Lattice Network Codes Based on Eisenstein Integers for Wireless Multiple-Access Relay Networks

Jinhong Yuan

原進宏

University of New South Wales (UNSW)

Chinese University of Hong Kong (CUHK)

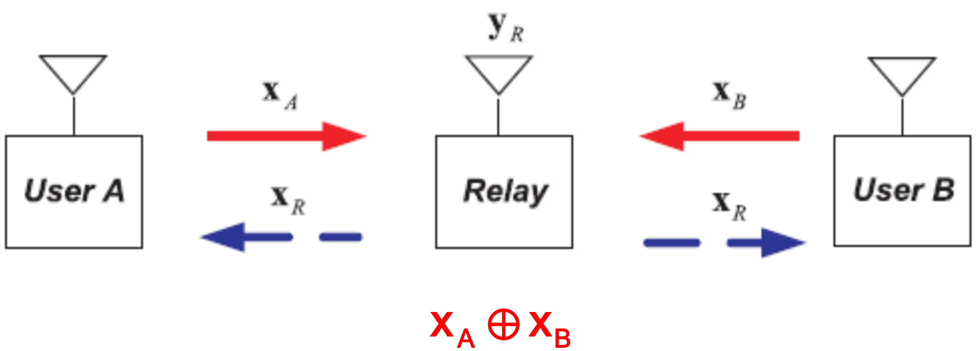
22.02.2012

Outlines

- Physical-layer Network Coding (PNC)
- Compute-and-forward (CF)
- Lattice Network Coding (LNC)
- Design Examples
- Union Bound Estimation (UBE)
- Conclusion

PNC

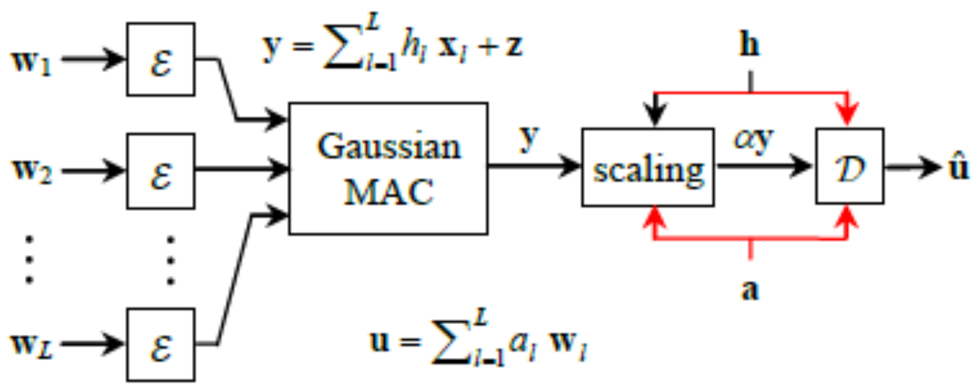
- Physical Layer Network Coding (PNC): decode the modulo-two sum of the two transmitted signals.
- Can enhance the throughput of a binary-input two-way relay channel (TWRC) [1]
- Approach the capacity upper bound of a Gaussian TWRC within ½ bits [2]



1. S. Zhang, S.-C. Liew, and P. P. Lam, Hot topic: physical layer network coding, Proc. 12th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 358-365, Los Angeles, California, USA, Sept. 2006..
2. W. Nam, S.-Y. Chung, and Y. H. Lee, Capacity of the Gaussian two-way relay channel to within 1/2 bit, IEEE Trans. Inform. Theory, vol. 56, no. 11, pp. 5488-5494, Nov. 2010.

Compute-and-Forward

- Nazer-Gastpar proposed a new strategy: Compute-and-forward (CF) for a Gaussian multiple access relay channel (MARC).
- CF is an extension of PNC: multiple-user/q-ary input/fading
- Key idea:
  - relay decodes a linear function of the transmitted messages
  - rather than decoding each user's message individually



3. B. Nazer and M. Gastpar, Compute-and-Forward: Harnessing Interference through Structured Codes, IEEE Trans. on Information Theory, 2011.

Compute-and-Forward

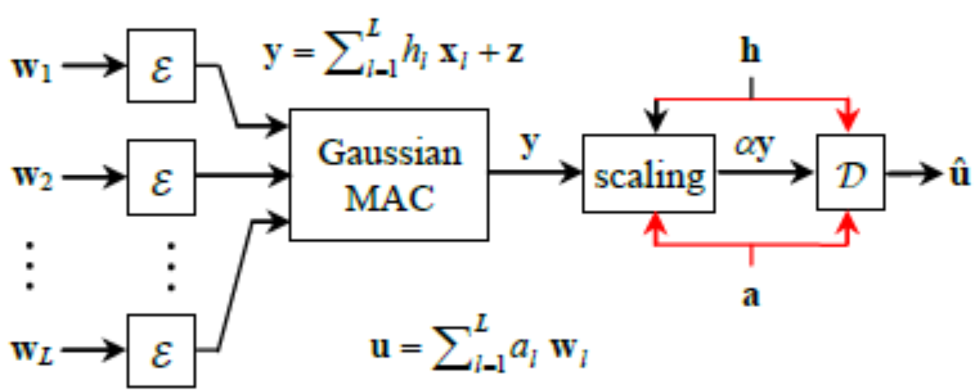
- Map the noisy linear C-combined signal from the channel

$$\mathbf{y} = \sum_{l=1}^{L} h_l \, \mathbf{x}_l + \mathbf{z}$$

to a linear (integer) function (network coding)

$$\mathbf{u} = \sum_{l=1}^{L} a_l \, \mathbf{w}_l$$

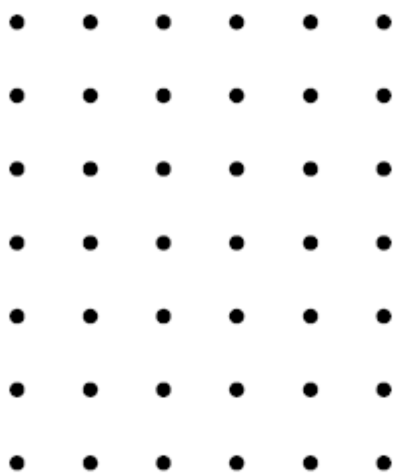
- Underlying principle: based on linear nested lattice codes
  - The integer combinations of the lattice points (codewords) is another lattice point (codeword).
  - It can be mapped back to the linear combinations of the messages **u** over the finite field.



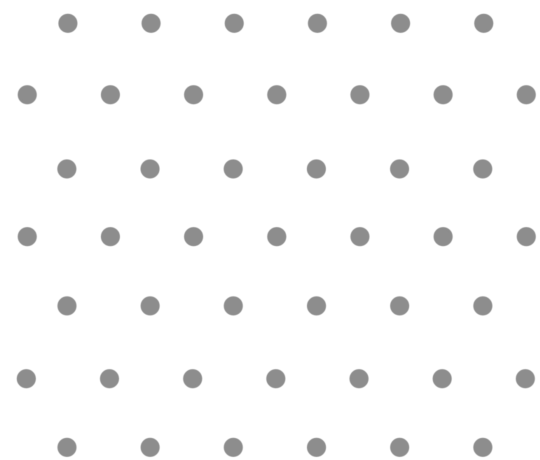
Lattice

- A lattice Λ is a discrete subset of n-space that has the group property.
- An integer lattice: Z^n
- A lattice can be viewed as the linear transformation of the integer lattice Z^n by a generator matrix B over R^{nxn}.

