

An Introduction to Physical Layer Network Coding: Lattice Codes as Groups

Brian M. Kurkoski

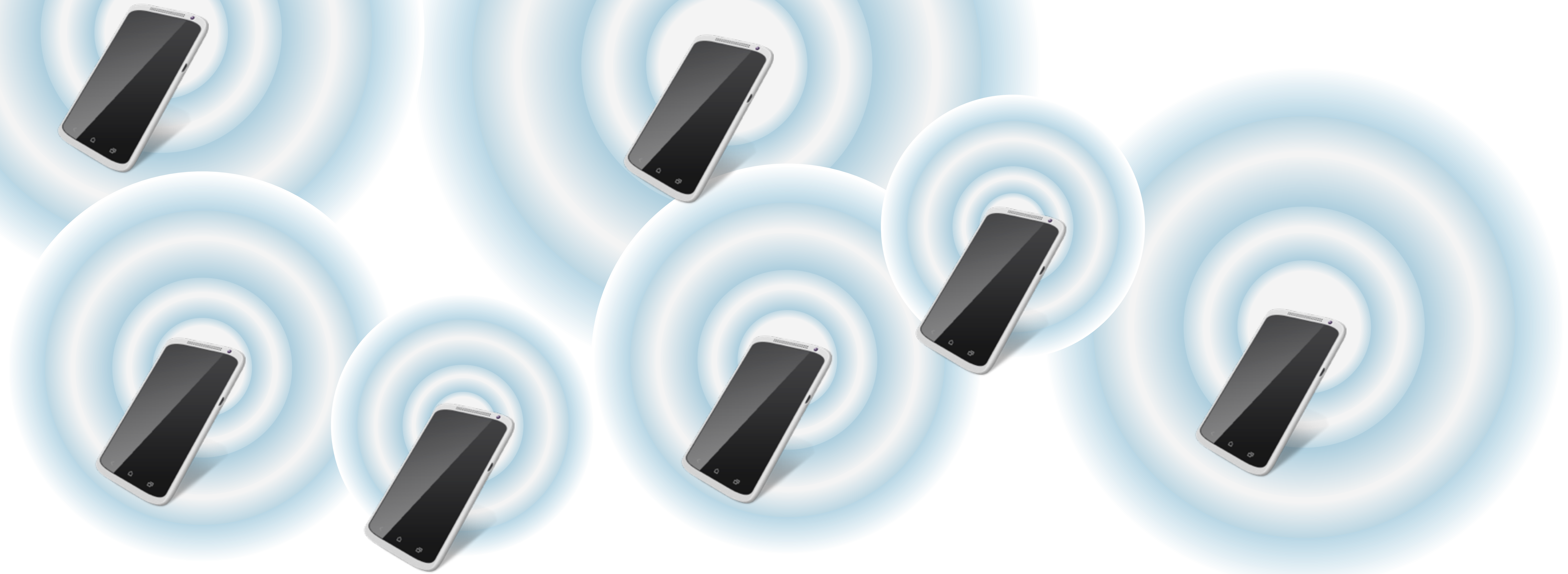
Japan Advanced Institute of Science and Technology



September 11, 2015
2015 ソサイエティ大会
Sendai, Miyagi, Japan

北陸先端科学技術大学院大学

Cooperative Wireless Networks



Wireless networks must deal with interference & noise

Overview

1 Motivation for physical-layer network coding

1A Network Coding

1B Physical Layer Network Coding

2 Nested Lattice Codes

2A Quotient Groups

2B Lattice Quotient Groups

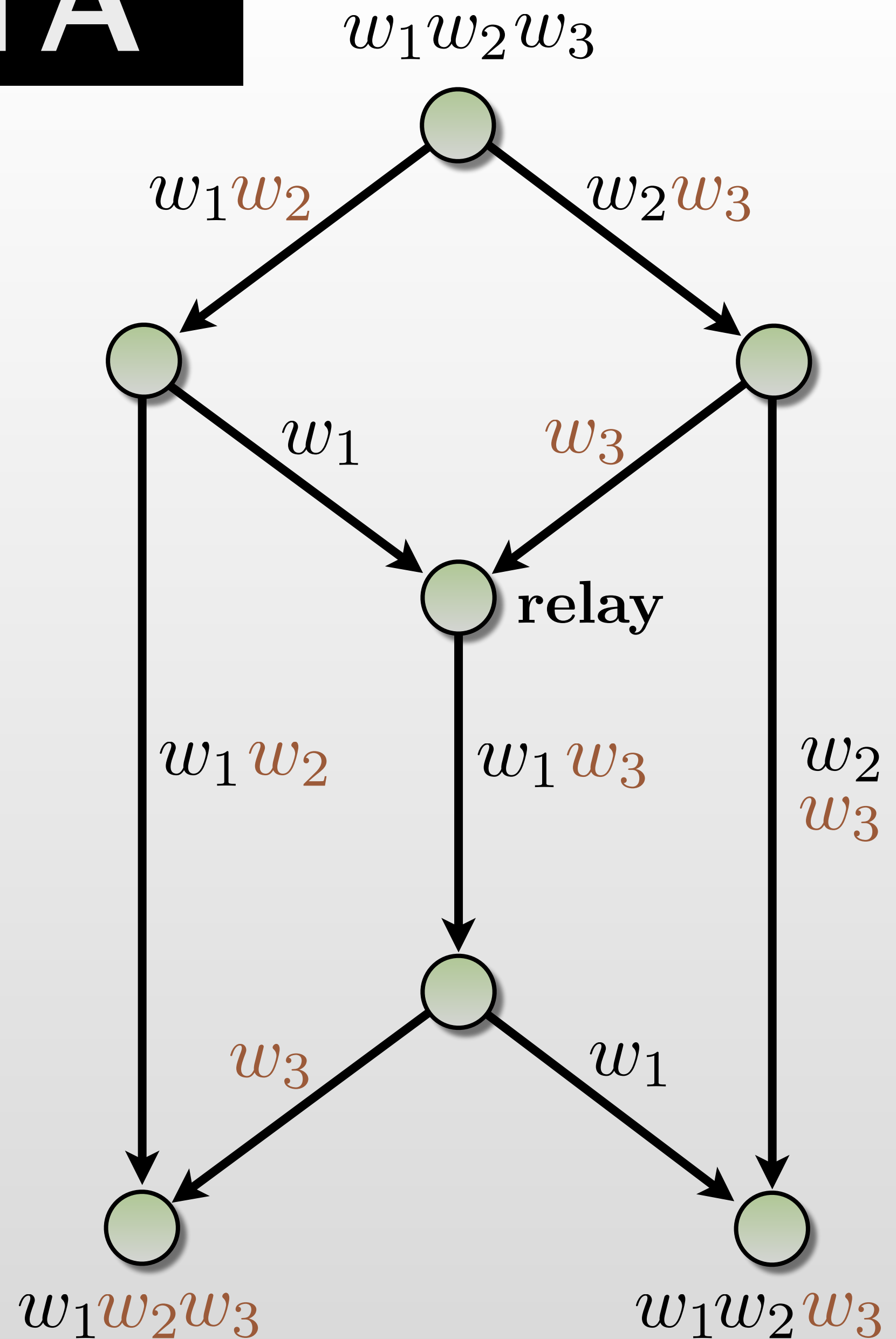
2C Nested Lattice Codes

3 Encoding and Isomorphisms in Nested Lattice Codes

3A Self-similar Voronoi codes

3B Non-Self-similar Voronoi Codes

Routing vs. Network Coding



Capacity: max rate from source to destination

Routing

- Capacity = $3/2$

Routing vs. Network Coding

Capacity: max rate from source to destination

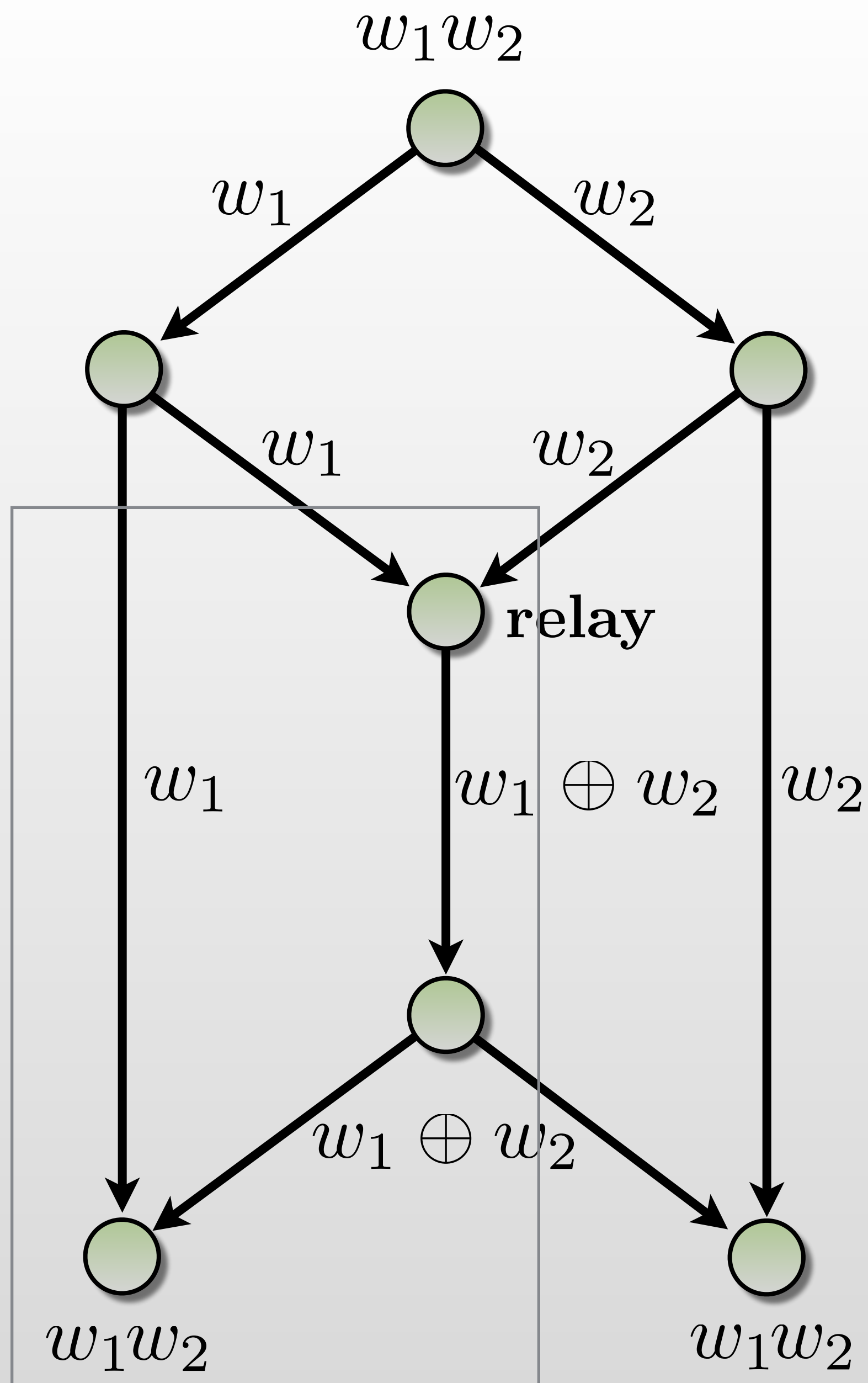
Routing

- Capacity = $3/2$

Network Coding

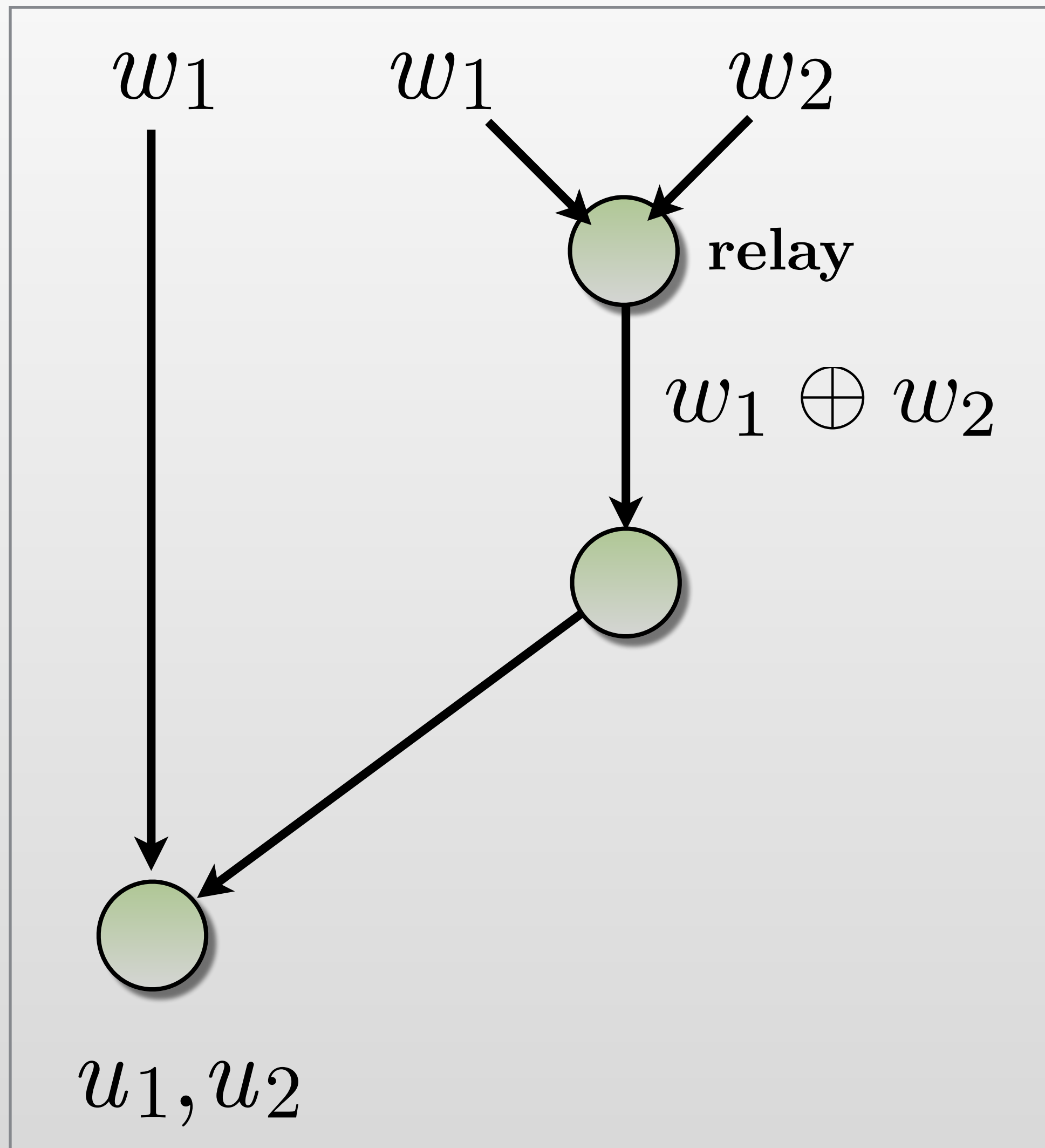
- Internal nodes perform linear operations
- Capacity = 2

Forwarding combinations of messages can increase capacity



matrix form...

Matrix Form Recovery of Messages



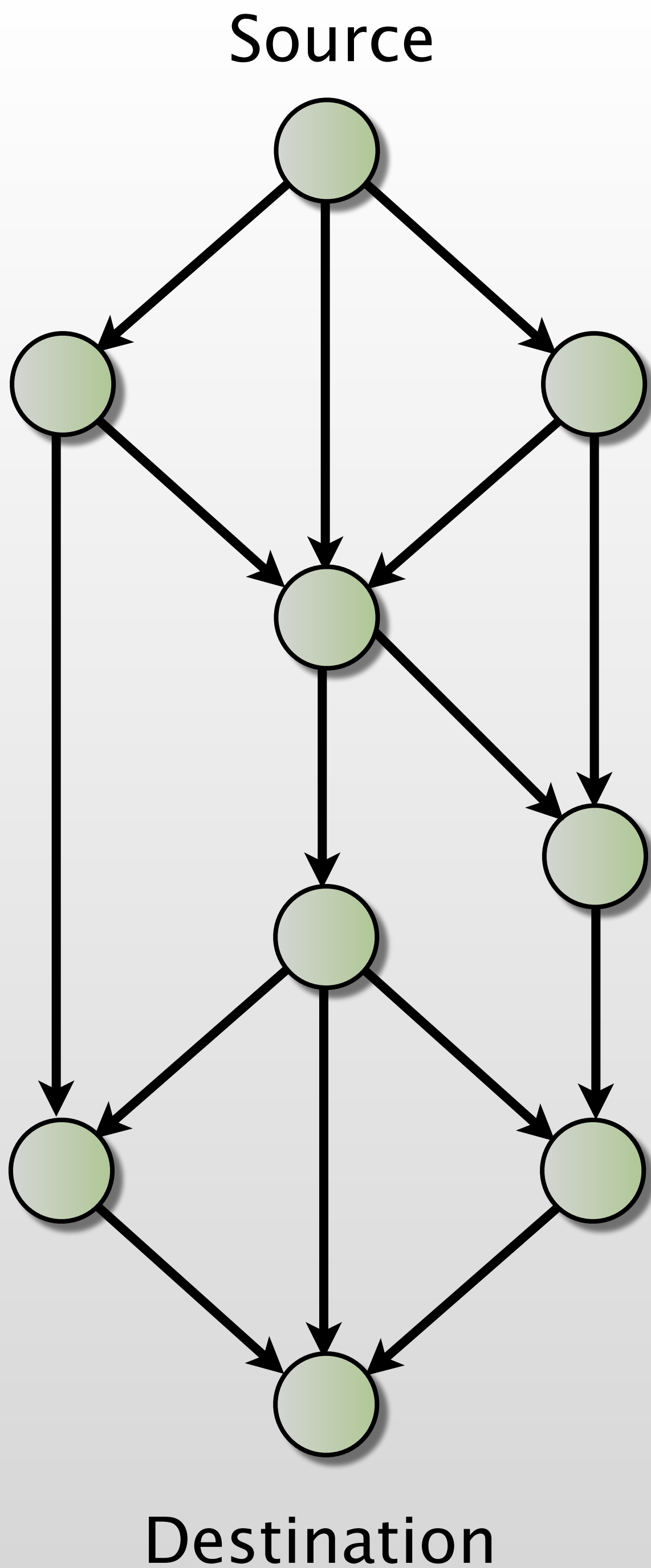
2 received messages and
2 desired messages:

$$\begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}}_Q \cdot \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} u_1 \\ u_2 \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$

↑ received messages ↑ desired messages

Generalized Network Coding



w, u, q in a field. Allow relay to multiply by q

$$Q = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1L} \\ q_{21} & q_{22} & \cdots & q_{2L} \\ \vdots & \vdots & \ddots & \vdots \\ q_{M1} & q_{M2} & \cdots & q_{ML} \end{bmatrix}$$

If Q has rank L , then all messages \mathbf{w} recoverable

How to design Q ?

