1}{\gamma}\cdot E_{MHS}\left\{\underbrace{\text{lattice-samples sum}}_{\textstyle \| \atop \textstyle \sum_{\lambda\in\Lambda} f(\lambda)}\right\}$$



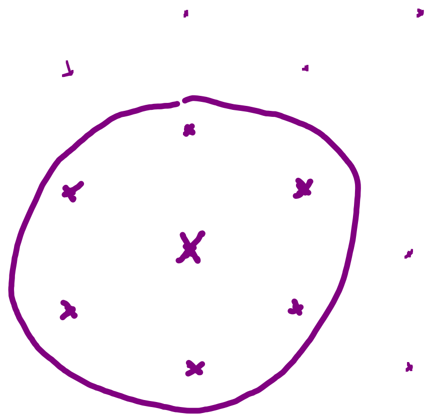


2. There exists (at least one) lattice which is (at least) as "good" as (1.)

Implication 1 : packing Goodness

$$S = Ball(0, r)$$

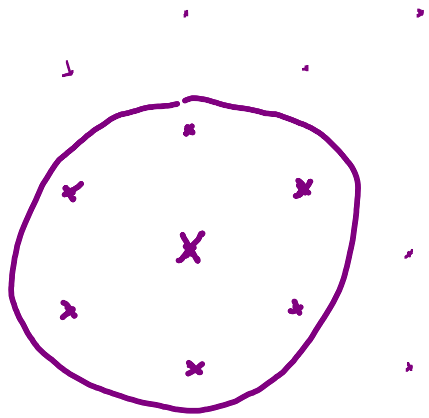
$$\boxed{E_{MHS}\left\{N_{\Lambda}(Ball)\right\} = \gamma \cdot V_n \cdot r^n}$$



Implication 1 : packing Goodness

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

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



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

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

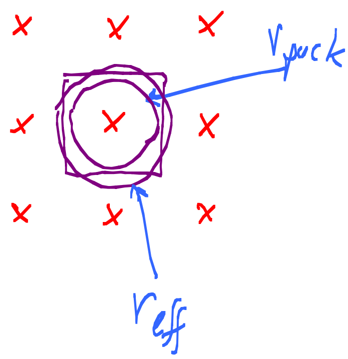
$\Longrightarrow \quad E\{N_\Lambda\} < 1$

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

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

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

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



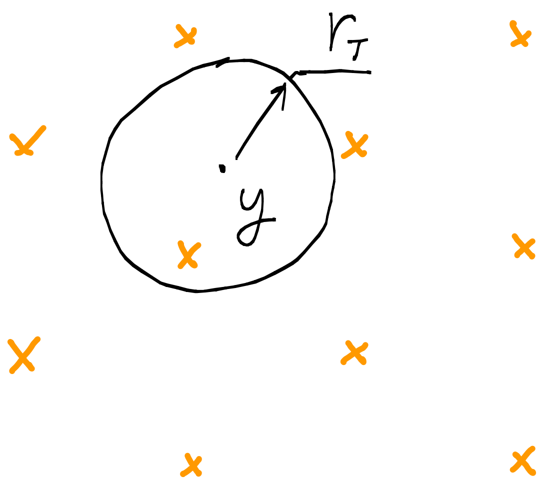
$(*) + (**) \Longrightarrow$ packing efficiency $= \dfrac{r_{pack}}{r_{eff}} \geq 1/2$

(for each dim n)

Implication 2: Modulation goodness

Theorem (achieving Poltyrev capacity):

$$\boxed{\exists\, \Lambda_n \text{ s.t. } \mu(\Lambda_n, P_e) \to 2\pi e, \quad n \to \infty.}$$



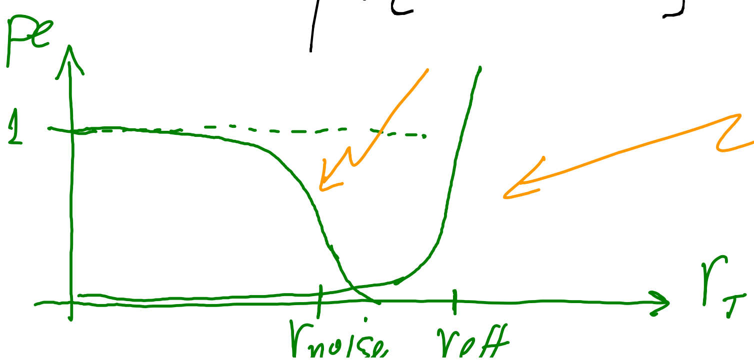
$$y = \lambda + Z$$

$$\hat{\lambda} = \begin{cases} \Lambda \cap Ball(y, r_T), & \text{if unique} \\ ?, & \text{if empty or non-unique} \end{cases}$$

where r_T = search radius ("threshold")

$$\Rightarrow \quad P_e = Pr\{\text{true } \lambda \text{ outside Ball OR other } \lambda \text{ inside Ball}\}$$

$$\leq Pr\{\|Z\| > r_T\} + N_\Lambda(Ball(Z, r_T))$$



$$\approx \gamma \cdot V_n \cdot r_T^n = (r_T / r_{eff})^n$$

Implication 3: Asymptotic Goodness
~ for Covering & Quantization ~

$\exists \Lambda_n$:

$$\rho_{cov}(\Lambda_n) \triangleq \frac{r_{cov}}{r_{eff}}(\Lambda_n) \xrightarrow[n\to\infty]{} 1$$ [Rogers 195*]

$$\Rightarrow \quad G(\Lambda_n) \longrightarrow \frac{1}{2\pi e}$$ [Poltyrev-Z-Feder 1995]

Note:

1. $\frac{1}{2\pi e}$ = Normalized Second Moment (Ball) $_{n\to\infty}$

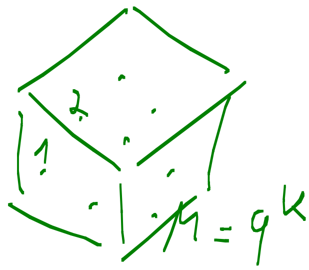
2. $\frac{1}{2}\log\left(2\pi e\, G(\Lambda)\right) = D\left(\mathrm{Unif}(\mathcal{V}_0) \,\|\, \mathrm{WGN}\right)$

$\Rightarrow$ Cell $\rightarrow$ Ball, unif(cell) $\rightarrow$ WGN

Alternative Ensemble:
Random Construction A (Loeliger97, Erez et al 2005)

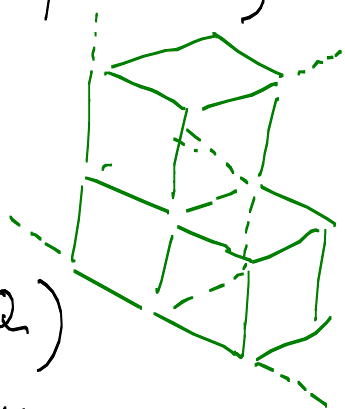
Let $\mathcal{C}$ = q-ary (n,k) liner code over $Q=\{0,\dots,q-1\}$

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



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

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



G random (iid uniform on Q)

$\Rightarrow$ $\Lambda_{\mathcal{C}}$ = <u>random</u> <u>lattice</u>

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

Simultaneous Goodness

Thm. [Erez - Litsyn - Z 2004]

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

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

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

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

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

Random Construction A:
How Large q, k, n Should Be?

good packing: $q, n \to \infty \quad , \quad 1 \le k \le n-1$

$\rho_{pack} \simeq 1/2$

good covering: $q, k, n \to \infty$

$\rho_{cov} \simeq 1$

good modulation:

$\mu(\Lambda, p_e) \simeq 2\pi e$

complete lattice → $q, n \to \infty \quad , \quad 1 \le k \le n-1$

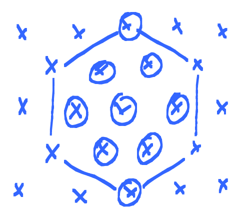
finite constellation (= cosets) → $n \to \infty \quad , \quad k \cdot \log(q) \propto n$

good quantization: $n \to \infty \quad , \quad k \cdot \log(q) \propto n$

$G(\Lambda) \simeq 1/2\pi e$

Tutorial - Part A Outline

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



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

Tutorial - Part A Outline

7. Error exponents

$E(\Lambda)$

Implication 2: Asymptotic Goodness for Modulation

[Gallager 1962]

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

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

$$N_\Lambda\big(Ball(\underline{z},r)\big)$$

Implication 2: Asymptotic Goodness for Modulation

[Gallager 1962]