$$\Lambda = \mathrm{B}\mathbb{Z}^n$$



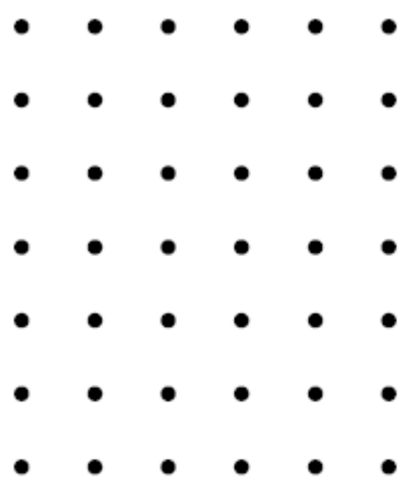
Z^2



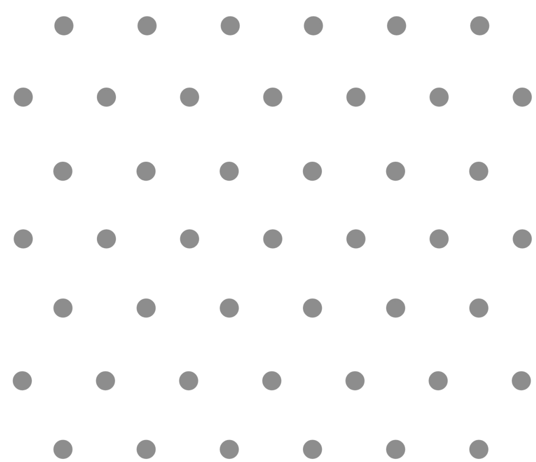
BZ^2

Lattice

- By the group property, any translation Λ+x by a lattice point x is just Λ, i.e. shift invariant.
- Closed under addition: $\lambda_1, \lambda_2 \in \Lambda \implies \lambda_1 + \lambda_2 \in \Lambda.$
- Symmetric: $\lambda \in \Lambda \implies -\lambda \in \Lambda$
- Implies: Lattice is geometrically uniform in Euclidean distance
  - Every point has the same number of neighbors at each distance.
  - All decision regions of a minimum-distance decoder are congruent.



Z^2



BZ^2

Lattice

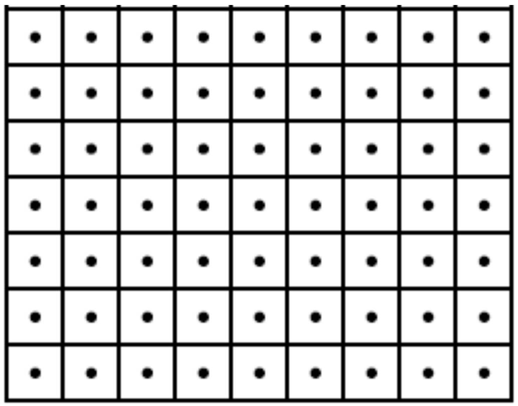
- Nearest neighbor quantizer (decoder): send a vector x to a nearest lattice point in terms of the Euclidean distance.

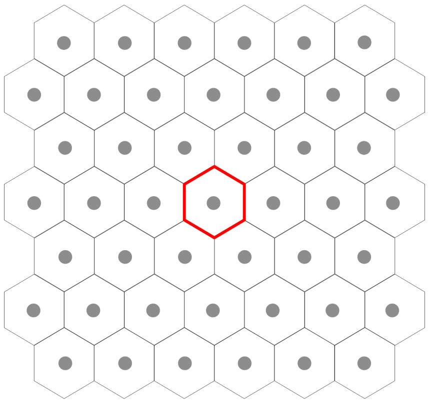
$$\mathcal{D}_\Lambda(\mathbf{x}) \triangleq \mathrm{argmin}_{\boldsymbol{\lambda}\in\Lambda}||\mathbf{x} - \boldsymbol{\lambda}||$$

- The Voronoi region of a lattice point: the set of all points that quantize to the lattice point.

- Fundamental Voronoi region $\mathcal{V}$: the sets of points quantize to the origin.

$$\mathcal{V} = \{\mathrm{x} : Q_\Lambda(\mathrm{x}) = 0\}$$



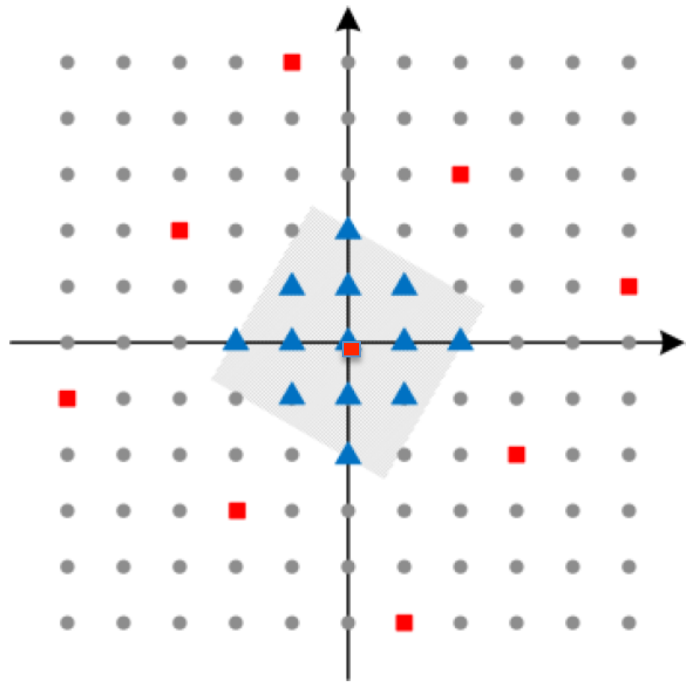


Nested Lattice

- Consider a sublattice Λ' of lattice Λ. They are **nested** as $\Lambda' \subset \Lambda$.
  - **Fine lattice** Λ
  - **Coarse lattice** Λ'

- **Nested Lattice code**: The set of lattice points of the fine lattice Λ in the fundamental Voronoi region $\mathcal{V}$ of the coarse lattice Λ'.

- The region $\mathcal{V}$ is also called the shaping region of the code.