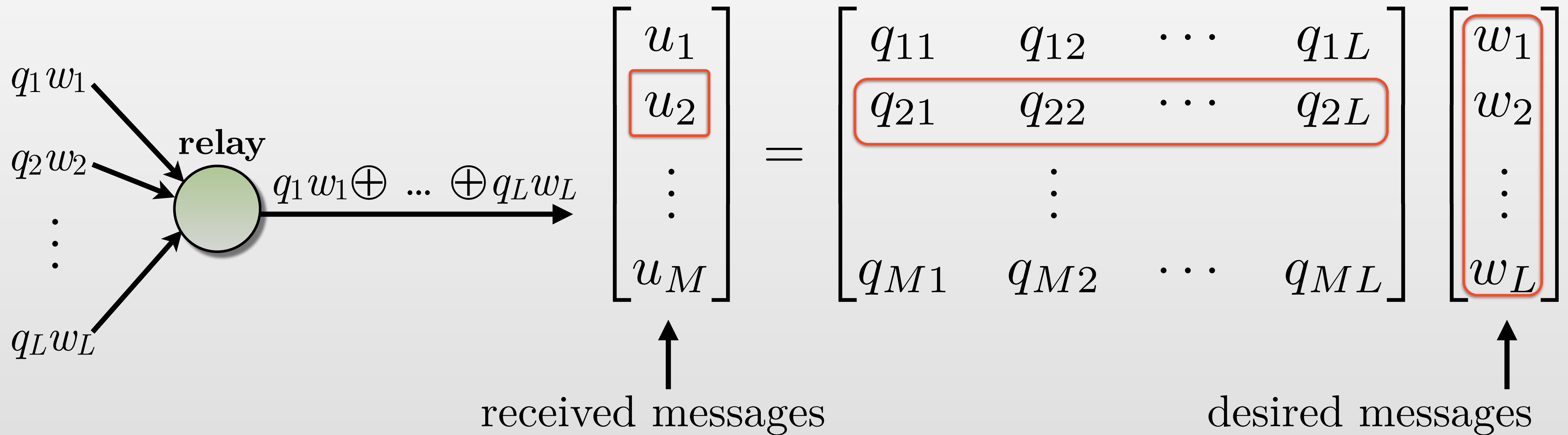
- Algorithmic approach (Jaggi et al.)

Success if field size $p >$ number of destinations

- Random approach (Kotter and Medard. Ho et al.)

Probability of valid solutions increases with p

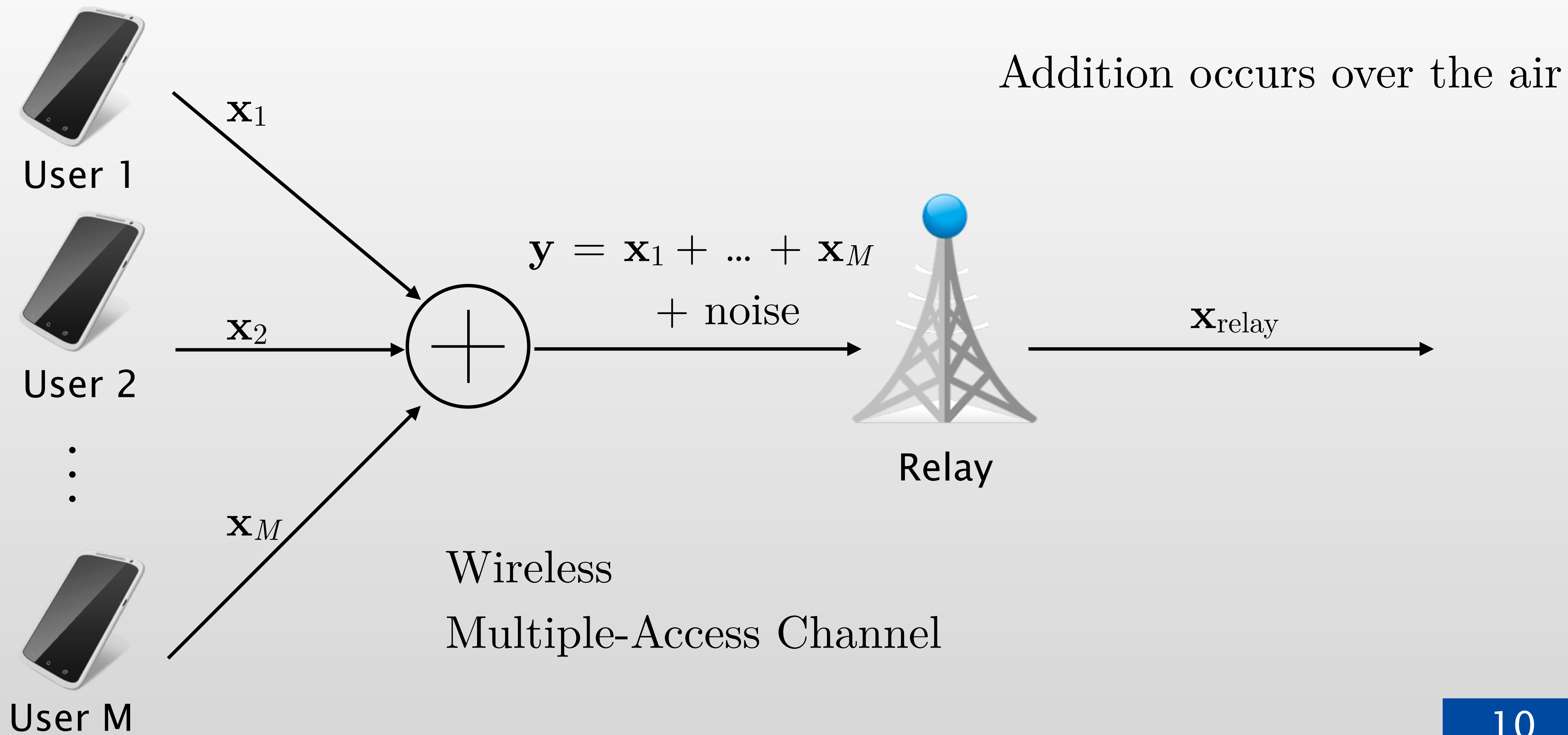
Action of One Row A “Relay”



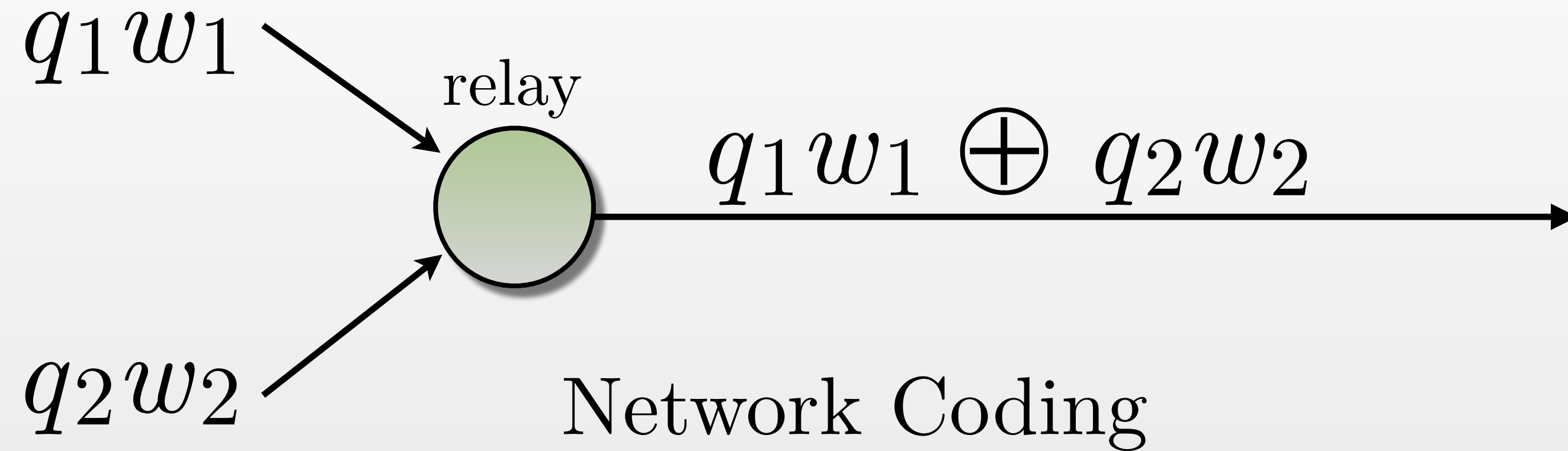
What if the relay is wireless...?

1B

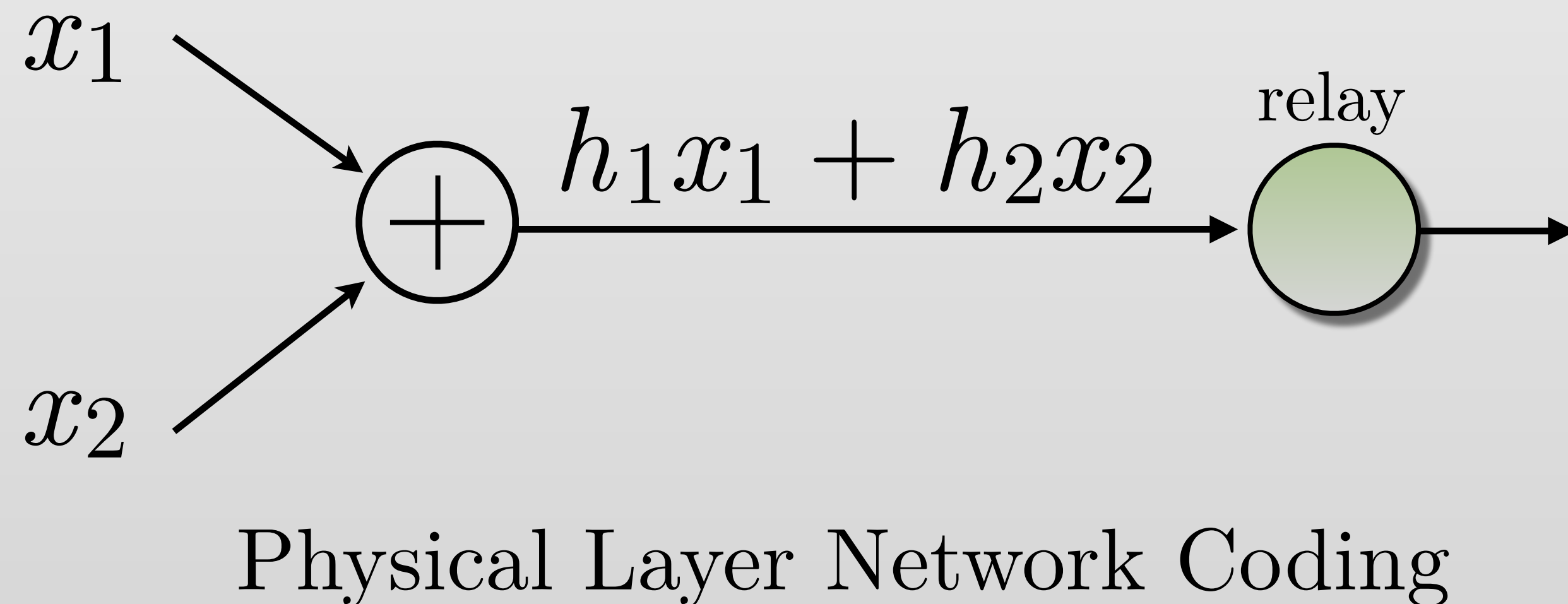
PLNC = Physical Layer Network Coding



Network Coding vs. PLNC

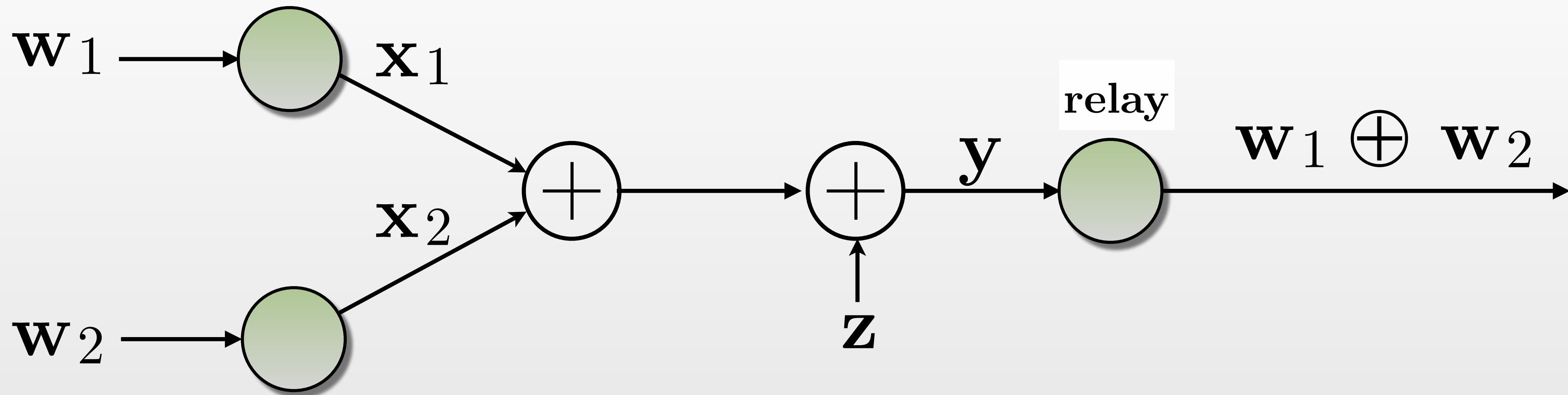


Network Coding:
relay adds incoming
messages



PLNC:
addition over the air
fading plays a role
combat noise

PLNC with Error-Correction



Perform error-correction coding on vectors:

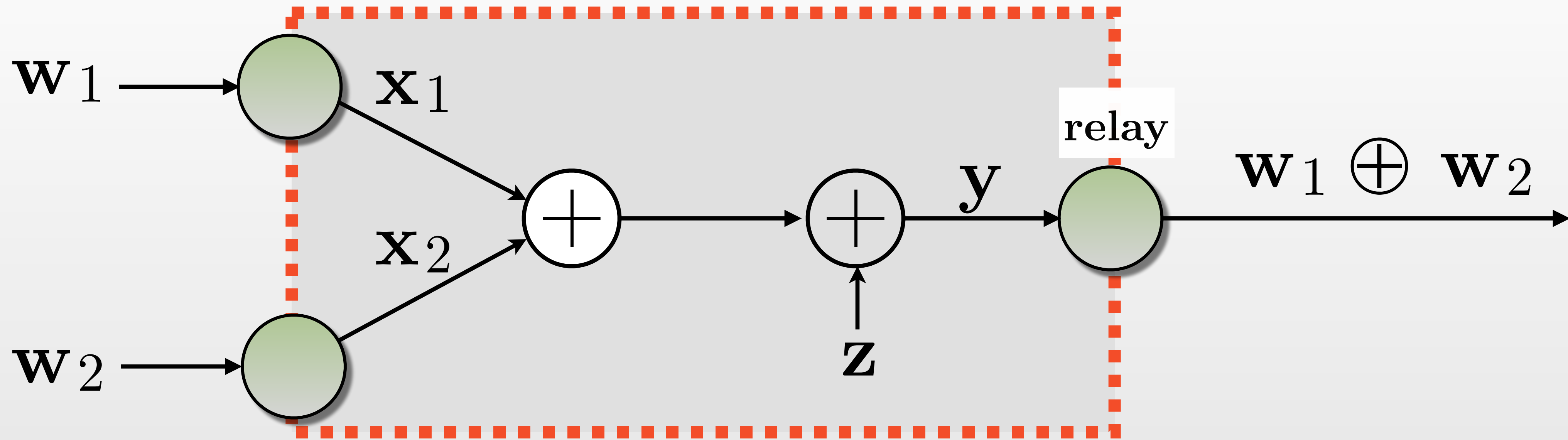
$$\mathbf{x}_i = \text{Enc}(\mathbf{w}_i)$$

Relay performs two functions:

$$\mathbf{x}_1 + \mathbf{x}_2 = \text{Decoder}(\mathbf{y})$$

$$\mathbf{w}_1 \oplus \mathbf{w}_2 = \text{Enc}^{-1}(\mathbf{x}_1 + \mathbf{x}_2)$$

PLNC with Error-Correction



Powerful idea:

- Relay only eliminates noise
- Relay does not need to separate inference
- Converted a noisy network into a noiseless network

We Need A Code to Perform PLNC

Code must correct errors, for noisy wireless channels

- Code must satisfy a power constraint.

Code must form a group over addition

- so addition over the channel makes sense.

Code must have a group isomorphism: $\text{Enc}(\mathbf{w}_1 \oplus \mathbf{w}_2) = \mathbf{x}_1 + \mathbf{x}_2$,

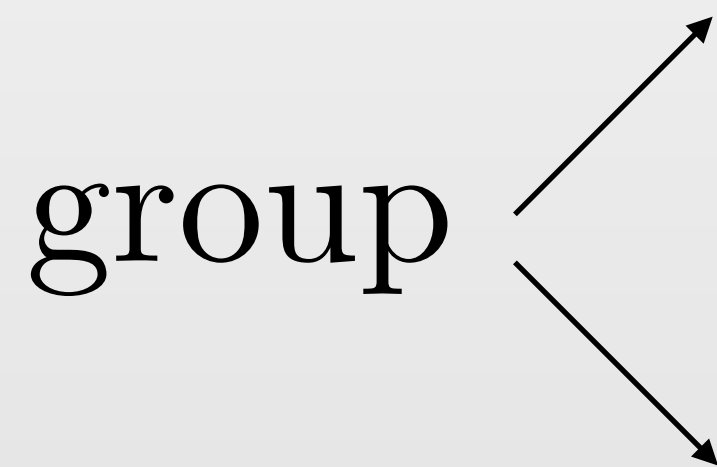
- so network coding can be performed

These properties are satisfied by nested lattice codes.

Quotient Groups

$$G/H$$

group



subgroup


$$\Lambda_C/\Lambda_S$$

Definition of a Coset

Definition Let G be a group and let H be a subgroup of G . For any $a \in G$, the set $a + H = \{a + h \mid h \in H\}$ is called the *coset of H in G containing a* .

Quotient Groups

Let G/H be the set of all cosets of H in G , that is:

$$G/H = \{a + H \mid a \in G\}$$

Note that G/H is a set of sets. The set G/H is called a *quotient group*.

Example

- Integers \mathbb{Z} are a group under addition
- $4\mathbb{Z}$ is a subgroup: $4\mathbb{Z} \subset \mathbb{Z}$.
- The quotient group $\mathbb{Z}/4\mathbb{Z}$, has four sets:

$$0 + 4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$$

$$1 + 4\mathbb{Z} = \{\dots, -7, -3, 1, 5, 9, \dots\}$$

$$2 + 4\mathbb{Z} = \{\dots, -6, -2, 2, 6, 10, \dots\}$$

$$3 + 4\mathbb{Z} = \{\dots, -5, -1, 3, 7, 11, \dots\}$$

The quotient group is closed under addition:

	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$0 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$1 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$
$2 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$
$3 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$	$0 + 4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$

Coset Leader (Coset Representative)

A coset leader is a single representative element from each coset.

