Notes on Indexing Cosets of Lattice Codes

Brian M. Kurkoski
Japan Advanced Institute of Science and Technology

JAIST
JAPAN ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY
1990

May 28, 2015
9th Asian-European Workshop on Information Theory (AEW9)
Dogo Onsen, Ehime, Japan

What I Want to Tell You

Lattices are codes over the real numbers.

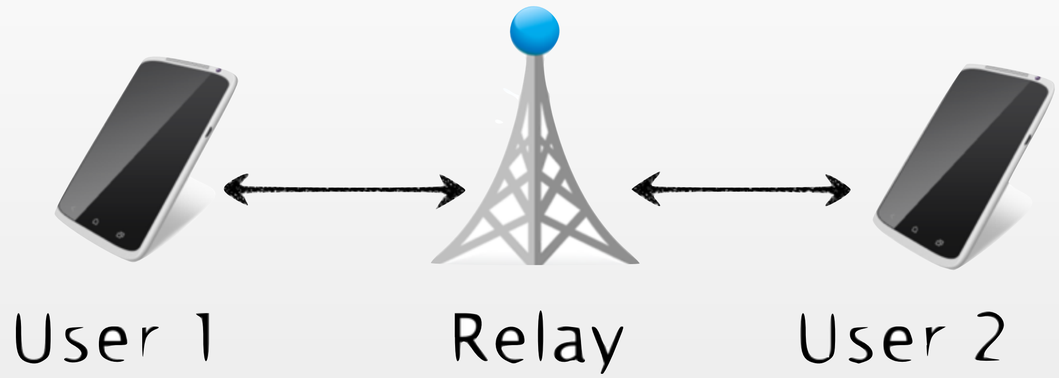
Network information theory uses **nested lattice codes,**

- Difficult to implement in practice.

Propose an alternative: “Non nested lattice codes”

- Shaping lattice is not a scaled coding lattice,
- Show: How to obtain group property,
- Show: How to map information.

Usefulness of Lattice Codes



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

Other *information theoretic* results 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]

How to construct practical, capacity-approaching lattices?

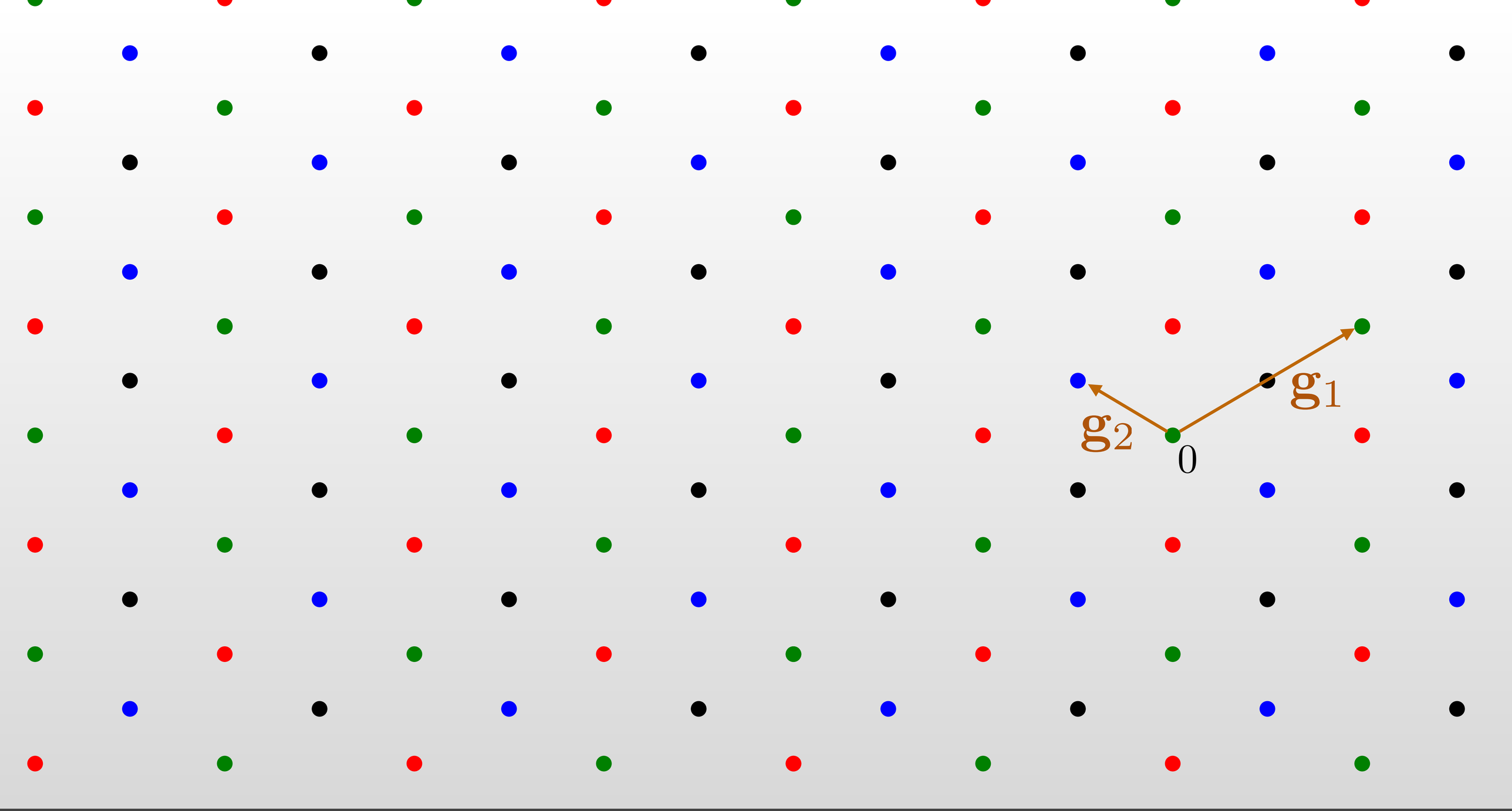
A lattice Λ is a linear additive subgroup of $\mathbb{R}^n$.

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 $b_i \in \mathbb{Z}$.

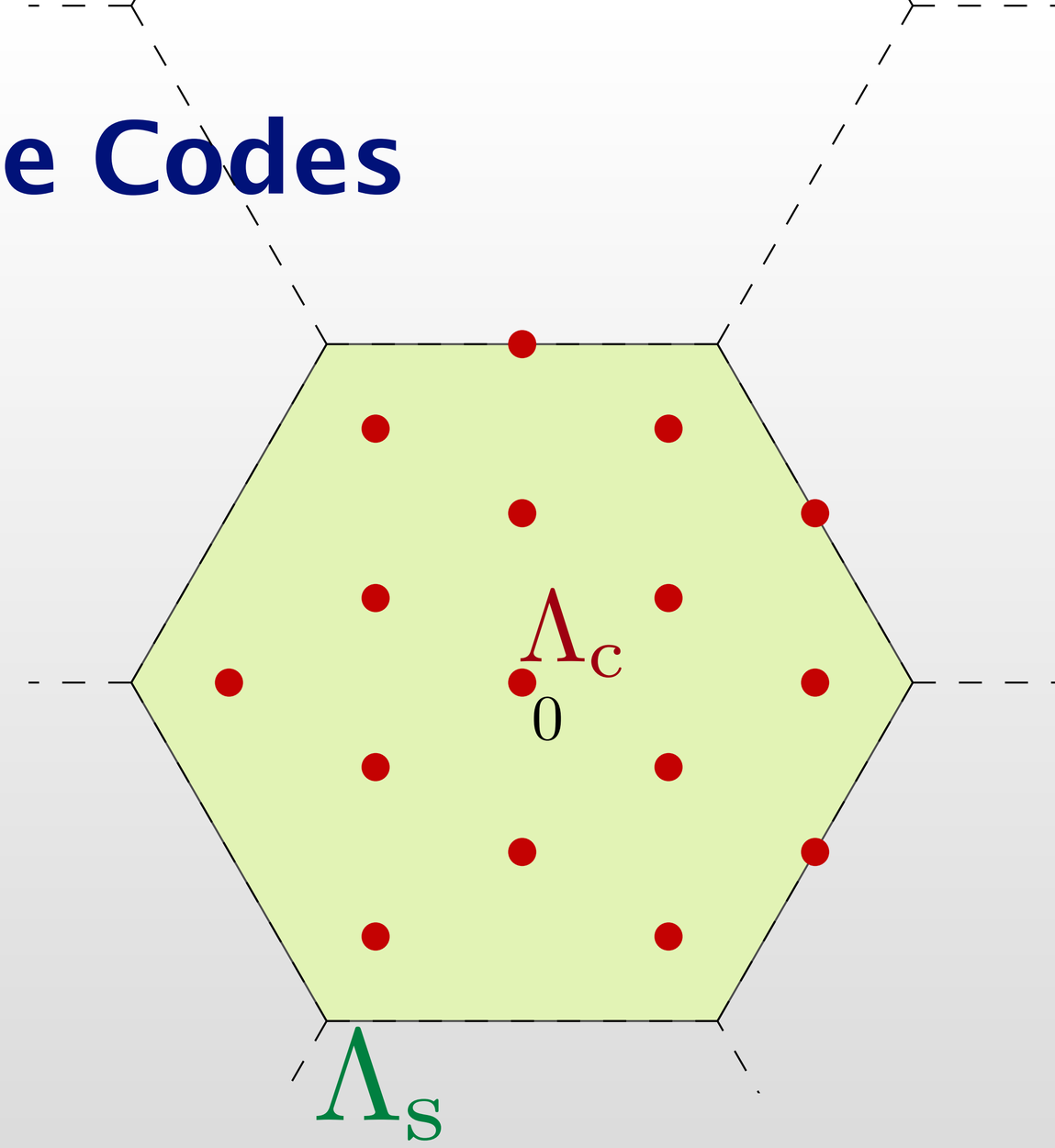
Given Λ, there are arbitrarily many possible bases.