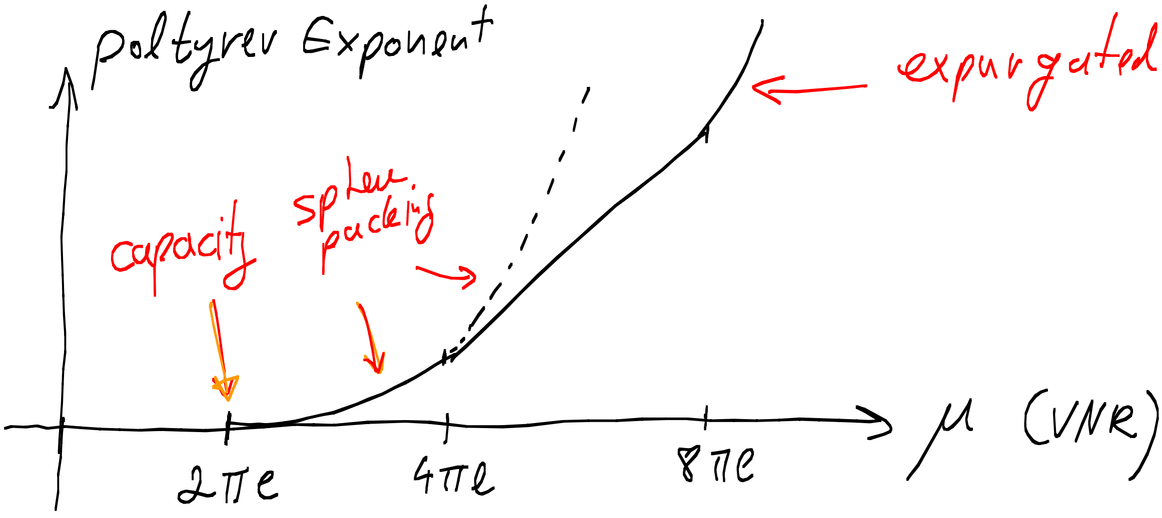
$$P_e^{ML}(\Lambda) = \int_0^\infty p(\|\underline{Z}\| = r)\cdot p\begin{pmatrix}\text{nonzero codeword}\\ \text{in Ball}(\underline{Z}, r)\end{pmatrix} dr$$

$$\wedge$$

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

$$\|$$

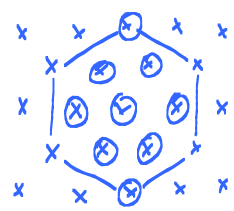
$$E_{MHS}\{\quad\} \Longrightarrow \quad \gamma\cdot V_n\cdot r^n$$



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

Tutorial - Part A Outline

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



9. Lattice (Voronoi-) shaping
10. Side-information problems — $Modulo^2(\Lambda)$
11. Gaussian networks — $Modulo^n(\Lambda)$

Tutorial - Part A Outline

8. Nested Lattices

$$\Lambda_2 \subset \Lambda_1$$

Nested Lattices

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

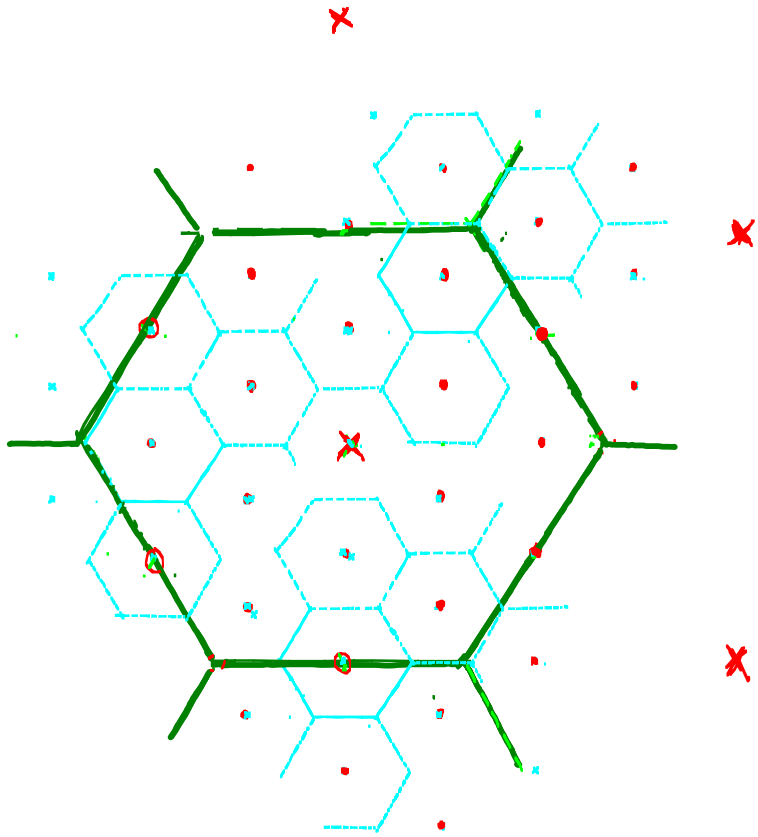
course lattice

fine lattice

integer matrix

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

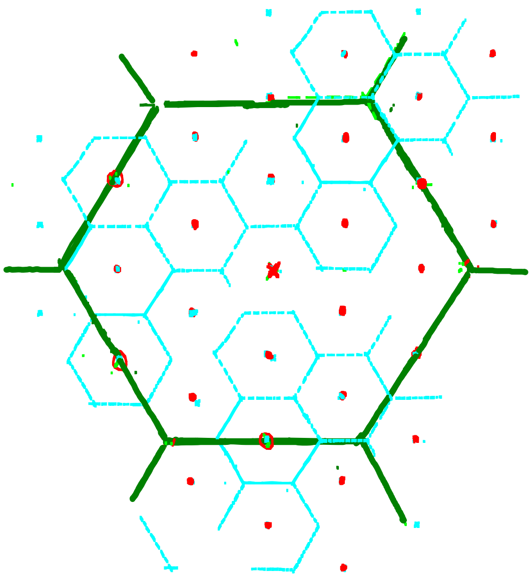
4:1

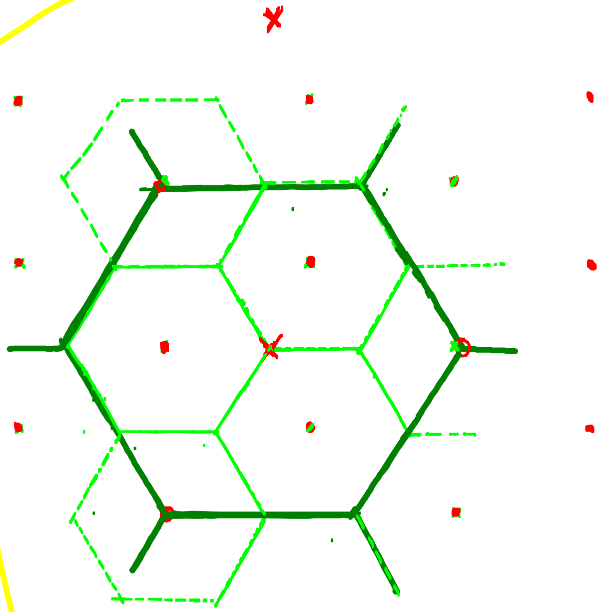


Not necessarily "Self Similar"!

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

Nested & Self Similar





Relatively Periodic
(non Nested)

Diagonal Form

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

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

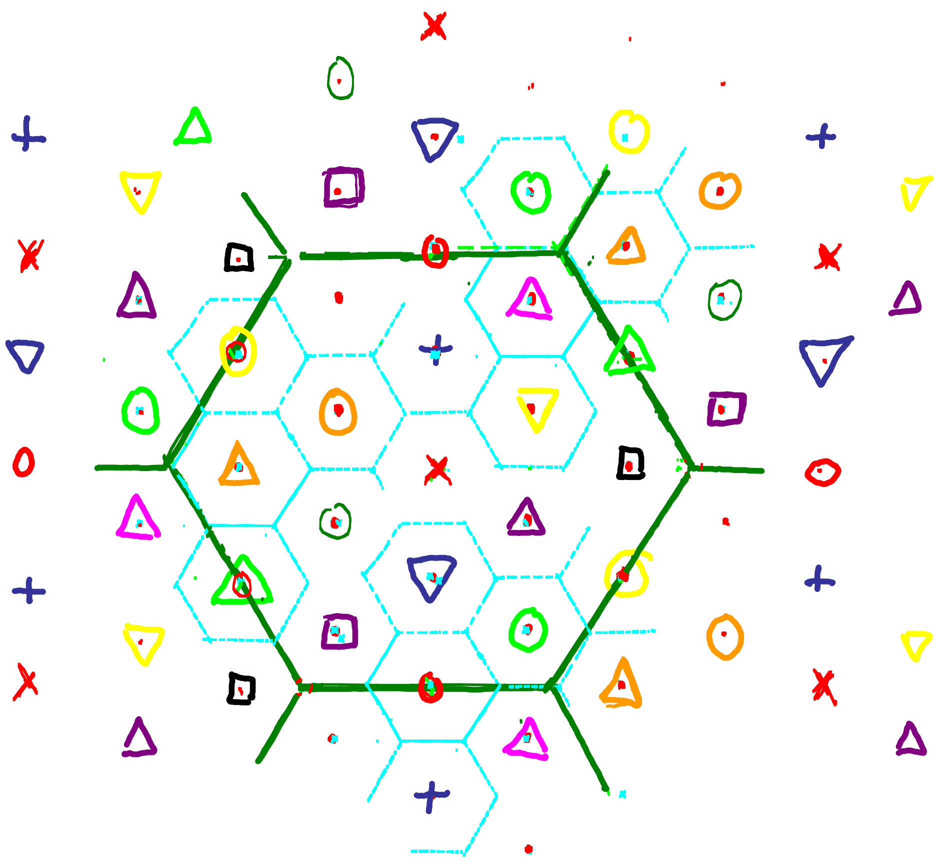
Nested Lattices

$$\Lambda_2 \subset \Lambda_1 \Rightarrow \underline{\underline{G}}_2 = \underline{\underline{G}}_1 \cdot \underline{\underline{J}}$$

Relative Cosets $= \Lambda_2 / \Lambda_1$

Coset $\triangleq l_1 + \Lambda_2$, for some $l_1 \in \Lambda_1$

$$|\Lambda_2 / \Lambda_1| = V_2 / V_1 = |\det(J)|$$



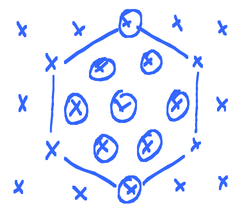
Open Question :

Good nested pairs ?