Continue $\mathbb{Z}/4\mathbb{Z}$ example:

Coset leaders: $\{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Coset leaders: $\{-2, -1, 0, 1\}$

+	0	1	-2	-1
0	0	1	-2	-1
1	1	-2	-1	0
-2	-2	-1	0	1
-1	-1	0	1	-2

Lattice: Linear code over real numbers

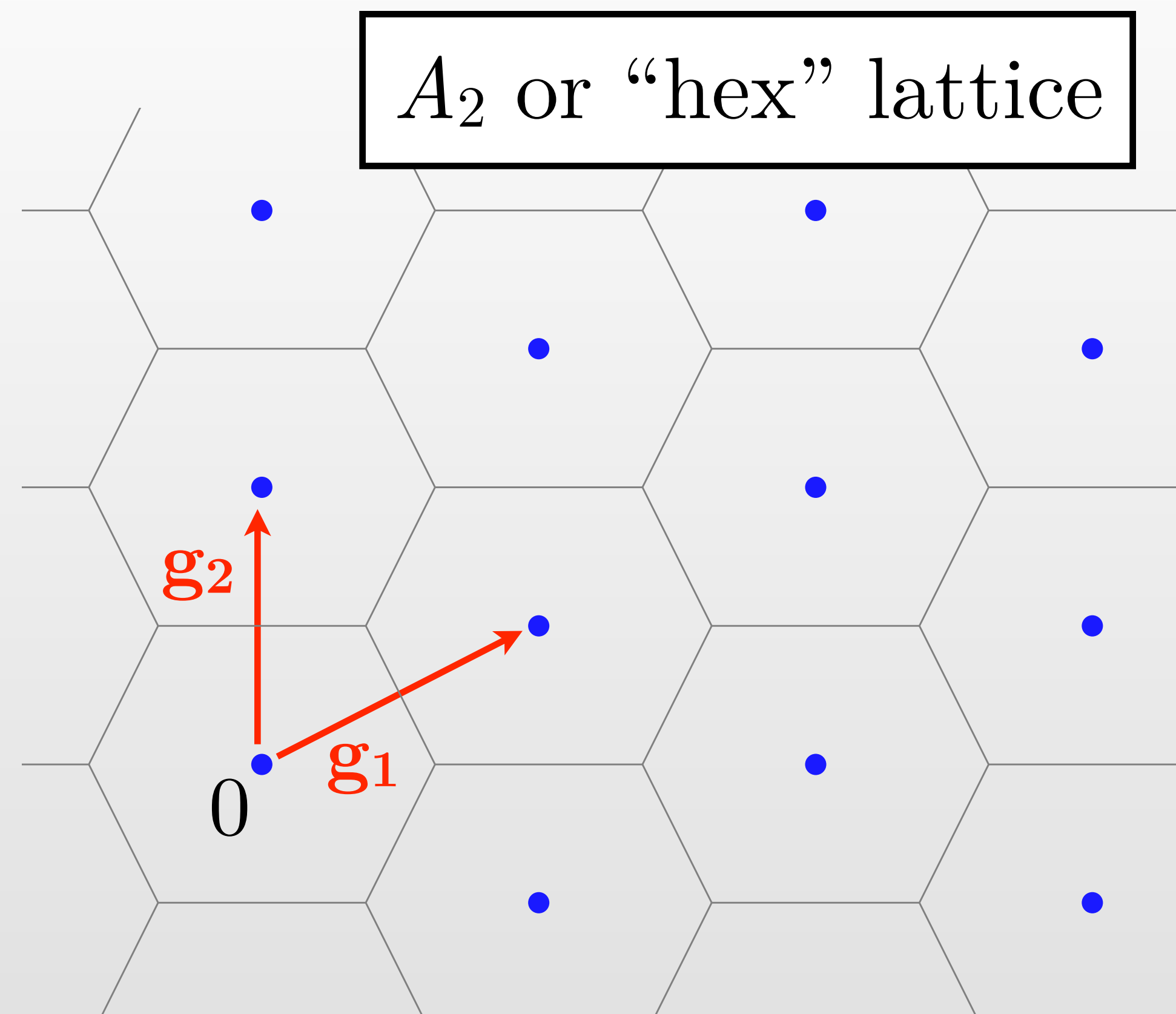
A lattice Λ is a linear additive subgroup of \mathbb{R}^n .

Λ may be represented by a basis of $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n$.

A lattice point $\mathbf{x} \in \Lambda$ is an integral, linear combination of the basis vectors:

$$\mathbf{x} = \mathbf{g}_1 b_1 + \mathbf{g}_2 b_2 + \dots + \mathbf{g}_n b_n,$$

where the b_i are integers.



$$G = \begin{bmatrix} 1 & 0 \\ 0.5 & 1 \end{bmatrix}$$

\mathbf{g}_1 \mathbf{g}_2

Quotient Groups Based on Lattices

Let Λ_c be a lattice

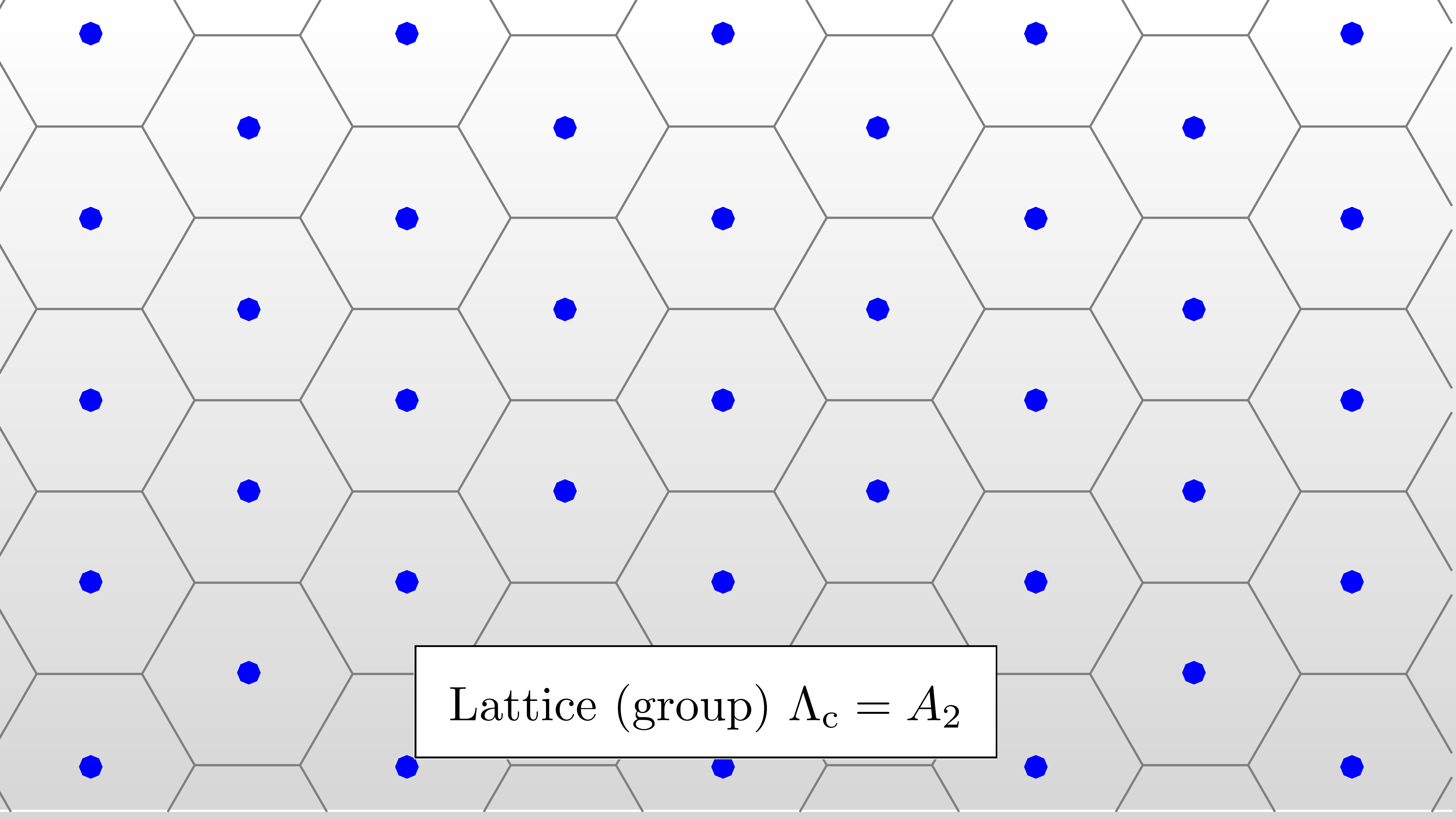
- “coding lattice” corrects errors. Also called fine lattice.

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

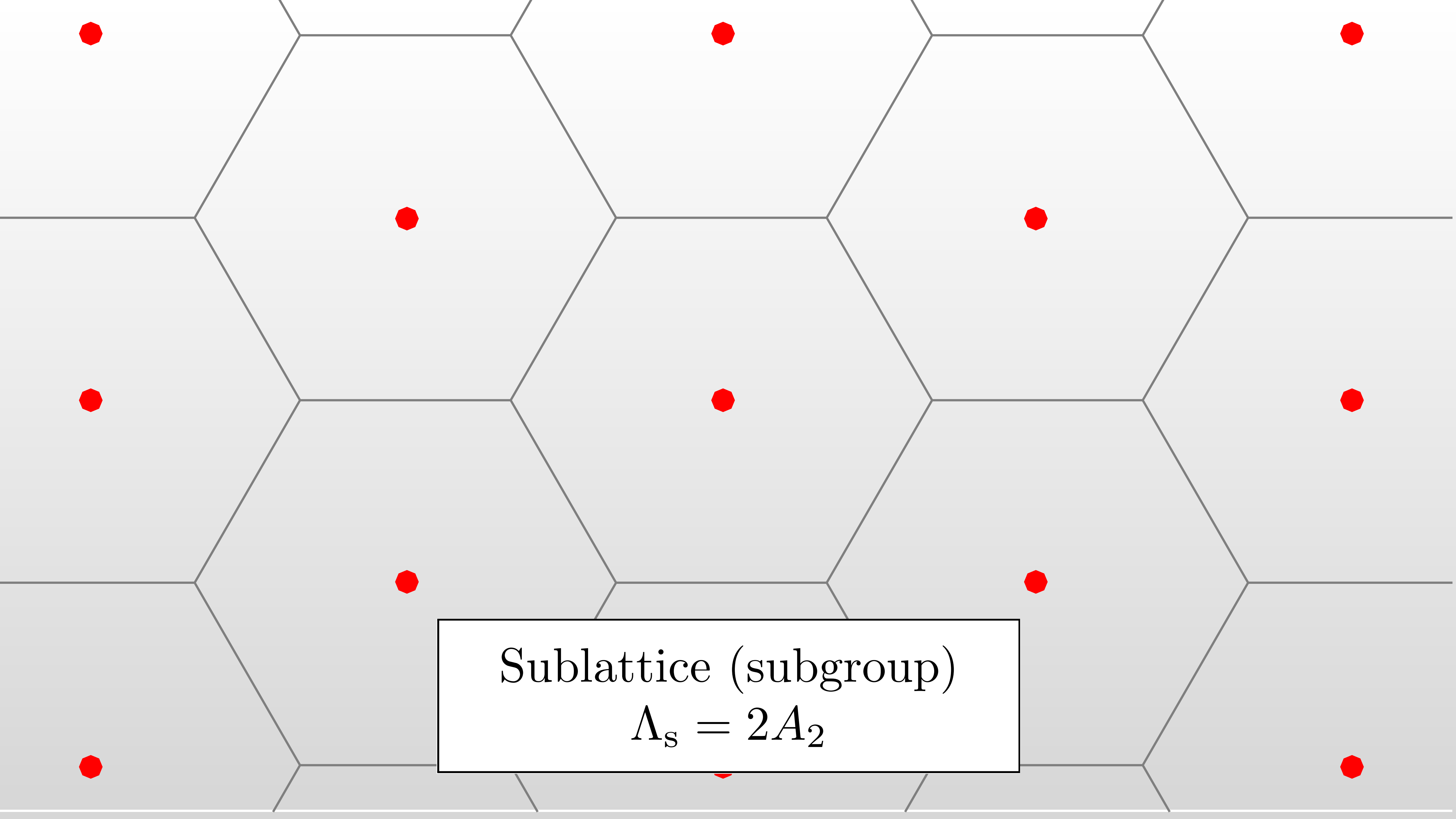
- “shaping lattice” enforces power constraint.
Also called coarse lattice.

$K\Lambda_c$ is a lattice expanded by K .

- Choosing $\Lambda_s = K\Lambda_c$ results in $\Lambda_s \subseteq \Lambda_c$ for $K = 1, 2, 3, \dots$

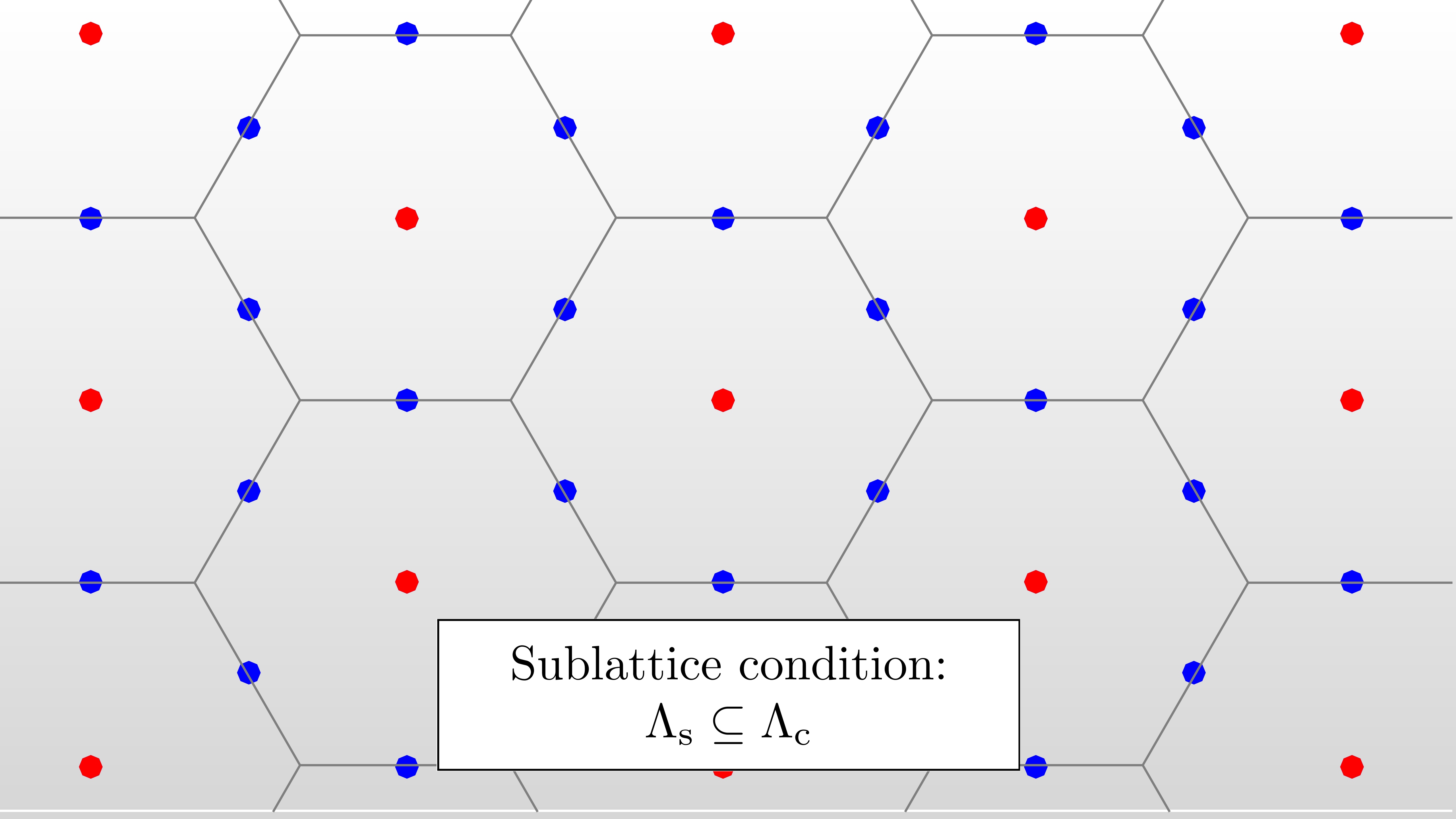


Lattice (group) $\Lambda_c = A_2$



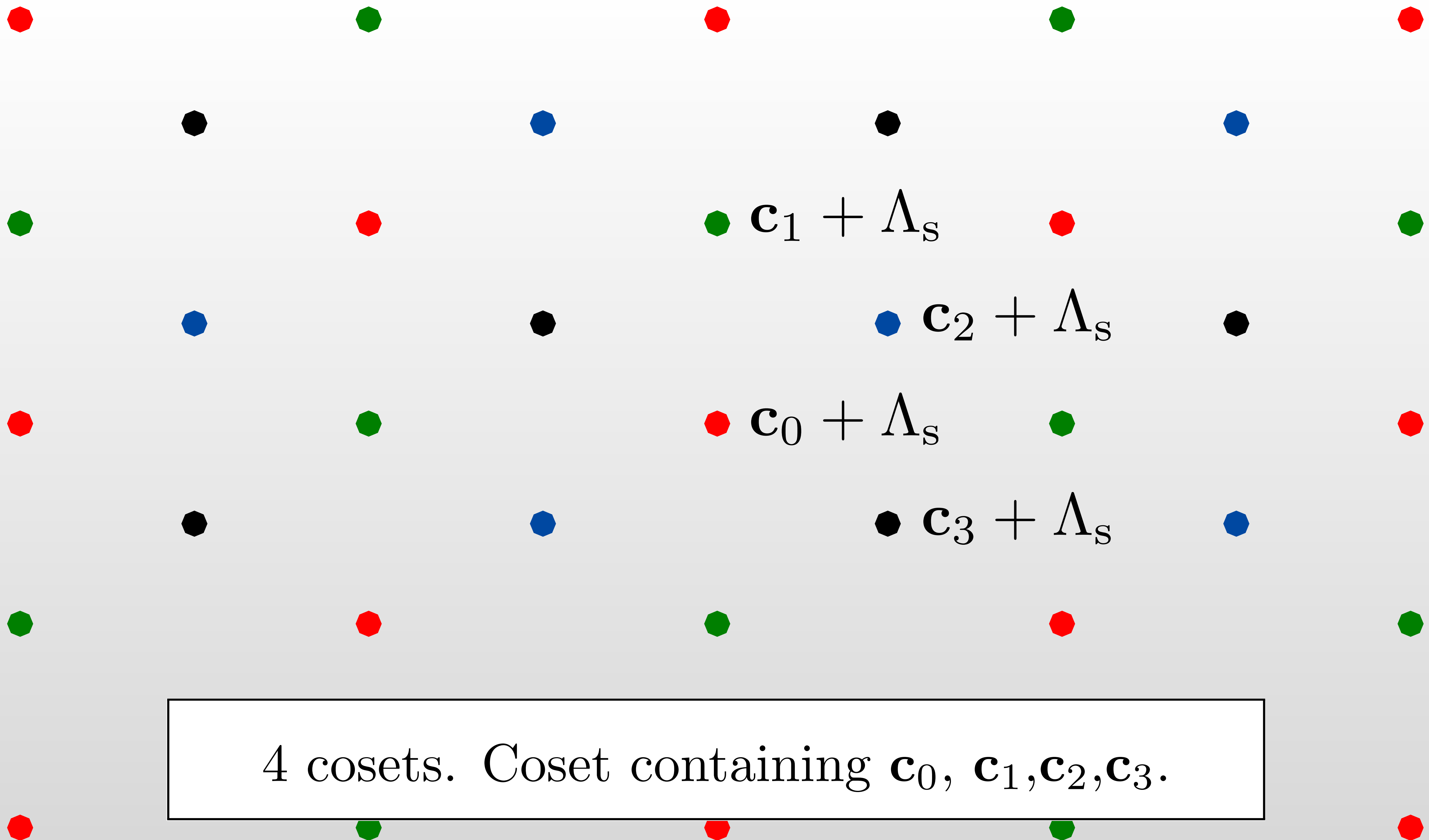
Sublattice (subgroup)

$$\Lambda_s = 2A_2$$



Sublattice condition:

$$\Lambda_S \subseteq \Lambda_C$$



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

Cosets form a group under addition

The set Λ_c/Λ_s is a quotient group.