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

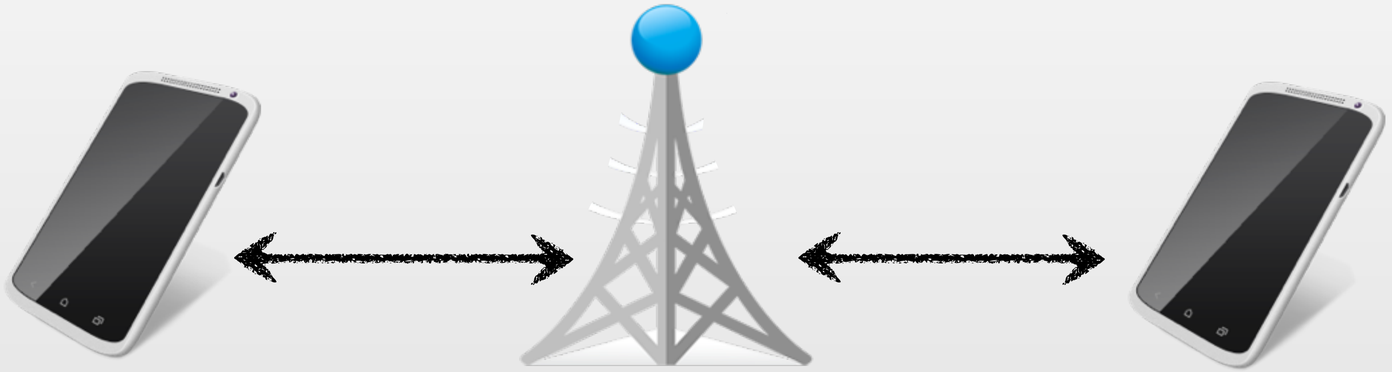
Nested Lattice Codes

Nested lattice code Λ_c/Λ_s:

- Λ_c is good for coding
- Λ_s is good for shaping, satisfies power constraint
- $\Lambda_s \subset \Lambda_c \Rightarrow$ quotient group Λ_c/Λ_s for network coding
- Nested lattice code: $\Lambda_s = M\Lambda_c, M = 2, 3, 4, \ldots$.



