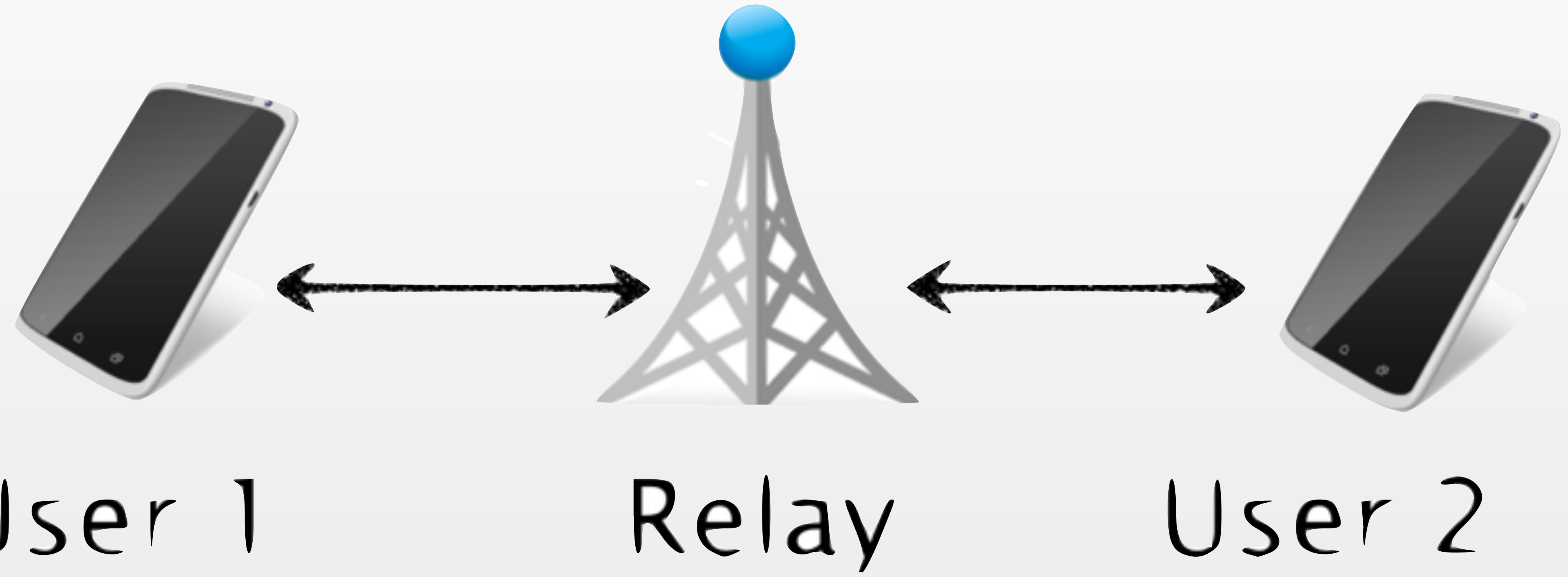
Generalized Voronoi Constellations

Brian M. Kurkoski
Japan Advanced Institute of Science and Technology

JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY 1990

November 26, 2015
Symposium on Information Theory and Its Applications (SITA2015)
Kurashiki, Okayama, Japan

Usefulness of Lattice Codes



Lattice codes can achieve the capacity of AWGN channel [Erez and Zamir '04]

Information theoretic results and physical layer network coding using lattices:

- Lattices for relay channel e.g. [Song-Devroye '13]
- Two-way (Bidirectional) relay channel e.g. [Wilson et al.]
- Compute-forward relaying [Nazer-Gastpar '11]

"Physical layer network coding"

How to construct practical, capacity-approaching lattices?

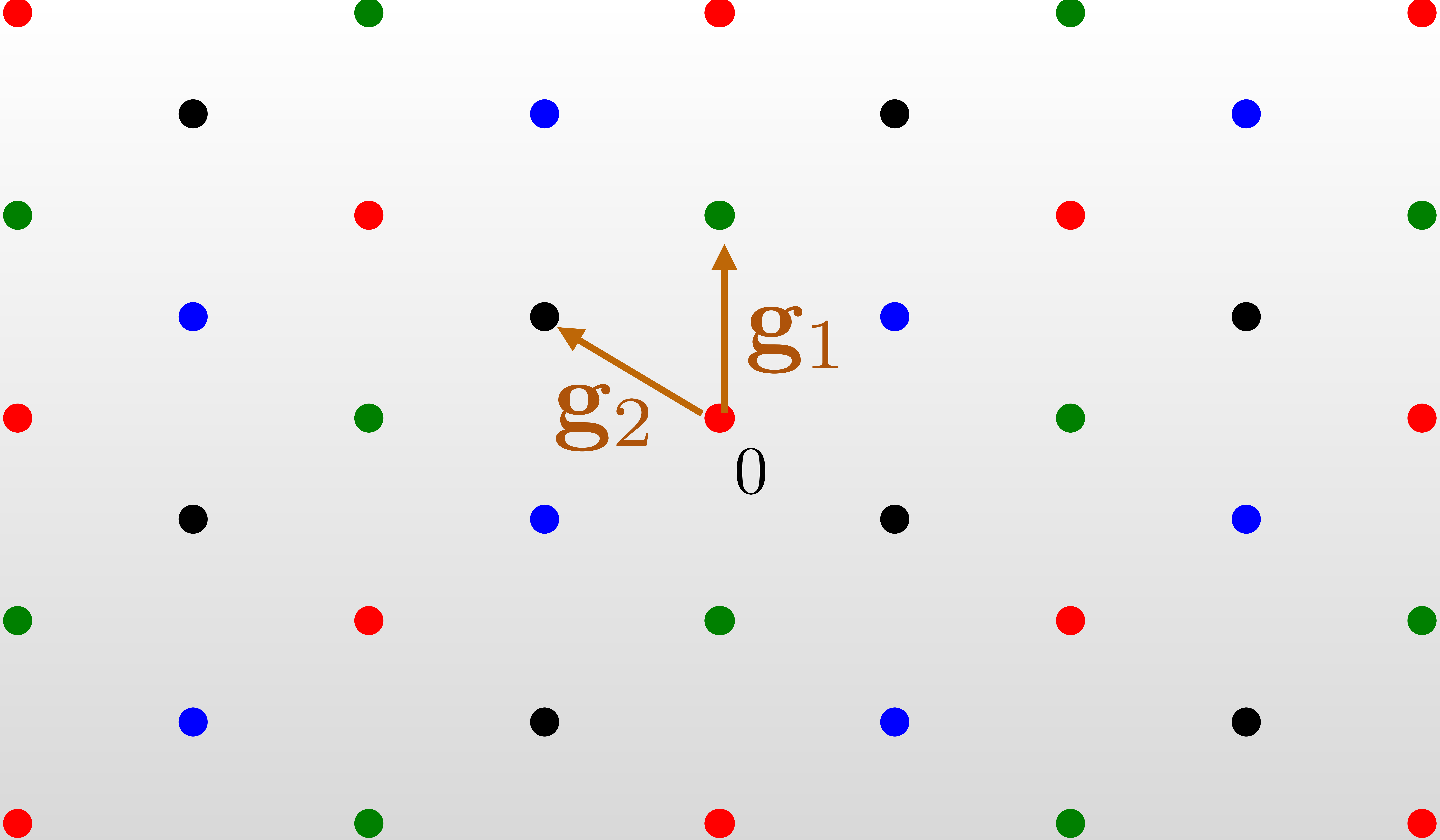
A lattice Λ is a linear additive subgroup of $\mathbb{R}^n$.

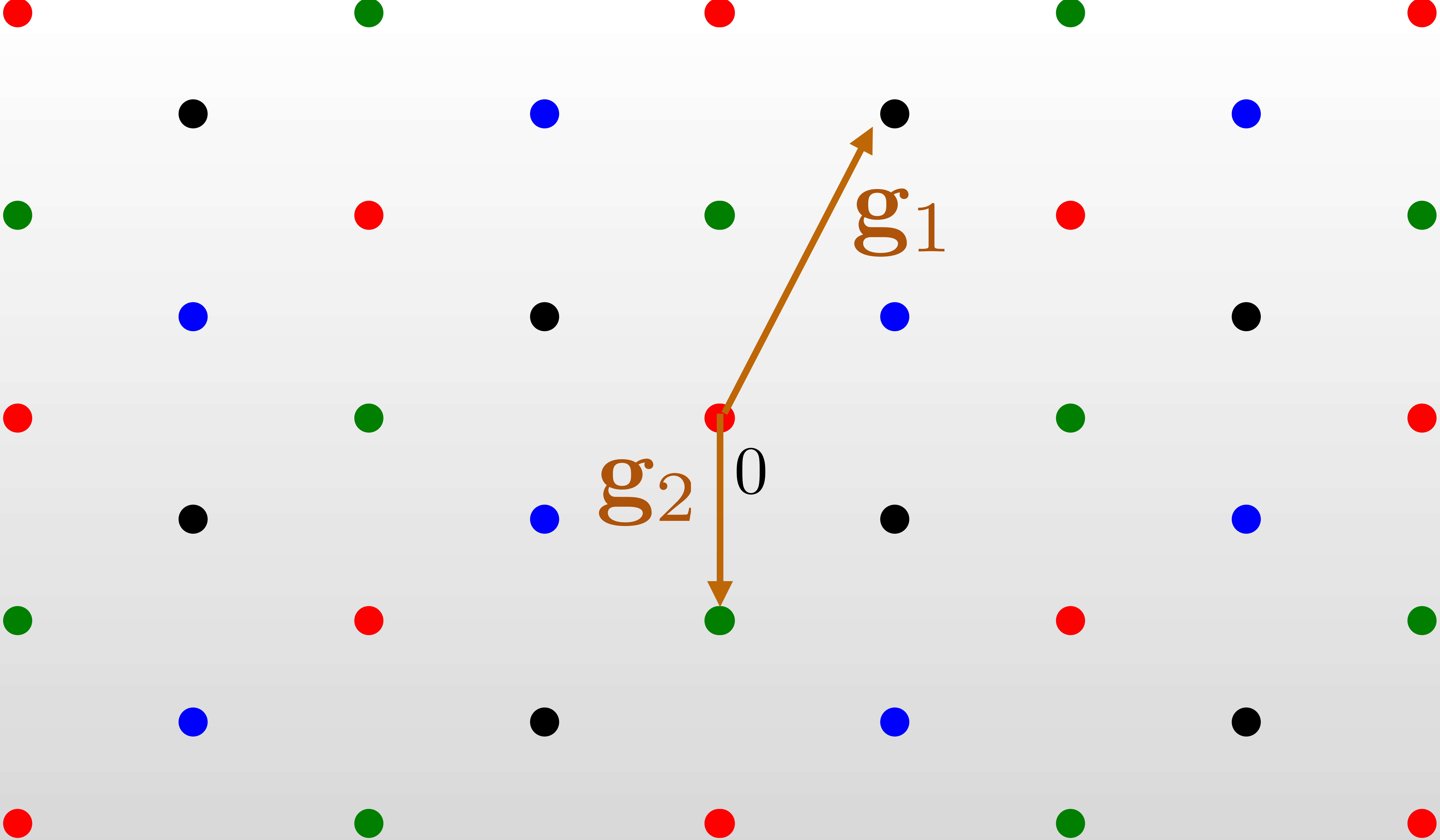
Given a basis $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n$, the lattice consists of all points

$$\begin{bmatrix} | & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n \\ | & | & & | \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

for $b_i \in \mathbb{Z}$.