(low shaping & coding losses $\Rightarrow$
low $G(\Lambda_2) * \mu(\Lambda_1, p_e)$)

Tutorial - Part A Outline

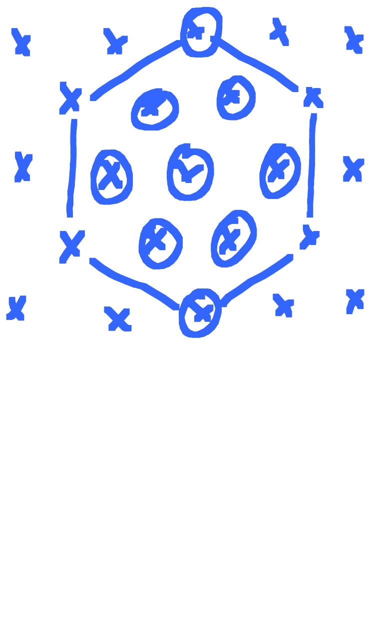
1. Definitions: Partition, Construction — $Vol(\Lambda)$, Modulo Λ
2. Figures of merit — $G(\Lambda)$
3. Dither & estimation — $noise(\Lambda)$
4. Entropy coding — $H(\Lambda)$
5. Infinite constellation — $Pe(\Lambda + noise)$
6. Asymptotic goodness — $(n \to \infty)$
7. Error exponents
8. Nested lattices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



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

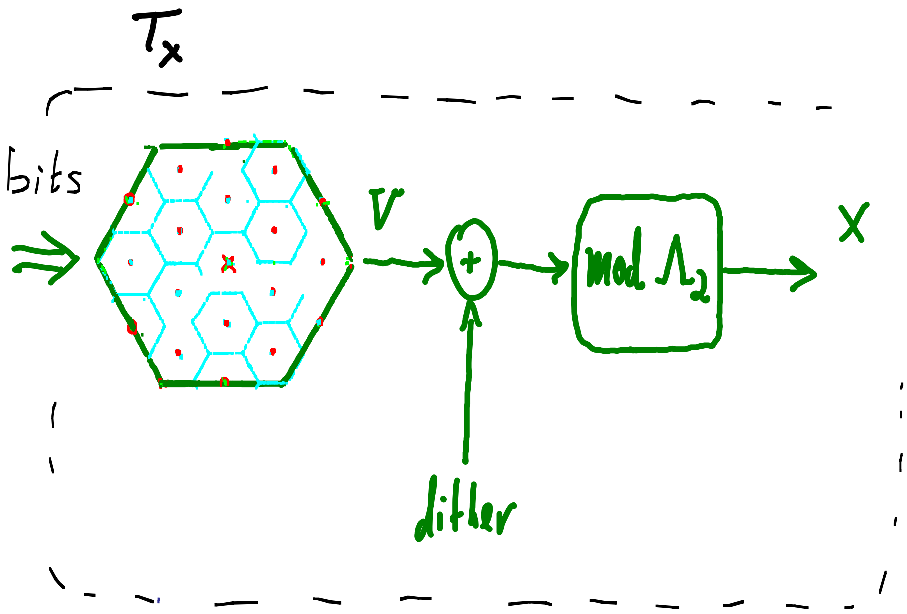
Tutorial - Part A Outline

9. Lattice (Voronoi-) shaping



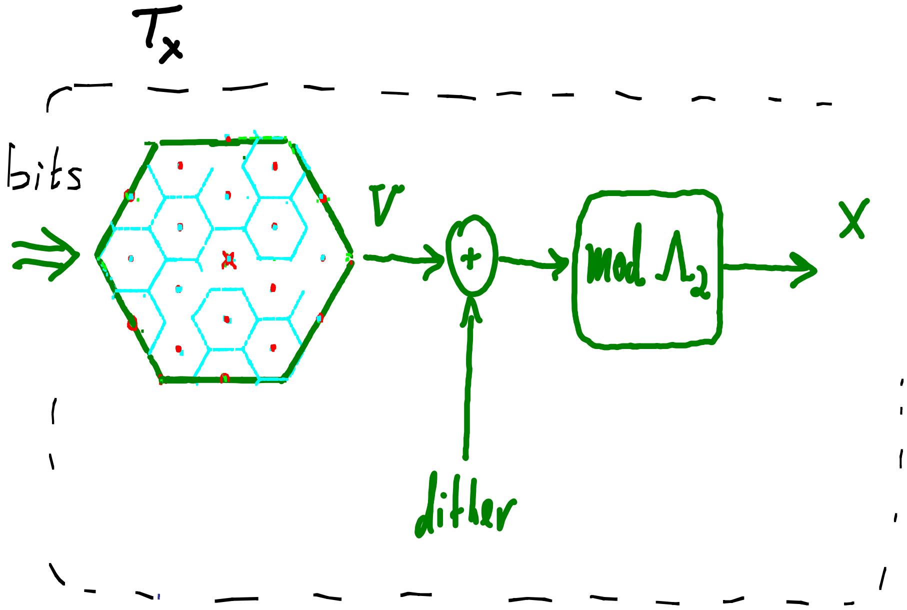
Dithered Voronoi Modulation

message = fine point in coarse fund. cell
$\Longleftrightarrow$ coset in Λ_1/Λ_2



transmitted vector = reduction to Voronoi cell
$\Longleftrightarrow$ min energy coset point

Dithered Voronoi Modulation

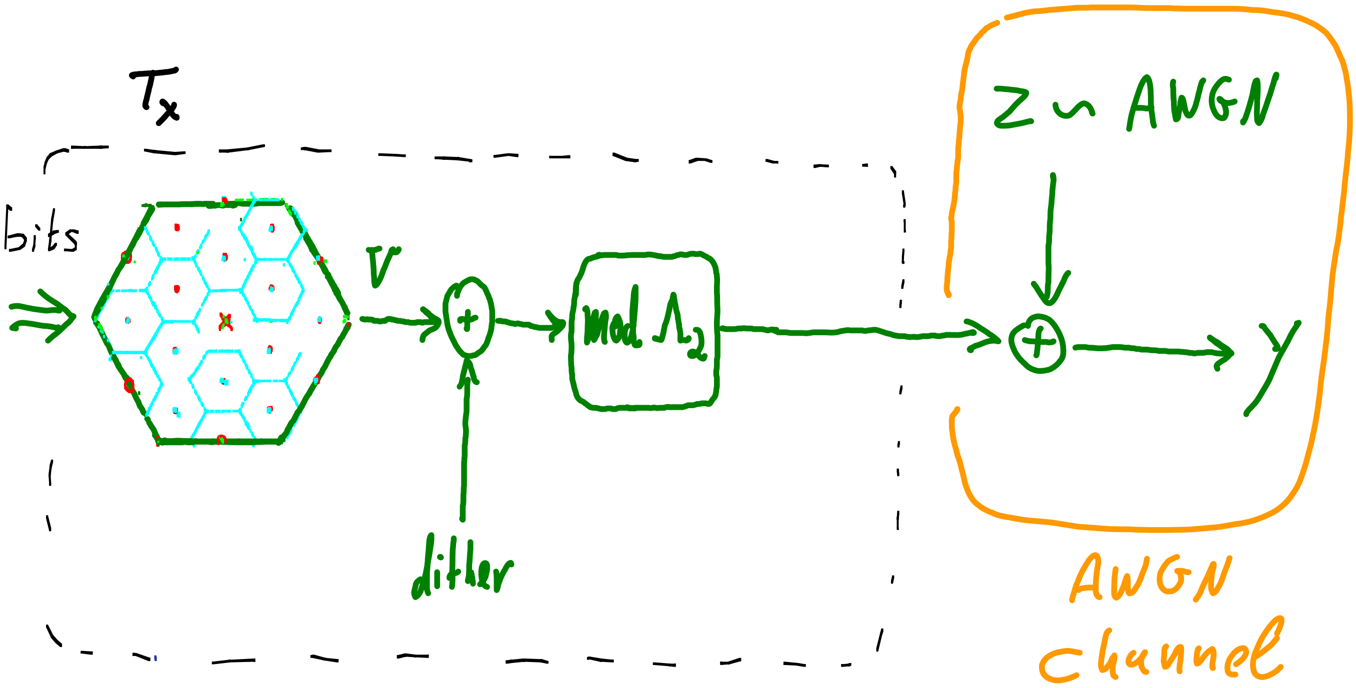


Crypto Lemma $\Rightarrow$ for any $v \in \mathcal{F}_\Lambda$:

$$X = [V + \text{dither}] \bmod \Lambda_2 \sim \text{Unif}(\mathcal{V}_0)$$

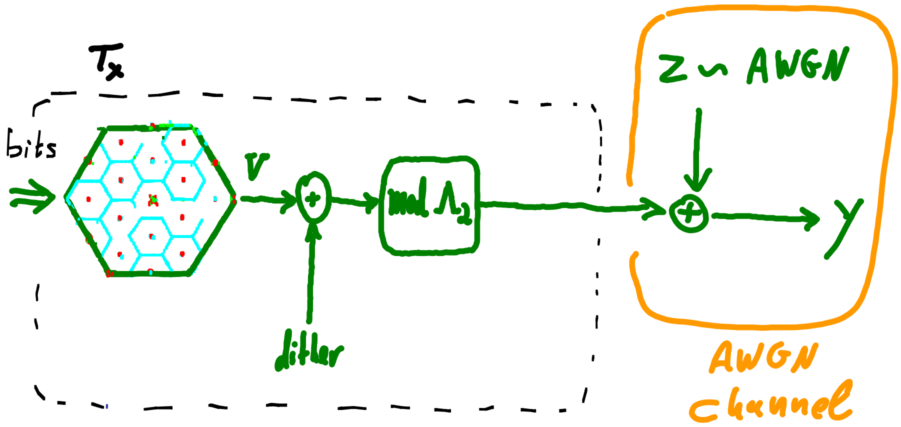
$\Rightarrow$ Tx Power $= \frac{1}{n} E\|X\|^2 = \sigma^2_{\Lambda_2}$