Physical Layer Network Coding for Bidirectional Relay Channel



User 1

has w_1

wants w_2

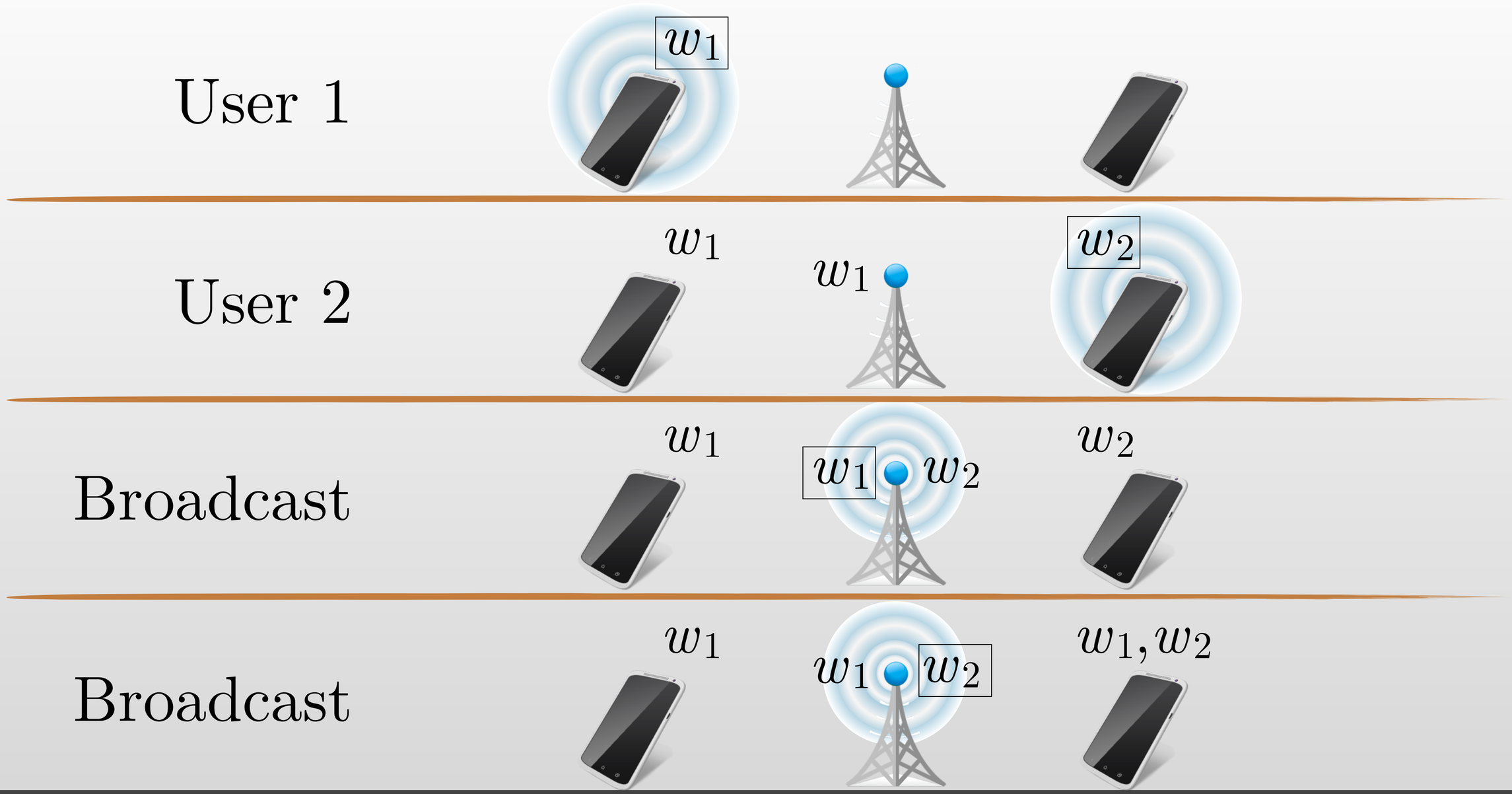
Relay

User 2

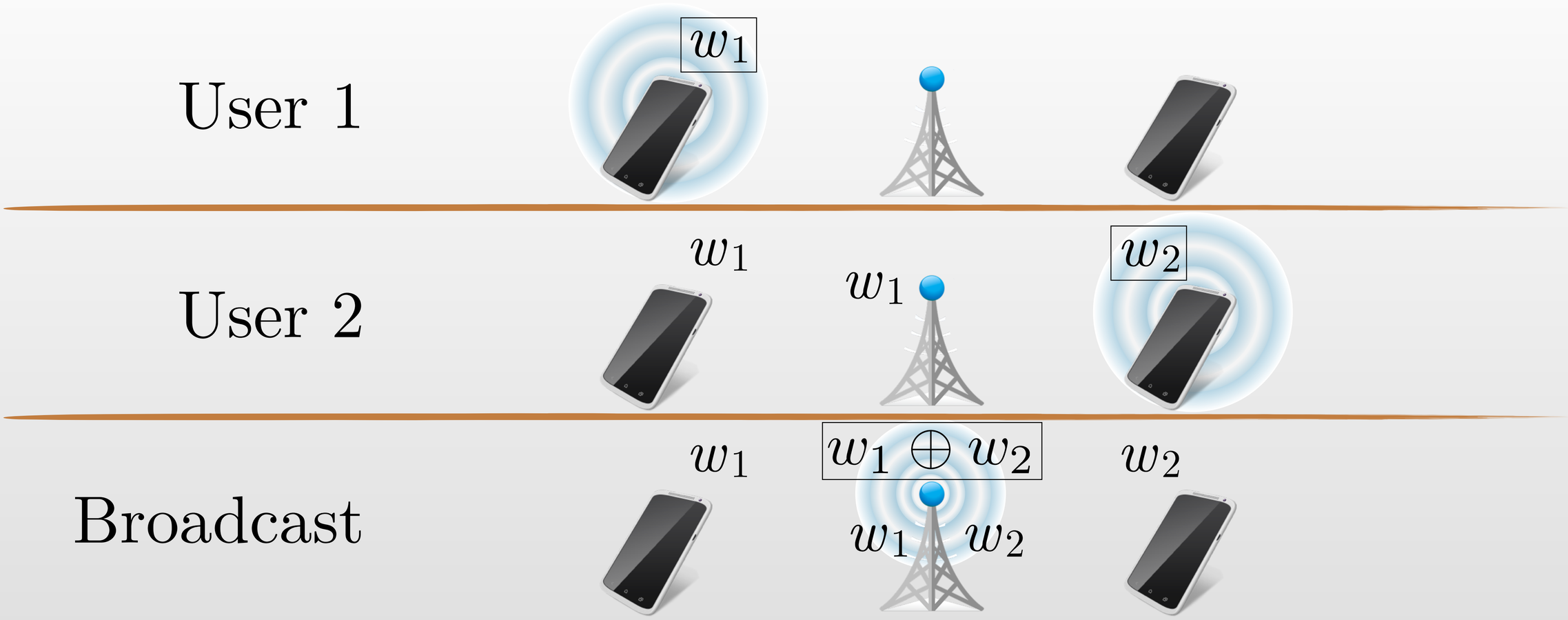
has w_2

wants w_1

Time Division/Orthogonal

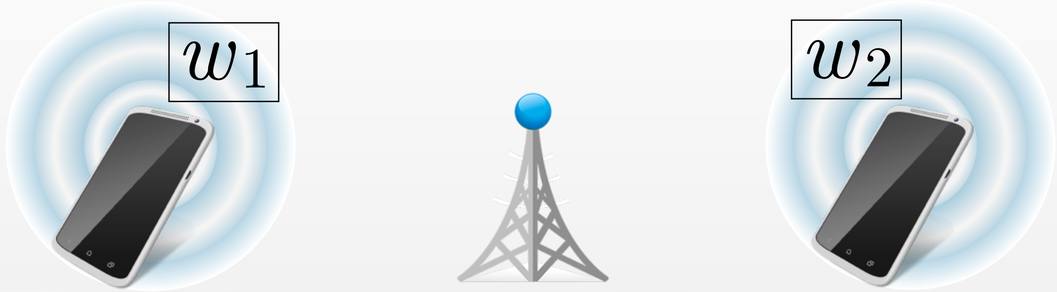


Network Coding

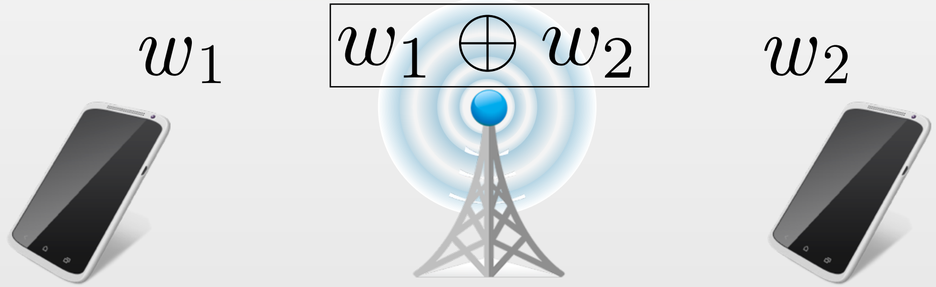


Physical Layer Network Coding

Phase 1: MAC



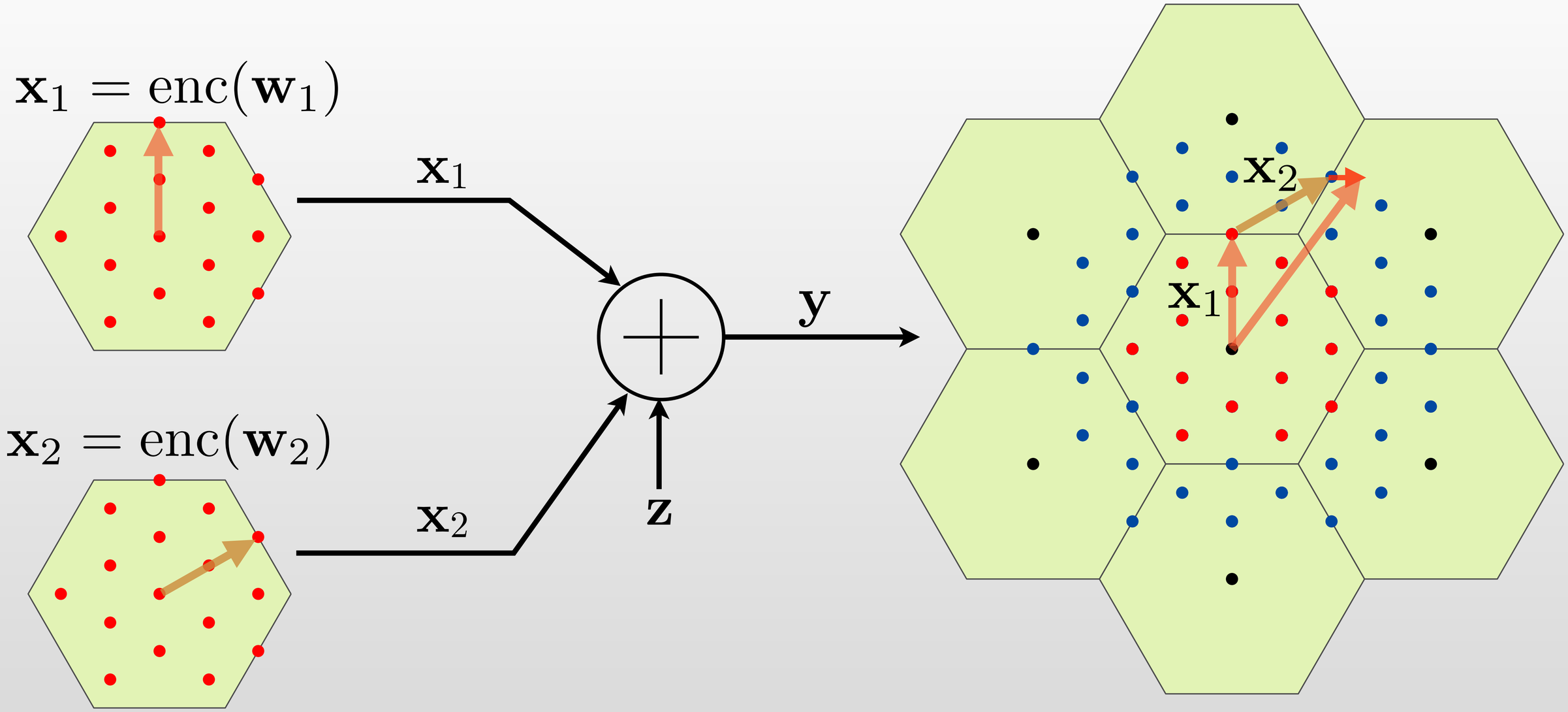
Phase 2: Broadcast

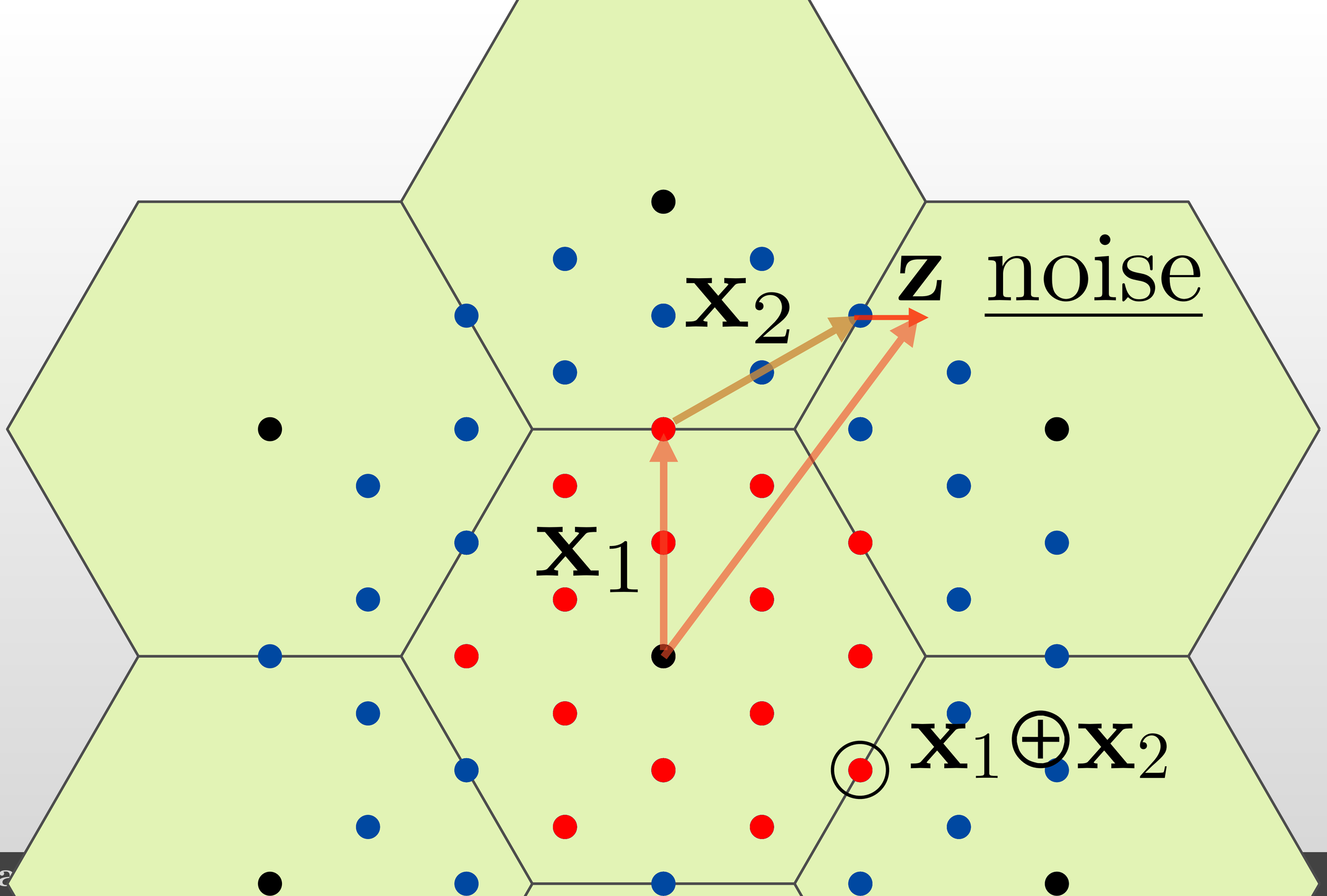


Summary

- Orthogonal: uses 4 time slots
- Network coding: uses 3 time slots
- Physical layer network coding: uses 2 time slots

Bidir Relay Channel: MAC Phase




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

What Should Lattice Codes Provide?

High coding gain

- means high error-correcting capability

High shaping gain

- AWGN channel wants a Gaussian-like input distribution
- As n $\rightarrow$ infinity, Voronoi region of a good lattice becomes sphere-like
  (and a sphere a Gauassian-like distribution)
- 1.53 dB "shaping gain" for a sphere

Lattice codes forms a group

- Enables physical-layer network coding

So What is the Problem?

✅ Already many lattices with high coding gain

Construction A, D; LDLC, etc.

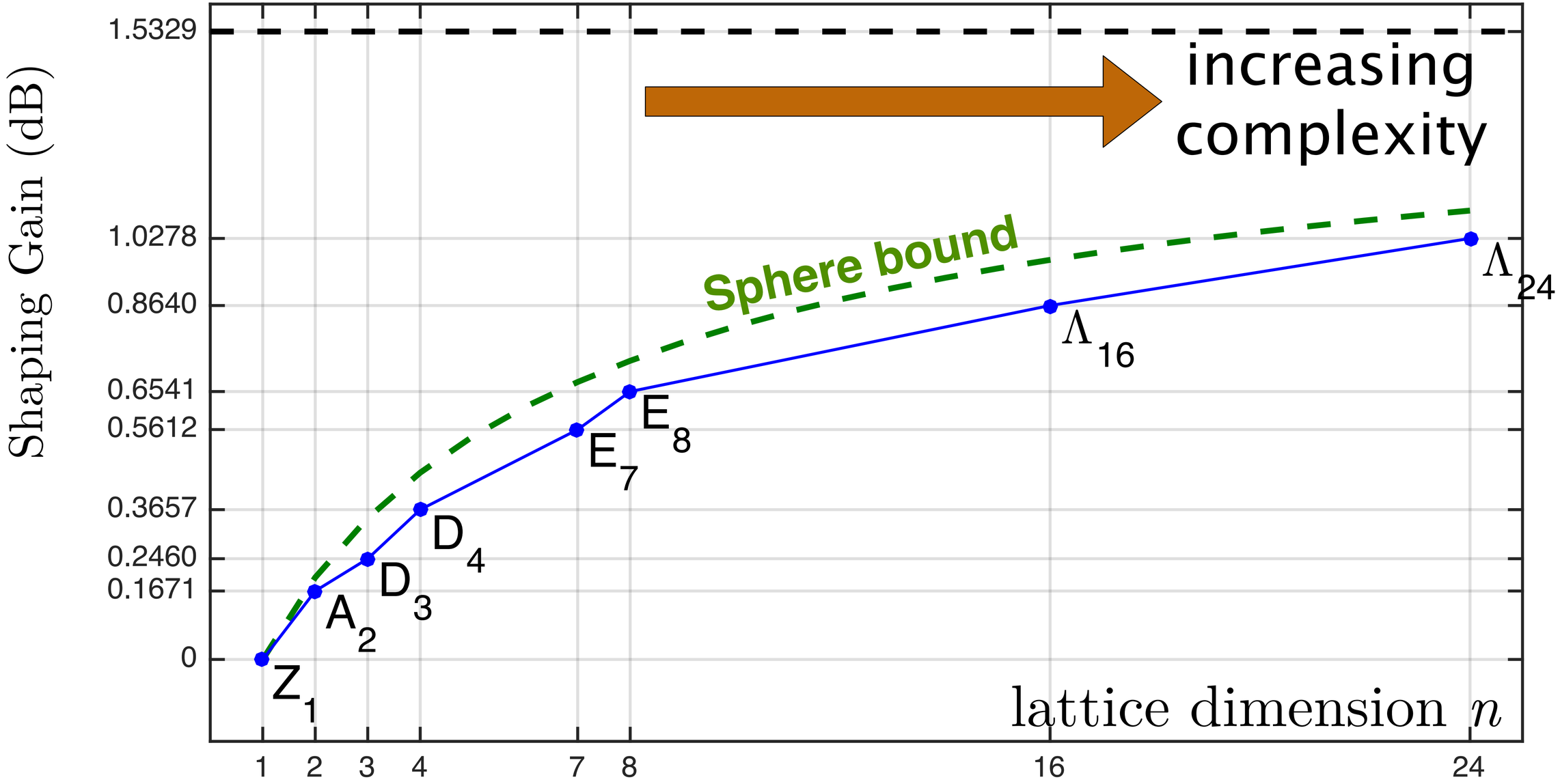
dimension $n = 1{,}000$ to $100{,}000$ no problem!