This table expresses group addition:

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

Nested Lattice Codes

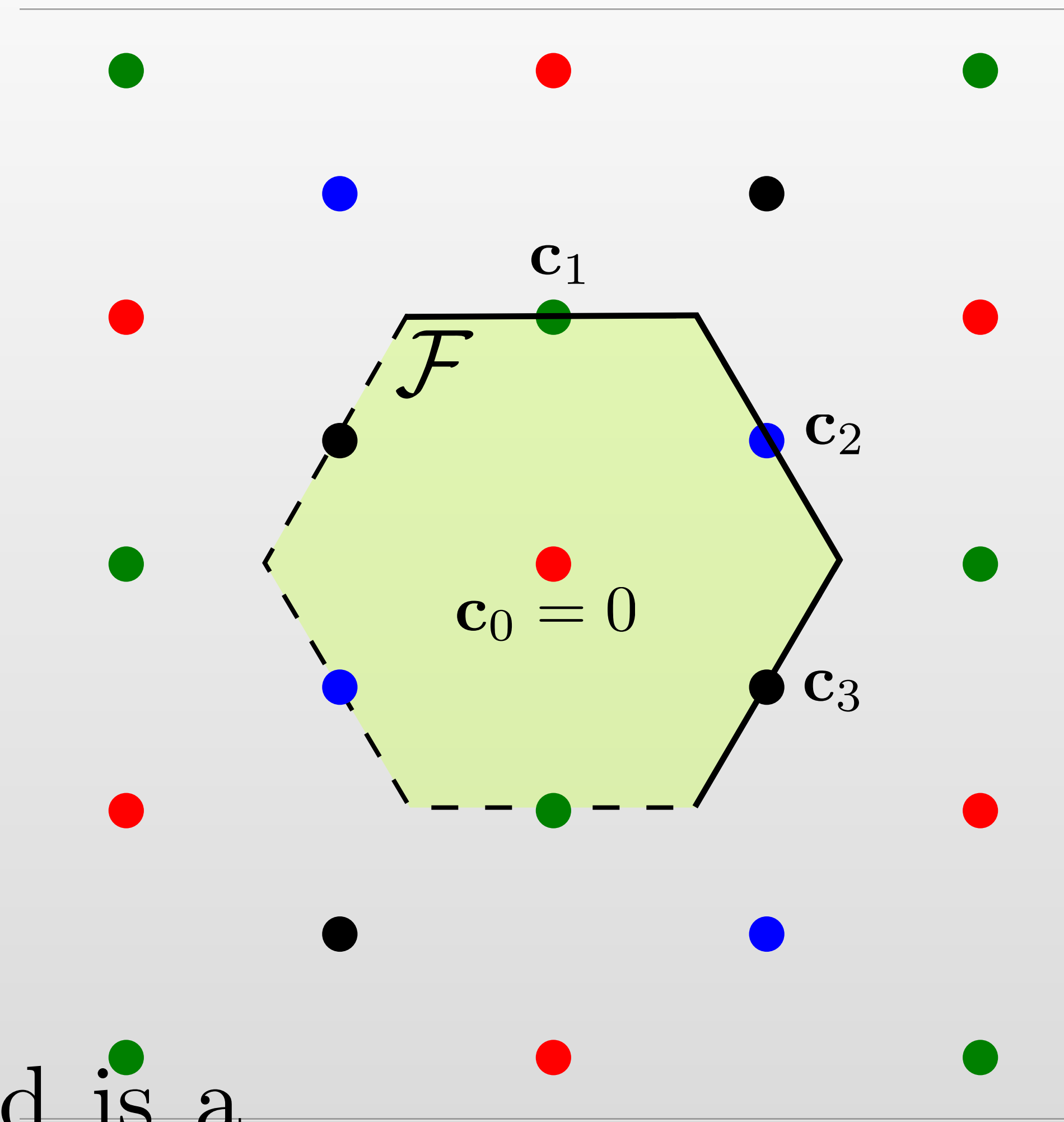
Construct a lattice code \mathcal{C} :

$$\mathcal{C} = \Lambda_c \cap \mathcal{F}$$

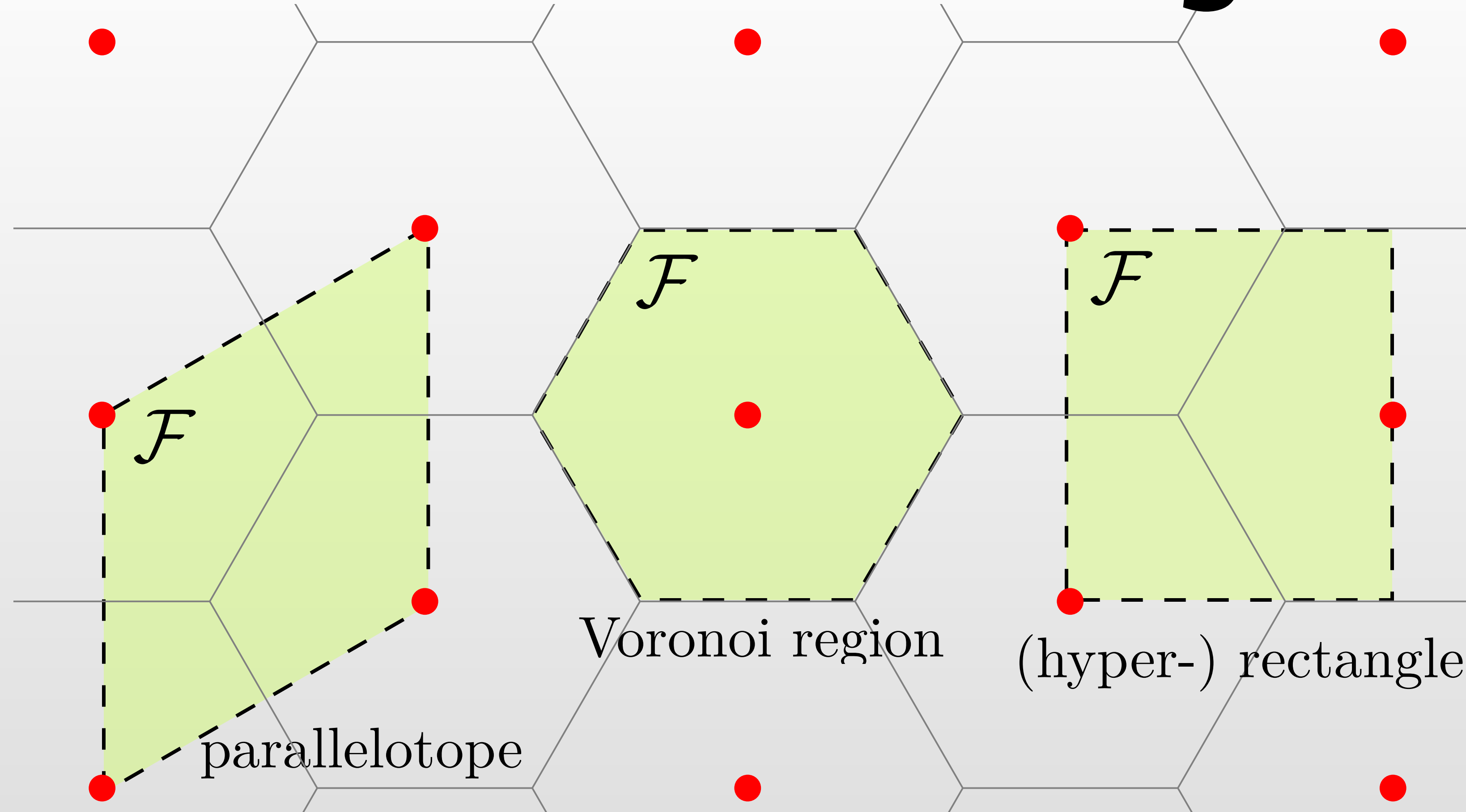
We need:

- Quotient Group Λ_c / Λ_s
- \mathcal{F} is a fundamental region for Λ_s

The code \mathcal{C} are coset leaders Λ_c / Λ_s , and is a group.



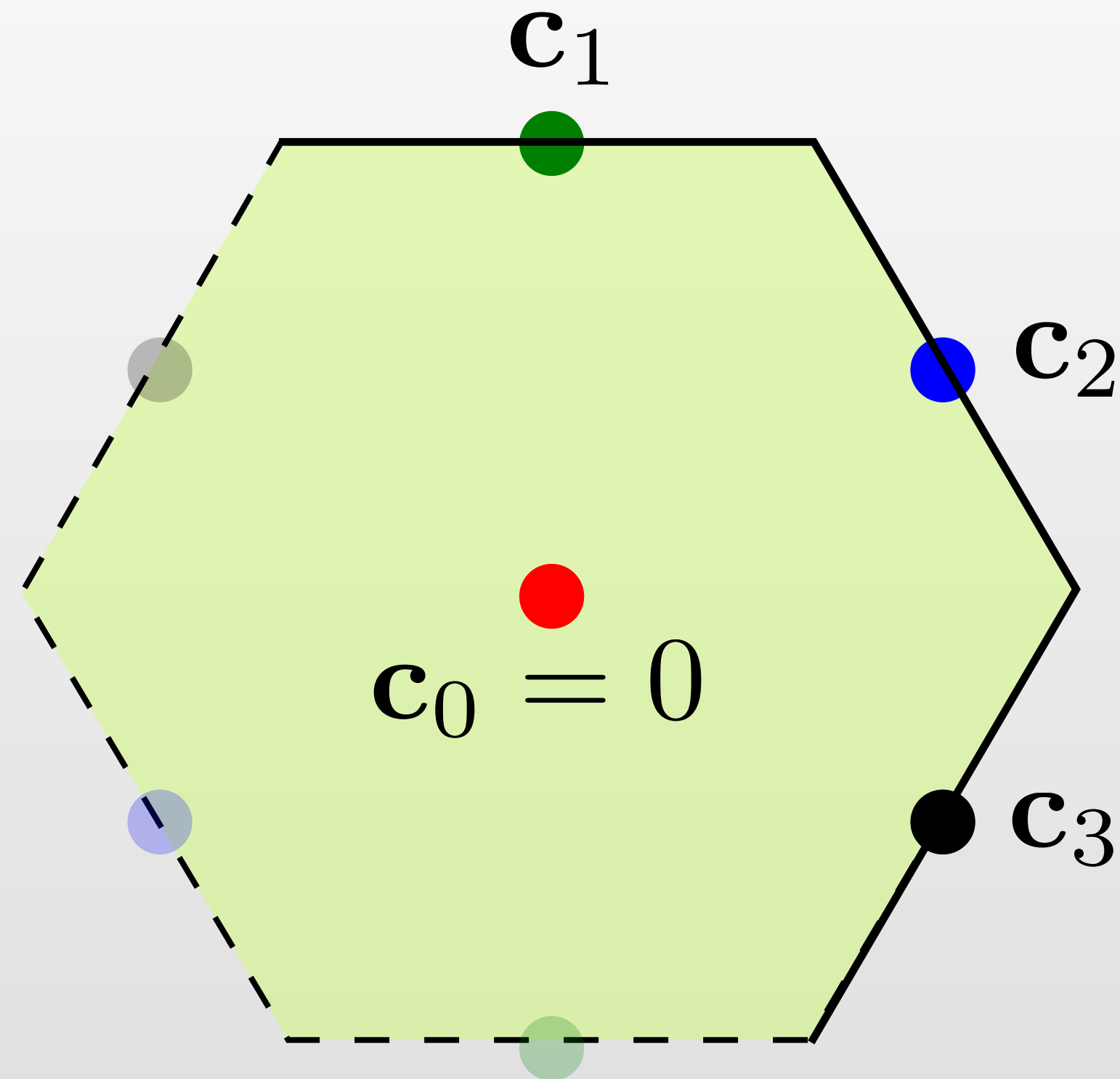
Fundamental Regions



A fundamental region $\mathcal{F} \subset \mathbb{R}^n$ is a shape that, if shifted by each lattice point, will exactly cover the whole real space.

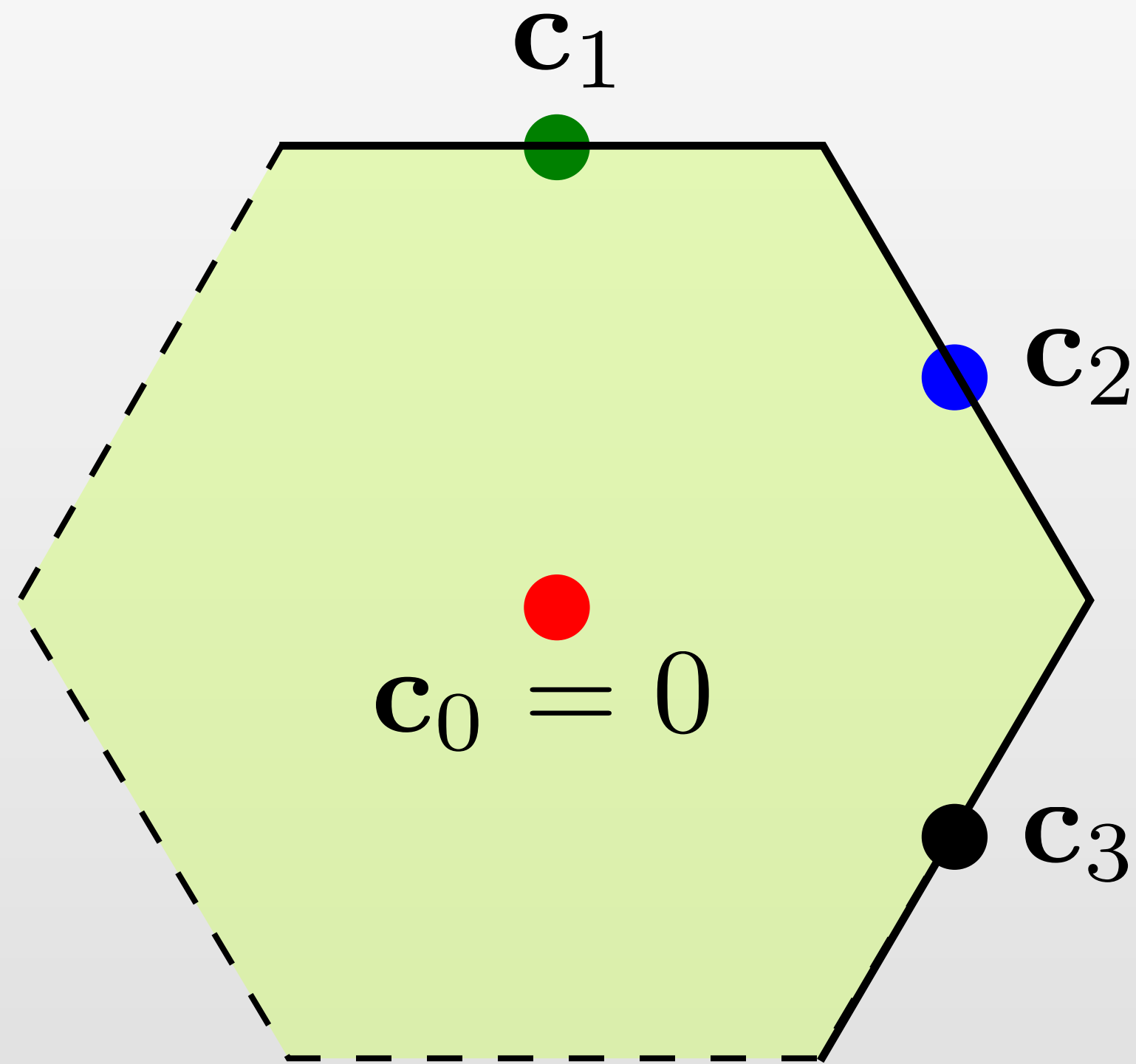
Volume $V(\mathcal{F})$ of \mathcal{F} is constant and $V(\mathcal{F}) = |\det \Lambda|$

Selecting the Coset Leaders



$$\mathcal{C} = \Lambda_{\mathbf{c}} \cap \mathcal{F}$$

Nested Lattice Codes Form a Group



$$\mathcal{C} = \Lambda_c \cap \mathcal{F}$$

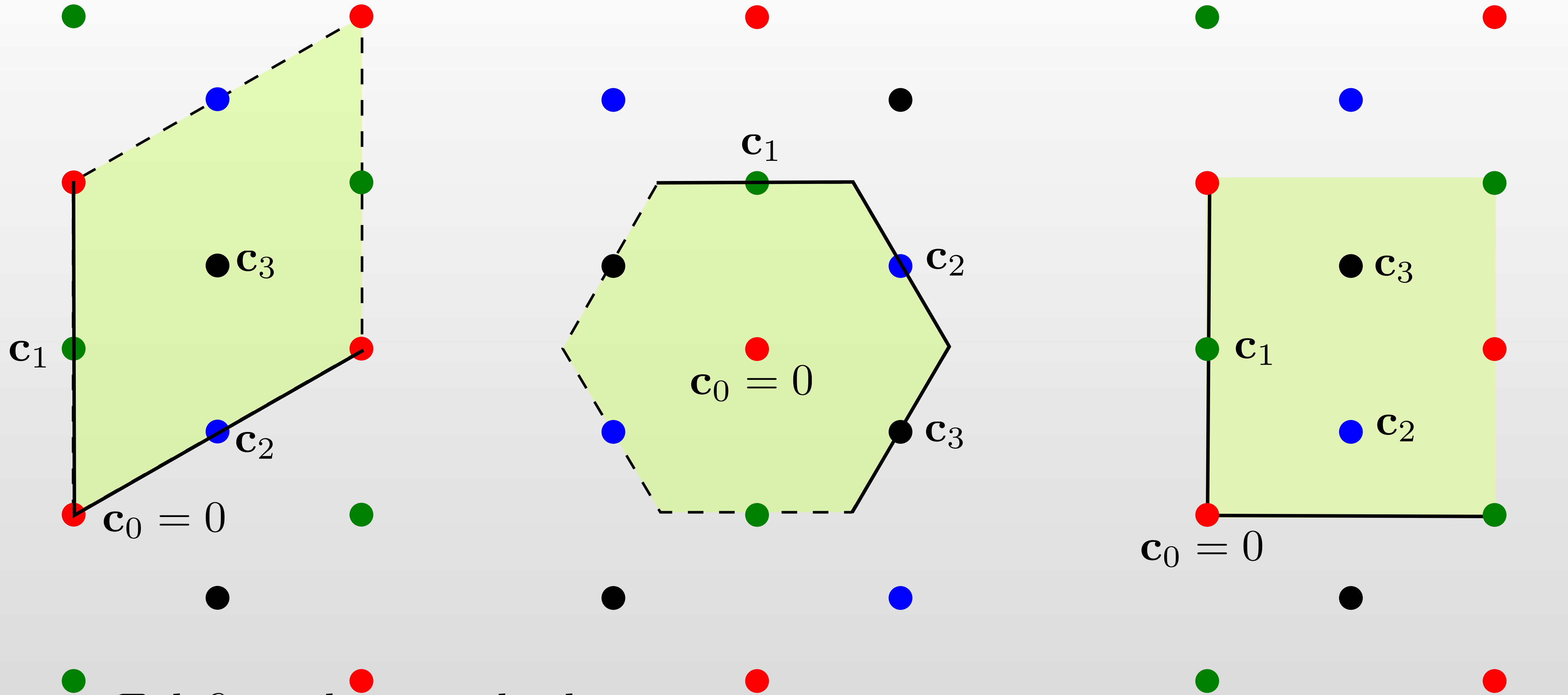
$+$	c_0	c_1	c_2	c_3
c_0	c_0	c_1	c_2	c_3
c_1	c_1	c_0	c_3	c_2
c_2	c_2	c_3	c_0	c_1
c_3	c_3	c_2	c_1	c_0

codebook $\mathcal{C} = \{c_0, c_1, c_2, c_3\}$

c_i are coset leaders of Λ_c/Λ_s .