Dithered Voronoi Modulation: Decoding



Dithered Voronoi Modulation:

Decoding



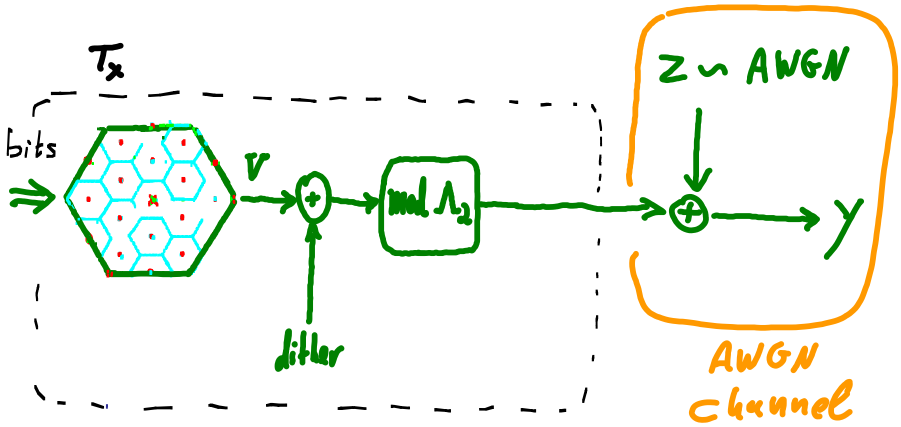
Maximum-Likelihood Decoding:

$$\hat{v}_{ML} = \underset{v \in \mathcal{C}_\Lambda}{\arg\max} \; \| y - [v + \text{dither}] \bmod \Lambda_2 \|$$

$\Rightarrow$ constrained search $\Rightarrow$ complex!

reduction to $\mathcal{V}_0$

Dithered Voronoi Modulation: Decoding



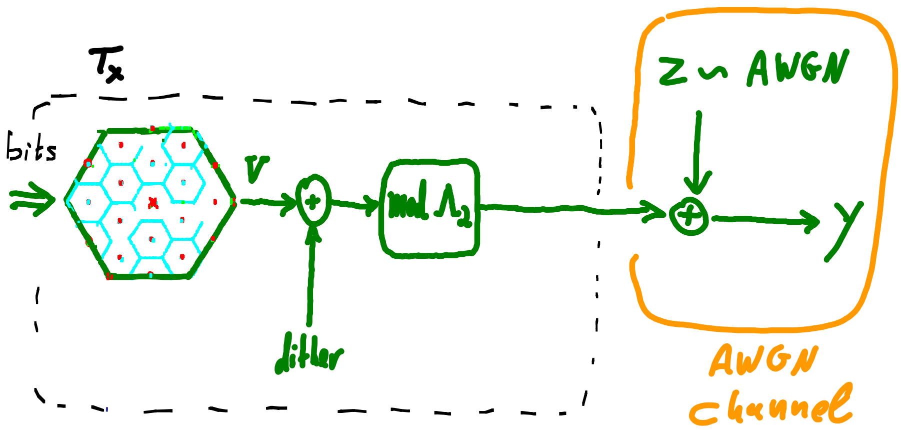
Maximum-Likelihood Decoding:

$$\hat{v}_{ML} = \underset{v \in \mathcal{C}_\Lambda}{\arg\max} \; \| y - [v + \text{dither}] \bmod \Lambda_2 \|$$

⇒ constrained search ⇒ complex!

reduction to $\mathcal{V}_0$

Dithered Voronoi Modulation: Decoding



Maximum-Likelihood Decoding:

$$\hat{v}_{ML} = \underset{v \in \mathcal{C}_\Lambda}{\arg\min} \; \| y - [v + \text{dither}] \bmod \Lambda_2 \|$$

$\Rightarrow$ constrained search $\Rightarrow$ complex!

Lattice Decoding:

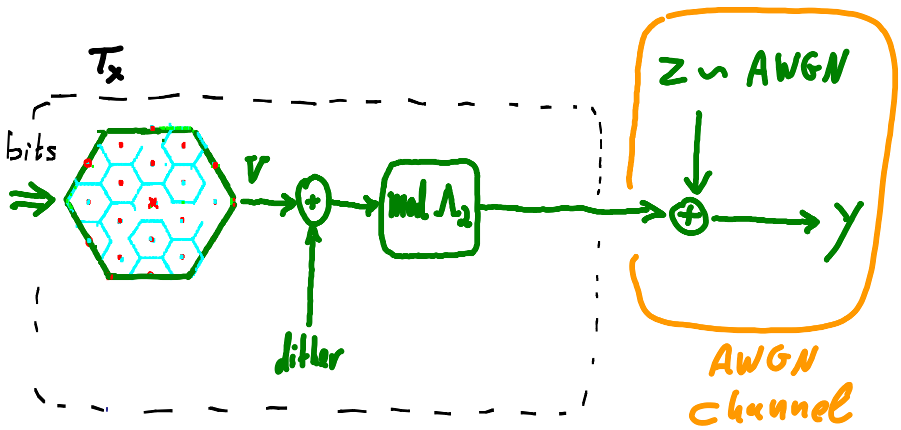
$$\hat{v}_{LD} = \left(\underset{\lambda \in \Lambda_1}{\arg\min} \; \| y - [\lambda + \text{dither}] \| \right) \bmod \Lambda_2$$

reduction to set of representatives

$\Rightarrow$ un-constrained search $\Rightarrow$ easier?

Dithered Voronoi Modulation:

Decoding



Coset Decoding:

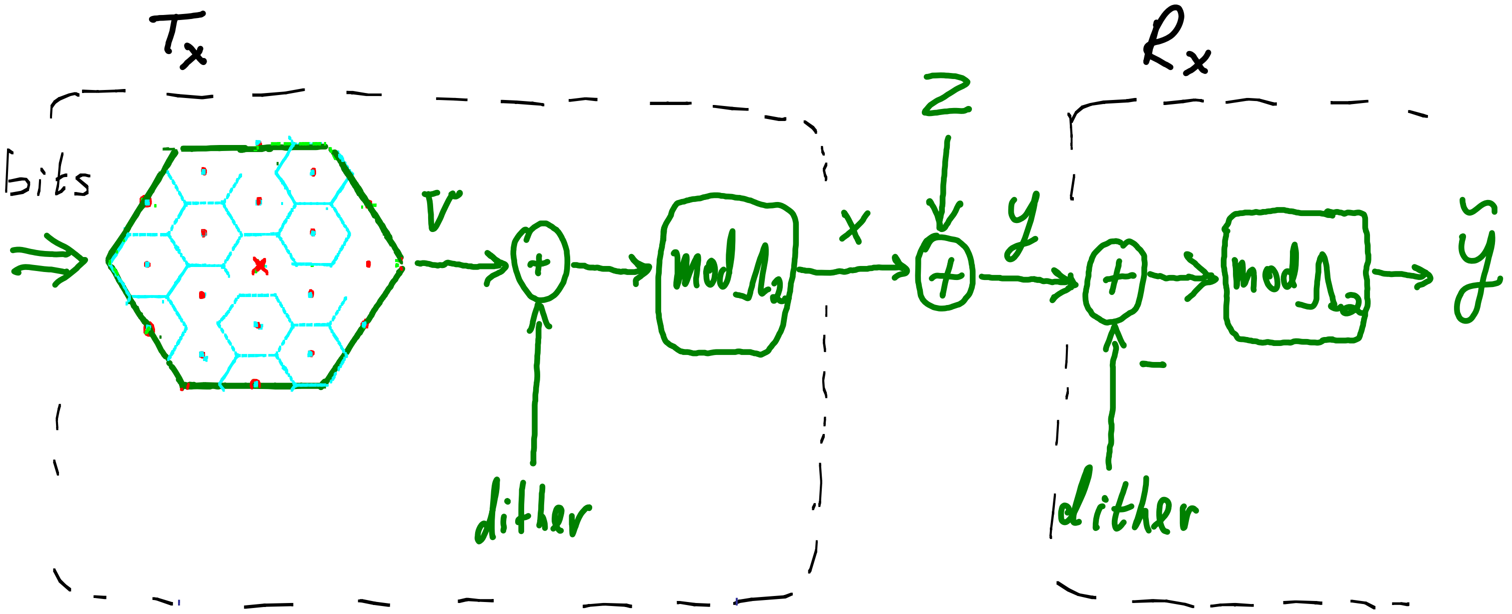
$$\hat{v}_{CD} = \underset{\text{coset} \in \Lambda_1/\Lambda_2}{\arg\max} \sum_{\lambda \in \text{coset}} e^{-\frac{\| \quad \|^2}{2\sigma^2}}$$

Open Question 5:

Simple Decoding of Shaped Lattices ?

Remark: keep symmetry of $P_{e,i}$, power, ?