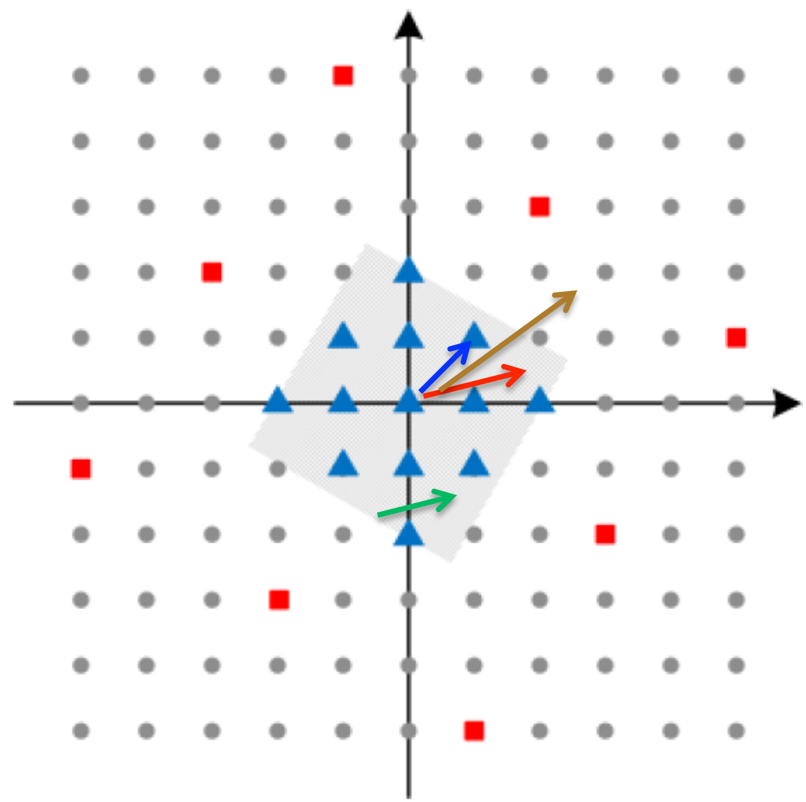


- The code rate

$$R = \frac{1}{n} \log_2 \frac{V(\Lambda')}{V(\Lambda)}$$

Nested Lattice Encoding

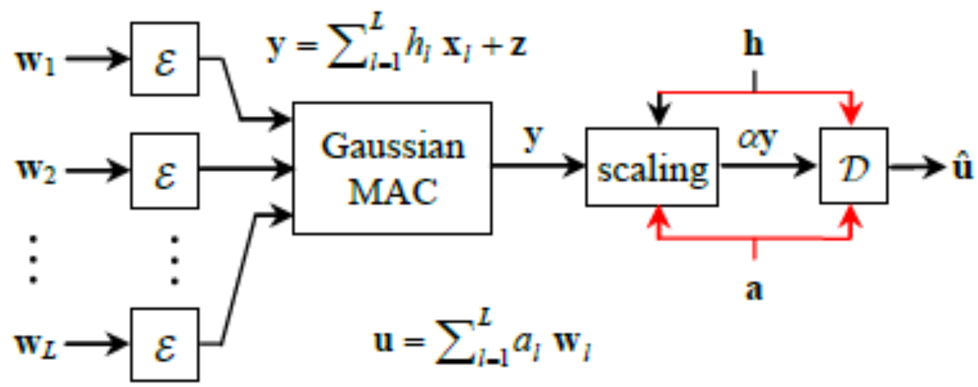
- Define a linear **code generator G** and **Lattice generator B**
- Generate codeword Gw for message w
- Map the scaled down version *r*Gw into the fundamental Voronoi region (**hypercube**) $\mathcal{V} = [-1/2, 1/2)^n$
- Generate **fine lattice** **t**=B*r*Gw
- Generate **coarse lattice Λ'**=BZ^n
- Generate a random **dither vector d** uniformly over $\mathcal{V}$
- Transmit a **dithered codeword**
  x = [**t+d**] mod Λ'



Nested Lattice Encoding/Decoding

- Encoders use the same nested lattice codes, **transmit dithered codewords**

$$\begin{aligned} \mathrm{x}_i &= [\mathrm{t}_i + \mathrm{d}_i] \bmod \Lambda' \\ &= [\mathrm{B}r\mathrm{Gw}_i + \mathrm{d}_i] \bmod \Lambda' \end{aligned}$$



- Decoder **scales by α**

Removes dithers

$$\begin{aligned} &\left[\alpha \mathrm{y} - \sum_i q_i \mathrm{d}_i\right] \bmod \Lambda' \\ &= \left[\alpha\left(\sum_i h_i \mathrm{x}_i + \mathrm{z}\right) - \sum_i q_i \mathrm{d}_i\right] \bmod \Lambda' \\ &= \left[\sum_i q_i \mathrm{x}_i + \sum_i (\alpha h_i - q_i)\mathrm{x}_i + \alpha \mathrm{z} - \sum_i q_i \mathrm{d}_i\right] \bmod \Lambda' \\ &= \left[\sum_i q_i [\mathrm{t}_i + \mathrm{d}_i] \bmod \Lambda' + \sum_i (\alpha h_i - q_i)\mathrm{x}_i + \alpha \mathrm{z} - \sum_i q_i \mathrm{d}_i\right] \bmod \Lambda' \\ &= \left[\sum_i q_i \mathrm{t}_i + \sum_i (\alpha h_i - q_i)\mathrm{x}_i + \alpha \mathrm{z}\right] \bmod \Lambda' \end{aligned}$$

- **Recovers linear equation (network code)**

$$\begin{aligned} \mathbf{u} &= \left[\sum_i q_i \mathbf{t}_i\right] \bmod \Lambda' \\ &= \sum_i a_i \mathbf{w}_i \end{aligned}$$

Effective noise: $\mathrm{n} = \sum_i (\alpha h_i - q_i)\mathrm{x}_i + \alpha \mathrm{z}$

Compute-and-Forward

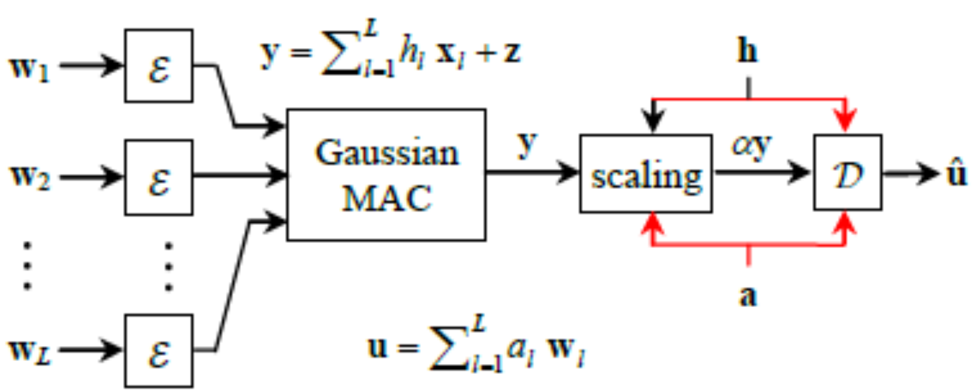
Effective noise: $\mathbf{n} = \sum_i (\alpha h_i - q_i)\mathbf{x}_i + \alpha \mathbf{z}$

Minimizing the effective noise by choosing α to be MMSE coefficient

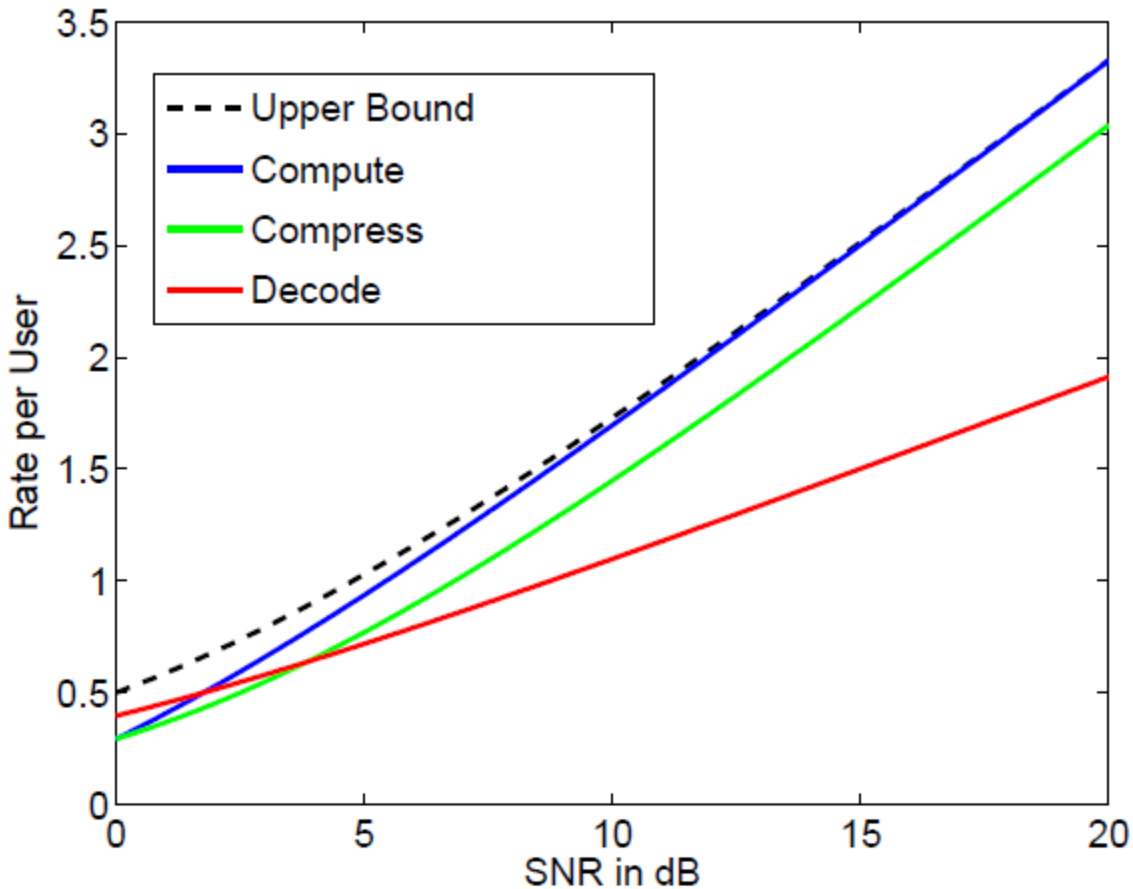
$$\alpha = \frac{P\mathbf{h}^*\mathbf{a}}{1 + P\|\mathbf{h}\|^2}$$