\mathcal{C} is closed under addition

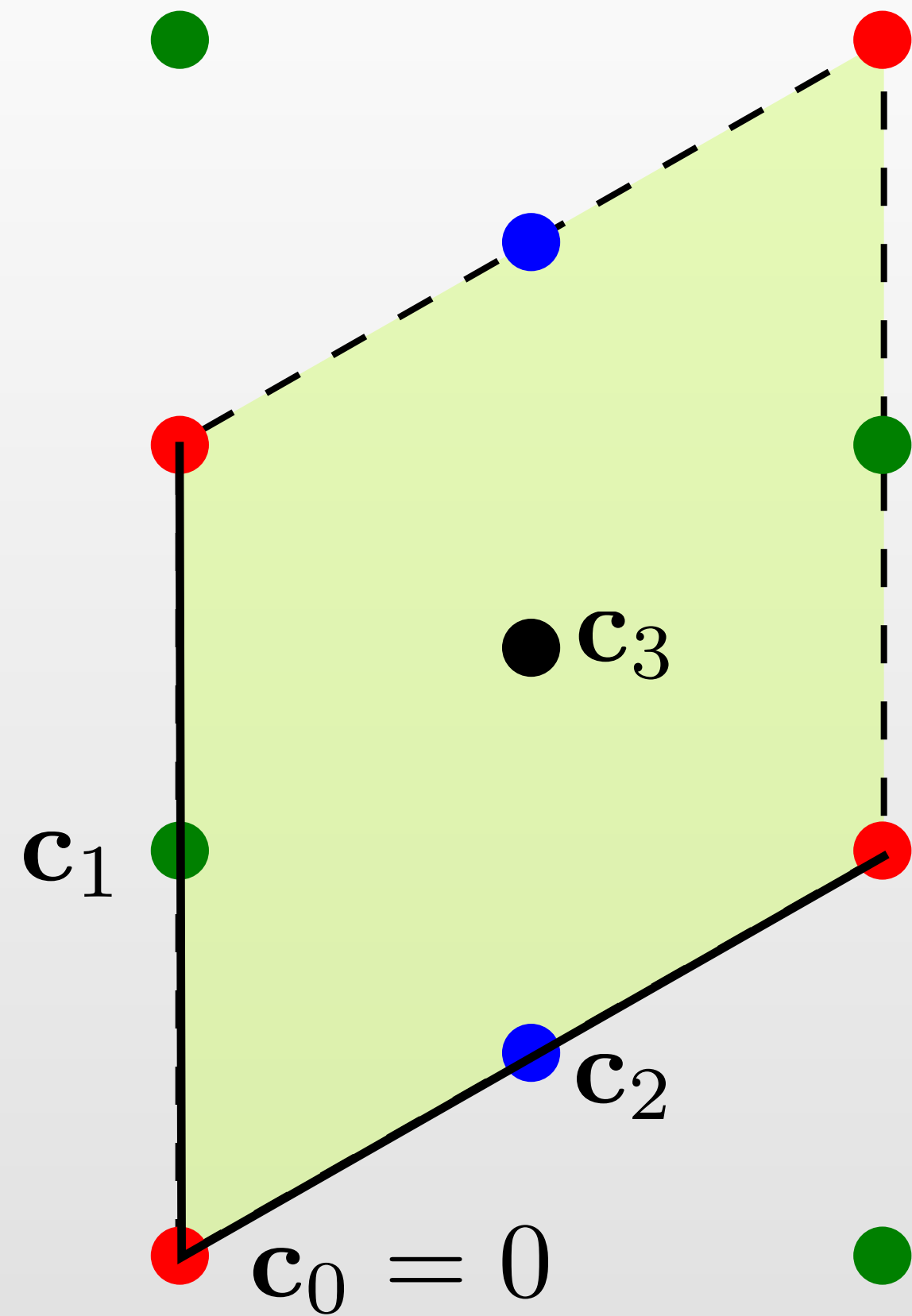
Various Nested Lattice Codes



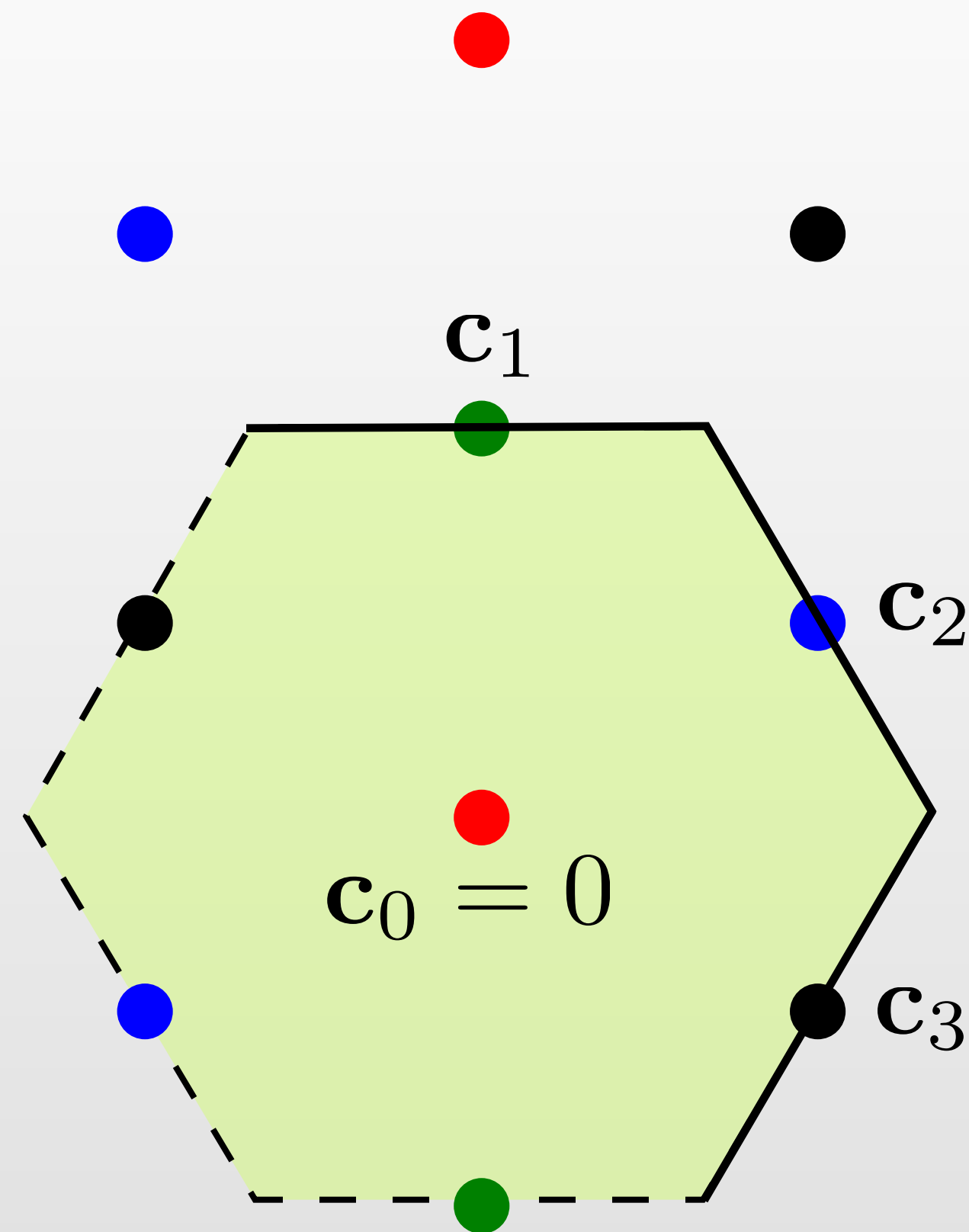
● \mathcal{F} defines the coset leaders:
 ●

3 Different Voronoi regions — All codes form Groups

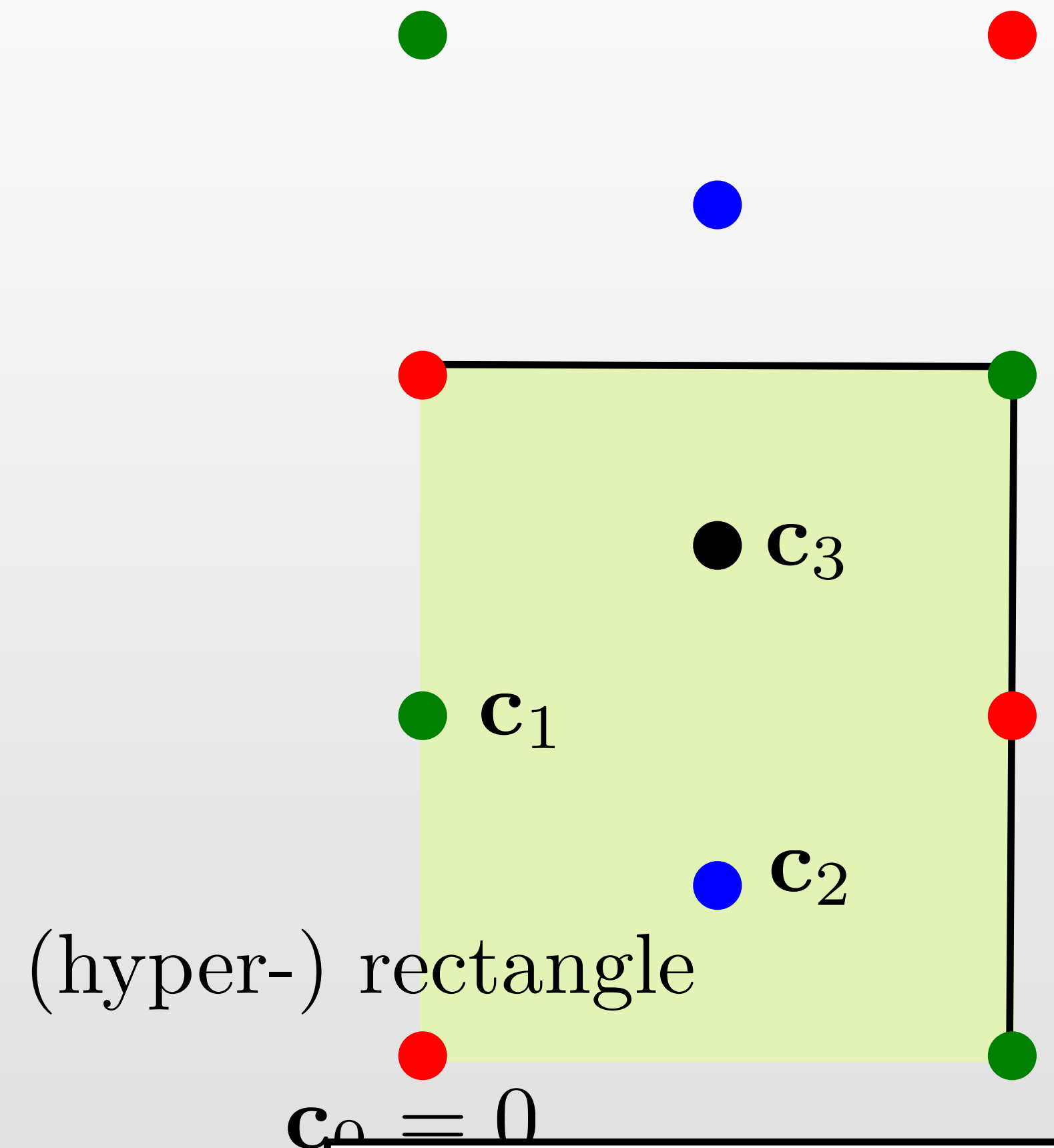
Various Nested Lattice Codes



paralleloptope
Important for
theory, not very
practical

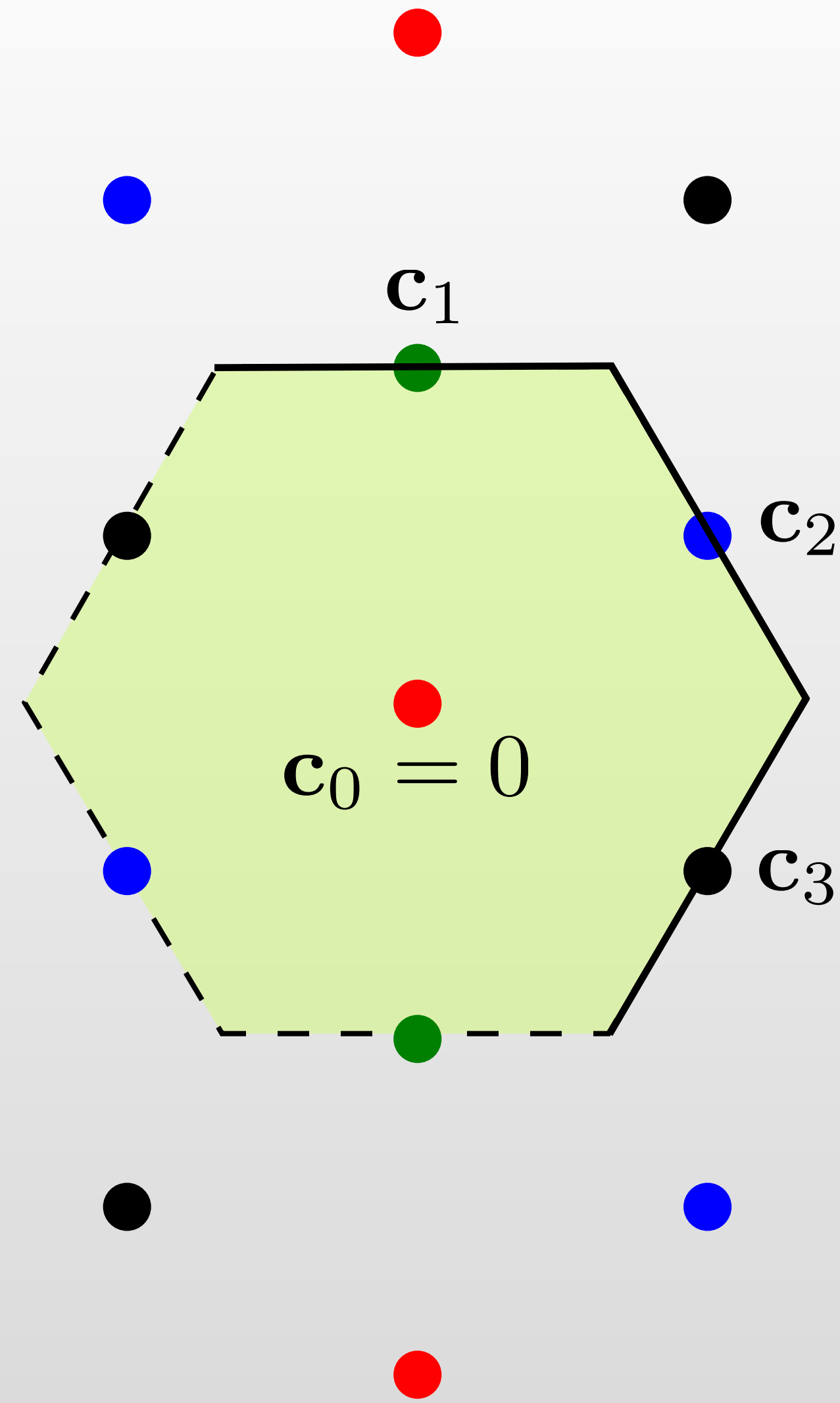


Voronoi region
Best transmit
power, not always
easy to implement



Rectangle
Easier to
implement, no
shaping gain

Voronoi is Best for AWGN Channel



Voronoi regions are sphere-like in high dimension.

A sphere satisfies the AWGN power constraint

$$\frac{1}{n} \sum_{i=1}^n x_i^2 \leq P$$

Encoding and Isomorphism

Encoding: mapping information to codewords

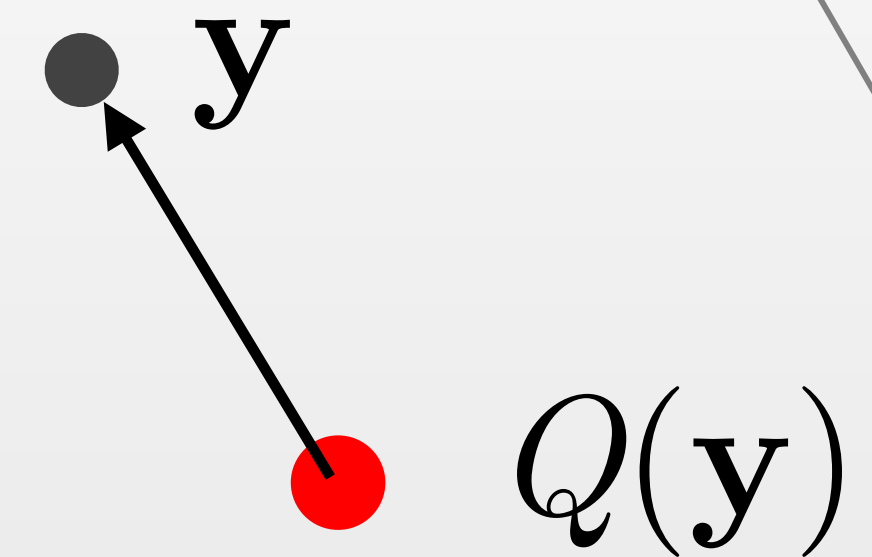
Indexing: mapping codewords to information

Isomorphism between information (ring) and codewords (group)

Quantization and Modulo

Quantization Closest point in Λ_s :

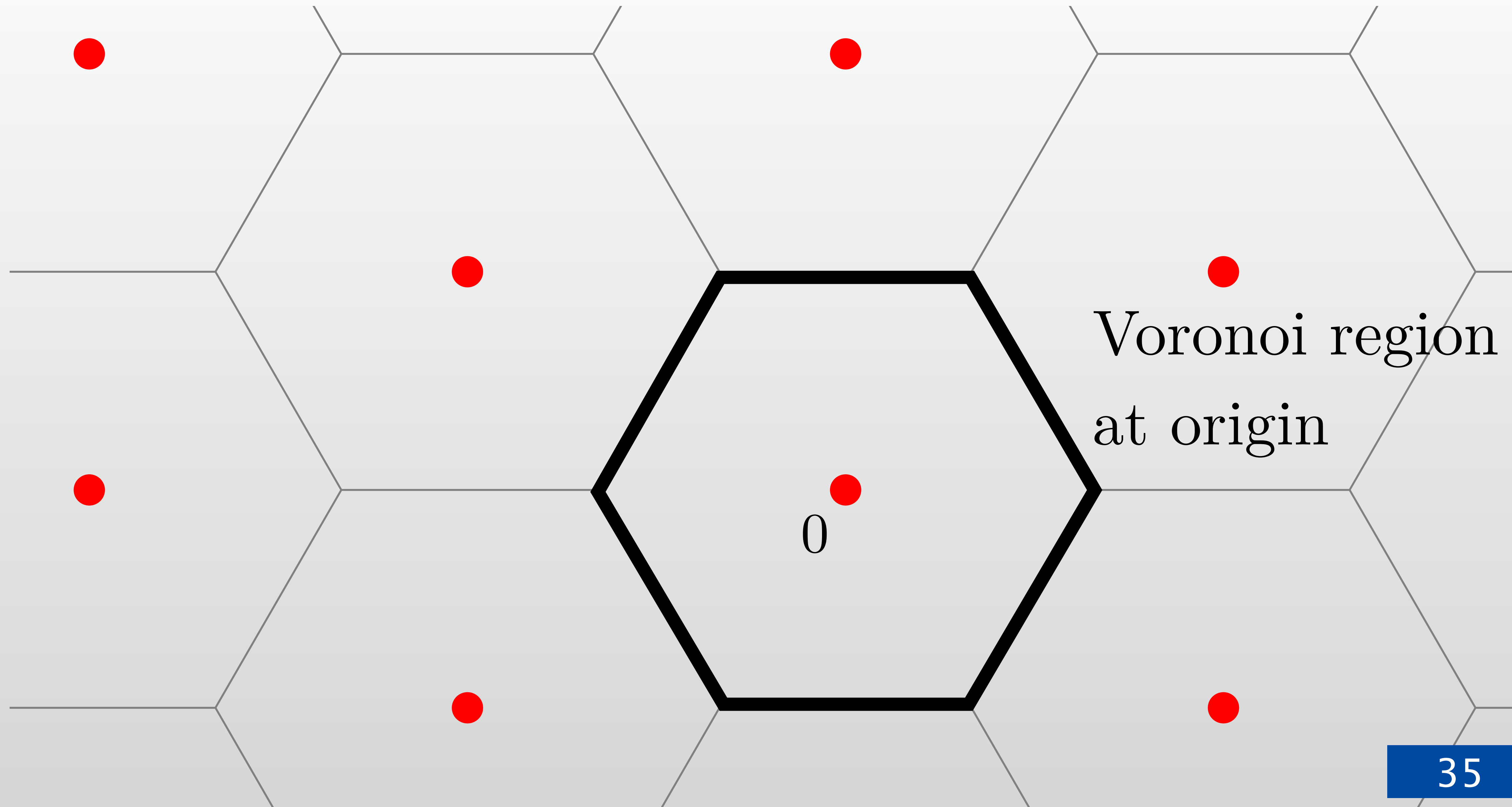
$$Q_{\Lambda_s}(\mathbf{y}) = \arg \min_{\mathbf{x} \in \Lambda_s} \|\mathbf{x} - \mathbf{y}\|^2$$