Nested lattice codes: $\Lambda_{\mathrm{s}} = M\Lambda_{\mathrm{c}}$ dimension is the same

Shaping requires performing quantization

❌ **Quantization in high dimension is very complicated**

Shaping Gain for Well-Known Lattices



This is the Solution

Target is construction of a lattice code:

$$n\text{-dim lattice} \longrightarrow \Lambda_c/\Lambda_s \times \Lambda_s \times \cdots \times \Lambda_s \longleftarrow \frac{n}{m} \text{ product of } m\text{-dim lattice}$$

Questions:

- Is $\Lambda_c \subseteq \Lambda_s \times \cdots \times \Lambda_s$?
- How to index the lattice code?

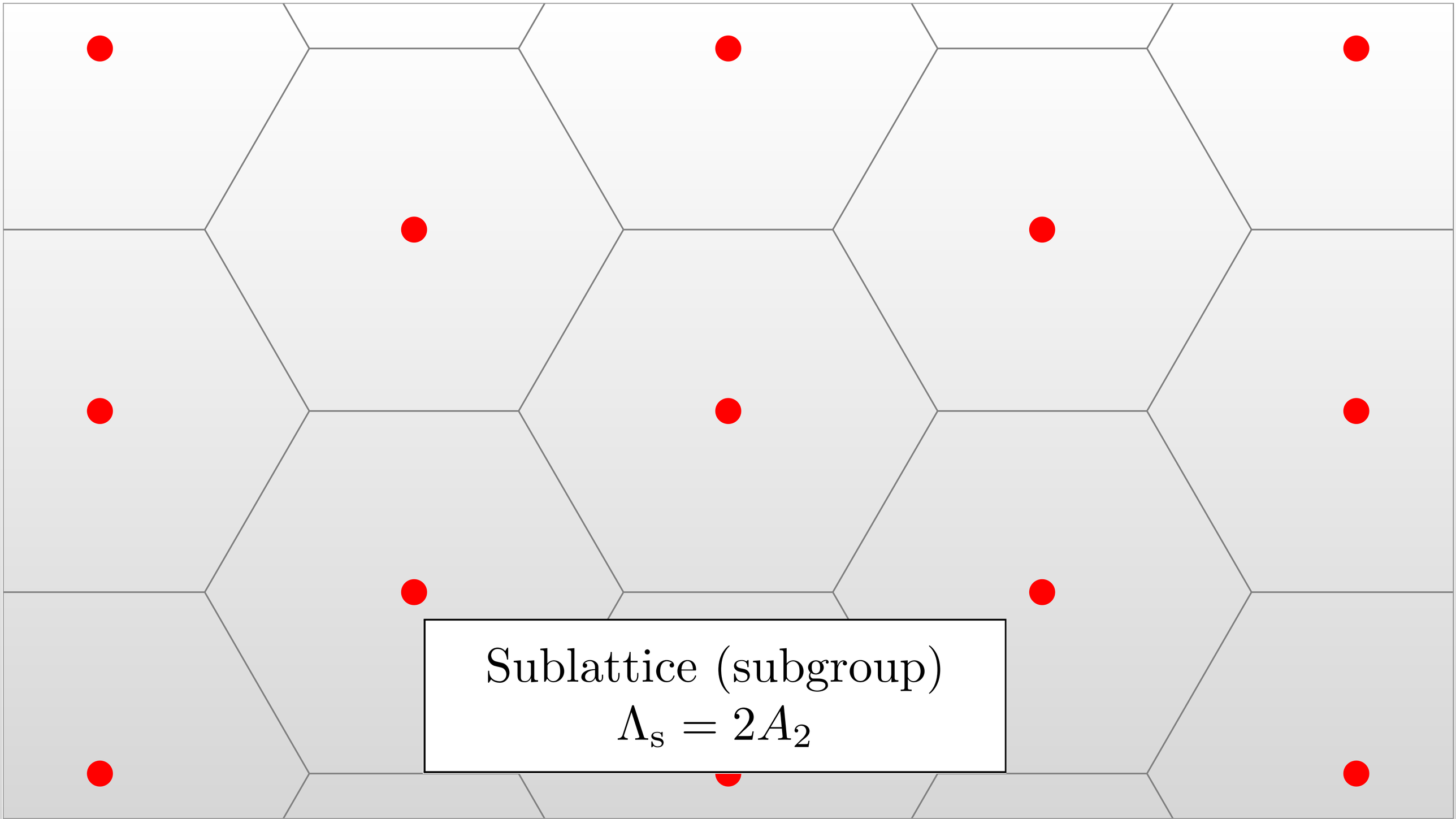
In this talk, just use Λ_c/Λ_s so we can easily handle 2-dim examples.