The computation rate

$$R(\mathbf{h}, \mathbf{a}) = \log_2^+\left(\|\mathbf{a}\|^2 - \frac{P|\mathbf{h}^*\mathbf{a}|^2}{1 + P\|\mathbf{h}\|^2} \right)$$



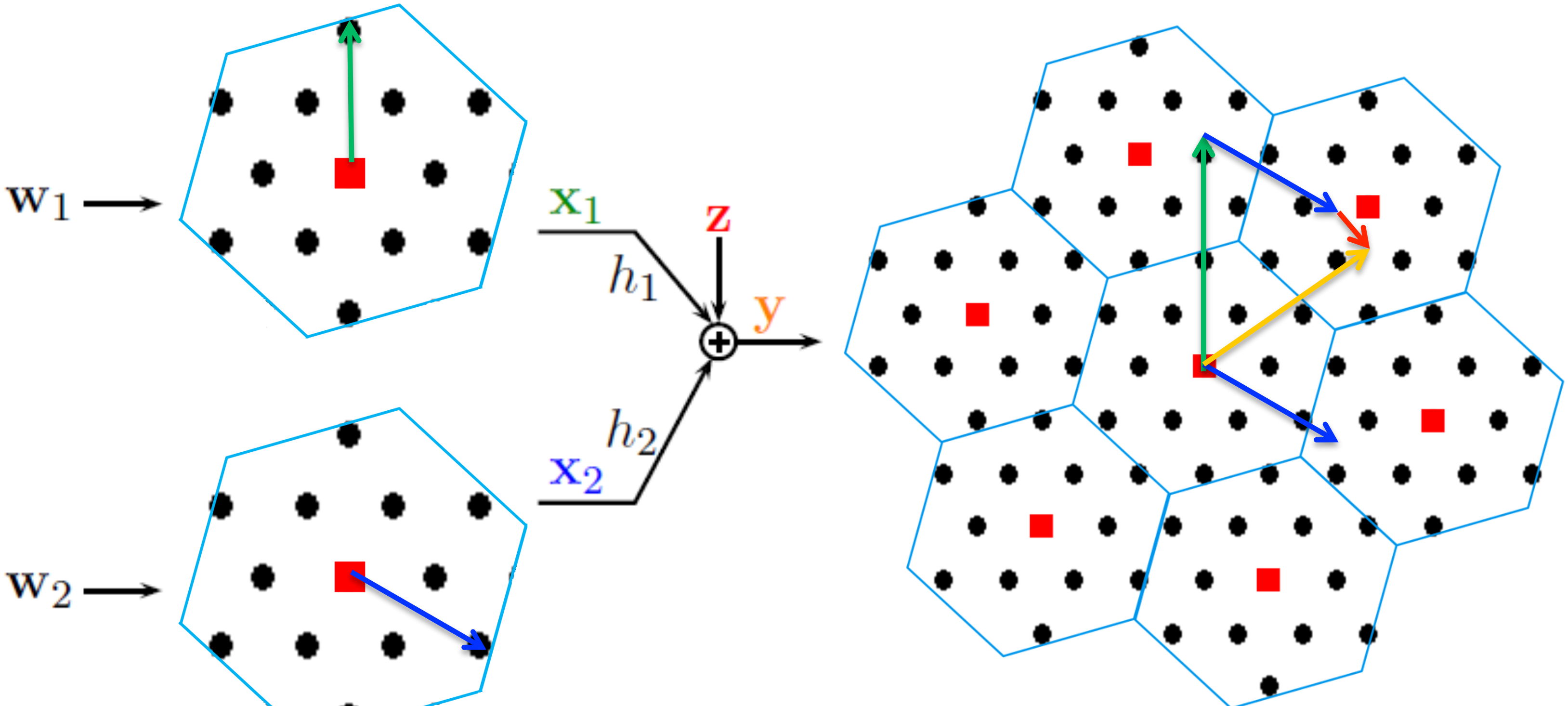
Compute-and-Forward



Performance of Gaussian TWRC

From: Nazer/Gastpar

Compute-and-Forward



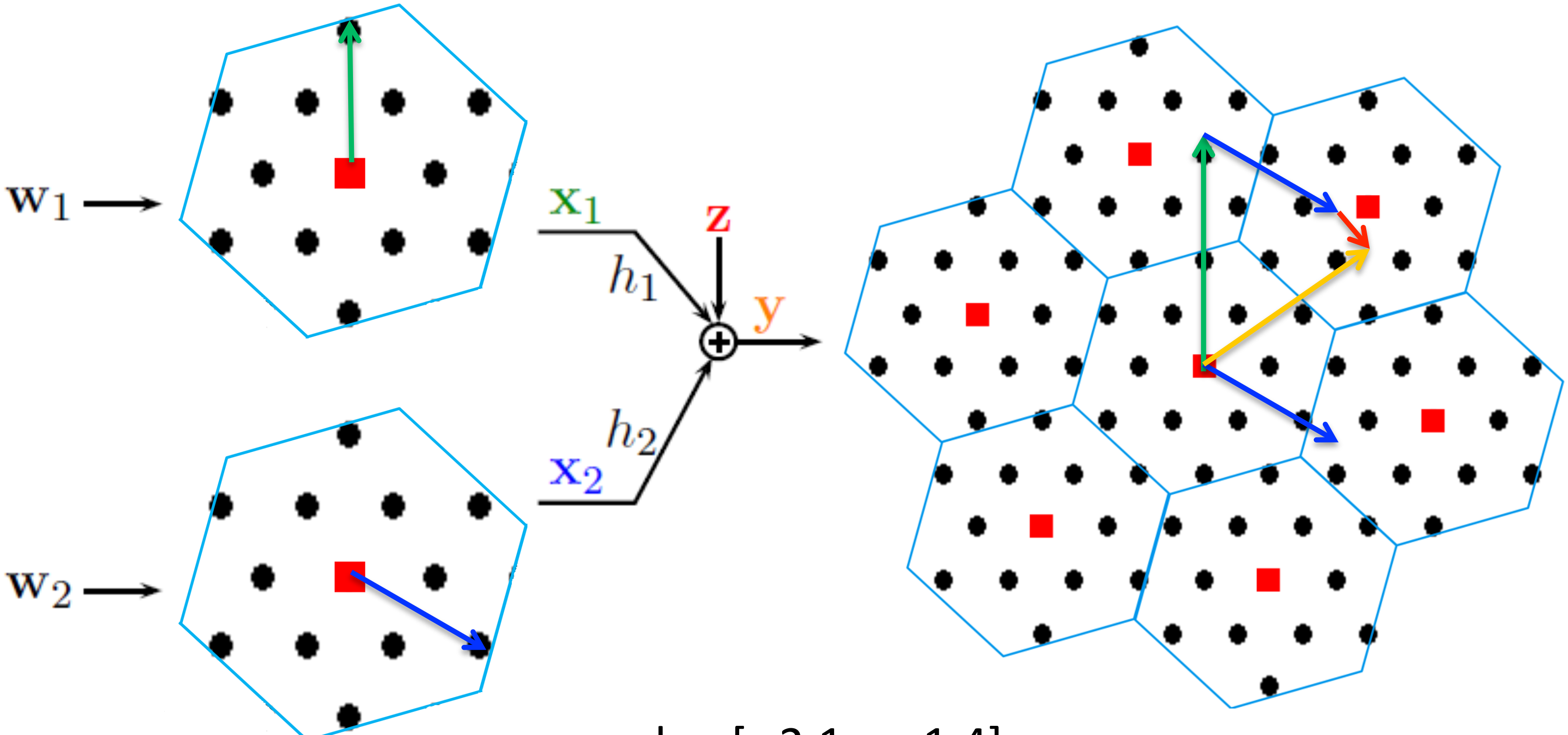
h = [2.1 1.4]

a = [3   2]