0

Quantization has exponential complexity in general

Quantization and Modulo

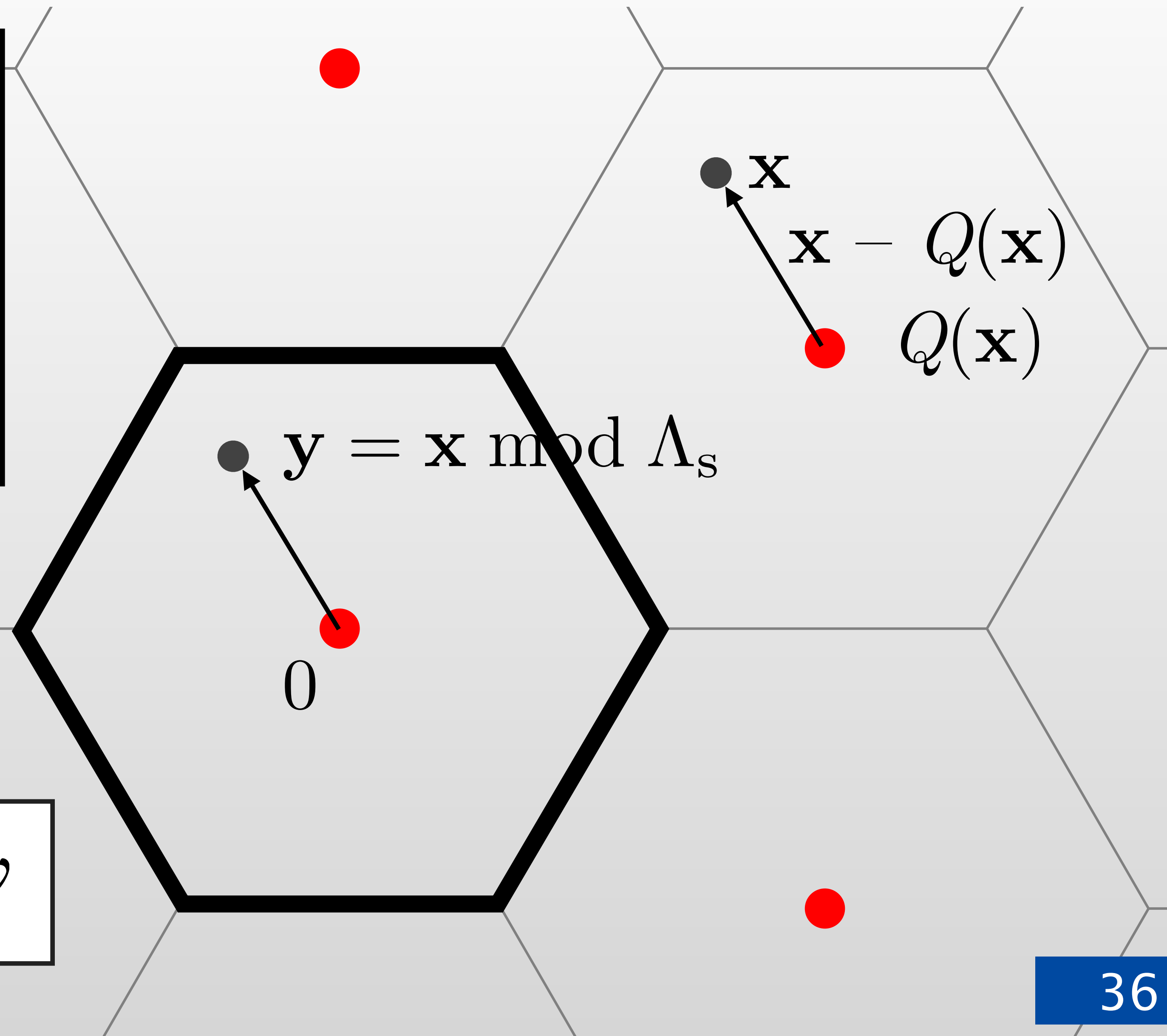


Quantization and Modulo

Modulo operation:

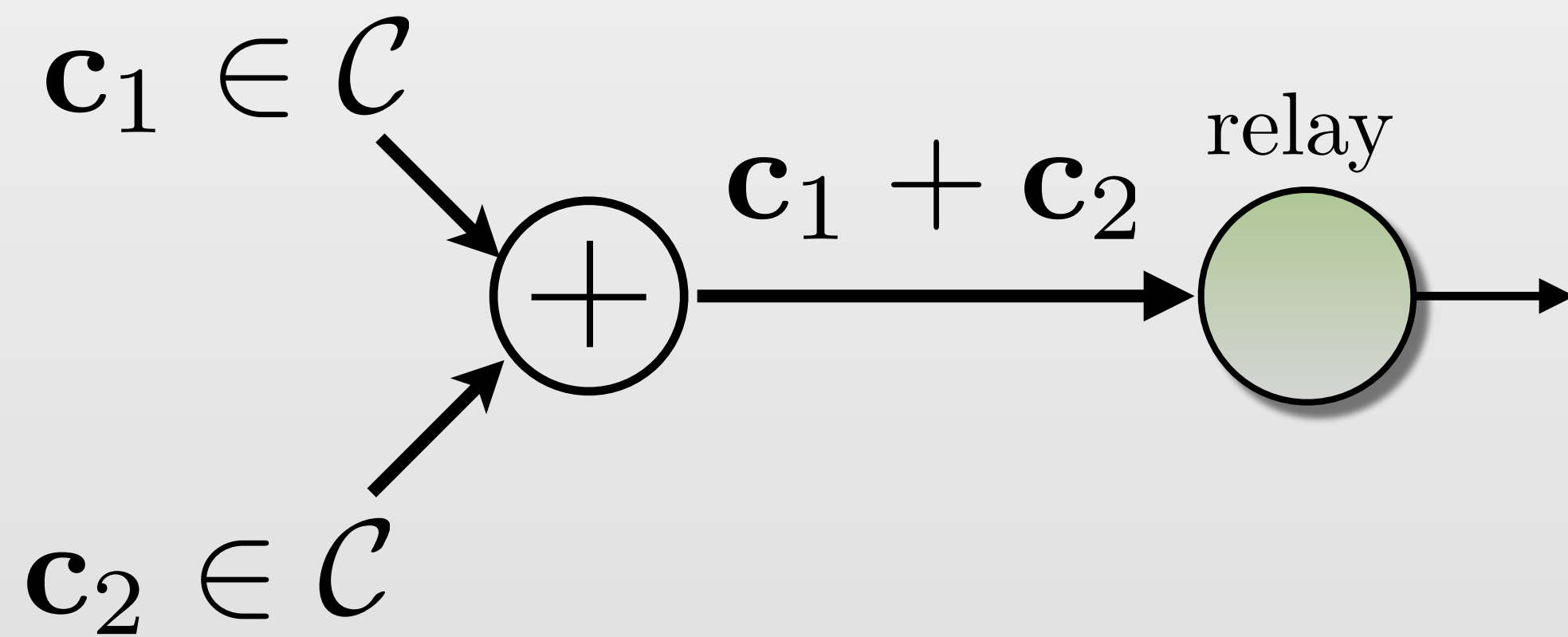
$$\begin{aligned} \mathbf{y} &= \mathbf{x} \bmod \Lambda_s \\ &= \mathbf{x} - Q_{\Lambda_s}(\mathbf{x}) \end{aligned}$$

find the image of \mathbf{x} in \mathcal{V}



Real Addition with Lattice Codes

Recall the multiple-access scenario



- $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ are finite group elements
- $\mathbf{c}_1 \oplus \mathbf{c}_2 \in \mathcal{C}$ is well defined
- But, real addition in the channel:

$$\mathbf{c}_1 + \mathbf{c}_2 \notin \mathcal{C}$$

- Solution: $\mathbf{c}_1 + \mathbf{c}_2 \bmod \Lambda_s \in \mathcal{C}$

Real Addition with Lattice Codes

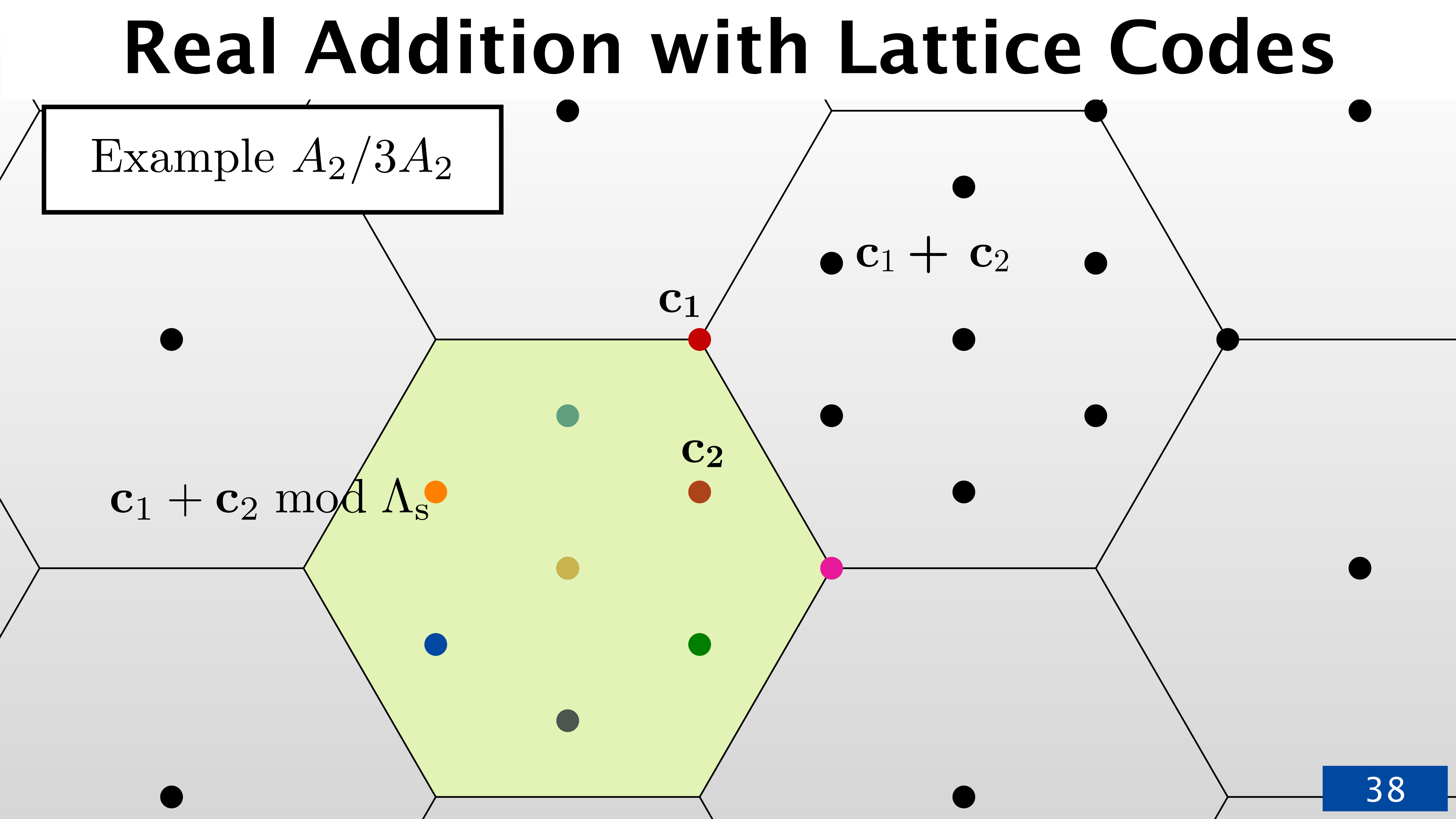
Example $A_2/3A_2$

$\mathbf{c}_1 + \mathbf{c}_2 \bmod \Lambda_s$

\mathbf{c}_1

\mathbf{c}_2

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



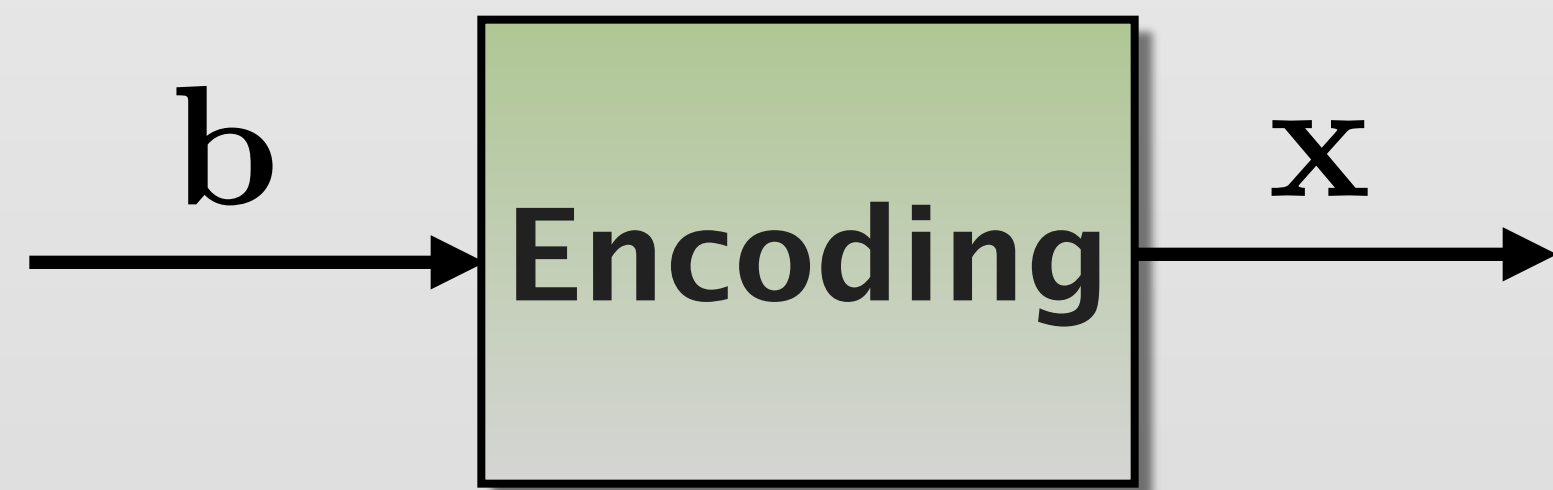
Encoding and Indexing

Index \mathbf{b} is information: $\mathbf{b} = [b_1 \ b_2 \ \cdots \ b_n]^t$,

where $b_i \in \{0, 1, \cdots, K - 1\}$.

given index \mathbf{b} , find $\mathbf{x} \in \mathcal{C}$

given $\mathbf{x} \in \mathcal{C}$, find index \mathbf{b}



$$\mathbf{x} = \text{enc}(\mathbf{b})$$



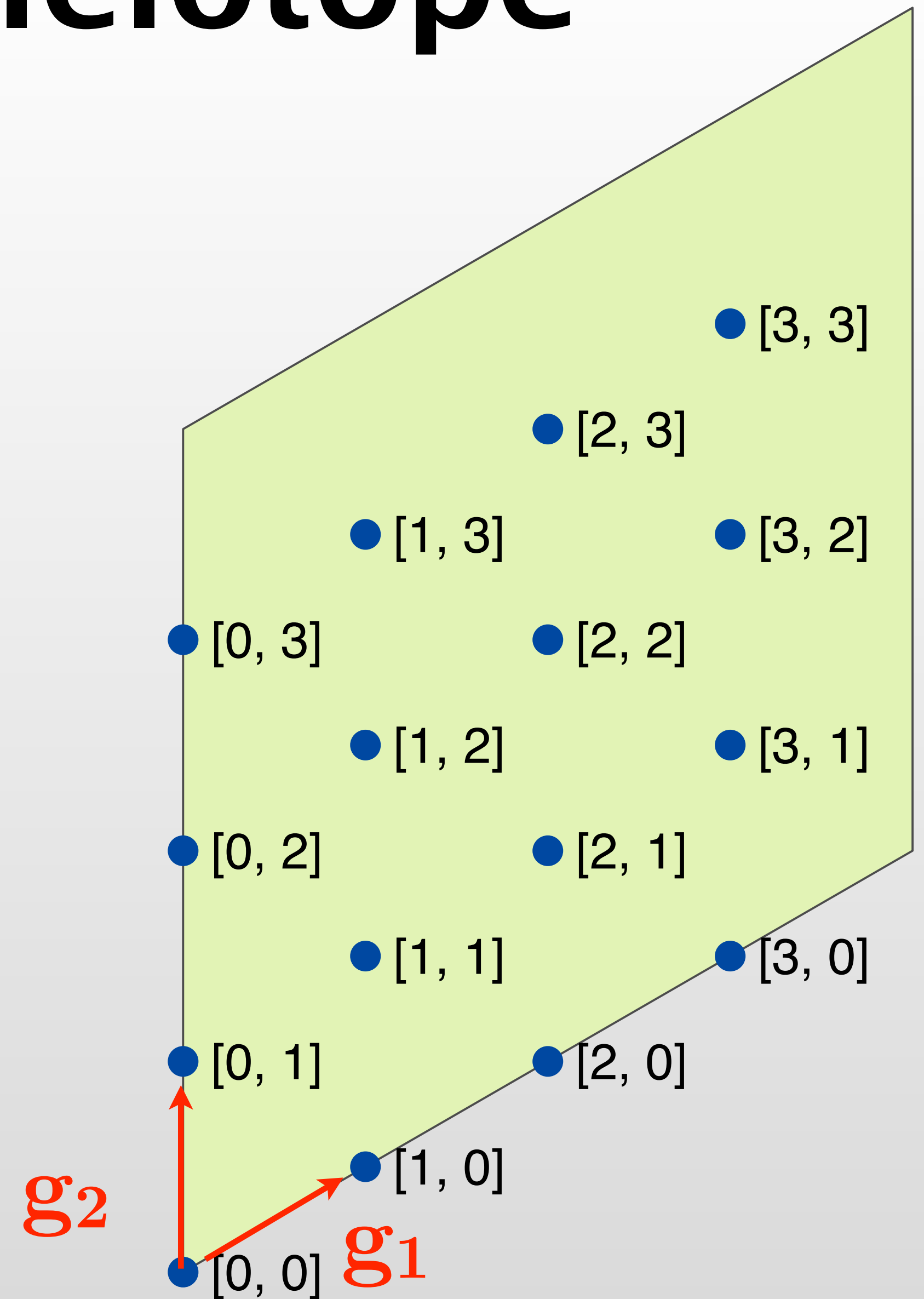
$$\begin{aligned} \mathbf{b} &= \text{enc}^{-1}(\mathbf{x}) \\ &= \text{index}(\mathbf{x}) \end{aligned}$$