Dithered Voronoi Modulation: Equivalent Channel



Tx: $\quad x = [v + \text{dither}] \bmod \Lambda_2$

reduction to $\mathcal{V}_0$

Channel: $\quad y = x + Z$

Rx: $\quad \tilde{y} = [y - \text{dither}] \bmod \Lambda_2$

$\hat{v}_{LD} = Q_{\Lambda_1}(\tilde{y})$

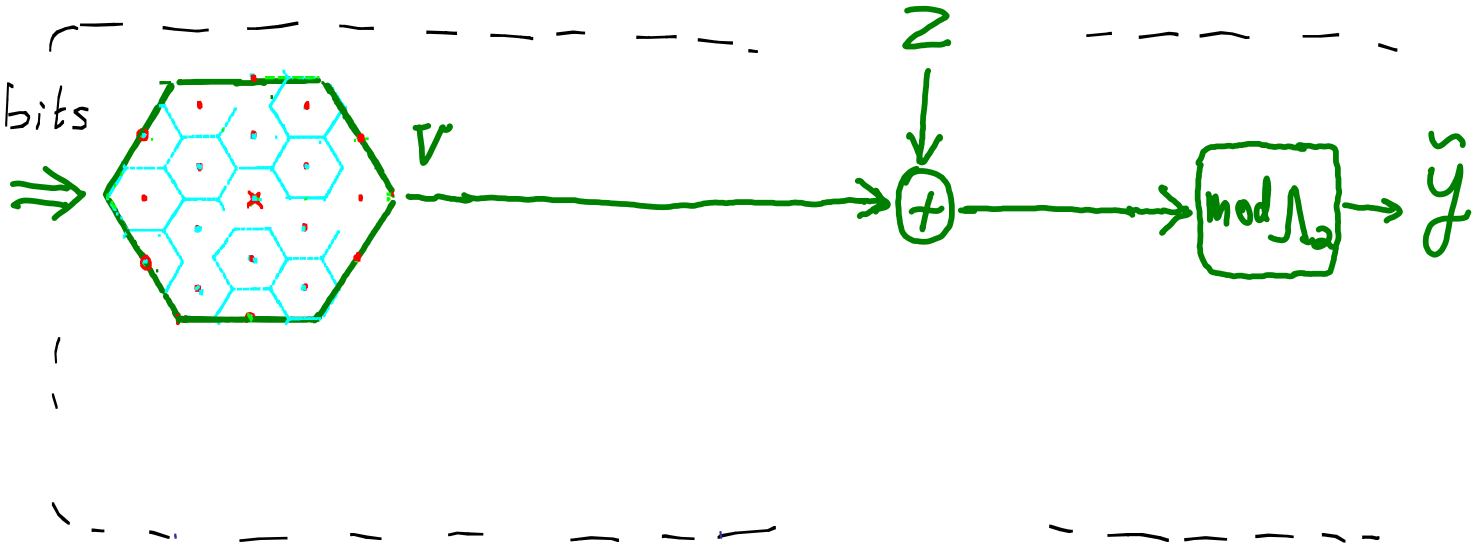
reduction to (any) set of coset rep.

Dithered Voronoi Modulation: Equivalent Channel

Distributive Property:

$$(a + b \bmod \Lambda) \bmod \Lambda = (a+b) \bmod \Lambda$$

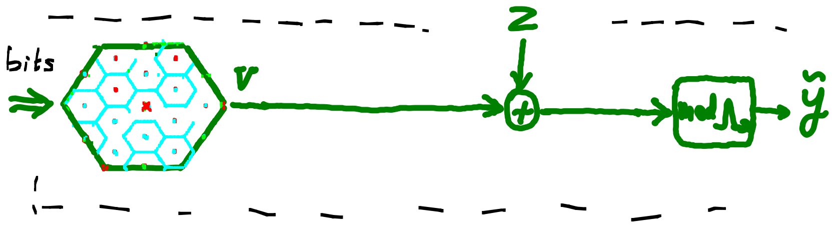
$\Rightarrow$



Dithered Voronoi Modulation: Performance

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

Λ_2 = good for quantization $\Rightarrow$ $\sigma^2_{\Lambda_2}$ small w.r.t V_2



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

NSM(Λ_2)

VNR(Λ_1)

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

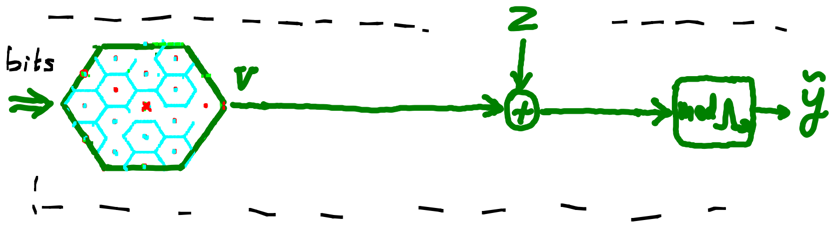
LOSS $\longrightarrow 0$ $\quad n \to \infty$

for good lattices ....

Dithered Voronoi Modulation: Performance

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

Λ_2 = good for quantization $\Rightarrow$ $\sigma^2_{\Lambda_2}$ small w.r.t V_2



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

NSM(Λ_2)
VNR(Λ_1)

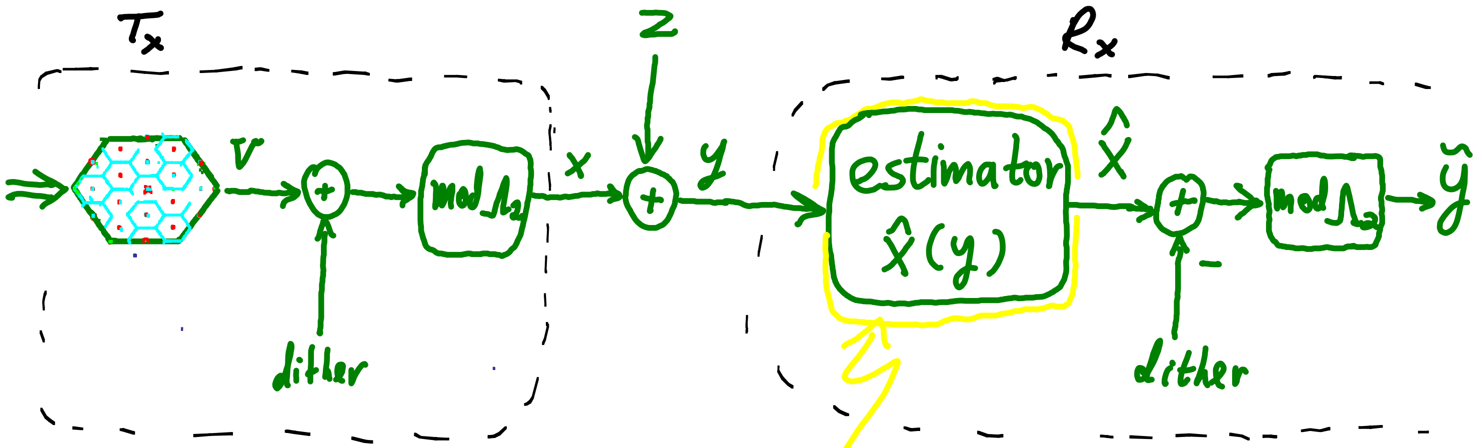
$$= \underbrace{\frac{1}{2}\log\left(\frac{P}{\sigma_z^2}\right)}_{\text{AWGN capacity @ High SNR}} - \underbrace{\frac{1}{2}\log\left(G(\Lambda_2)\cdot\mu(\Lambda_1,\varepsilon)\right)}_{\text{Loss}}$$

Loss $\xrightarrow[n\to\infty]{} 0$ for good lattices....

Shaping loss $\triangleq \frac{1}{2}\log(2\pi e\, G(\Lambda_2))$

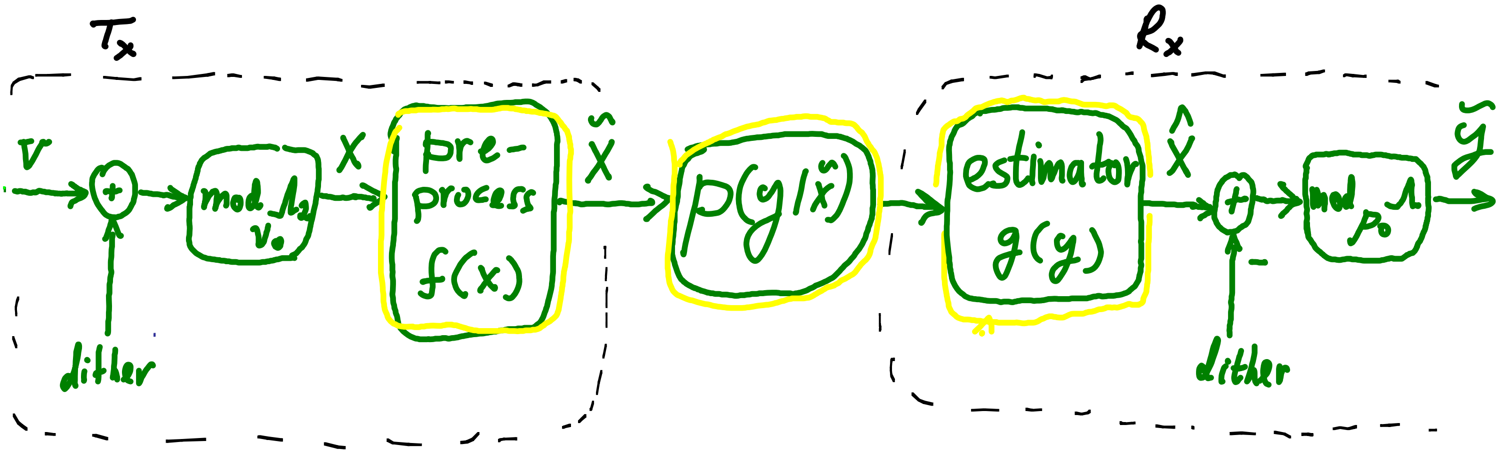
coding loss $\triangleq \frac{1}{2}\log(\mu(\Lambda_1, P_e)/2\pi e)$