Effective Noise: $N+P|h-a|^2$

From: Nazer/Gastpar

Compute-and-Forward



$\alpha h = [\alpha 2.1 \quad \alpha 1.4]$

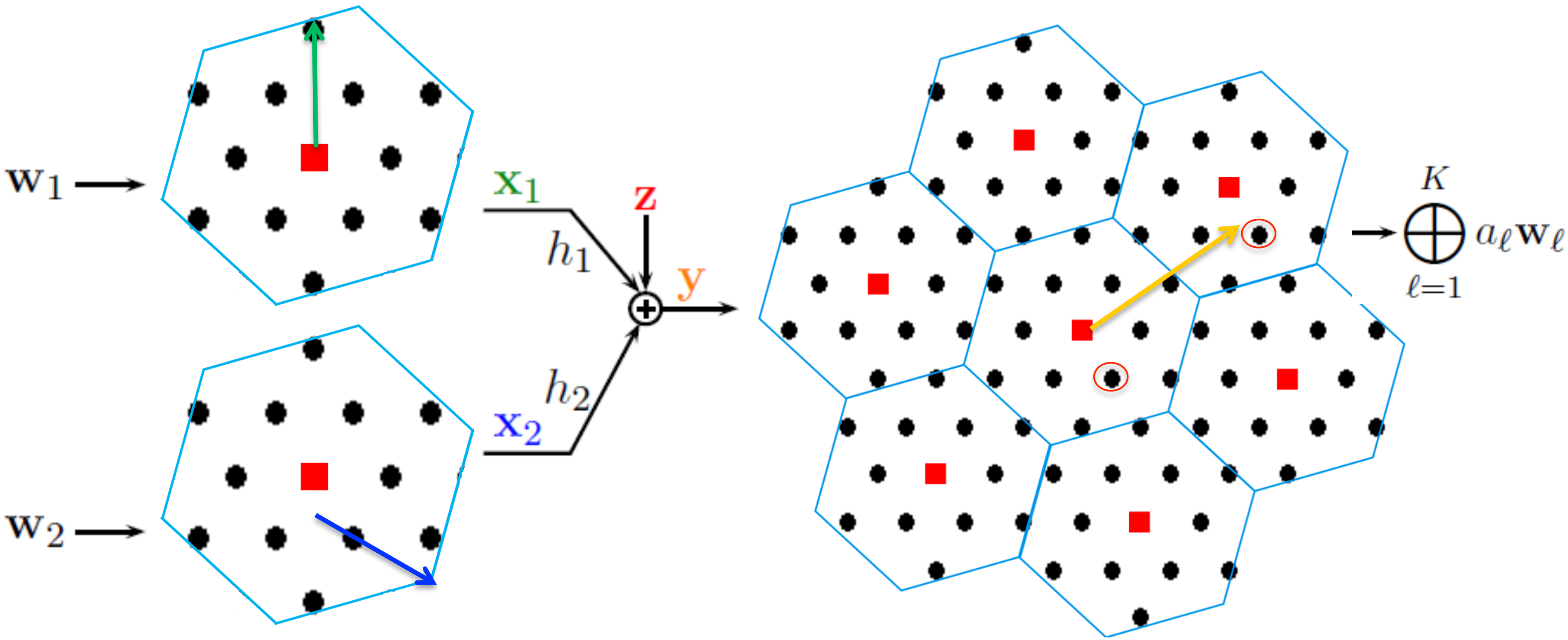
$a = [3 \qquad 2\,]$

Effective Noise: $\alpha^2 N + P|\alpha h - a|^2$

From: Nazer/Gastpar

Compute-and-Forward

Map back to equation of message symbols over the field:



$\alpha h = [\alpha 2.1 \quad \alpha 1.4]$

$a = [3 \qquad 2\,]$

Effective Noise: $\alpha^2 N + P|\alpha h - a|^2$

From: Nazer/Gastpar

Compute-and-Forward

- A theoretic guideline as it assumes an infinite sequence of good lattice partition.

- Map message to a lattice point

$$\mathrm{t}_i = \phi(\mathrm{w}_i)$$

- Transmit dithered codeword

$$\mathrm{x}_i = \left[\mathrm{t}_i + \mathrm{d}_i\right] \bmod \Lambda'$$

- The decoder recovers

$$\sum_i q_i \mathrm{t}_i \bmod \Lambda'$$

- Map it back to the linear combination of the messages

$$\sum_i a_i \mathrm{w}_i = \phi^{-1}\left(\sum_i q_i \mathrm{t}_i \bmod \Lambda'\right)$$

- **Question:**
  - How to design the mapping functions?
  - How to implement modulo operation in n-space?

Lattice Network Coding

- A general algebraic framework proposed by *Feng/Silva/Kschischang* to design and implement practical compute-and-forward scheme using finite dimension lattice partition.

- It makes direct connection between the CF strategy and module theory.

- Using the algebraic properties of principal ideal domain (PID), it links the C-linear combination operation performed by the channel

$$y = \sum_i h_i \mathrm{x}_i + z$$

and the R-linear combination operation in the message space for the network coding

$$\sum_i a_i \mathrm{w}_i$$

4. *C. Feng, D. Silva and F. R Kschischang, An algebraic Approach to Physical-layer Network Coding, submitted to IEEE Trans. On Information Theory, 2011.*

Lattice Network Coding

- Let R be a discrete subring of C forming a principal ideal domain PID (e.g., integer numbers, Gaussian integers Z[i])

- Define an **R-lattice** $\Lambda = \left\{ \mathrm{r}G_{\Lambda} : \mathrm{r} \in R^{n} \right\}$ (R-module) and its sublattice of Λ'.

- The set of all the cosets of Λ' in Λ, denoted by Λ/Λ', forms an **R-lattice partition** of Λ. The message space W=Λ/Λ'. (Figure)

- Define a **linear labelling**

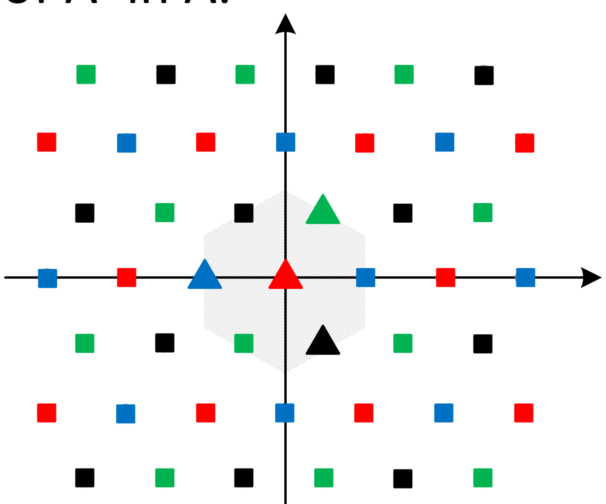
  $\phi^{-1}: \Lambda \rightarrow \Lambda/\Lambda'$

  taking a lattice point λ in Λ, map to a coset λ+ Λ' of Λ' in Λ.

- Define an **embedding map**

  $\phi: \quad W \rightarrow \Lambda$

  embedding each message to a lattice point in the same coset.