Encoding Parallelotope

Example: $A_2/4A_2$

Index \mathbf{b} is information $b_i \in \{0, 1, 2, 3\}$:

$$\mathbf{x} = \underbrace{\begin{bmatrix} | & | & \cdots & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_n \\ | & | & \cdots & | \end{bmatrix}}_{\text{generator matrix}} \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$



Encoding the Voronoi Region

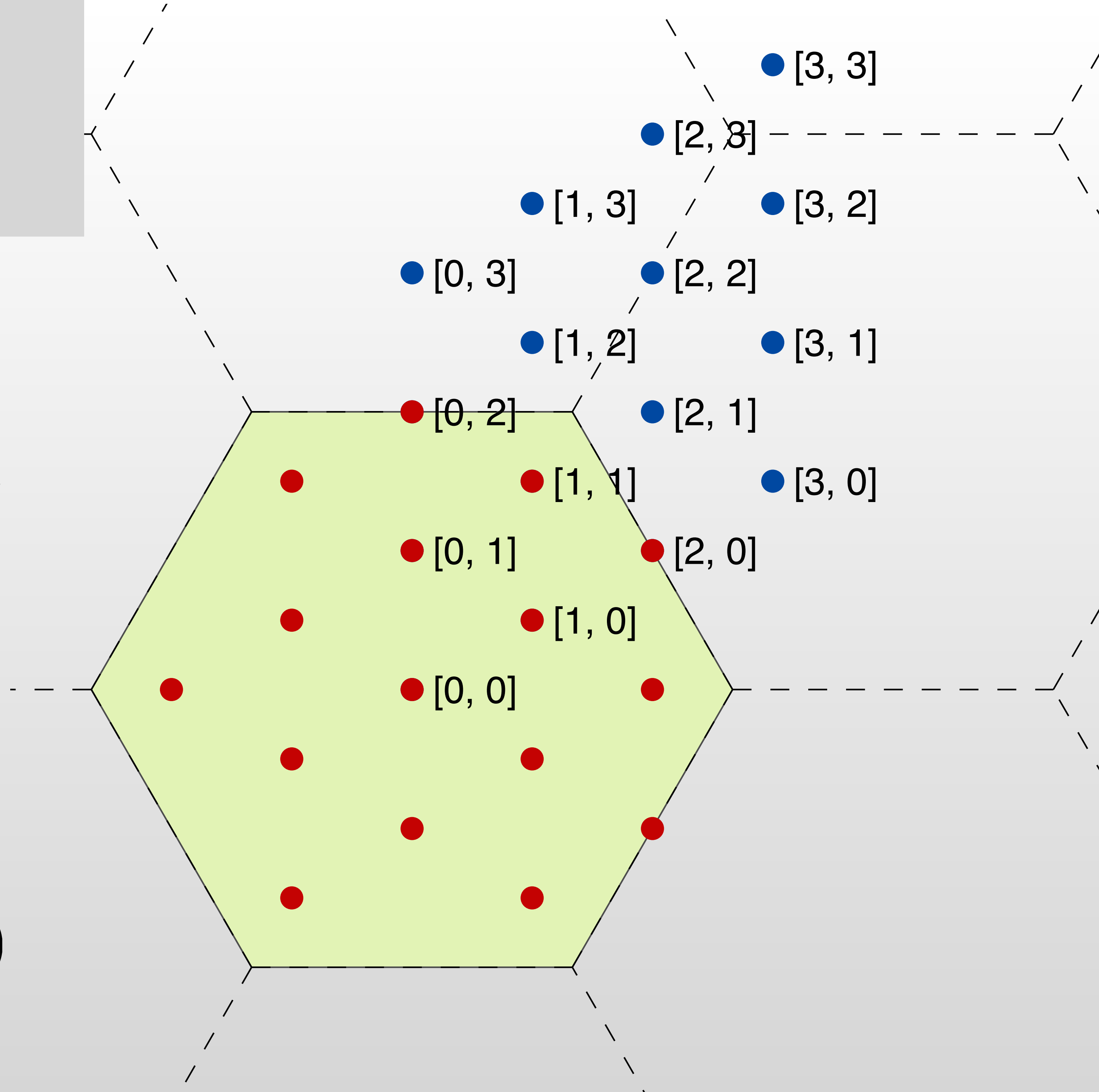
Two steps:

1. Parallelootope encoding

$$\mathbf{x} = G \cdot \mathbf{b}$$

2. Modulo operation

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



Encoding the Voronoi Region

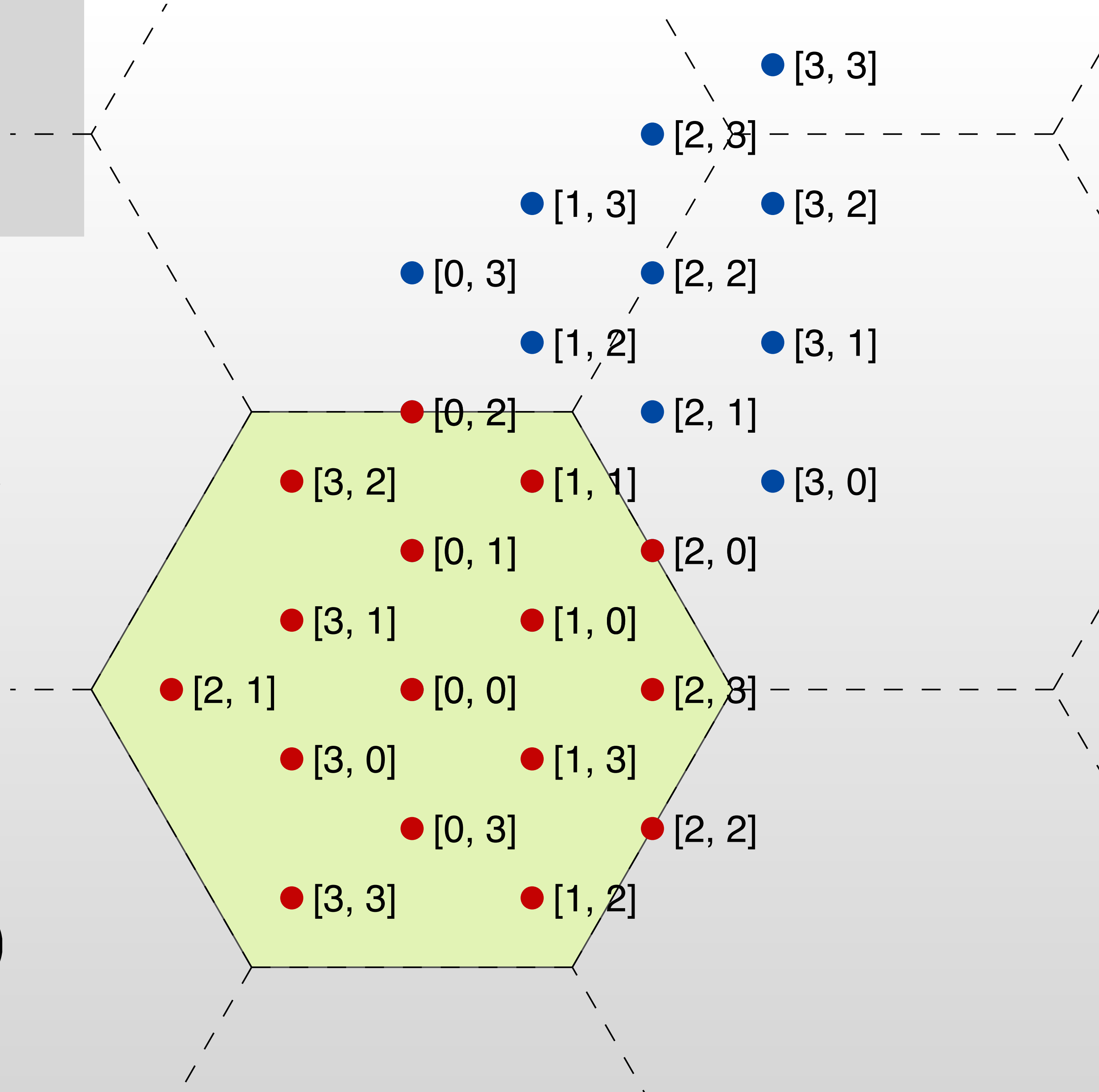
Two steps:

1. Parallelootope encoding

$$\mathbf{x} = G \cdot \mathbf{b}$$

2. Modulo operation

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



Group Isomorphism for PLNC

Information (indices) $\mathbf{b}_i \in \mathbb{Z}/K\mathbb{Z}$ form a ring with operation \oplus, \otimes (integers modulo K).

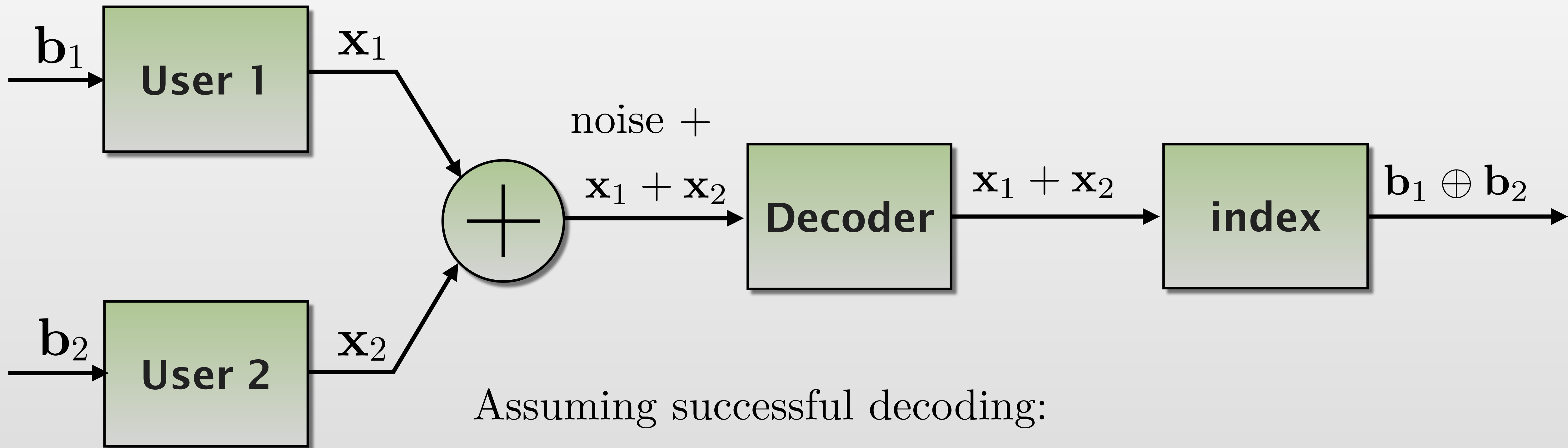
Lattice codewords $\mathbf{x} \in \mathcal{C}$ for a group with operation $+$ (vector addition modulo Λ_s).

Easy to show there is isomorphism:

$$\begin{aligned} \text{enc}(\mathbf{b}_1 \oplus \mathbf{b}_2) &= \text{enc}(\mathbf{b}_1) + \text{enc}(\mathbf{b}_2) \text{ or} \\ \text{index}(\mathbf{x}_1) \oplus \text{index}(\mathbf{x}_2) &= \text{index}(\mathbf{x}_1 + \mathbf{x}_2) \end{aligned}$$

Group Isomorphism for PLNC

Simple multiple access channel



Assuming successful decoding:

Decoder produces $\mathbf{x}_1 + \mathbf{x}_2$ (not \mathbf{x}_1 , \mathbf{x}_2 individually)

Indexing produces $\mathbf{b}_1 \oplus \mathbf{b}_2$ (not \mathbf{b}_1 , \mathbf{b}_2 individually)

Highly suitable for network coding

And now for something new...

Nested lattice codes with non-self-similar lattices

- High dimension lattices (LDLC, etc.): excellent coding gain, computationally hard to perform shaping,
- Low dimension lattices (E8, Barnes-Wall): Good shaping gain with efficient algorithms, not very good coding gain.

Nested lattice codes with non-self-similar lattices

Proposed method. Construct a quotient group:

$$\Lambda_{\mathbf{C}} / \Lambda_{\mathbf{S}}$$

High-dimension lattice:

$$n = 1,000 \text{ to } 10^5$$

E8, Barnes-Wall, etc. lattice

$$n = 8, 16$$

Nested lattice codes with non-self-similar lattices

Proposed method. Construct a quotient group:

$$\Lambda_{\mathbf{C}} / \Lambda_{\mathbf{S}} \times \cdots \times \Lambda_{\mathbf{S}}$$

High-dimension lattice:

$$n = 1,000 \text{ to } 10^5$$

E8, Barnes-Wall, etc. lattice

$$n = 8, 16$$

Sufficient Conditions to form a Group

Given a coding lattice Λ_c and a shaping lattice Λ_s , we need to test the condition $\Lambda_s \subseteq \Lambda_c$.

Let G_s be a $n \times n$ generator matrix for Λ_s .

Let $H = G^{-1}$ be the check matrix for Λ_c

Lemma $\Lambda_s \subseteq \Lambda_c$ if and only if $H \cdot G_s$ is a matrix of integers.

Easy to design Λ_c such that $\Lambda_c \subseteq \Lambda_s$

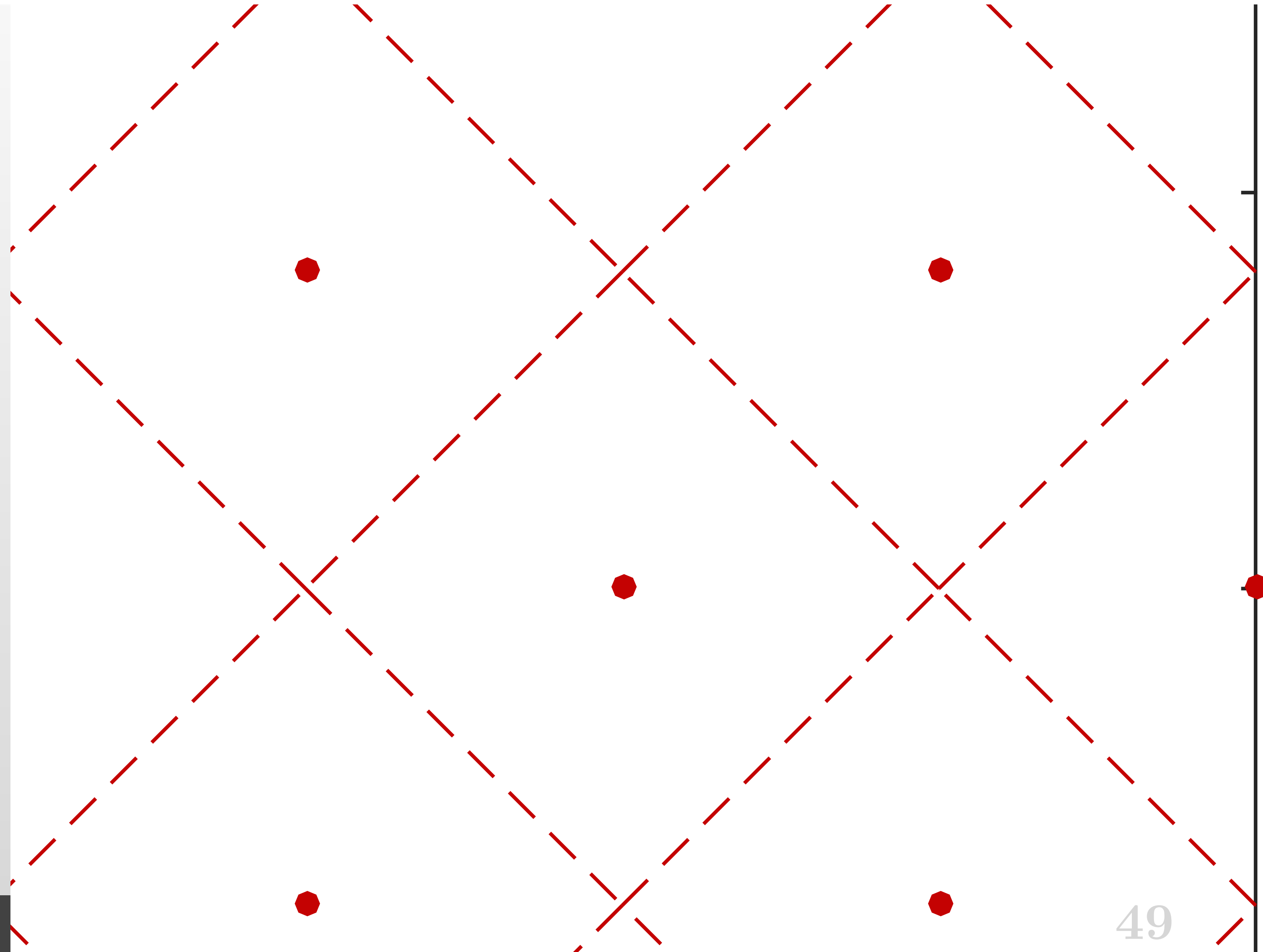
Achieving $\Lambda_s \subset \Lambda_c$ is easy.

Encoding/indexing is nontrivial.

Example for $n = 2$:

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

Indexing Non-Nested Lattice Codes



Achieving $\Lambda_s \subset \Lambda_c$ is easy.

Encoding/indexing is nontrivial.