Given Λ, there are arbitrarily many possible bases.


$\mathbf{g}_1$
$\mathbf{g}_2$
0



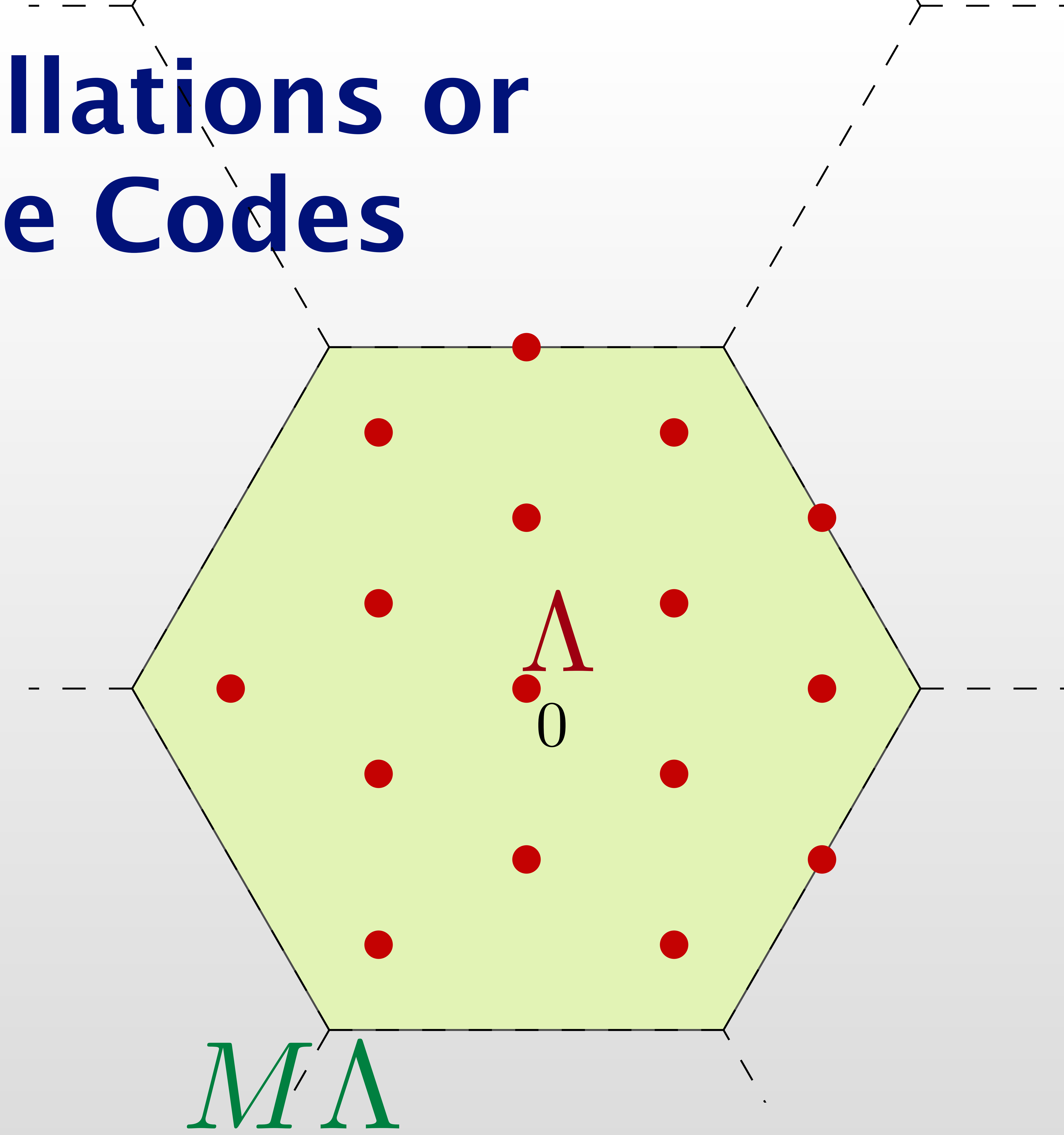
$\mathbf{g}_1$
$\mathbf{g}_2$
0

Voronoi Constellations or Nested Lattice Codes

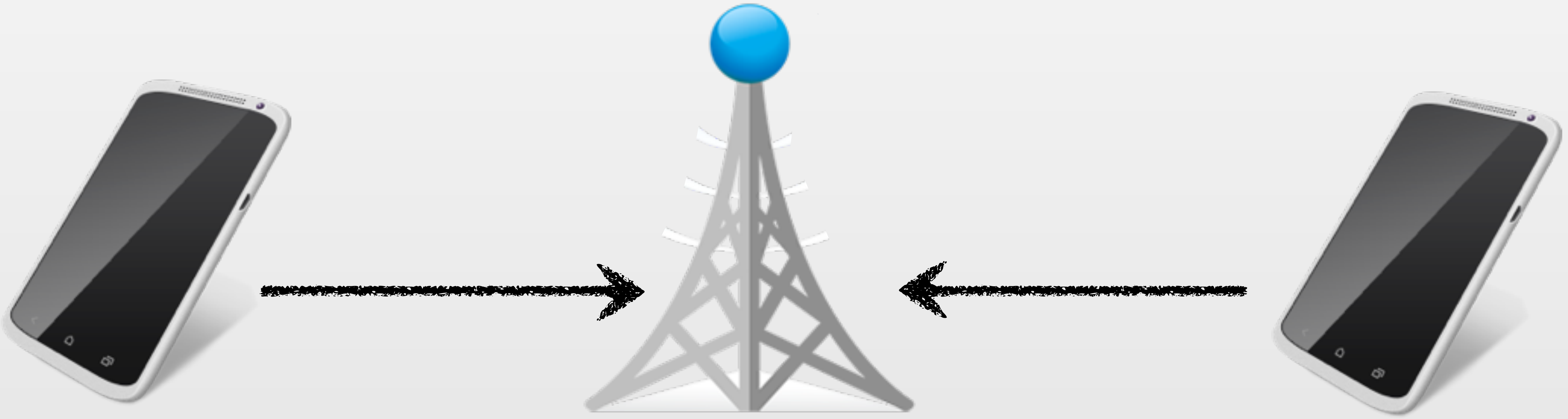
Conway and Sloane [IT 83] described *Voronoi constellations*

- Λ is a lattice
- $M\Lambda$ is scaled by M.
- $\Lambda/M\Lambda$ is a quotient group
- coset leaders Euclidean-space code

Also called *nested lattice codes*



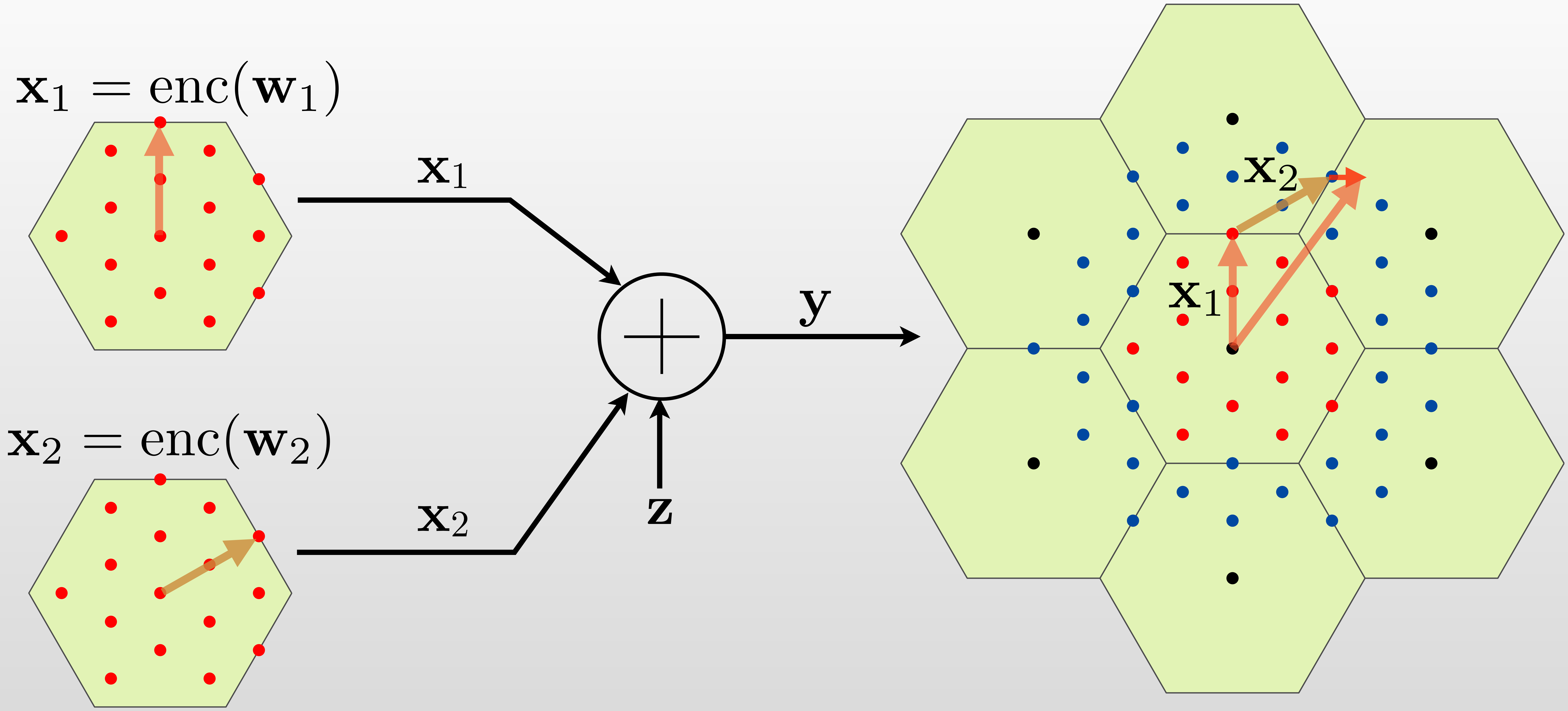
Physical Layer Network Coding: Signals Add Over the Air