Lattice Network Coding

- **The encoder** maps a message w=λ+Λ’ to a coset leader, using the **embedding map.**

$$\mathrm{x}_i = \varepsilon\left(\mathrm{w}_i\right) = \phi\left(\mathrm{w}_i\right) - D_{\Lambda'}\left(\phi\left(\mathrm{w}_i\right)\right)$$

- **The decoder** estimates an R-linear combination

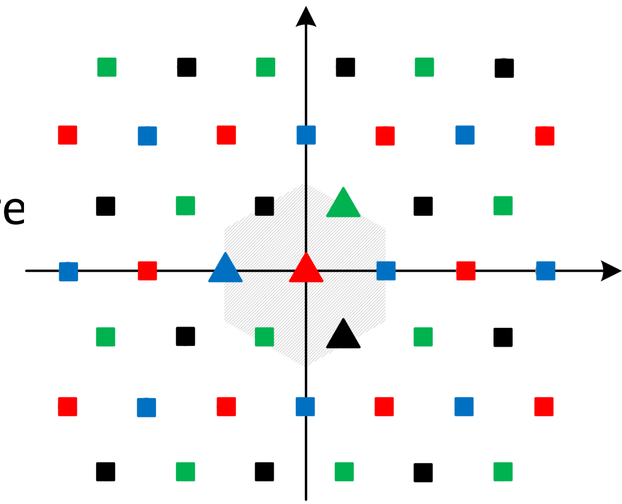
$$\sum_i q_i \mathrm{x}_i$$

from the C-linear combination

$$y = \sum_i h_i \mathrm{x}_i + z$$

and maps the R-linear combination to a coset Λ/Λ’ by using **linear labelling**

$$\sum_i a_i \mathrm{w}_i = \phi^{-1}\left(D_\Lambda\left(\alpha \mathrm{y}\right)\right)$$



- R is a subring of C, the linear labelling induces a nature bridge between the C-linear combining and the R-linear combining in the message space.

Lattice Network Coding

How to **construct linear labelling** $\phi^{-1}: \Lambda \to \Lambda/\Lambda'$?

Theorem (Feng/Silva/Kschischang)

Let R be a PID and Λ/Λ′ be a finite R-lattice partition. There exist generator matrices for Λ and Λ′ satisfying

$$G_{\Lambda'} = \begin{bmatrix} \mathrm{diag}(\pi_1, \ldots, \pi_k) & 0 \\ 0 & I_{n-k} \end{bmatrix} G_{\Lambda}$$

where $\pi_1 | \pi_2 | \cdots | \pi_k$ are the invariant factors of Λ/Λ′.

And the linear labelling is represented by a direct sum of modules R/π

$$\phi^{-1}: \ \Lambda \to \Lambda / \Lambda' \cong R/(\pi_1) \oplus R/(\pi_2) \oplus \ldots \oplus R/(\pi_k)$$

$$\phi^{-1}(\mathrm{r}G_{\Lambda}) = (r_1 + \pi_1, r_2 + \pi_2, \ \ldots, r_k + \pi_k)$$

Implies:

– Construct high-D lattice from low-D lattice.

– We only consider linear labelling for 1-D baseline lattice R/π.

LNC Based on Gaussian Integer

- **Gaussian integer** $\mathrm{Z}[i] = \{a + bi : a, b \in \mathrm{Z}\}$
- Discrete subring of the complex numbers.

Example.

Consider a lattice Z[i] and its sublattice βZ[*i*], where β=2+3*i* (Gaussian integer).

A finite field F_{13} is isomorphic to Z[i]/βZ[i].

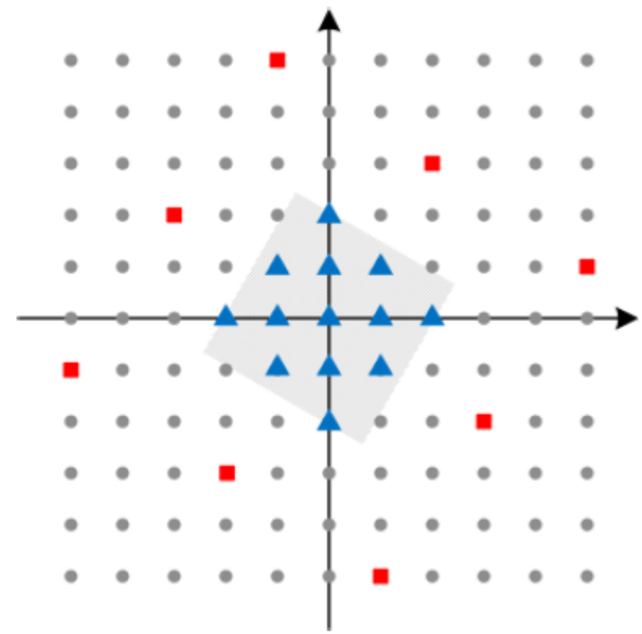
The message space $W=(Z[i]/\beta Z[i])^k$

The shaping is a rotated **hypercube** in C^n.

The encoder maps a message $w=\lambda+(Z[i]/\beta Z[i])^k$ into its coset leader.

The decoder uses the linear labelling

$$\phi^{-1}(\mathrm{r}) = ((r_1 - \lfloor r_1/\beta \rceil \times \beta) + \beta, \ldots, (r_k - \lfloor r_k/\beta \rceil \times \beta) + \beta)$$



(a) $\mathbb{Z}[i]$

LNC Based on Gaussian Integer

Union bound Estimation (UBE) of the error probability for hypercube shaping

$$P_e(\mathbf{h},\mathbf{a}) \approx K(\Lambda/\Lambda')\exp\left(-\frac{d^2(\Lambda/\Lambda')}{4N_0Q(\alpha,\mathbf{a})}\right)$$

where $$Q(\alpha,\mathbf{a}) = |\alpha|^2 + SNR\|\alpha\mathbf{h}-\mathbf{a}\|^2$$

The **effective noise** is $N_o Q(\alpha, \mathbf{a})$.

The minimum **inter-coset distance** of Λ/Λ': $d(\Lambda/\Lambda')$.

It is also called the length of the shortest vectors in the set difference $\Lambda \backslash \Lambda'$

The **number of shortest vectors**: $K(\Lambda/\Lambda')$

The kissing number.

LNC Based on Gaussian Integer

Union bound Estimation (UBE) of the error probability

$$P_e(\mathbf{h},\mathbf{a}) \approx K(\Lambda/\Lambda')\exp\left(-\frac{d^2(\Lambda/\Lambda')}{4N_0 Q(\alpha,\mathbf{a})}\right)$$

$$= K(\Lambda/\Lambda')\exp\left(-\frac{\gamma_c(\Lambda/\Lambda')3\mathrm{SENR}_{\mathrm{norm}}}{2}\right)$$

The normalized signal-to-effective-noise ratio

$$\mathrm{SENR}_{\mathrm{norm}} = \frac{\mathrm{SENR}}{2^R} = \frac{\mathrm{SNR}}{2^R Q(\alpha,\mathbf{a})}$$

The nominal coding gain:

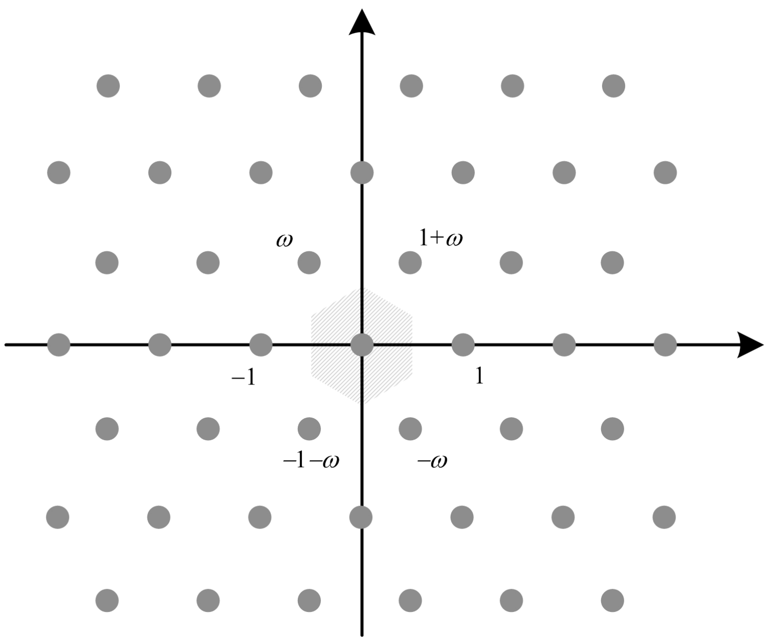
$$\gamma_c(\Lambda/\Lambda') = \frac{d^2(\Lambda/\Lambda')}{V(\Lambda)^{1/n}}$$

Measures the increase in density of Λ over the baseline uncoded hypercube lattice.