Example for $n = 2$:

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

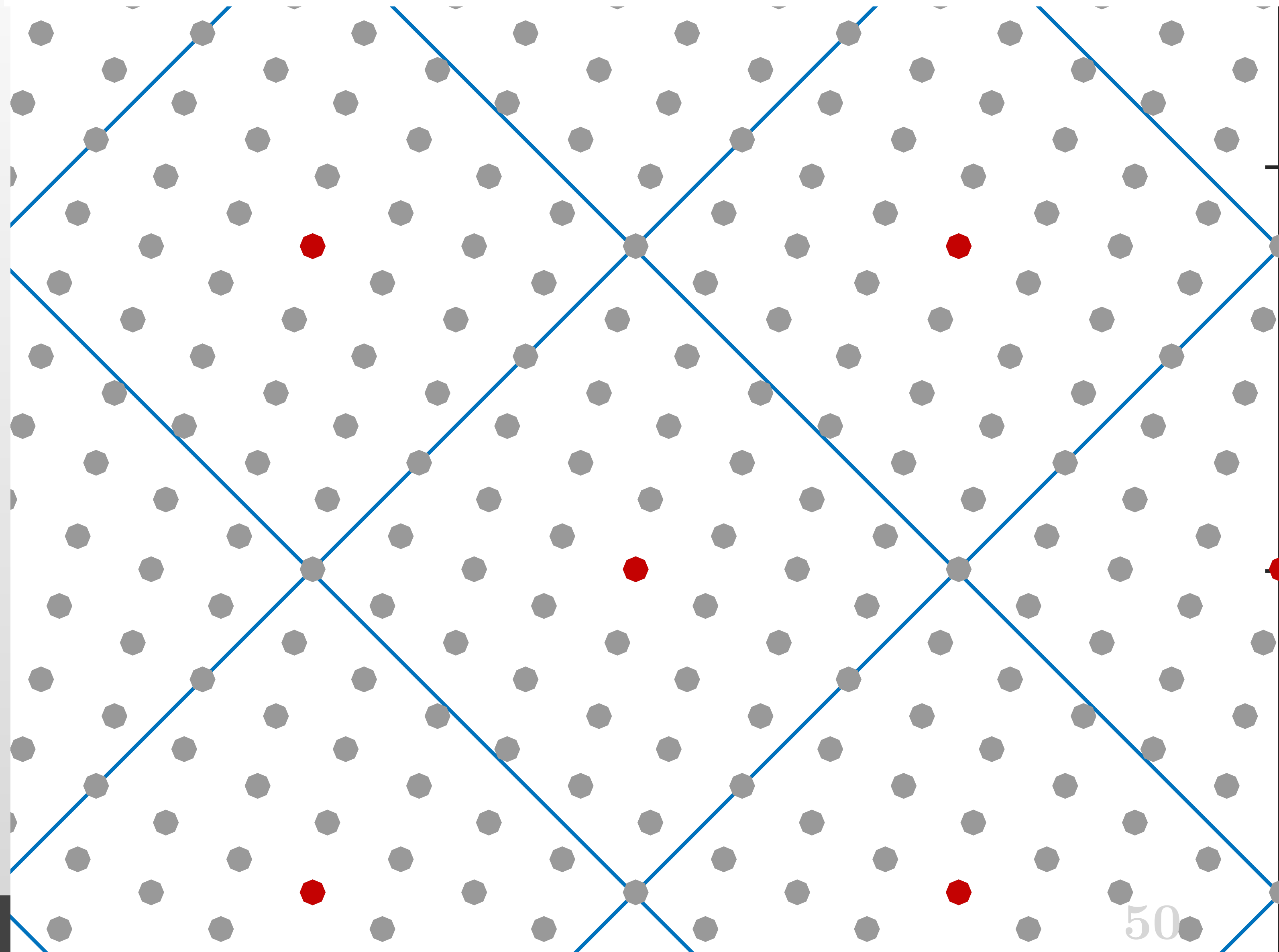
$$G_c = \begin{bmatrix} 8/9 & 2/9 \\ -4/9 & 8/9 \end{bmatrix} \longleftarrow \Lambda_c$$

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

Note:

- $\Lambda_s \neq K\Lambda_c$ not self similar
- but $\Lambda_s \subset \Lambda_c \Rightarrow \Lambda_c/\Lambda_s$

Indexing Non-Nested Lattice Codes



Indexing Non-Nested Lattice Codes

Number of codewords:

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

Natural candidate:

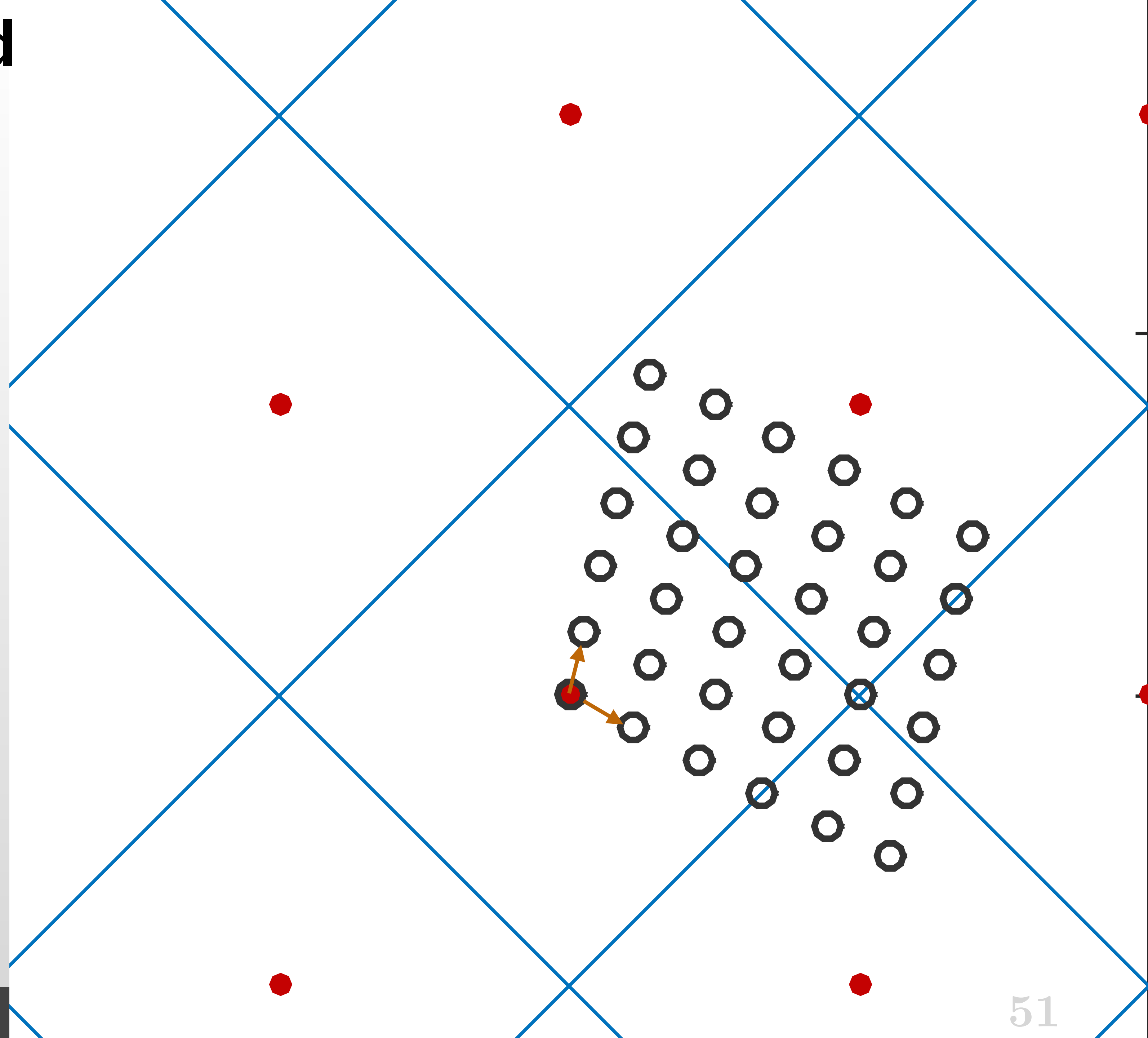
$$b_1 \in \{0, 1, 2, 3, 4, 5\}$$

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

Parallelotope encoding step:

$$G_c \mathbf{b} = \begin{bmatrix} 8/9 & 2/9 \\ -4/9 & 8/9 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

Do these points form coset leaders?



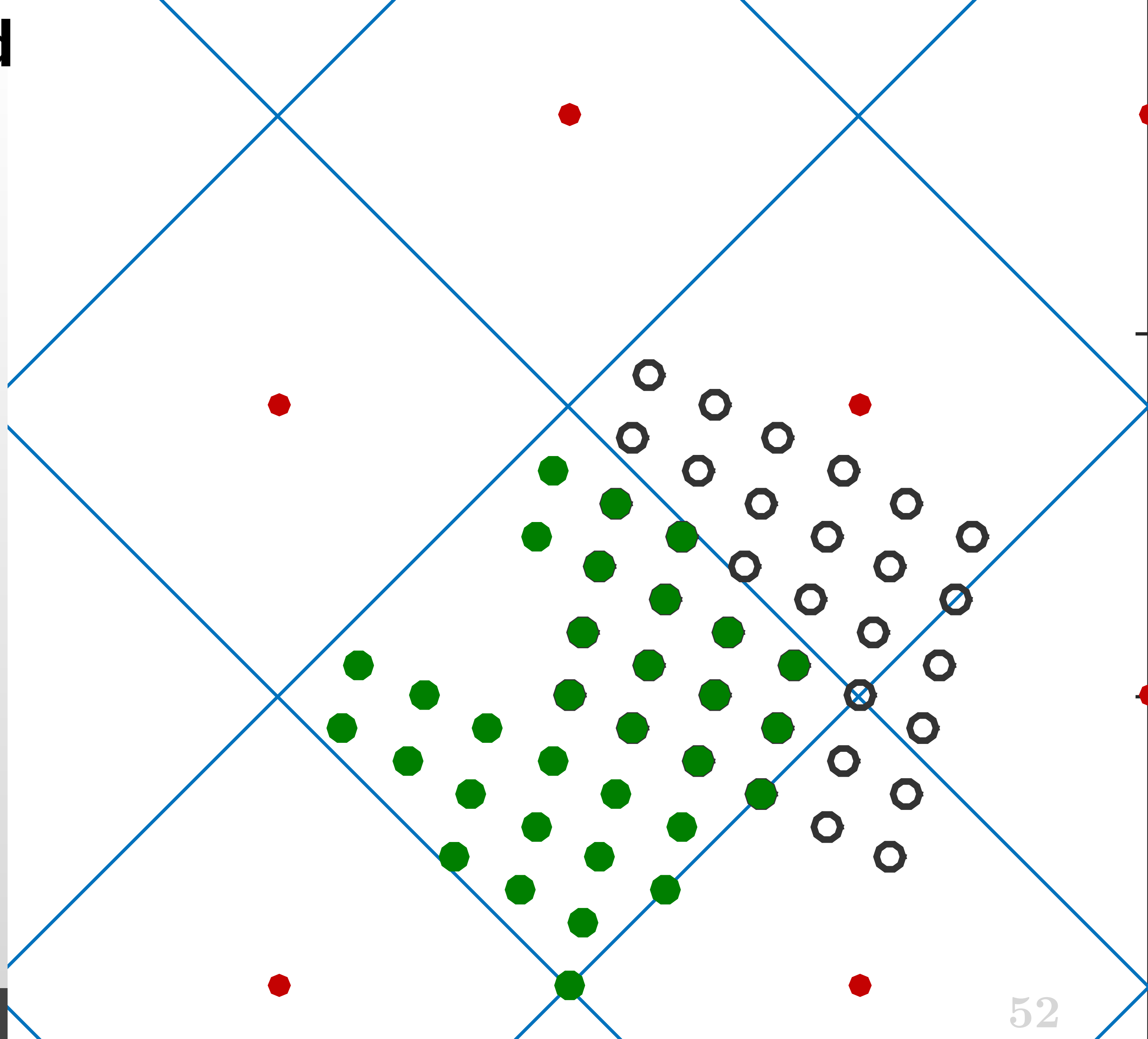
Indexing Non-Nested Lattice Codes

Encoding Step 2:

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

No! Coset leaders not formed.

What about a change of basis?



Finding a Basis Suitable for Encoding

We want to transform the basis of G_c :

$$G'_c = G_c W$$

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

$$G'_c = \left[\begin{array}{cccc} \frac{\mathbf{g}_1}{M_1} & \frac{\mathbf{g}_2}{M_2} & \cdots & \frac{\mathbf{g}_{n-1}}{M_{n-1}} & \mathbf{q} \end{array} \right]$$

\mathbf{g}_i from shaping lattice

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

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

$$= \left[\begin{array}{cccc|c} w_{11} & w_{12} & \cdots & w_{1,n-1} & z_1 \\ w_{21} & w_{22} & \cdots & w_{2,n-1} & z_2 \\ & \vdots & & & \\ w_{n,1} & w_{n,2} & \cdots & w_{n,n-1} & z_n \end{array} \right]$$

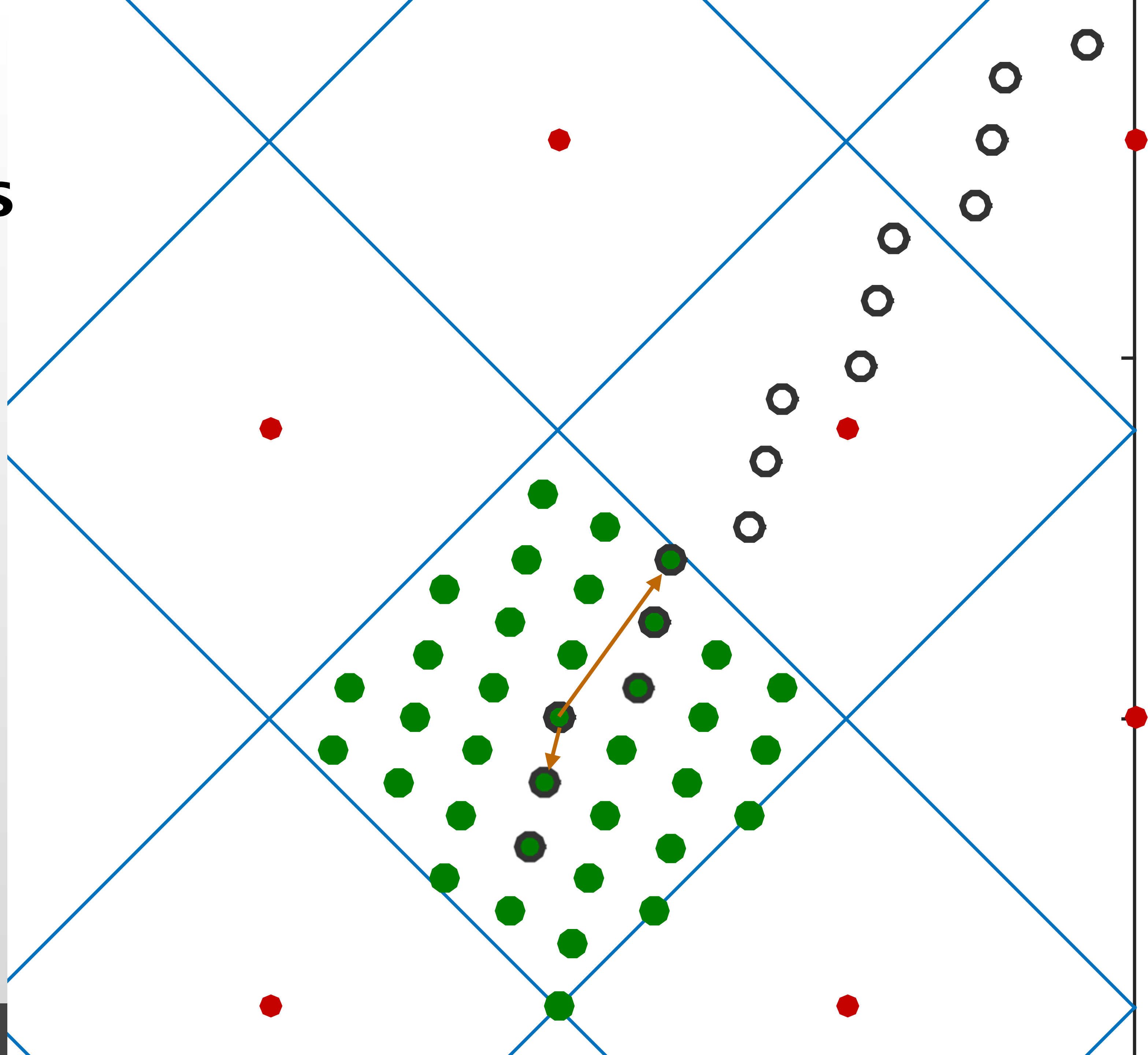
linearly dependent

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



Summary – Physical Layer Network Coding

PLNC:

- Technique for cooperative wireless networks
- Exploit network coding to increase capacity
- Lattices: real codes to correct errors, shaping gain
- Remove noise first, and interference later
- Compute-and-Forward relaying also deals with fading

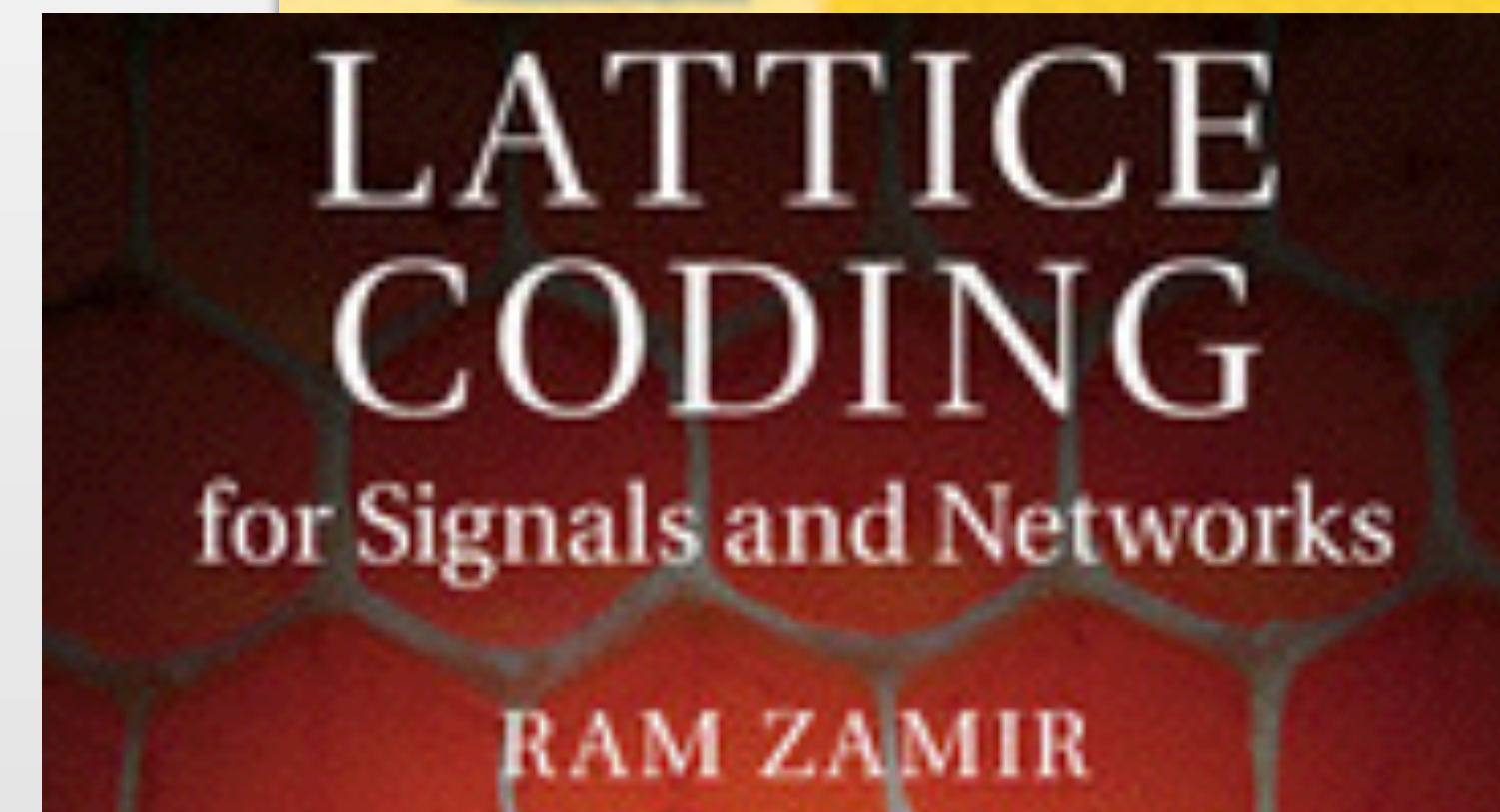
Recommended Reading

John Conway and Neil Sloane, *Sphere Packings, Lattices and Groups*, Springer, Third Edition, 1999



G. David Forney, Lecture notes for Principles of Digital Communications II Course at MIT

<http://dspace.mit.edu/>



Ram Zamir, *Lattice Coding for Signals and Networks*, Cambridge Univ Press, September 2014



Bobak Nazer and Michael Gastpar, “Reliable Physical Layer Network Coding,” *Proceedings of the IEEE*,

March 2011

Reliable Physical Layer Network Coding

Using the idea of network coding in the physical layer, as a means to improve throughput in wireless networks.

By BOBAK NAZER, Member IEEE, AND MICHAEL GASTPAR