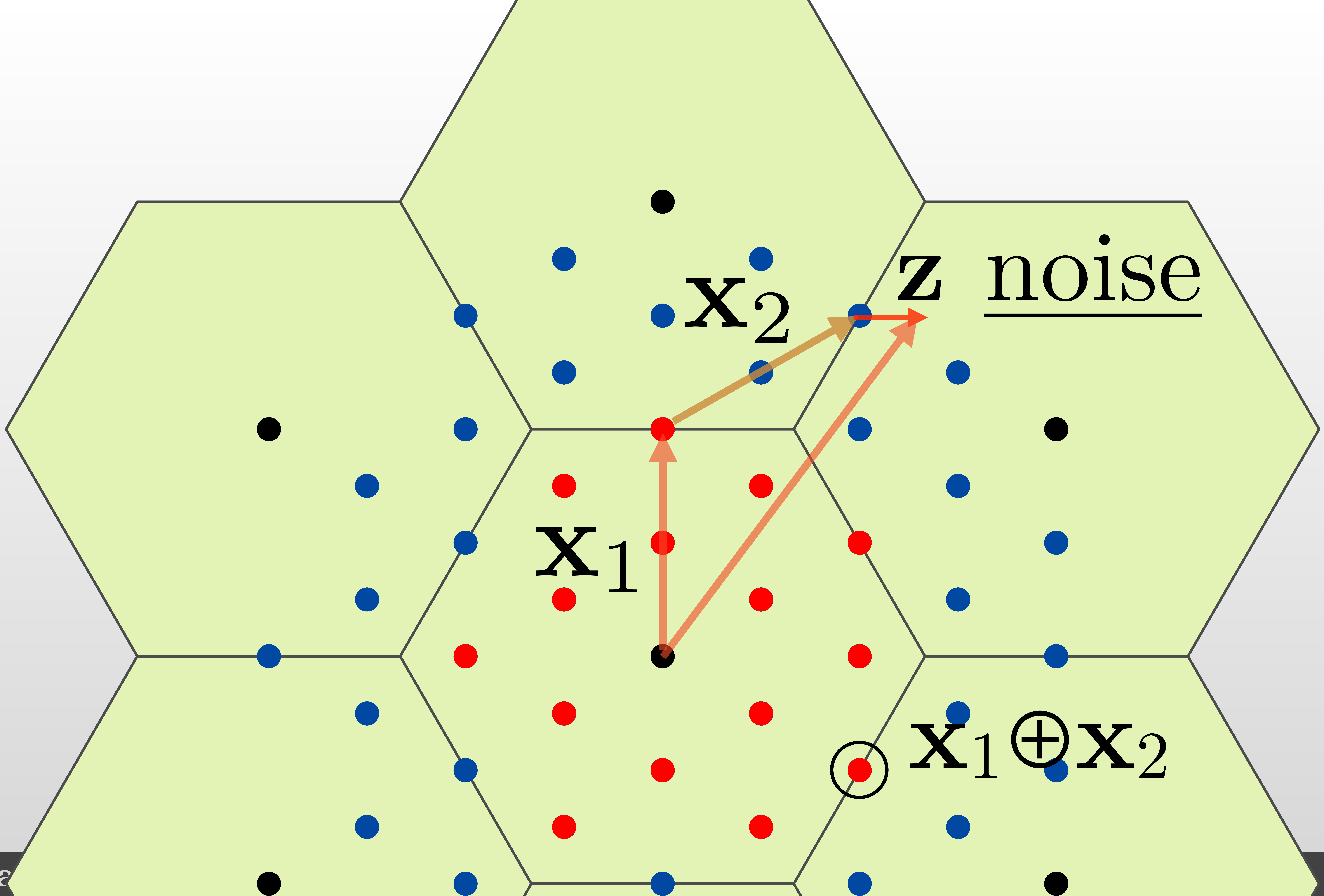


User 1 | Relay | User 2

has w_1 | wants $w_1 + w_2$ | has w_2

Two Users Transmit to Relay




$\mathbf{z}$
noise
$\mathbf{x}_2$
$\mathbf{x}_1$
$\mathbf{x}_1 \oplus \mathbf{x}_2$

Background Summary

Lattices are codes over the real numbers.

Network coding for wireless networks: signals add over the air: **physical layer network coding**

Voronoi constellations (nested lattice codes) have three properties:

1. Coding lattice Λ — good for error correction
2. Shaping lattice $M\Lambda$ —
   - As $n \to \infty$ Voronoi region is sphere like
   - A sphere achieves optimal AWGN input distribution (and Shannon capacity). Optimal 1.53 dB shaping gain
3. Forms a quotient group required for physical layer network coding

Good for theoretical results, difficult to construct capacity-achieving codes

Contributions

Generalized Voronoi Constellations — Practical lattice codes

- Shaping lattice is not a scaled coding lattice:

$$\underset{\substack{\text{is high dimension,}\\ \text{capacity-approaching}}}{\textit{coding lattice}} \longrightarrow \quad \Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}} \quad \longleftarrow \underset{\substack{\text{high shaping gain}\\ \text{efficient shaping algorithm}}}{\textit{shaping lattice}}$$

- Give necessary and sufficient condition so $\Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}}$ is a group
- Encoding for triangular coding matrices: easy
- Encoding for general coding matrices: not so easy

How to Design a Coding Lattice

Approach unconstrained lattice capacity, lattice dimension n should be large

Construction A and Construction D

- Construction D using LDPC codes [Sadeghi et al IT 2006]
- Construction A using non-binary LDPC codes [Huang et al ISIT 2014]
- Construction D using polar codes [Yan et al ITW 2012]

Derive generator matrix G, and check matrix $H = G^{-1}$ from the design

Low-Density Lattice Codes (LDLC lattices)

- [Sommer et al, 2008]
- Spatially-coupled LDLCs [Uchikawa et al, ISIT 2012]

Design the H matrix to be sparse and other easy conditions.

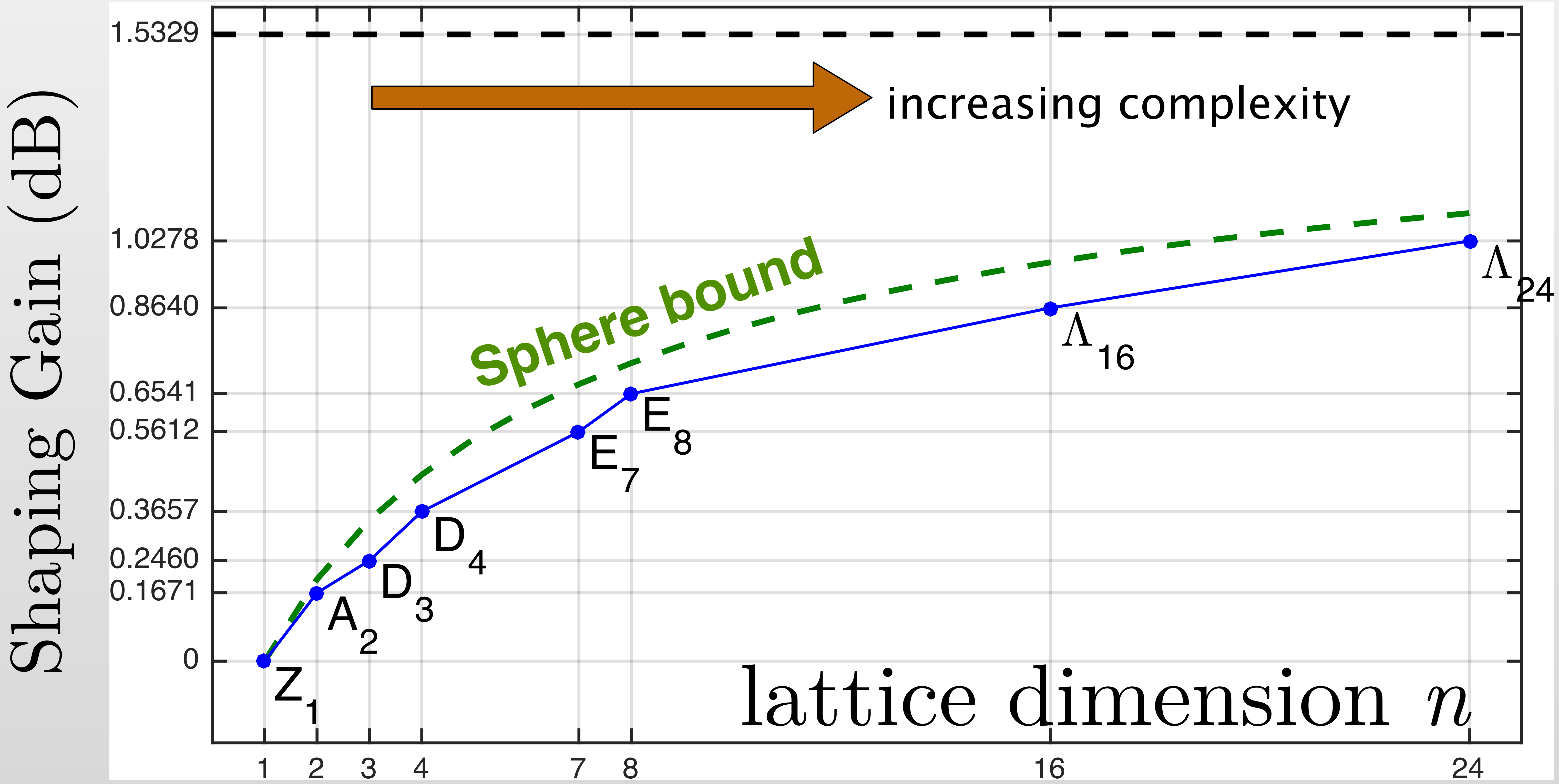
How to Design a Shaping Lattice

Ideally, want a shaping lattice with efficient maximum-likelihood decoding:

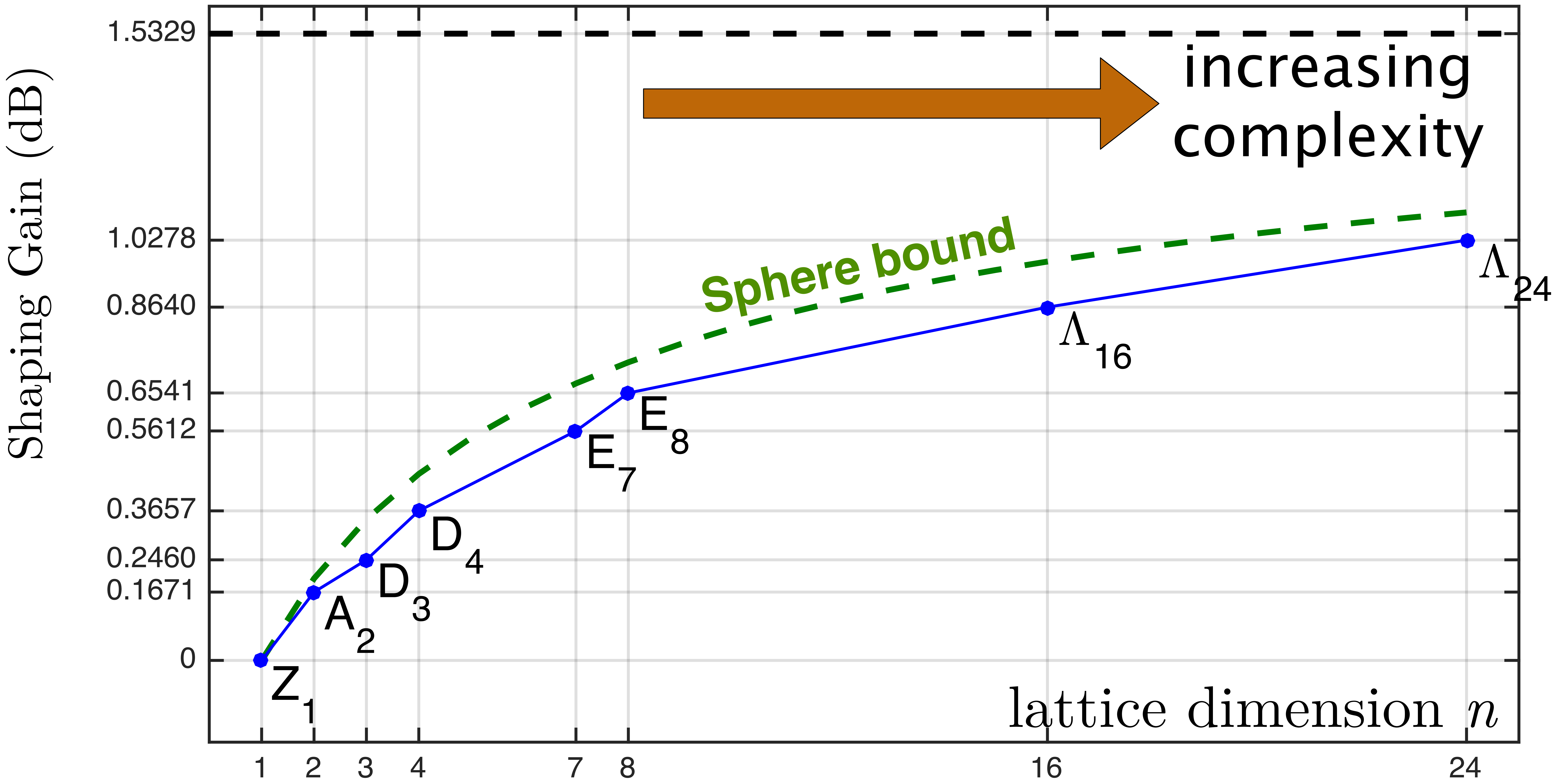
1. Lattices based on convolutional codes (Viterbi-based decoding)
2. Low-dimension lattices, E8, BW16, etc.

Shaping lattice is concatenation of low-dimension lattices:

$$\underbrace{\Lambda_s \times \Lambda_s \times \cdots \times \Lambda_s}_{\text{dimension } n}$$



Shaping Gain for Well-Known Lattices

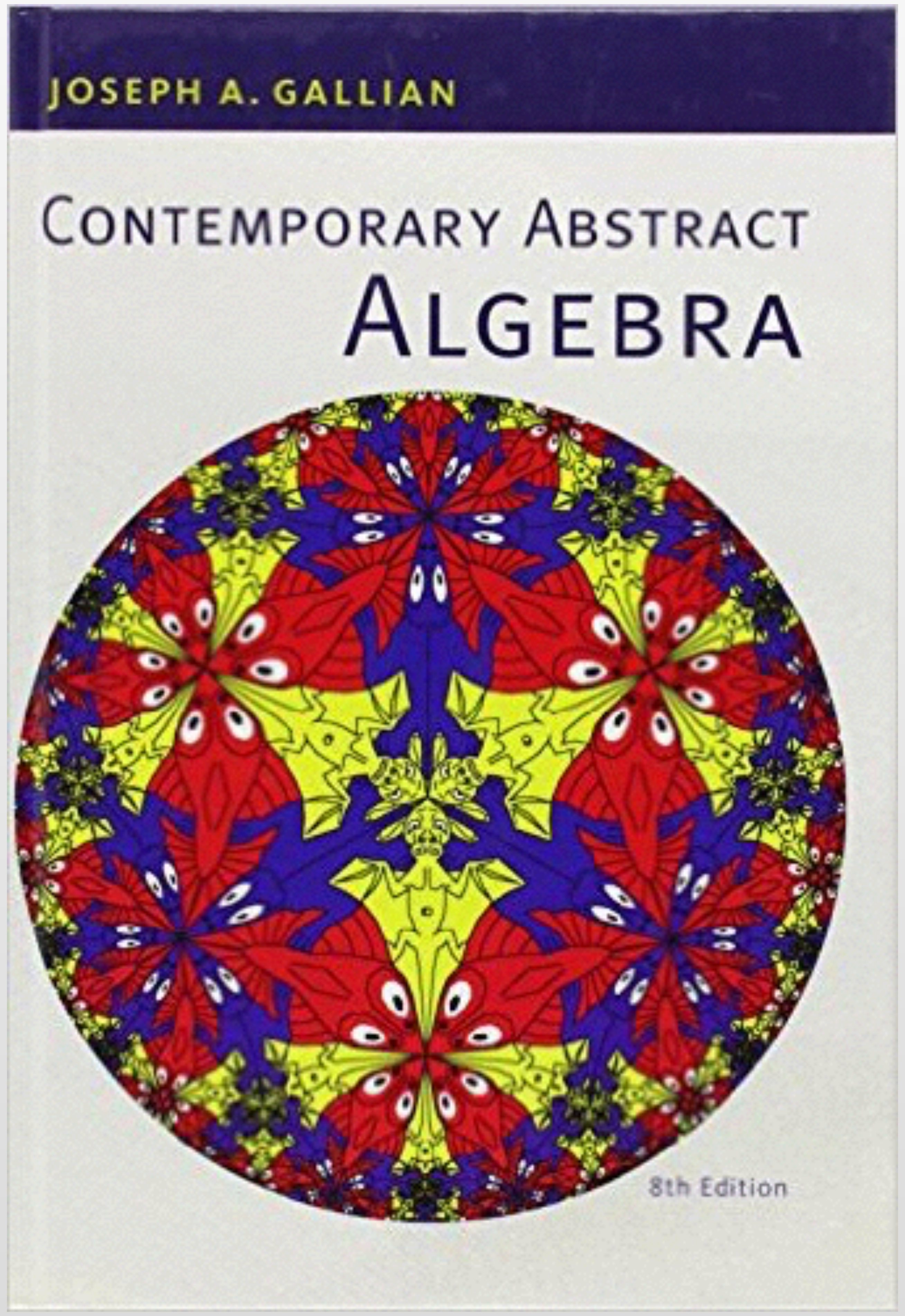


Basic Group Theory

If G is a group, and $H \subseteq G$ is a subgroup then G/H is a quotient group.

$$\boxed{\text{If } \Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}} \Rightarrow \Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}} \text{ is a quotient group.}}$$

Conway and Sloane: $\Lambda/M\Lambda$ is a quotient group.



Joseph A. Gallian, *Contemporary Abstract Algebra*, 2012


Sublattice (subgroup)
$\Lambda_{\mathrm{s}} = 2A_2$


subgroup
group but
not subgroup
Lattice (group) $\Lambda_c = A_2$

$+$	$\mathbf{c}_0$	$\mathbf{c}_1$	$\mathbf{c}_2$	$\mathbf{c}_3$
$\mathbf{c}_0$	$\mathbf{c}_0$	$\mathbf{c}_1$	$\mathbf{c}_2$	$\mathbf{c}_3$
$\mathbf{c}_1$	$\mathbf{c}_1$	$\mathbf{c}_0$	$\mathbf{c}_3$	$\mathbf{c}_2$
$\mathbf{c}_2$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\mathbf{c}_0$	$\mathbf{c}_1$
$\mathbf{c}_3$	$\mathbf{c}_3$	$\mathbf{c}_2$	$\mathbf{c}_1$	$\mathbf{c}_0$

4 cosets. Coset containing $\mathbf{c}_0$, $\mathbf{c}_1$,$\mathbf{c}_2$,$\mathbf{c}_3$.

The Subgroup Condition

- Shaping lattice Λ_{s} has generator matrix G_{s}.
- Coding lattice Λ_{c} has check matrix H_{c}.

Lemma Let Λ_{s} have an all-integer generator matrix G_{s}. $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}}$ if and only if $H_{\mathrm{c}} G_{\mathrm{s}}$ is a matrix of integers.

- Simple test for $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}}$.
- If $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}} \Rightarrow$ quotient group $\Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}}$ exists, and is a candidate for physical layer network coding.

The Subgroup Condition: Example

- dimension $n = 8$ coding lattice Λ_{c} is LDLC-style
- shaping lattice Λ_{s} on D_4

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & \frac{1}{2} & 0 & 0 & -\frac{1}{4} & 0 \\ \frac{1}{4} & 1 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} \\ 0 & \frac{1}{2} & 1 & 0 & 0 & 0 & 0 & \frac{1}{4} \\ 0 & 0 & \frac{1}{4} & 1 & 0 & 0 & -\frac{1}{2} & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 1 & -\frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{4} & 0 & 1 & 0 & 0 \\ 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{2} & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{4} & \frac{1}{2} & 0 & 1 \end{bmatrix}}_{\text{coding: LDLC } H_c} \cdot \underbrace{\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -4 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 8 \end{bmatrix}}_{\text{shaping } 4D_4 \times 4D_4} = \begin{array}{c}\text{matrix} \\ \text{of} \\ \text{integers}\end{array}$$

- Condition is satisfied. Thus $\Lambda_{\mathrm{c}}/\Lambda_{\mathrm{s}}$ is a quotient group.

Encoding Λ_c/Λ_s

Encoding is mapping information to lattice points Λ_c/Λ_s.

For Conway and Sloane, indexing $\Lambda/M\Lambda$ is easy:

$$\{0, 1, \cdots, M-1\}^n \to \Lambda/M\Lambda$$

For Λ_c/Λ_s satisfying the subgroup condition

1. If coding check matrix H_c is triangular, then indexing is also easy
2. If H_c is full, then indexing is harder.

1. Encoding When Hc is Triangular

g_{ii} are diagonal elements of G_s, h_{ii} are diagonal elements of H_c, then:

$$\text{information is } \{0, 1, \cdots, g_{ii}h_{ii}\}$$

and encoding info to $\Lambda_\mathrm{c}/\Lambda_\mathrm{s}$ is straightforward.