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



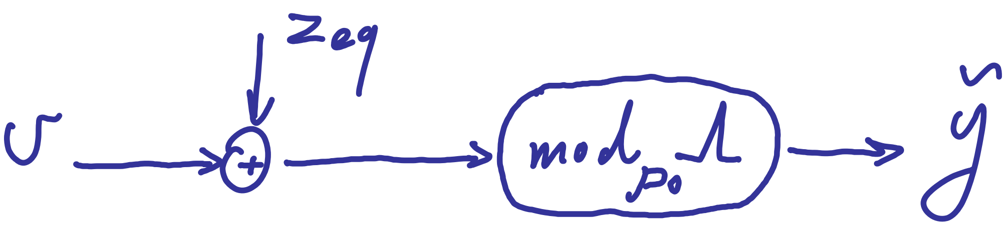
minimize error $\hat{x}-x \triangleq z_{eq}$

The Equivalent Mod-Λ Channel



Thm. [Mod-Λ channel]

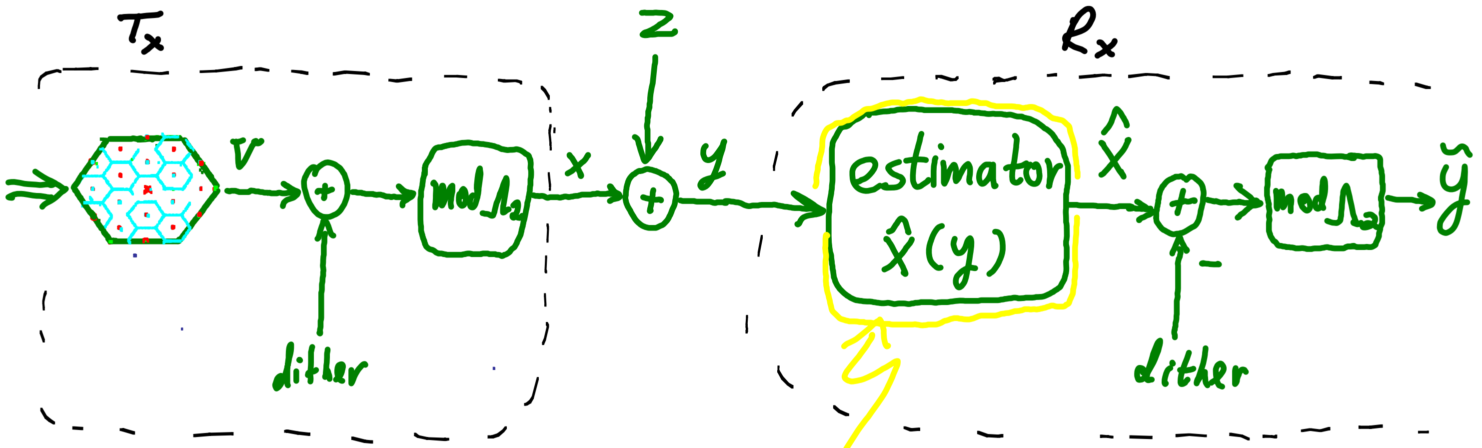
The channel $v \to \breve{y}$ is equivalent to a mod-Λ channel



$$Z_{eq} \overset{dist.}{=} \hat{X} - X \quad \perp\!\!\!\perp \quad v$$

$$X \sim \mathrm{unif}(V_0) \quad , \quad \hat{X} = g(p(y|f(x)))$$

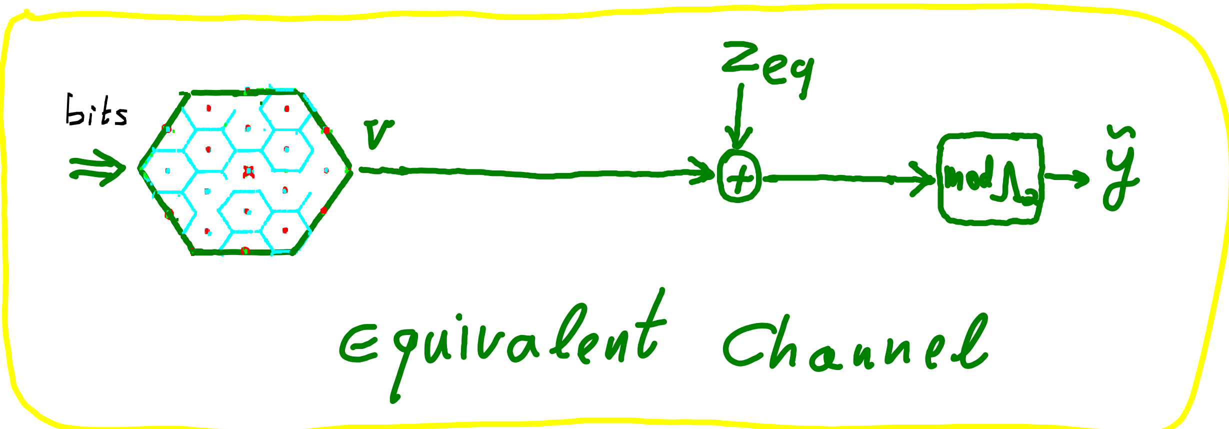
Achieving $\frac{1}{2}\log(1+\text{SNR})$ @ general SNR



minimize
error $\hat{x}-x \triangleq z_{eq}$

Crypto-Lemma $\Rightarrow$ $X \perp\!\!\!\perp V$ $\Rightarrow$ $z_{eq} \perp\!\!\!\perp V$

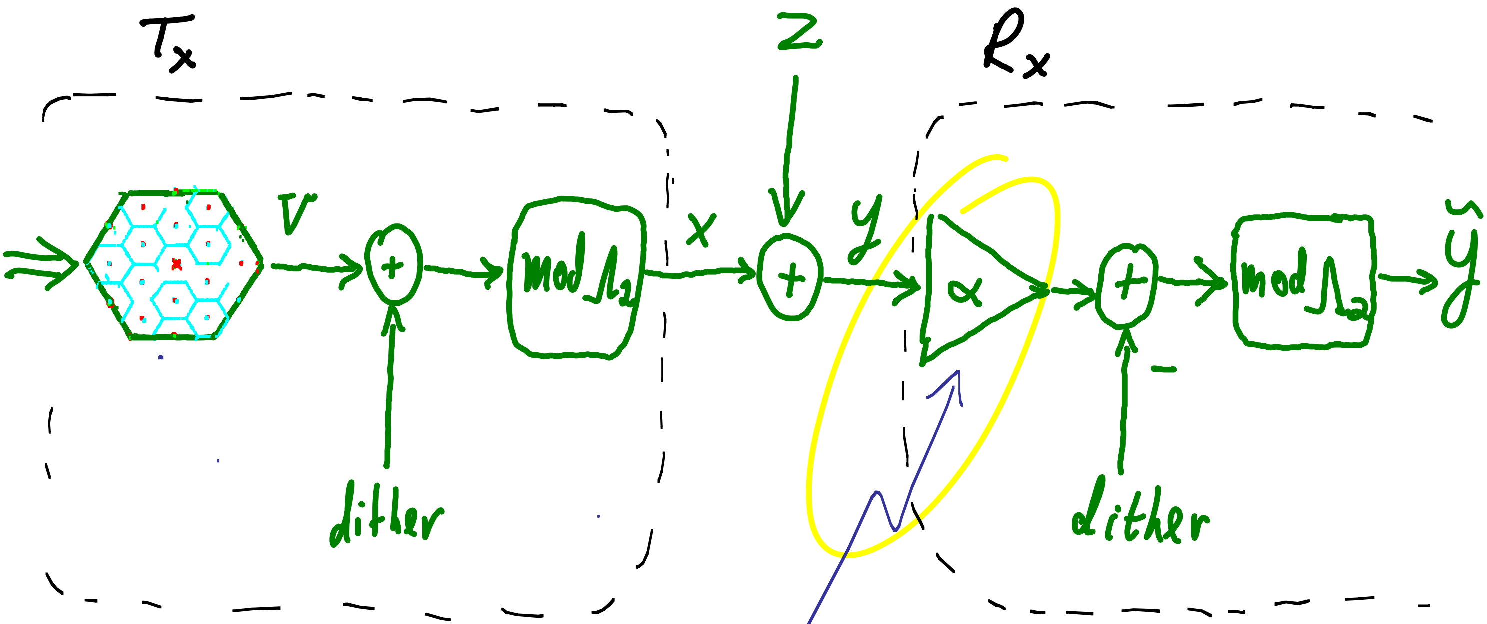
distributive property $\Rightarrow$ $\tilde{y} = (v + z_{eq}) \bmod \Lambda_2$



$\therefore$ Need to find $\hat{x}(y)$ to optimize channel!