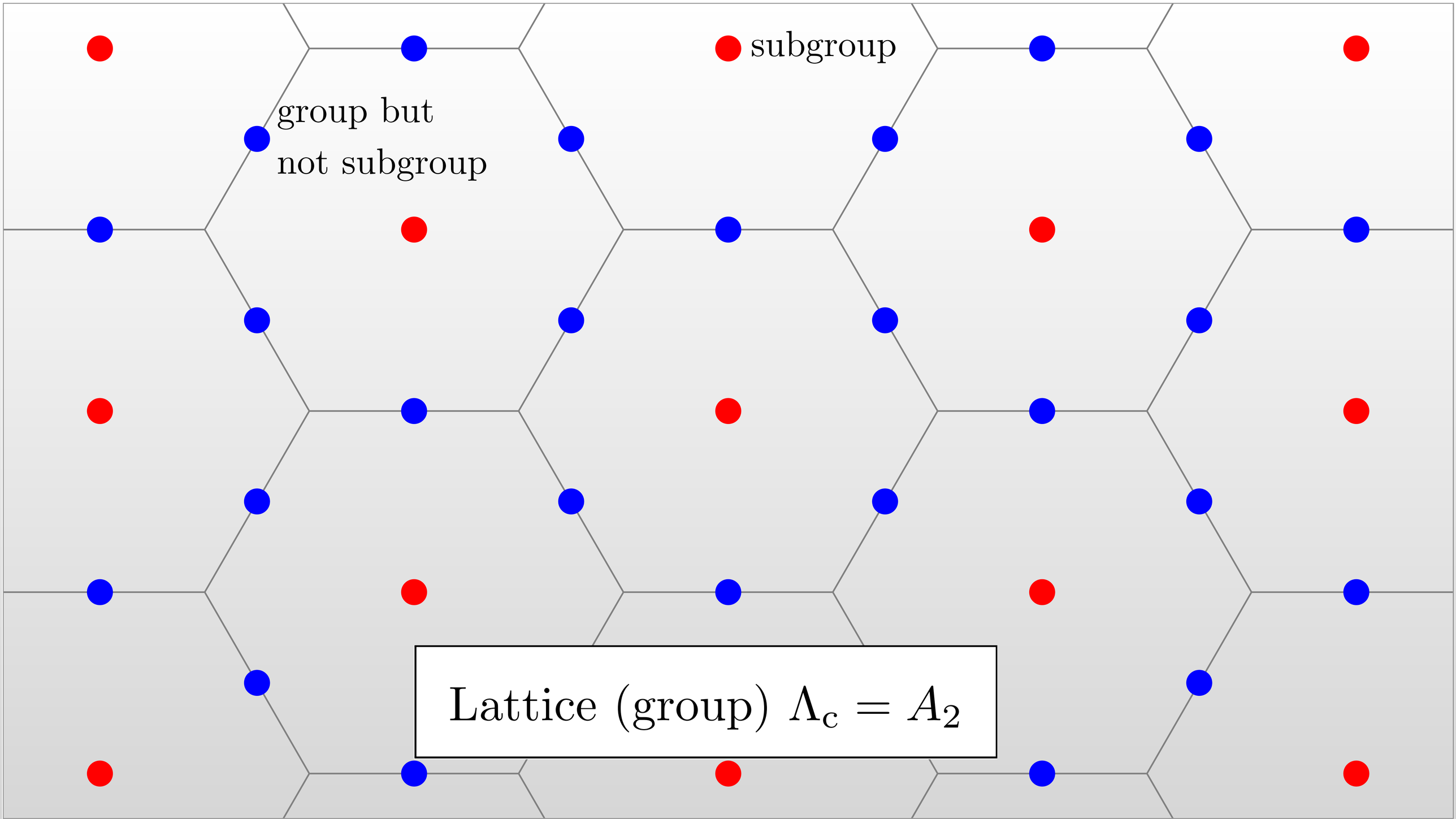
Quotient Groups Based on Lattices

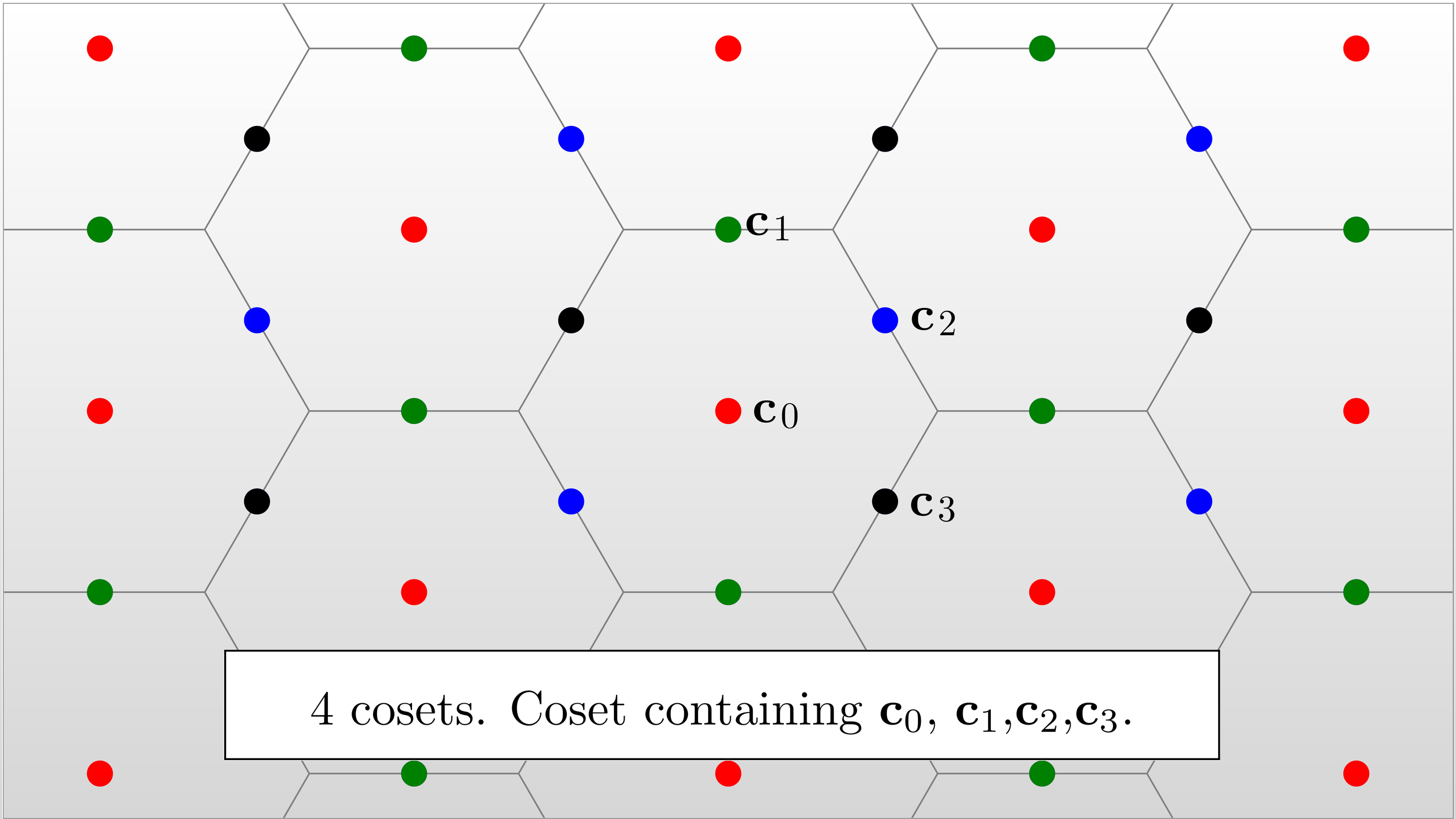
Let Λ_c be a lattice.

Let Λ_s be a sublattice: $\Lambda_s \subset \Lambda_c$.

Note that $\Lambda_s = M\Lambda_c$ satisfies this condition.


Sublattice (subgroup)
$\Lambda_s = 2A_2$


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



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

Sufficient Conditions to form a Group

Λ_{s} has a generator matrix G with all entries $g_{i,j}$ integers.

Definition $g_{\min}$ is the greatest common divisor: $g_{\min} = \mathrm{GCD}(|g_{i,j}|)$

Λ_{c} has a check matrix $H = G_{\mathsf{c}}^{-1}$, with entries $h_{i,j}$

Lemma

$$\text{If } \; h_{i,j} \in \frac{1}{g_{\min}}\mathbb{Z} \quad \Rightarrow \quad \Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}}$$

If $\Lambda_{\mathrm{s}} \subseteq \Lambda_{\mathrm{c}}$, then $\Lambda_{\mathrm{s}}/\Lambda_{\mathrm{c}}$ forms a quotient group.

Indexing Lattice Codes

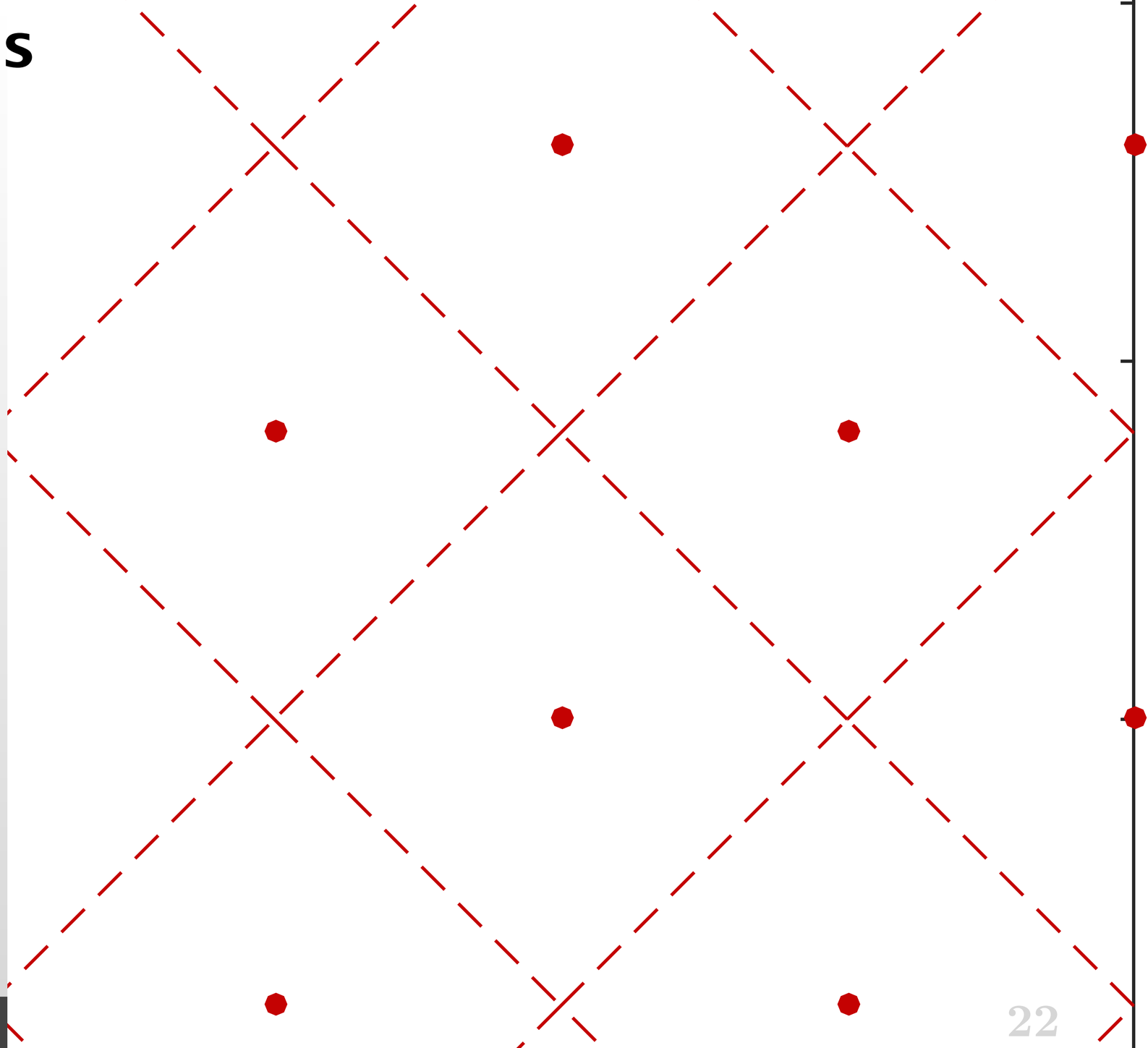
"Indexing" means mapping information to lattice code points.

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



Indexing Lattice Codes

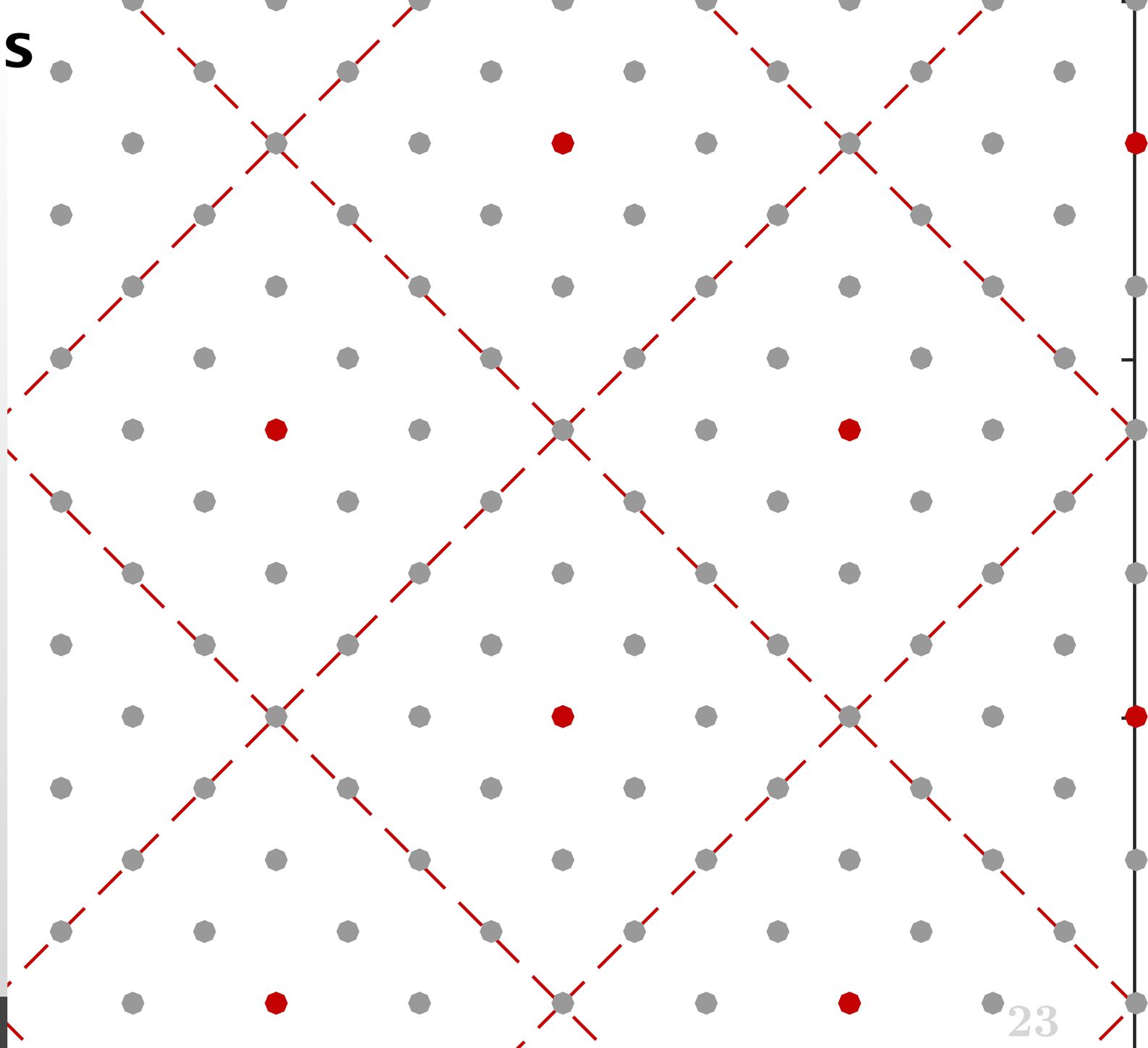
"Indexing" means mapping information to lattice code points.