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & \frac{1}{4} & 0 & 1 & 0 & 0 \\ 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{2} & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -\frac{1}{4} & \frac{1}{2} & 0 & 1 \end{bmatrix}}_{\text{coding } H_c} \cdot \underbrace{\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -4 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -4 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -4 & 8 \end{bmatrix}}_{\text{shaping } G_\mathrm{s}}$$

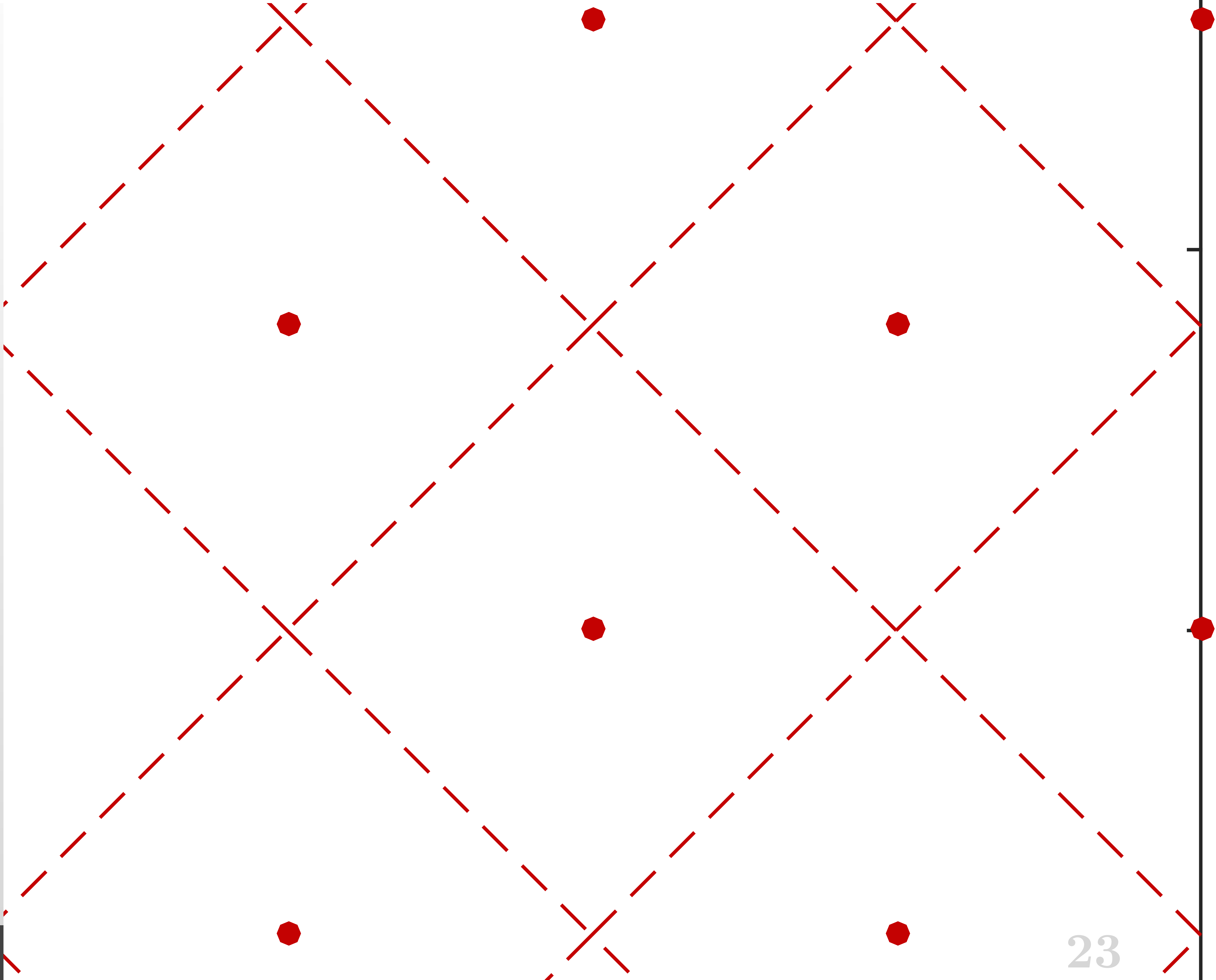
Encoding Lattice Codes, Conway and Sloane Style

Easy when $\Lambda_\mathrm{s} = M\Lambda_\mathrm{c}$ (Conway and Sloane 1983). Example:

$$G_\mathrm{s} = \begin{bmatrix} 4 & 0 \\ 4 & 8 \end{bmatrix} (\Lambda_\mathrm{s})$$

$$G_\mathrm{c} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} (\Lambda_\mathrm{c})$$

$\Lambda_\mathrm{s} = 4\Lambda_\mathrm{c}$ nested lattice code



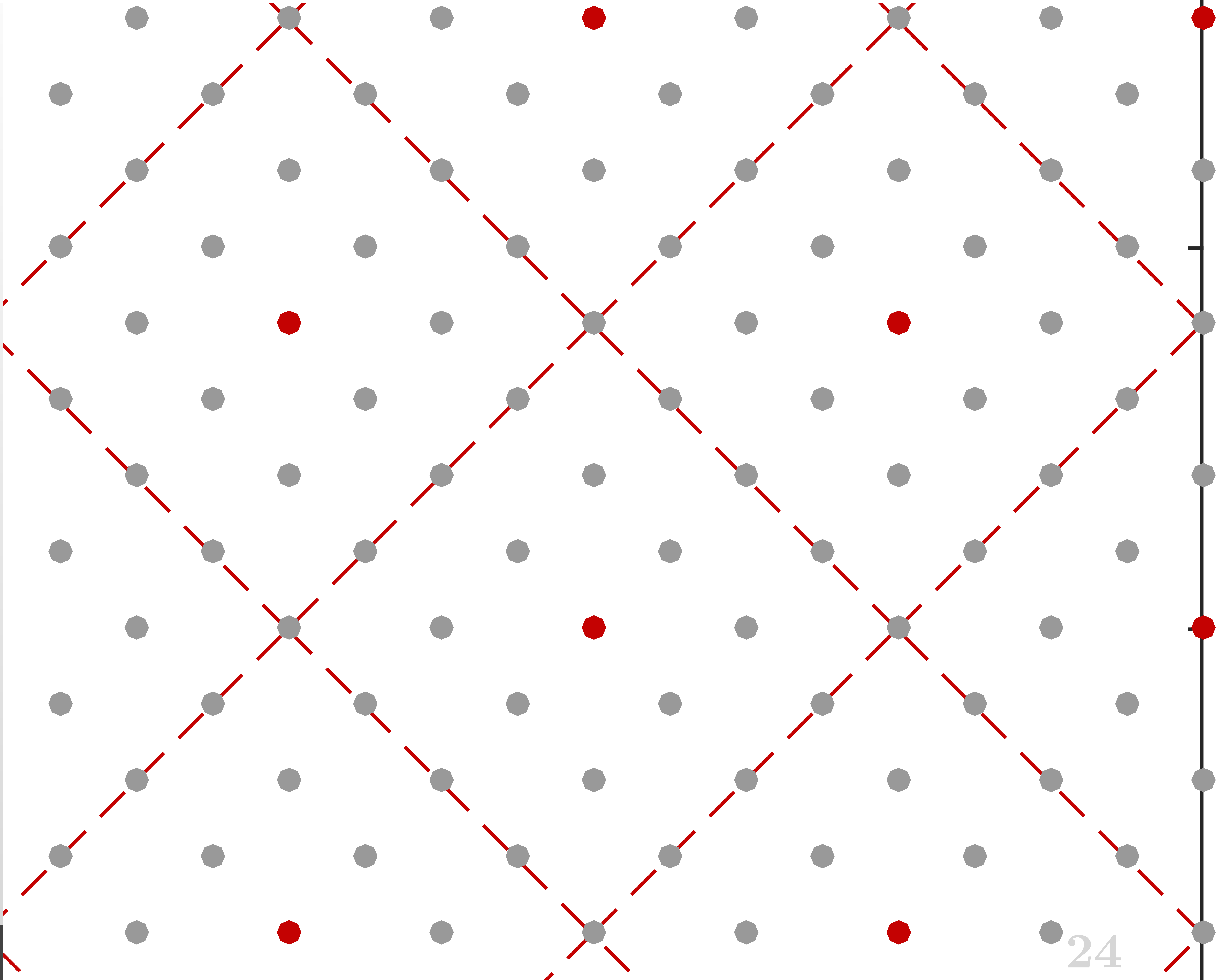
Encoding Lattice Codes, Conway and Sloane Style

Easy when $\Lambda_s = M\Lambda_c$ (Conway and Sloane 1983). Example:

$$G_s = \begin{bmatrix} 4 & 0 \\ 4 & 8 \end{bmatrix} (\Lambda_s)$$

$$G_c = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix} (\Lambda_c)$$

$\Lambda_s = 4\Lambda_c$ nested lattice code

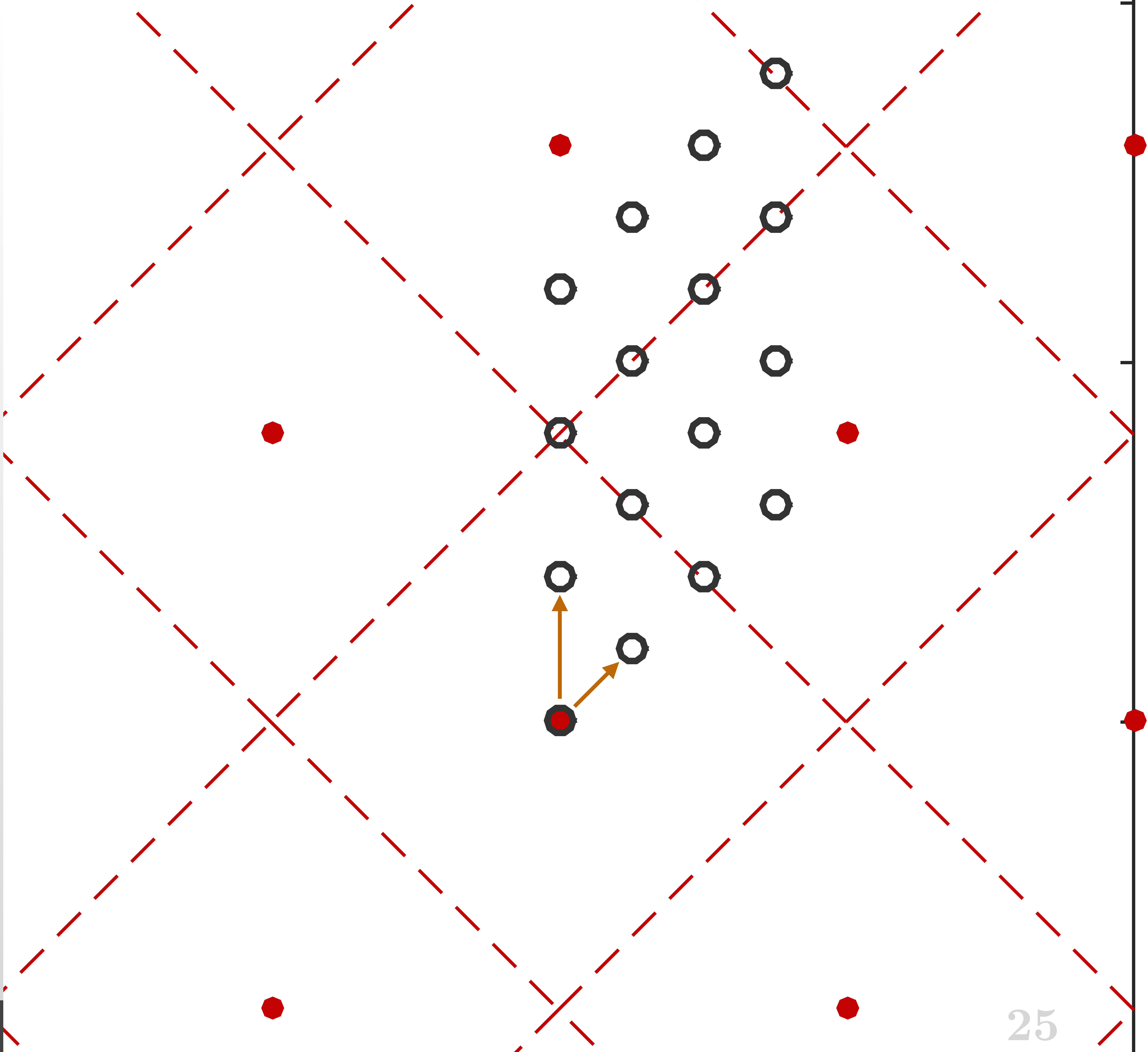


Information is $b_i \in \{0, 1, 2, 3\}$,

Indexing Step 1:

$$G\mathbf{b} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$$

(clearly these points form coset representatives)