The nominal coding gain for the baseline system is 0 dB.

LNC Based on Eisenstein Integer

- **Eisenstein integer** $Z[w] = \{a + bw : a, b \in Z\}$ $w = \left(-1 + \sqrt{-3}\right)/2$
- Z[w] forms a PID.
- Lattice partitions over Z[w] enrich the candidates of finite fields.
- It has six Eisenstein units.
- The Voronoi region of Z[w] lattice is a regular hexagon (better shaping region).
- It has efficient division algorithms, essential for practical encoder/decoder.
- Optimum lattice/packing in 2-D.



LNC Based on Eisenstein Integer

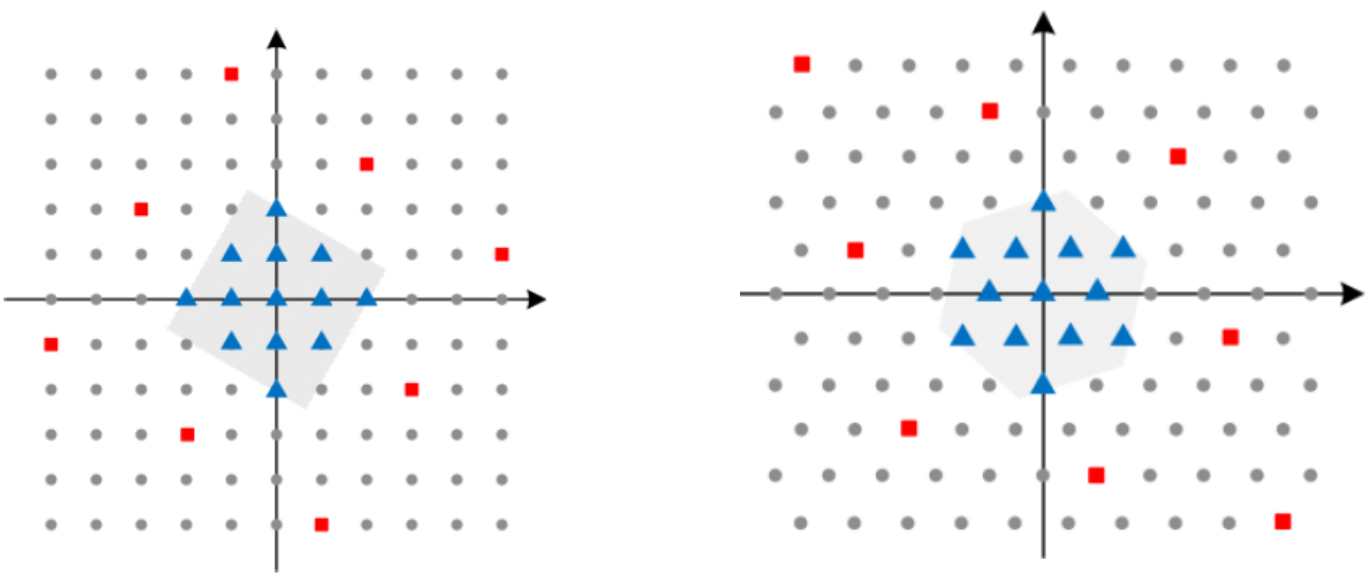
Example.

Consider a lattice Z[w] and its sublattice *r*Z[w], where *r*=4+3w (Eisenstein integer).

A finite field F_{13} is isomorphic to **Z[w]/*r*Z[w]**.

The message space W=**(Z[w]/*r*Z[w])**^{k}

The shaping is a rotated **product of *n* regular hexagons** in C^n .



(a) $\mathbb{Z}[i]$ (b) $\mathbb{Z}[\omega]$

LNC Based on Eisenstein Integer

Quantizer of a complex value x to an Eisenstein Integer

$$D_\Lambda(x) = \arg\min\left\{\left|x-\beta_i\right|^2\right\}$$

$$\beta_1 = \lfloor \mathrm{Re}\{x\} \rceil + \sqrt{-3}\lfloor \mathrm{Im}\{x\}/\sqrt{3} \rceil$$

$$\beta_2 = \lfloor \mathrm{Re}\{x-w\} \rceil + \sqrt{-3}\lfloor \mathrm{Im}\{x-w\}/\sqrt{3} \rceil + w$$

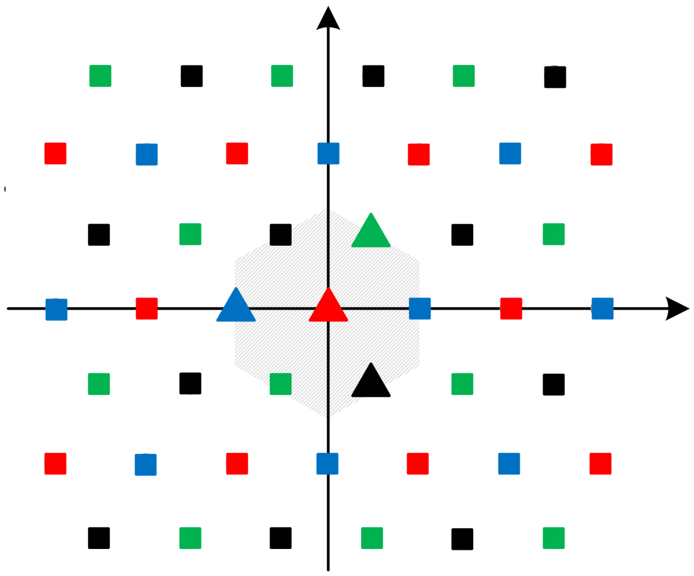
For lattice partition Z[w]/*r*Z[w], the encoder ε: W→Λ=Z[w] uses a division algorithm.

Example.

Consider the lattice Z[w] and its sublattice *r*Z[w].

When *r*=2, F_4 is isomorphic to Z[w]/2Z[w].

W={0+*r*Z[w], 1+*r*Z[w], w+*r*Z[w], 1+w+*r*Z[w]}.



One possible encoder:

ε(W)={0, -1, -w, 1+w}

LNC Based on Eisenstein Integer

Theorem: Union bound Estimation (UBE) of the error probability

$$P_e(\mathbf{h}, \mathbf{a}) \approx K(\Lambda / \Lambda')\exp\left(-\frac{d^2(\Lambda / \Lambda')}{4N_0 Q(\alpha, \mathbf{a})}\right)$$

where

$$Q(\alpha, \mathbf{a}) = |\alpha|^2 + SNR\|\alpha\mathbf{h} - \mathbf{a}\|^2$$

The minimum **inter-coset distance** of Λ/Λ': *d*(Λ/Λ').

It is also called the length of the shortest vectors in the set difference Λ\Λ'

The **number of shortest vectors**: *K*(Λ/Λ')

The kissing number.

LNC Based on Eisenstein Integer

Corollary: Union bound Estimation (UBE) of the error probability

$$P_e(\mathbf{h}, \mathbf{a}) \approx K(\Lambda / \Lambda') \exp\left(-\frac{d^2(\Lambda / \Lambda')}{4N_0 Q(\alpha, \mathbf{a})} \right)$$

$$= K(\Lambda / \Lambda') \exp\left(-\frac{\gamma_c(\Lambda / \Lambda')\gamma_s(\Lambda / \Lambda') 3\mathrm{SENR}_{\mathrm{norm}}}{2} \right)$$

The normalized signal-to-effective-noise ratio

$$\mathrm{SENR}_{\mathrm{norm}} = \frac{\mathrm{SENR}}{2^R} = \frac{\mathrm{SNR}}{2^R Q(\alpha, \mathbf{a})}$$

The nominal coding gain:

$$\gamma_c(\Lambda / \Lambda') = \frac{d^2(\Lambda / \Lambda')}{V(\Lambda)^{1/n}}$$

Measures the increase in density of Λ over the baseline uncoded hypercube lattice.