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



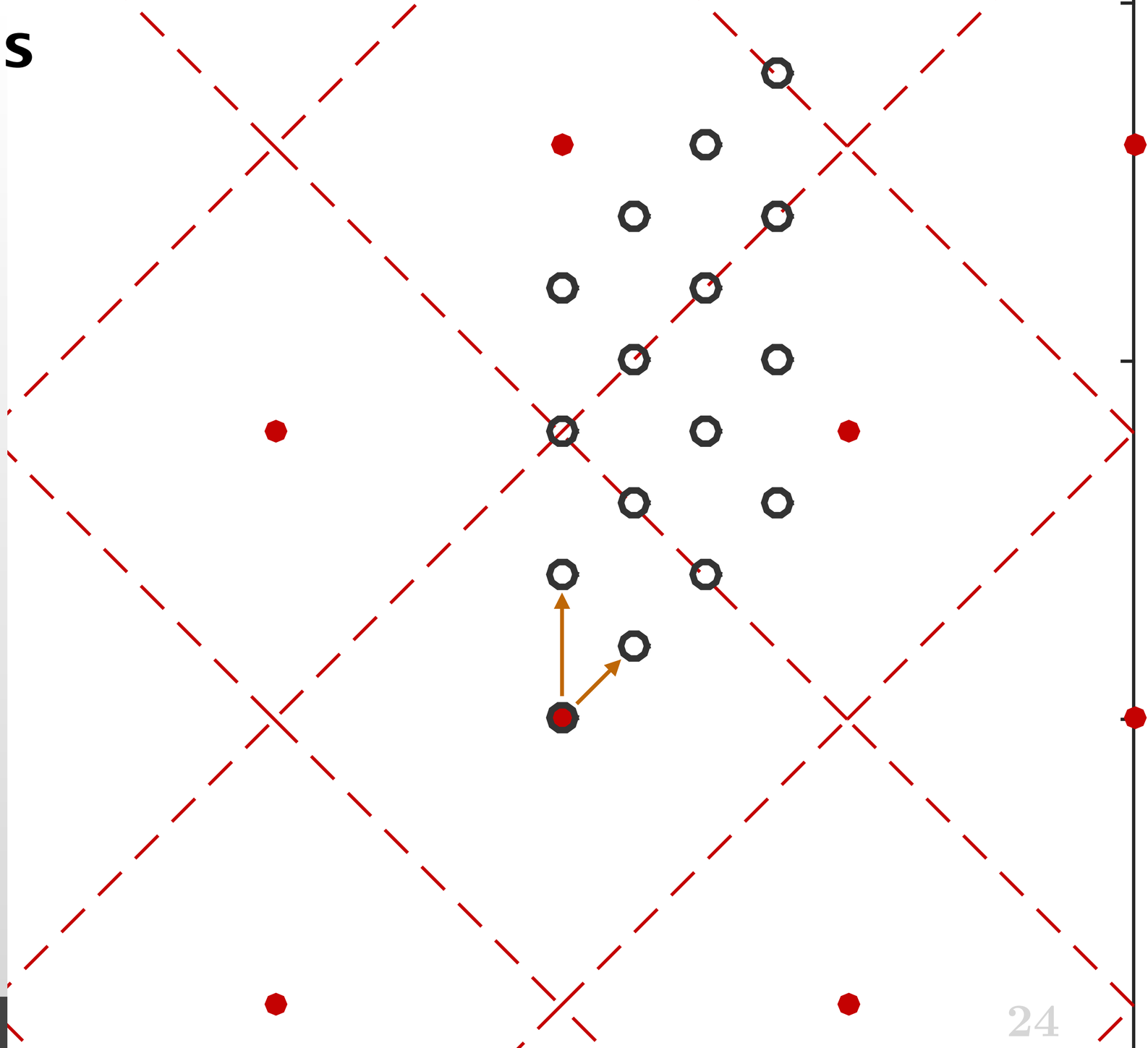
Indexing Lattice Codes

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)

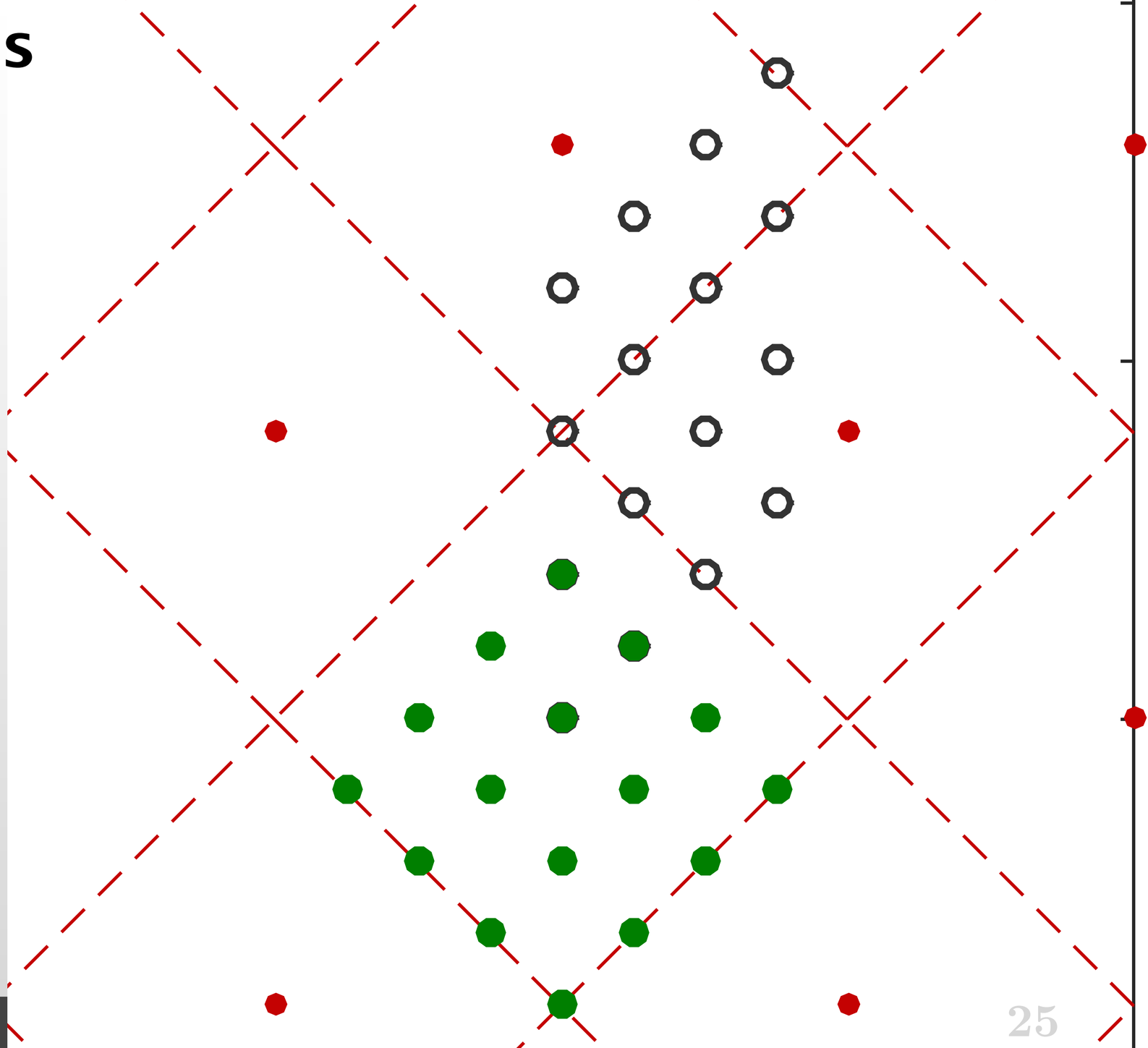


Indexing Lattice Codes

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

Indexing Step 2:

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



Indexing Non-Nested Lattice Codes

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

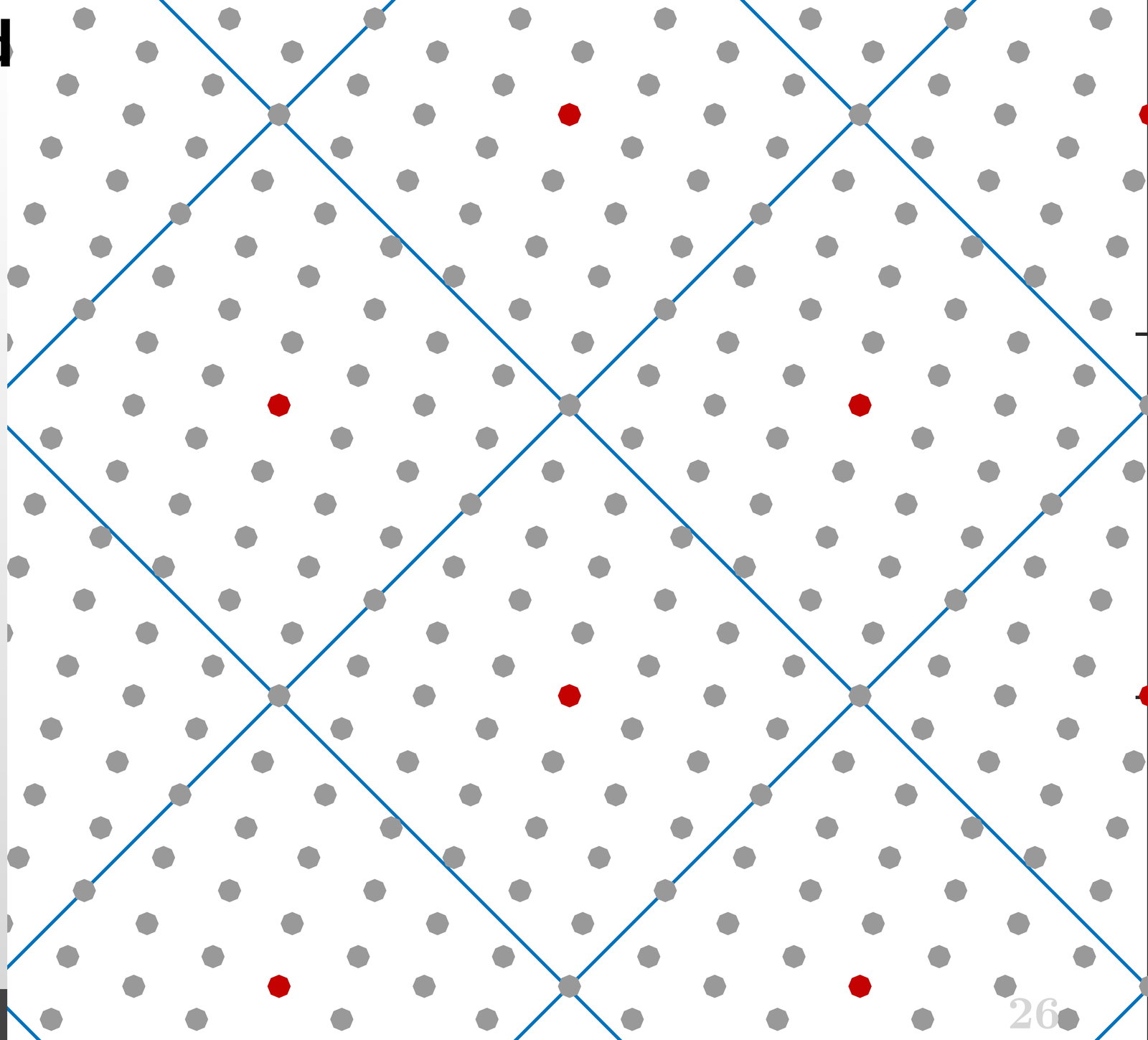
Example:

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

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

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

Not a nested lattice code!