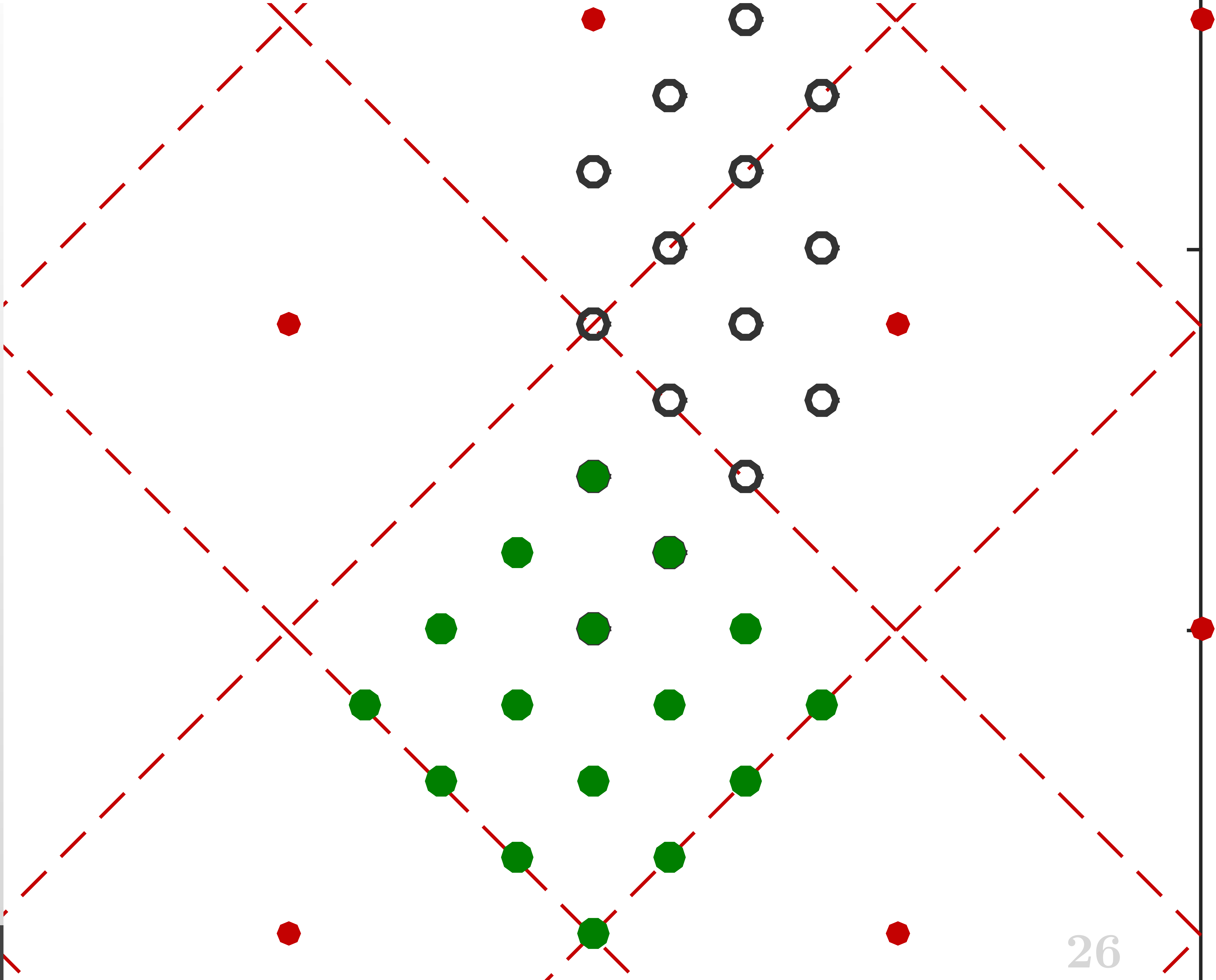


Encoding Lattice Codes, Conway and Sloane Style

Codebook is coset representatives inside Voronoi region for Λ_s around 0:

Indexing Step 2:

$$x = G\mathbf{b} - Q_{\Lambda_s}(G\mathbf{b})$$



2. Encoding When Hc is Full Matrix

Weakness of Hc triangular:

- Hc may not be available in triangular form
- triangular form reducing coding gain or rate.

If Hc full:

- Give conditions under which encoding is possible
- requires solving a diophantine equation

Encoding Lattice Codes, Generalized Voronoi Constellations

What if the lattices are not nested? Recall we want to use distinct lattices for coding and shaping.

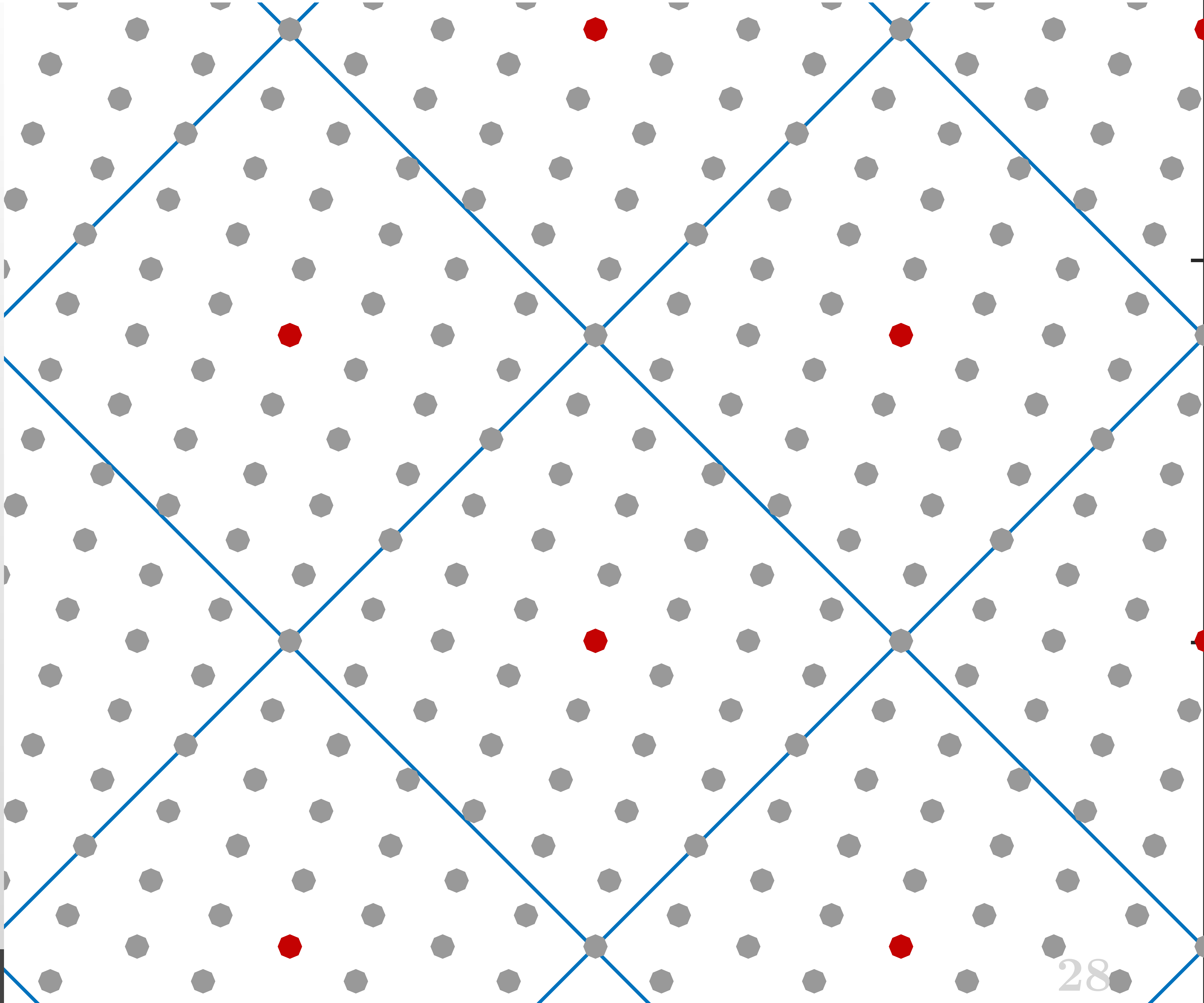
Example:

$$G_{\mathrm{s}} = \begin{bmatrix} 4 & 0 \\ 4 & 8 \end{bmatrix} (\Lambda_{\mathrm{s}})$$

$$G_{\mathrm{c}} = \begin{bmatrix} 8/9 & 2/9 \\ -4/9 & 8/9 \end{bmatrix} (\Lambda_{\mathrm{c}})$$

$$\left(G_{\mathrm{c}}^{-1} = \begin{bmatrix} 1 & -1/4 \\ 1/2 & 1 \end{bmatrix} \right)$$

Not a nested lattice code!