LNC Based on Eisenstein Integer

Corollary: Union bound Estimation (UBE) of the error probability

$$P_e(\mathbf{h}, \mathbf{a}) \approx K(\Lambda/\Lambda')\exp\left(-\frac{d^2(\Lambda/\Lambda')}{4N_0 Q(\alpha,\mathbf{a})}\right)$$

$$= K(\Lambda/\Lambda')\exp\left(-\frac{\gamma_c(\Lambda/\Lambda')\gamma_s(\Lambda/\Lambda')3\mathrm{SENR}_{\mathrm{norm}}}{2}\right)$$

Second Moment (average energy per dimension of a uniform PDF):

$$P(\Lambda) = \int_V \frac{\|x\|^2}{n} p(x)dx = \int_V \frac{\|x\|^2}{nV(\Lambda)} dx$$

Normalized Second Moment

(dimensionless, invariant to scaling, orthogonal transformation and Cartesian products):

$$G(\Lambda) = \frac{P(\Lambda)}{V(\Lambda)^{1/n}}$$

The shaping gain:

$$\gamma_s(\Lambda/\Lambda') = \frac{G(\text{hypercube})}{G(\Lambda)} = \frac{1/6}{G(\Lambda)} = \frac{V(\Lambda)^{1/n}}{6P(\Lambda)}$$

Measures how much less is the average energy of Λ relative to a hypercube.

LNC Based on Eisenstein Integer

Consider LNC based on Eisenstein integer β and lattice partition Z[w]/βZ[w]

The **baseline system** has a nominal coding gain

$$\gamma_c(\Lambda/\Lambda') = 2\sqrt{3}/3 = 0.625\ \mathrm{dB}$$

The shaping gain

$$\gamma_s(\Lambda/\Lambda') = 3\sqrt{3}/5 = 0.167\ \mathrm{dB}$$

Corollary:

For an LNC by complex construction A over Z[w]/πZ[w], where π is an Eisenstein prime, the **nominal coding gain** based

$$\gamma_c(\Lambda/\Lambda') = \frac{2\sqrt{3}}{3} \frac{w_E^{\min}(C)}{|\pi|^{2(1-k/n)}}$$

Union bound Estimation (UBE) of the error probability

$$P_e(\mathbf{h},\mathbf{a}) \approx K(\Lambda/\Lambda') \exp\left(-\frac{9}{5} \frac{w_E^{\min}(C)\mathrm{SENR}_{\mathrm{norm}}}{|\pi|^{2(1-k/n)}} \right)$$

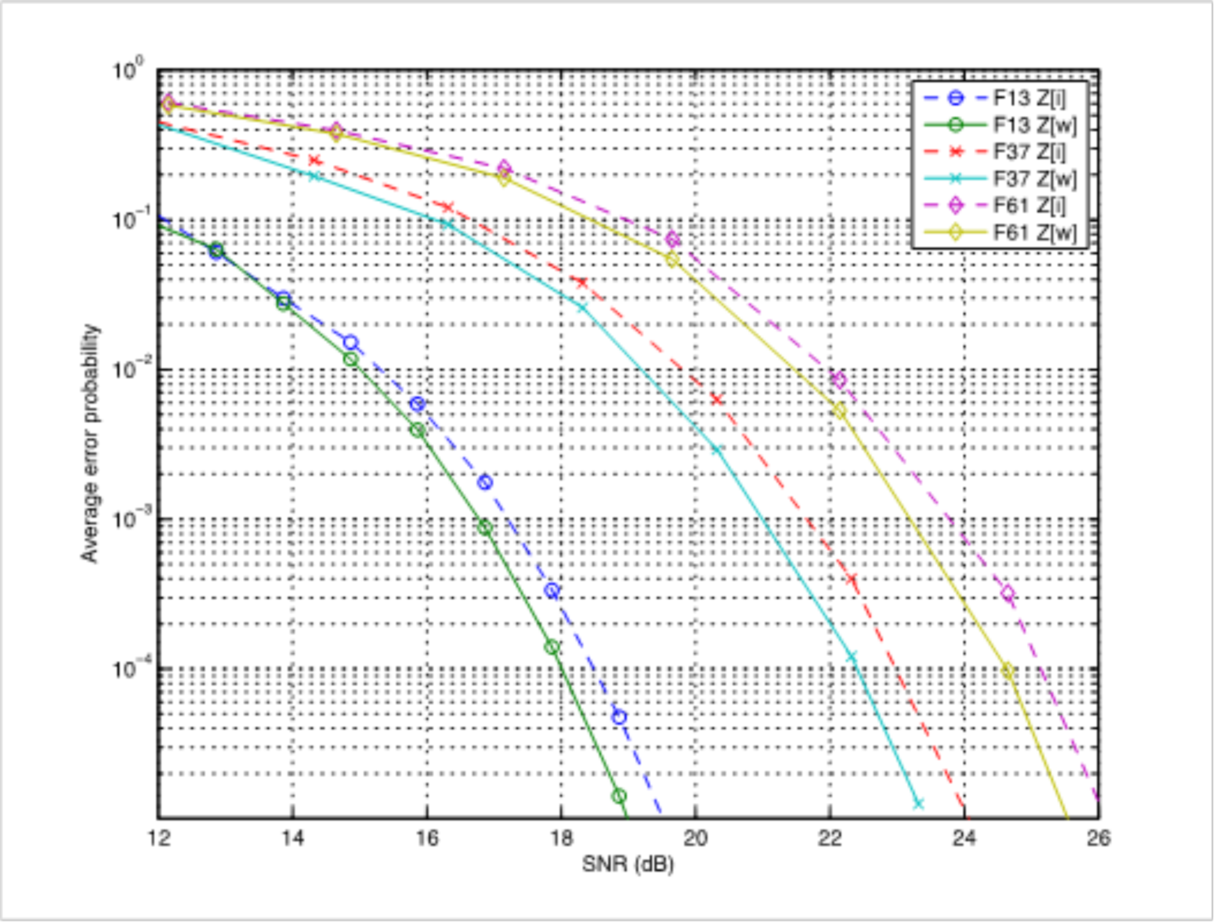
LNC Based on Eisenstein Integer

Compare two LNC baseline systems' performance

Two transmitter and a single relay.

Eisenstein prime *r* and lattice partition Z[w]/*r*Z[w]

Gaussian prime β and lattice partition Z[i]/βZ[i]



LNC Based on Eisenstein Integer

Design Examples (maximize the coding gain)

Convolutional codes with rate ½ over lattice partition Z[i]/βZ[i], β=2+3i

ν	g(D)	γ_c	w_{min}	K
1	$[1+2D,\ 2+(1+i)D]$	2.22 (3.36 dB)	8	4
2	$[1+D+2iD^2,\ (-1-i)+(-1+i)D+(-1-i)D^2]$	3.33 (5.22 dB)	12	4

Convolutional codes with rate ½ over lattice partition Z[w]/rZ[w], r=4+3w

ν	g(D)	γ_c	w_{min}	K
1	$[1+D,\ (-1+w)+(2+w)D]$	2.56 (4.09 dB)	8	12
2	$[1+D+(-1+w)D^2,\ (-1+w)+(1-w)D+(1+w)D^2]$	3.84 (5.85 dB)	12	24

(a) $\mathbb{Z}[i]$ (b) $\mathbb{Z}[\omega]$

Summary

- Reviewed physical-layer network coding and compute-and-forward
- Investigated the lattice network coding based on Eisenstein integer
- Quantizer/encoding algorithms
- Derived Union bound estimation in a unified way
- A few code examples
- LNC based on Eisenstein integer has a high nominal coding and shaping gain.

Open problems:

- Lattice-reduction algorithms to find optimal combination coefficients
- Design more power codes
- Other Lattice Constructions (Construction D algorithm)

Acknowledgement

Qifu Tyler Sun, CUHK

Kenneth W. Shum, CUHK

INC

Thank You!