Indexing Non-Nested Lattice Codes

Number of codewords:

$$\frac{\det(G_{\mathrm{s}})}{\det(G_{\mathrm{c}})} = 36$$

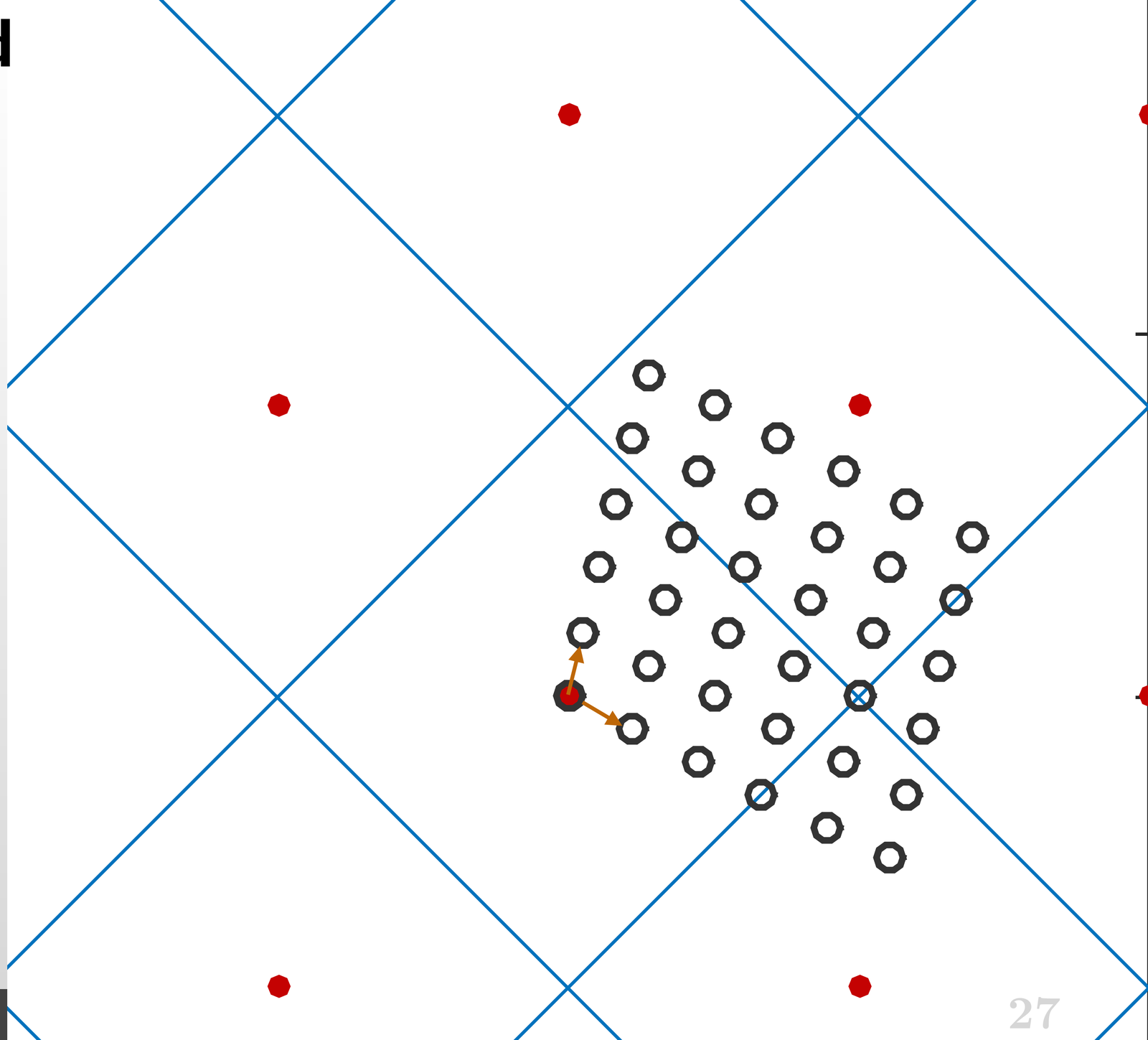
Natural candidate:

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

Indexing Step 1:

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

Do these points form coset representatives?

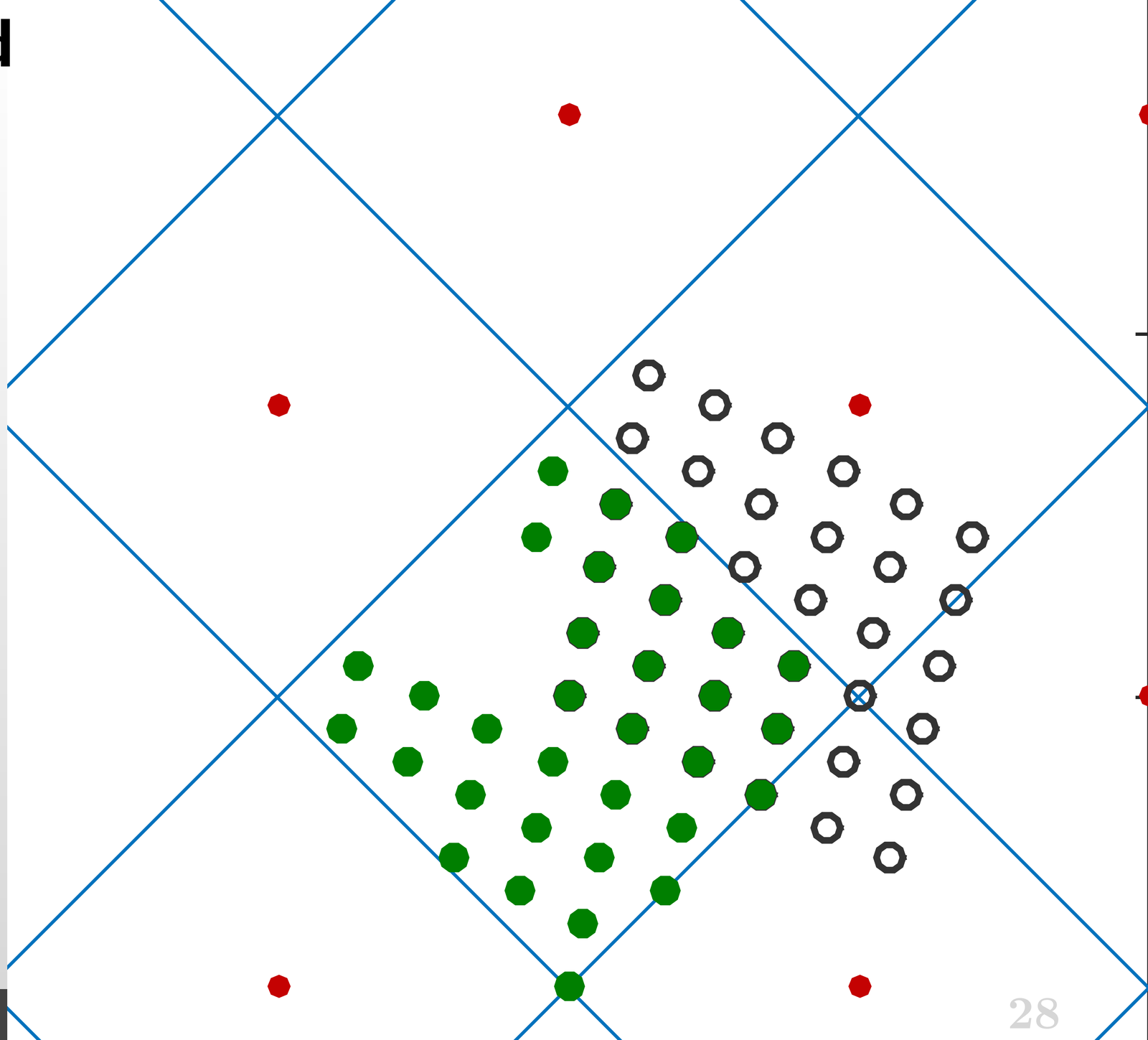


Indexing Non-Nested Lattice Codes

Indexing Step 2:

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

No! Coset representatives not formed.