Encoding Lattice Codes, Generalized Voronoi Constellations

Number of codewords:

$$\frac{\det(G_s)}{\det(G_c)} = 36$$

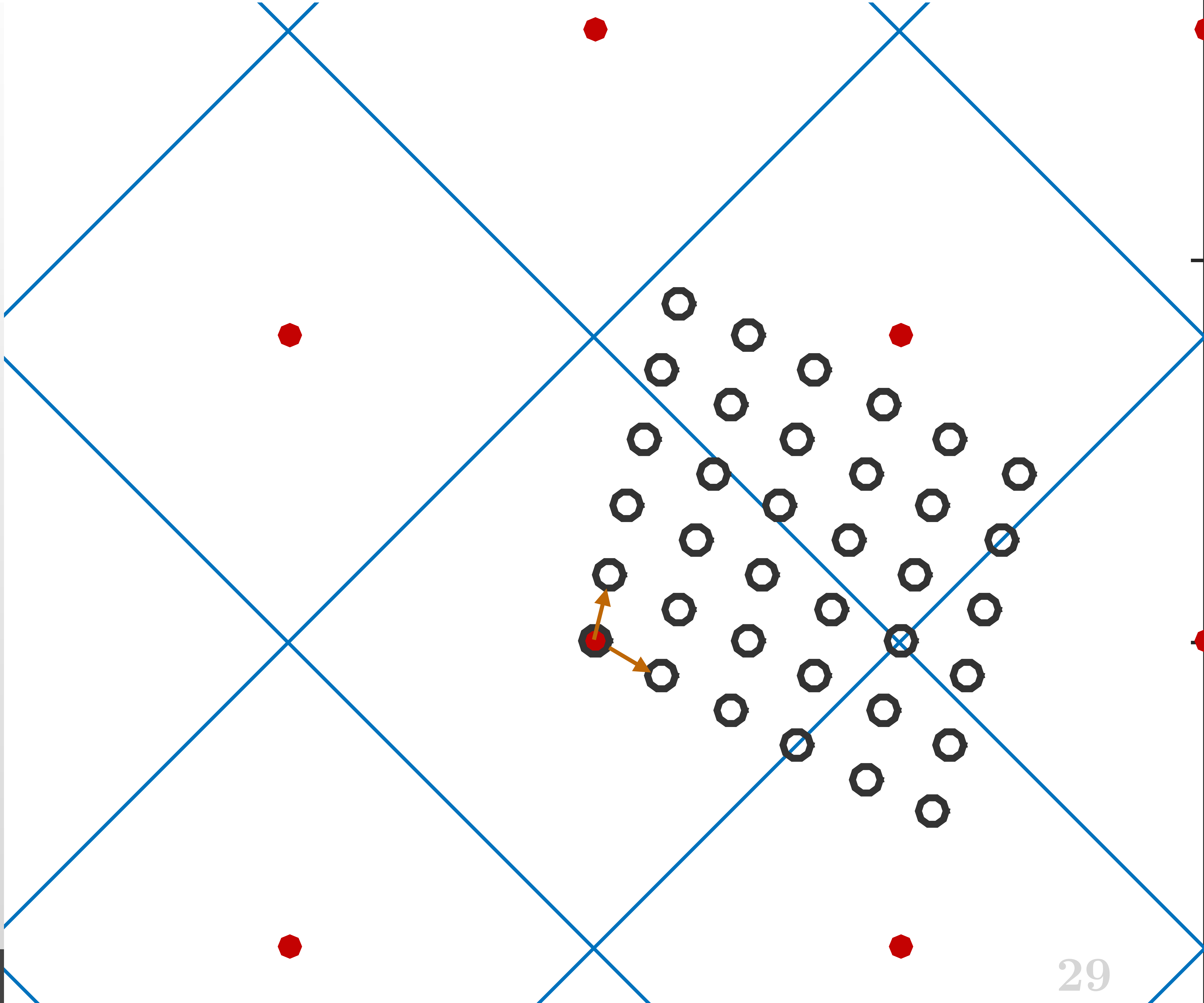
Natural candidate:

$$b_1 \in \{0,1,2,3,4,5\}$$
$$b_2 \in \{0,1,2,3,4,5\}$$

Indexing Step 1:

$$G\mathbf{b} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$$

Do these points form coset representatives?

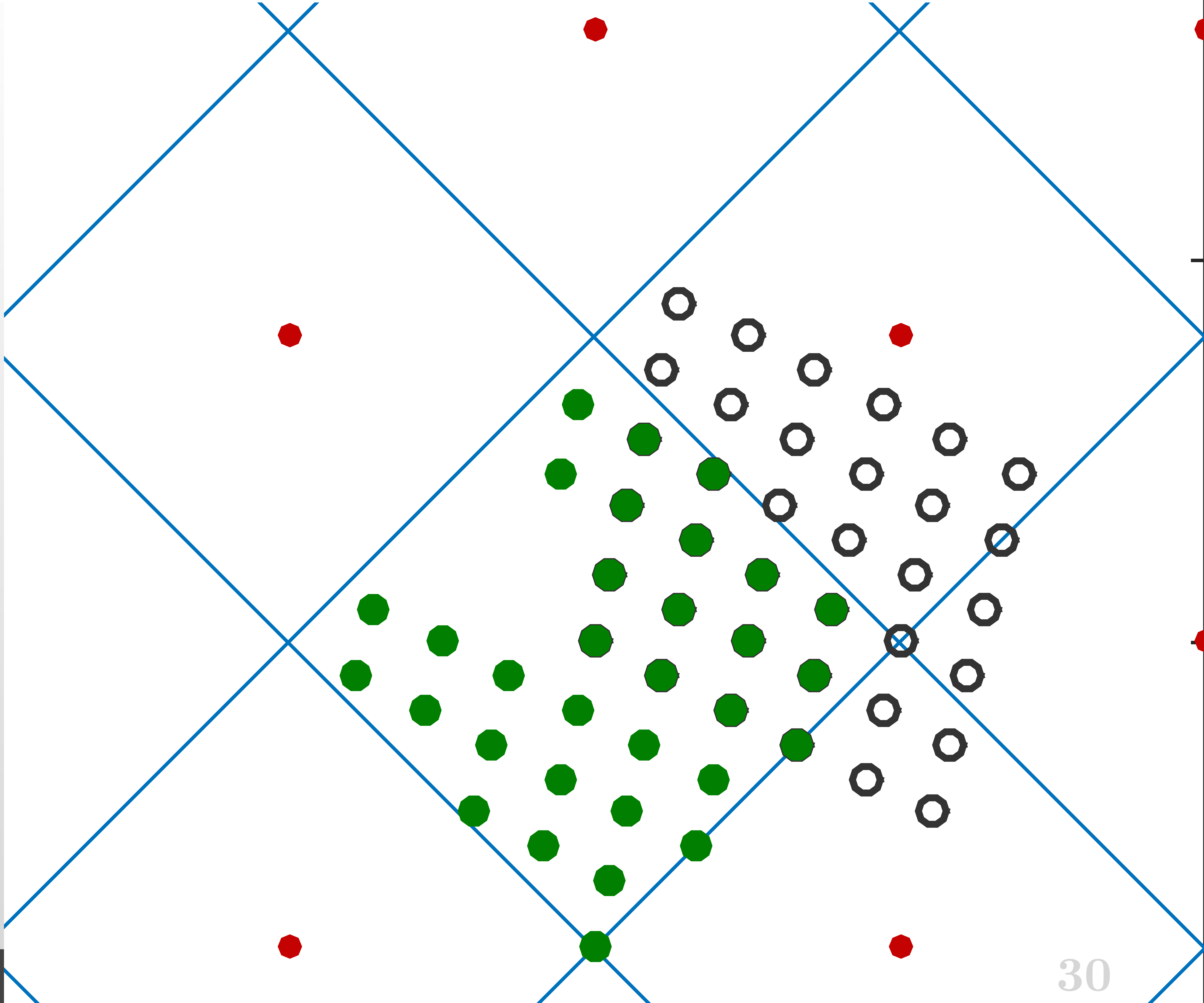


Encoding Lattice Codes, Generalized Voronoi Constellations

Indexing Step 2:

$$x = G\mathbf{b} - Q_{\Lambda_\mathrm{s}}(G\mathbf{b})$$

No! Coset representatives not formed.



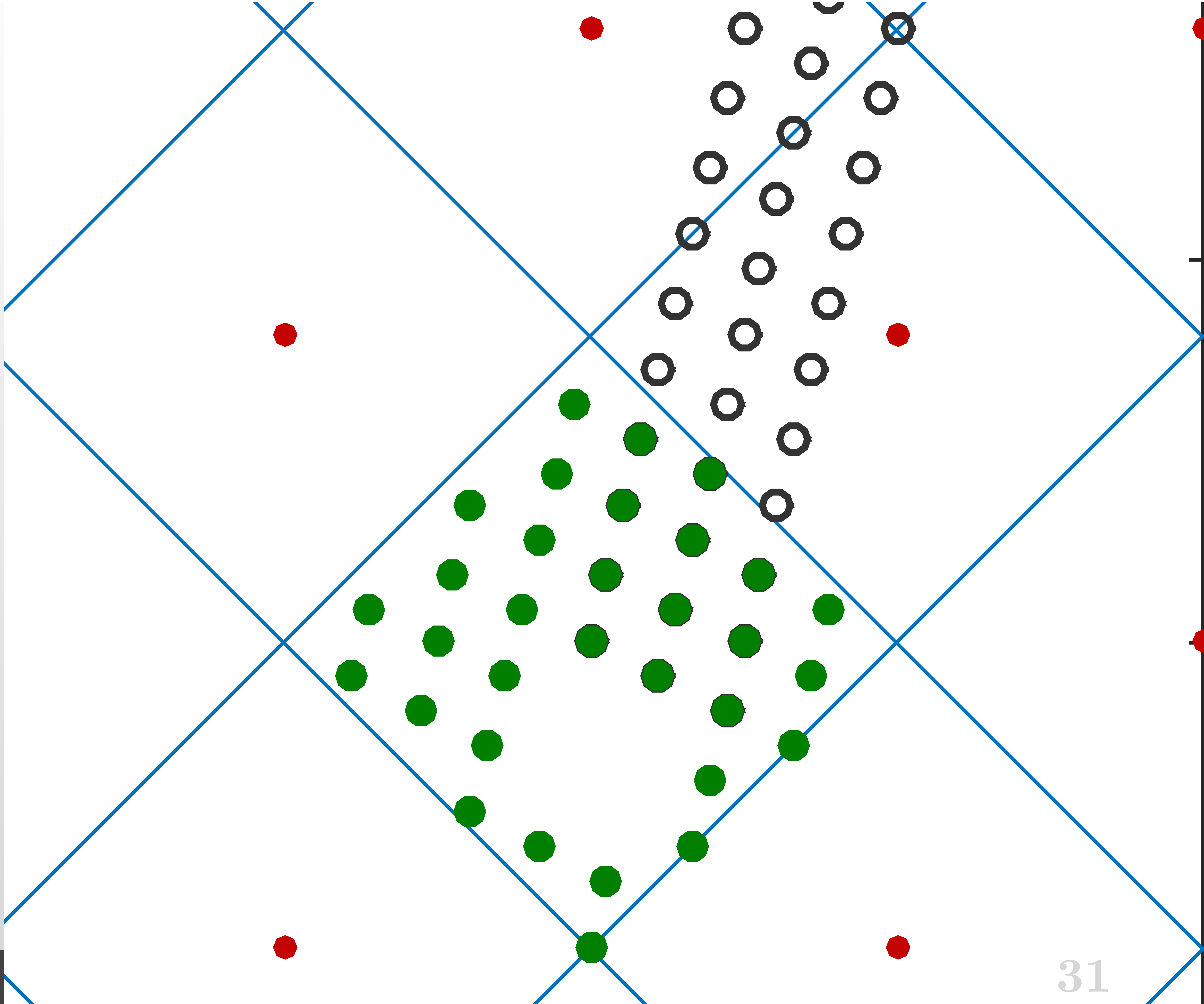
Encoding Lattice Codes, Generalized Voronoi Constellation

Another candidate:

$$b_1 \in \{0, 1, 2\}$$
$$b_2 \in \{0, 1, 2, 3, \ldots, 11\}$$

Still, no coset representatives found

What about a change of basis for G_{c}?