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

Linear Estimation



$$Var\{\underbrace{\alpha Z}_{\text{AWGN}} + \underbrace{(1-\alpha)\cdot dither}_{\text{"self noise"}}\} = \sigma_Z^2 \cdot \frac{SNR}{1+SNR}$$

$@\ \alpha = \alpha_{wiener}$

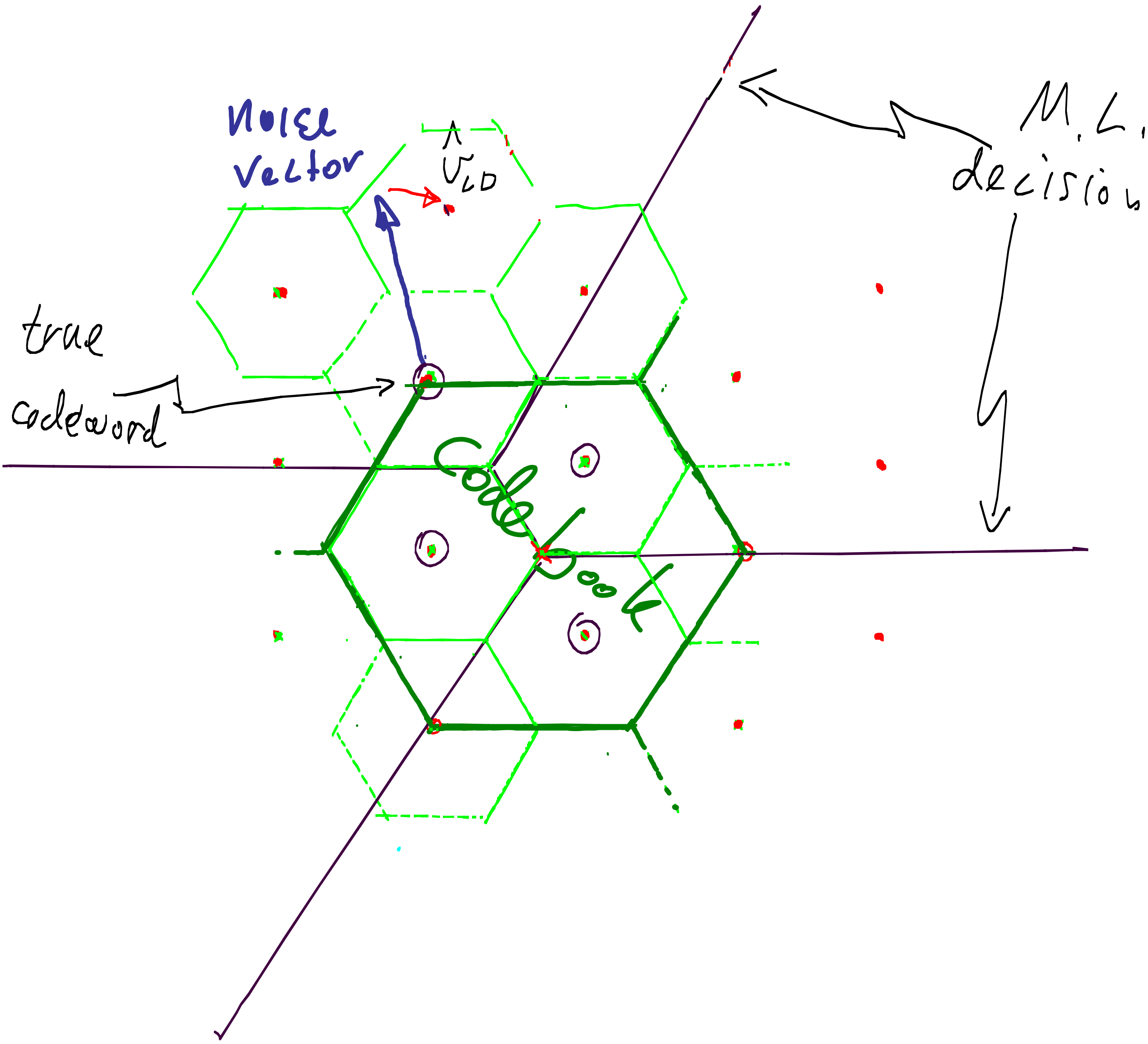
$$\Rightarrow \text{Rate} = \underbrace{\tfrac{1}{2}\log(1+SNR)}_{\text{AWGN capacity}} - \underbrace{\text{Shaping * Coding loss}}_{\xrightarrow{n\to\infty} 0}$$

Open Question:

- Bounds on Volum to Noise Ratio relative to mixture noise $\mu(\lambda, p_e, \alpha)$?

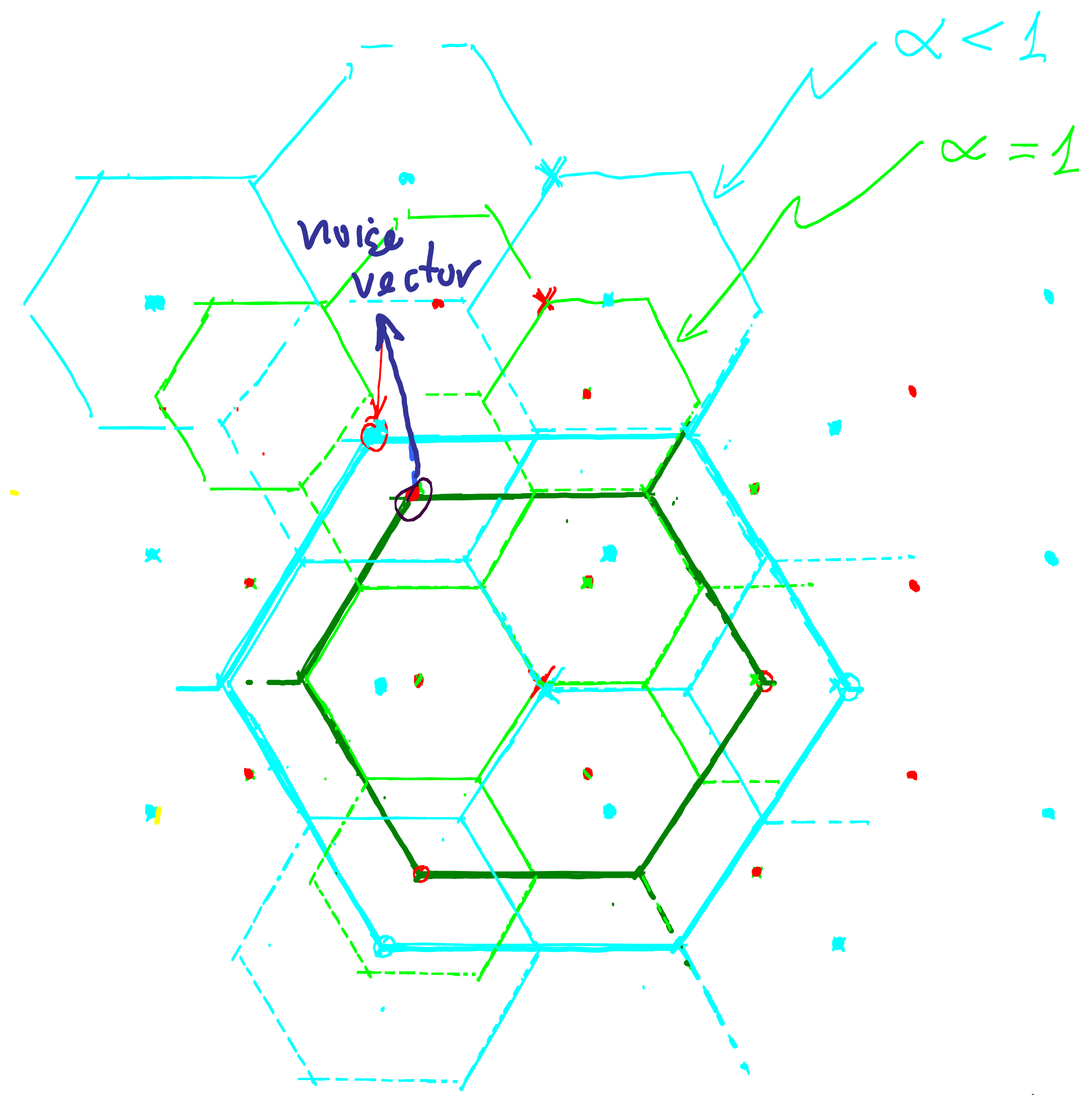
- Good nested pairs @ general SNR?

Geometric picture:
ML versus Lattice Decoding ($\alpha = 1$)



Geometric Picture :

Linear Scaling ($\alpha=1$) $\Rightarrow$ Lattice Inflation



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

But Noise is Not Quite Gaussian ...