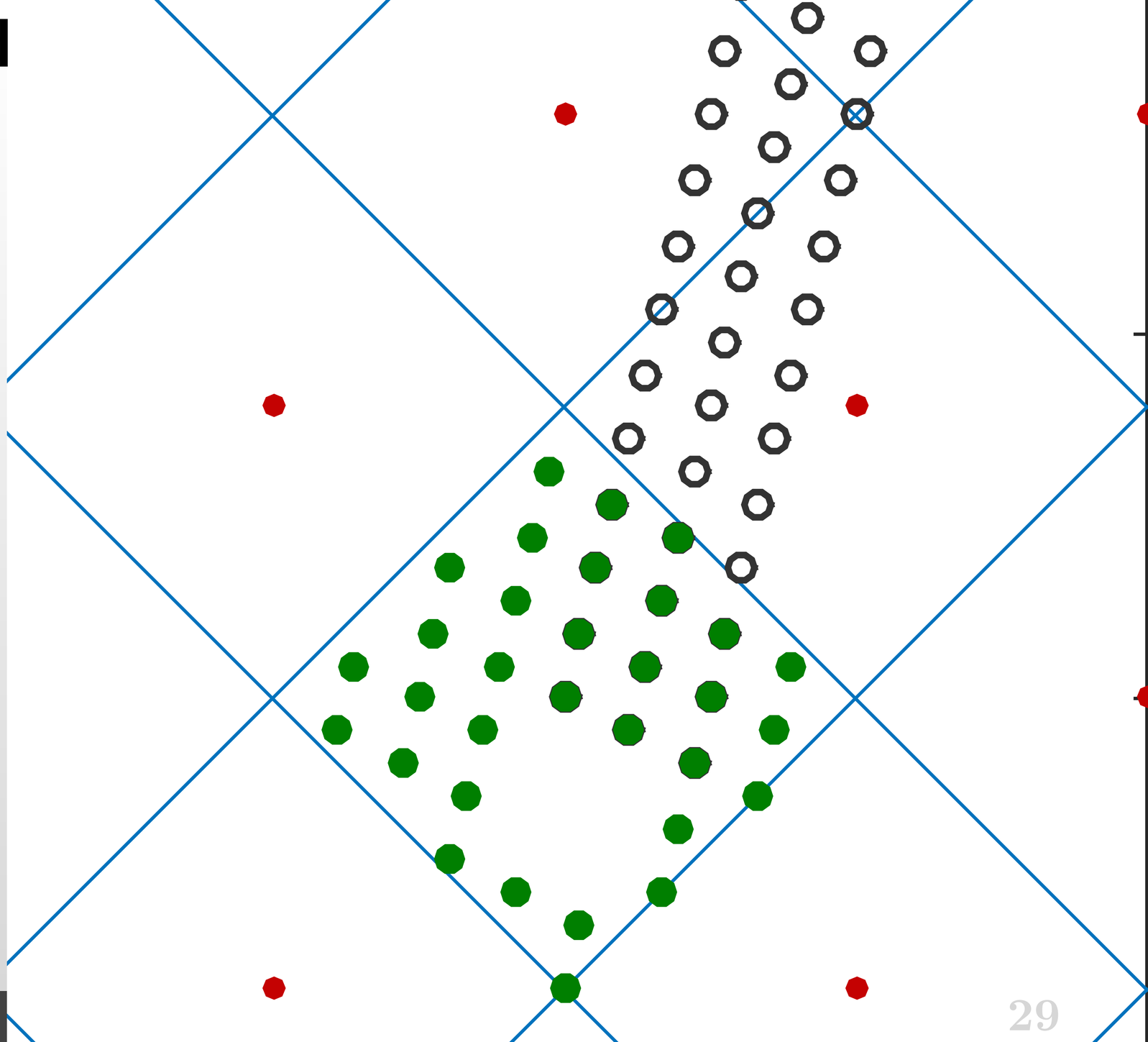
Indexing Non-Nested Lattice Codes

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

We want to transform the basis of G_c:

$$G'_c = G_c W$$

$\mathbf{g}_i$ from shaping lattice

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

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

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

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

linearly dependent

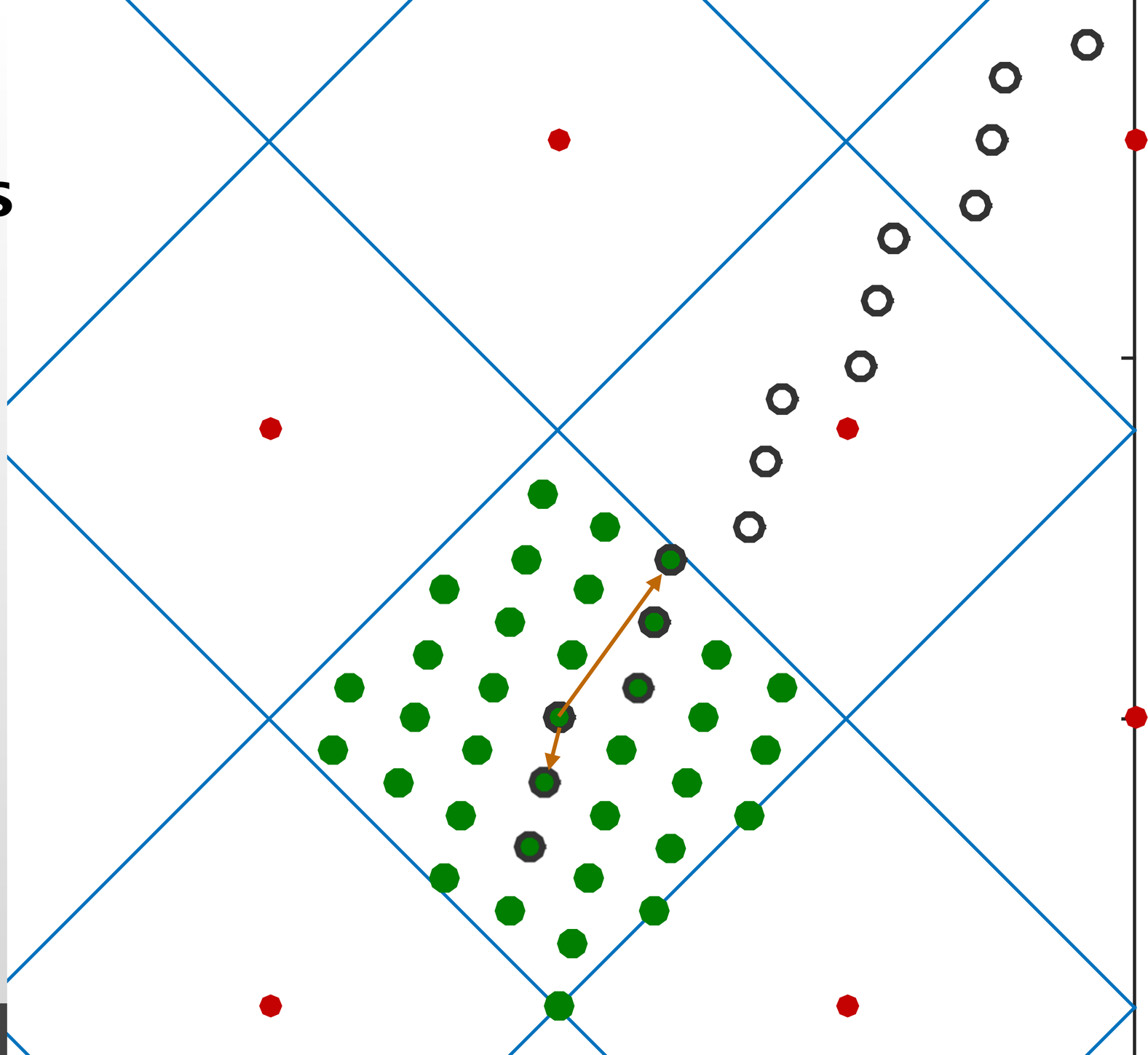
$$= \begin{bmatrix} w_{11} & w_{12} & \cdots & w_{1,n-1} & z_1 \\ w_{21} & w_{22} & \cdots & w_{2,n-1} & z_2 \\ & \vdots & & & \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n-1} & z_n \end{bmatrix}$$

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

Indexing 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.



Brian Kurkoski, JAIST

Conclusion

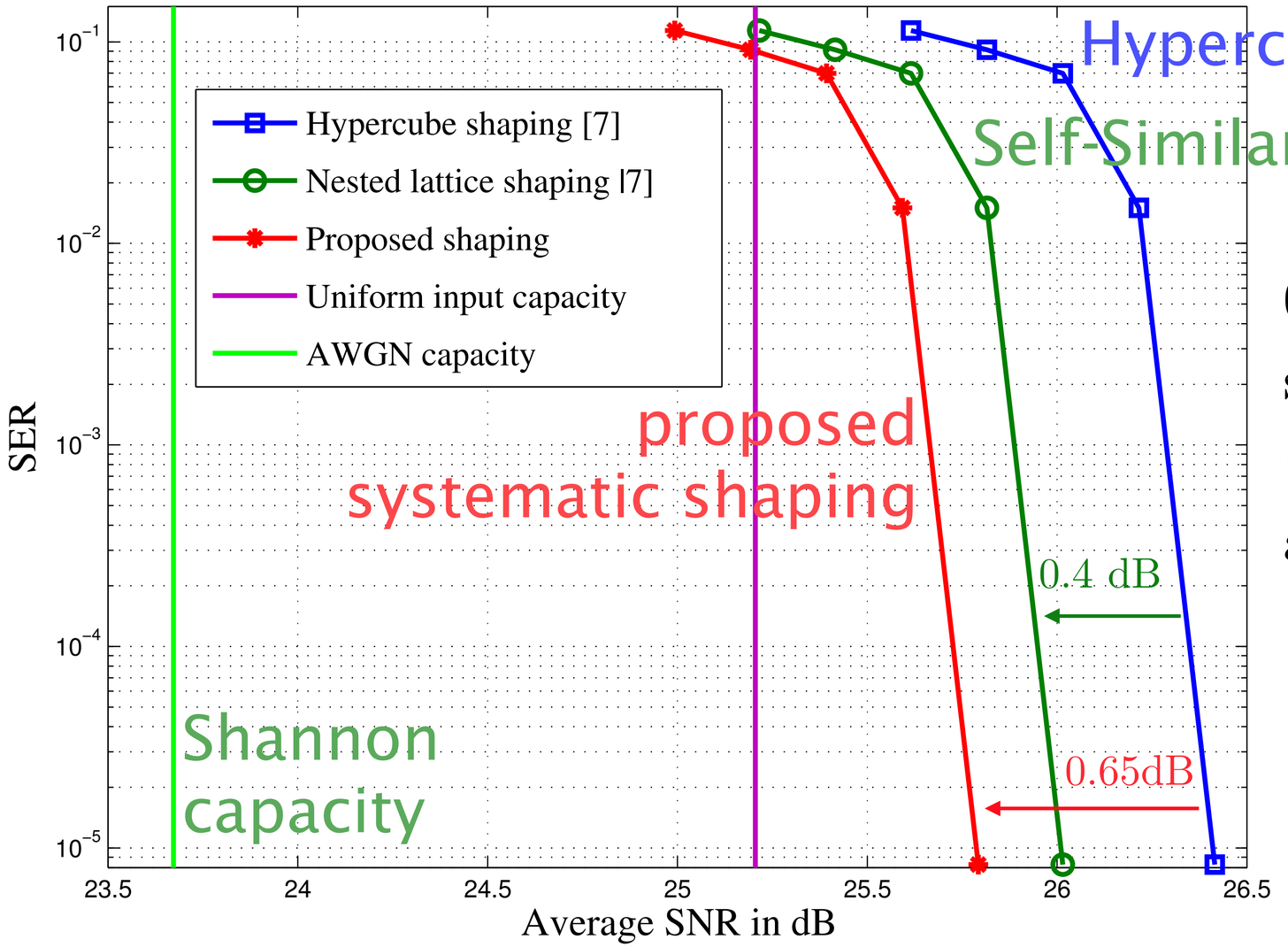
Indexing lattice codewords is not as easy as I thought

- Perform a basis change.
- Need to know necessary/sufficient conditions

Application Scenario:

- Coding lattice: LDLC with $n = 10000$
- Shaping lattice like E8 or Leech

LDLCs: 0.65 dB Gain Over Hypercube



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