Finding a Basis Suitable for Encoding

Transform the basis of Λ_c from G_c to G'_c should "align" with Λ_s.

Basis transformation:

$\mathbf{g}_i$ from shaping lattice

$$G'_\mathrm{c} = G_\mathrm{c} W$$

where W is has integer entires and $\det W = 1$.

New basis is:

$$G'_\mathrm{c} = \begin{bmatrix} \frac{\mathbf{g}_1}{M_1} & \frac{\mathbf{g}_2}{M_2} & \cdots & \frac{\mathbf{g}_{n-1}}{M_{n-1}} & \mathbf{q} \end{bmatrix}$$

where $\mathbf{q}$ is some vector to be found.

Finding a Basis Suitable for Encoding

Find basis transformation W:

$$G_c' = G_c \cdot W$$
$$(G_c)^{-1} \cdot G_c' = W$$

linearly dependent

$$W = \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1,n-1} & z_1 \\ w_{21} & w_{22} & \cdots & w_{2,n-1} & z_2 \\ & \vdots & & & \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n-1} & z_n \end{bmatrix}$$

Then $\det W = 1$ is a **linear diophantine equation** in $z_1, z_2, \ldots, z_n$.

Example

$$G_c^{-1} \cdot G_c' = W$$

$$W = \begin{bmatrix} 1 & -1/4 \\ 1/2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4/3 & q_1 \\ 4/3 & q_2 \end{bmatrix} = \begin{bmatrix} 1 & z_1 \\ 2 & z_2 \end{bmatrix}$$

$$\det W = 1$$

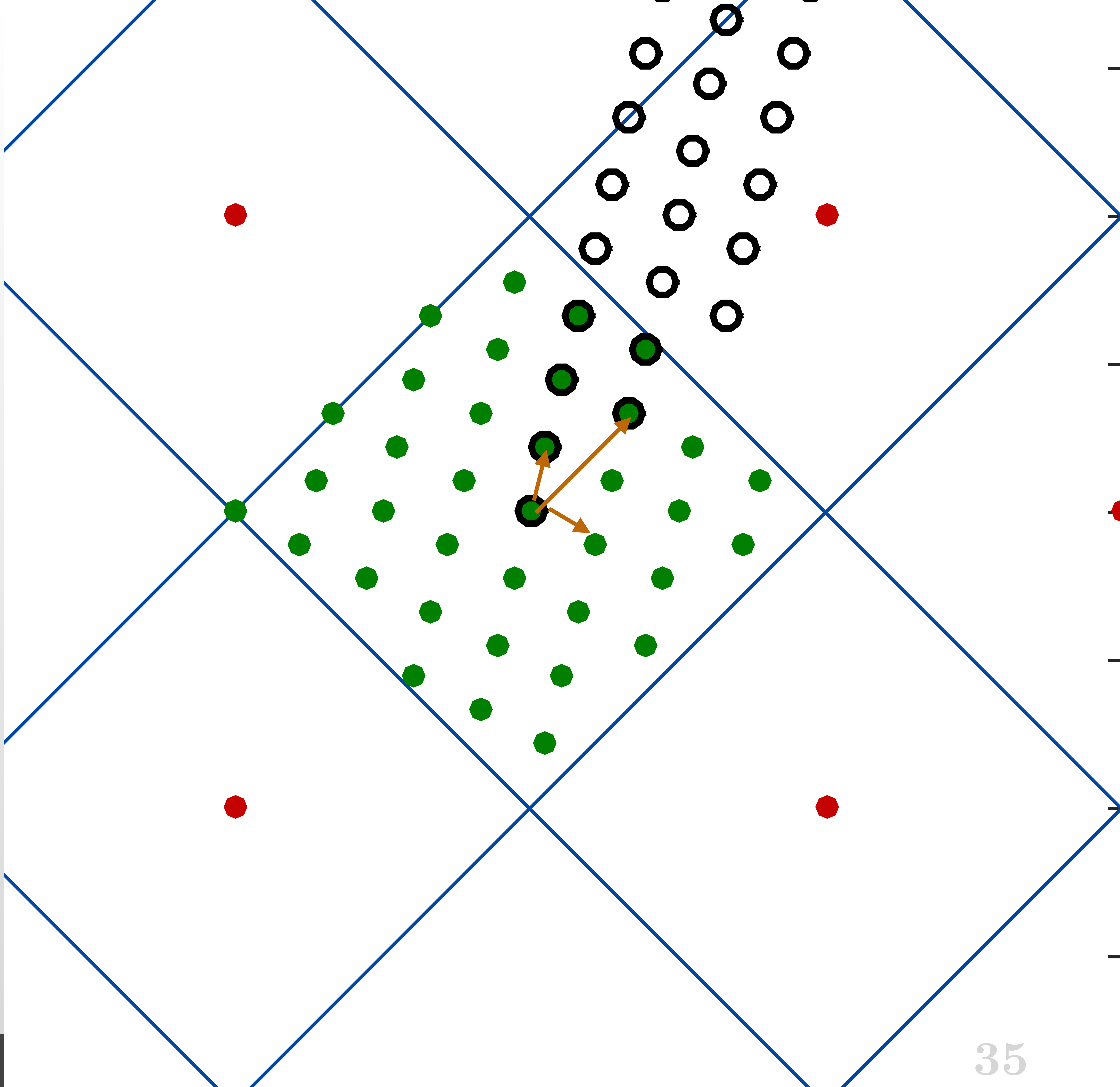
$$1z_2 - 2z_1 = 1 \qquad \leftarrow \text{diophantine equation}$$

$$\{z_1, z_2\} = \{0, 1\} \qquad \leftarrow \text{one of many solutions}$$

Encoding Non-Nested Lattice Codes Using a Suitable Basis

$$\begin{bmatrix} 1 & -1/4 \\ 1/2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4/3 & q_1 \\ 4/3 & q_2 \end{bmatrix} = \begin{bmatrix} 1 & z_1 \\ 2 & z_2 \end{bmatrix}$$

$\det W = 1 \Rightarrow 1z_2 - 2z_1 = 1$ has numerous solutions.



Discussion

Shaping gain means designing the codebook to have a sphere-like shape, to approximate the Gaussian input distribution of the AWGN channel

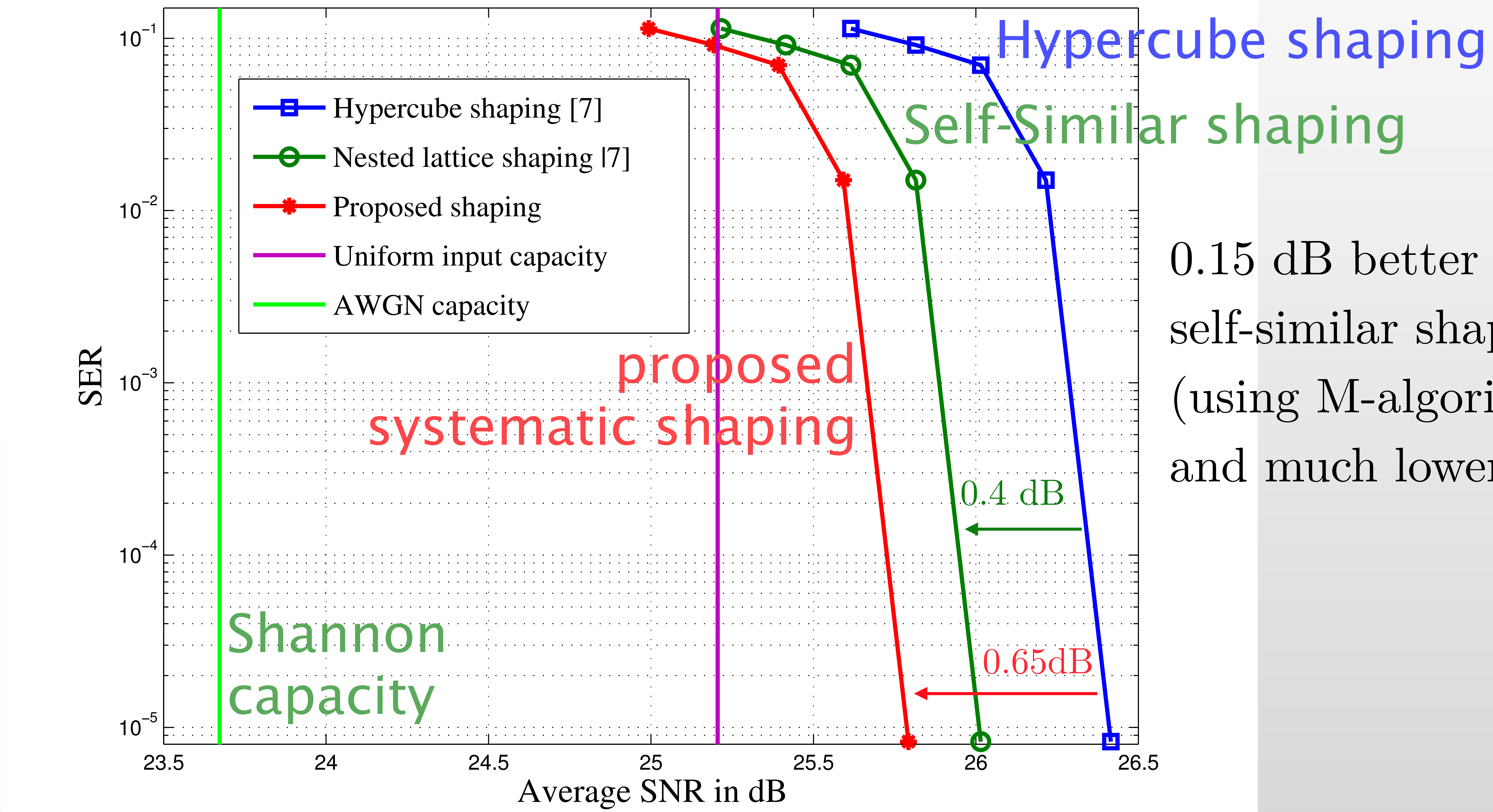
For coding lattice (LDLC, Constuction A LDPC, etc) triangular matrix:

- No shaping/cubic is easy but no shaping gain.
- Shaping using E8, BW16, etc. is also easy. Gain 0.65 to 0.86 dB
- A little bit of effort gives a big gain!
- But, triangular matrix lattices may not perform as well

For a general (non-triangular) matrices

- Shaping if we can solve a linear diophantine equation,
- Currently those coefficients get large quickly in n, practical solutions still needed

LDLCs: 0.65 dB Gain Over Hypercube



0.15 dB better than self-similar shaping (using M-algorithm) and much lower complexity