$\alpha = 1$

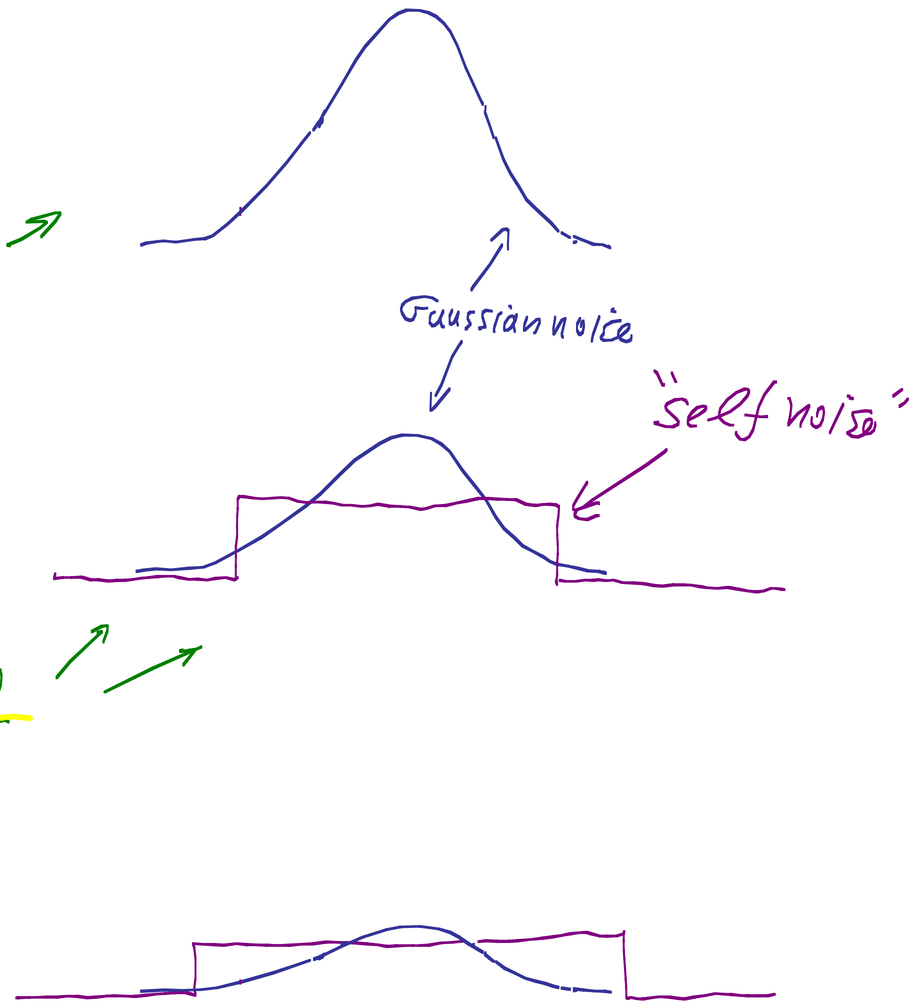
pure Gaussian

$\alpha = \alpha_{wiener}$

minimum-energy mixture

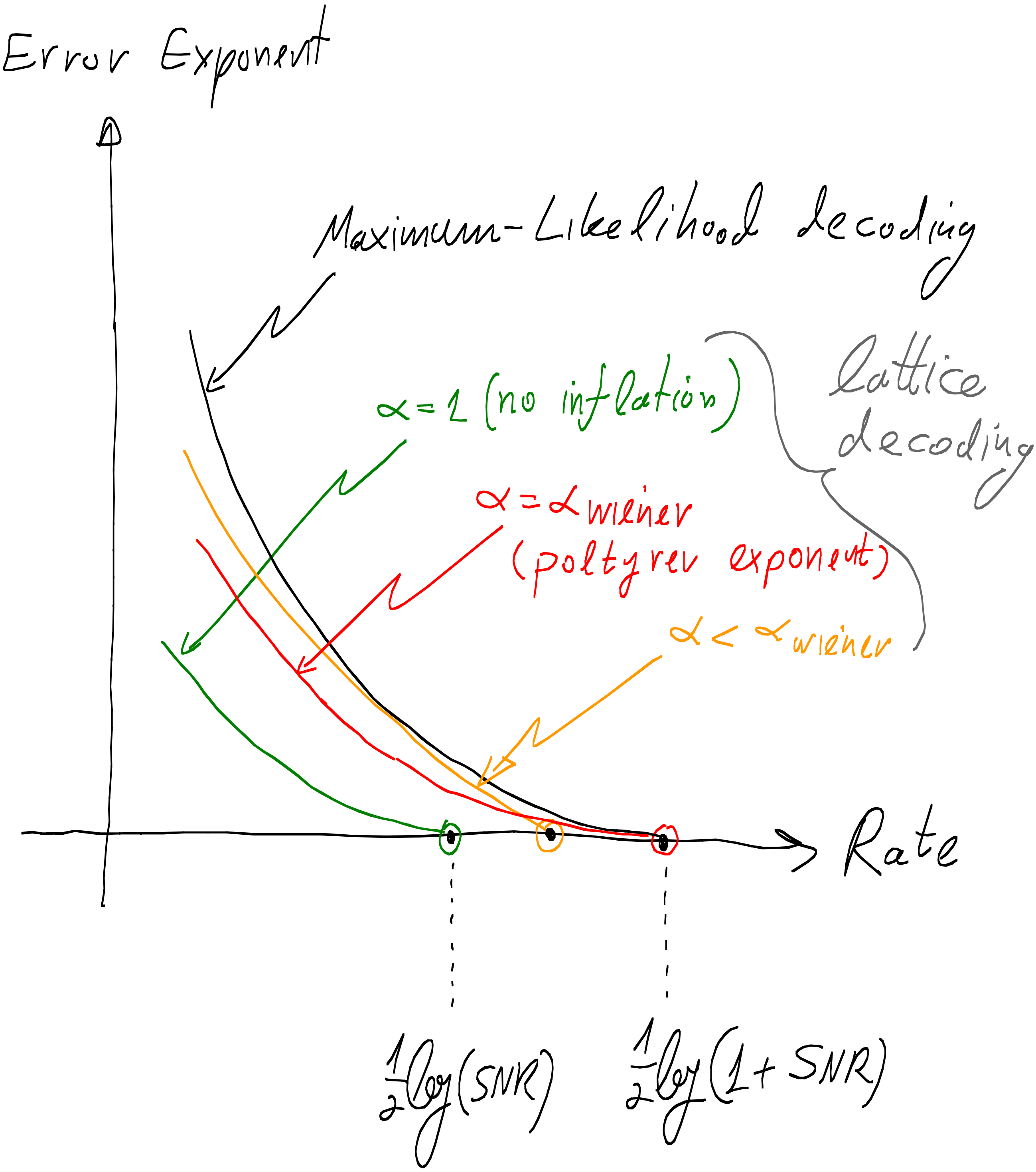
$\alpha < \alpha_{wiener}$

reduced-tail mixture

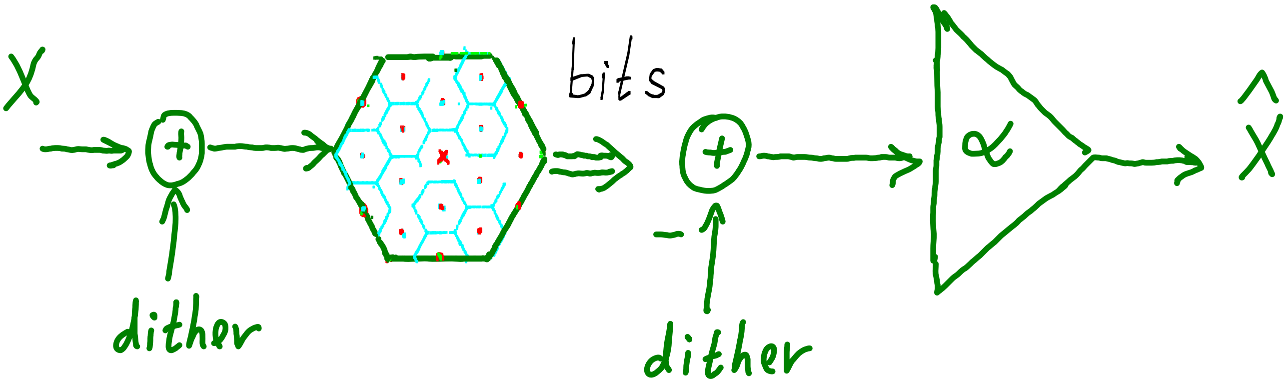


$\Rightarrow$ inflation-coefficient α affects equivalent noise distribution

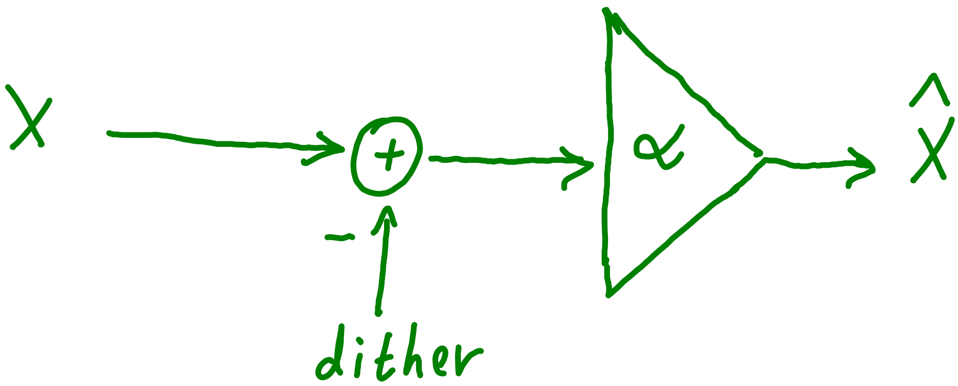
Effect of α on Lattice-Decoding



Voronoi Quantization



Crypto Lemma $\Rightarrow$ Equivalent channel



$$\text{Distortion} = \operatorname{Var}\{\alpha \cdot \text{dither} + (1-\alpha) X\} = \frac{\sigma_x^2 \sigma_n^2}{\sigma_x^2 + \sigma_n^2}$$

@ $\alpha = \alpha_{\text{wiener}}$

$$\text{Rate} = \underbrace{\frac{1}{2}\log\left(\frac{\sigma_x^2}{D}\right)}_{\text{Q-Gaussian RDF}} - \underbrace{\frac{1}{2}\log\left(G(\Lambda_1)\cdot \mu(\Lambda_2, P_e, \alpha)\right)}_{\text{loss} \longrightarrow 0 \text{ as } n \to \infty}$$

Next file ... →