Lattice-Partition-Based Physical-Layer Network Coding over GF(4)

Jinhong Yuan

School of Electrical Engineering and Telecommunication
The University of New South Wales, Sydney, Australia

June 26, 2013

Outline

Physical-layer Network Coding (PNC)

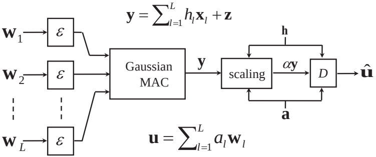
- PNC for two-way relay channel (TWRC):
  - Enhance the throughput of a binary-input TWRC.[1]
  - Approach the capacity upper bound of a Gaussian TWRC within $\frac{1}{2}$ bits.[2]

- Compute-and-forward (CF) for a Gaussian multiple access relay channel (MARC) [3].
  - Multiple-user/q-ary input/fading.
  - Relay decodes a linear function of the transmitted message.

[1] S. Zhang, S.-C. Liew, and P. P. Lam, "Hot topic: Physical layer network coding," *ACM MobiCom*, pp. 358-365., Los Angeles, CA, Sep., 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.
[3] B. Nazer and M. Gastpar, "Compute-and-forward: harnessing interference through structured codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 10, pp. 6463-6486, Oct., 2011.

Compute-and-Forward (CF)

UNSW THE UNIVERSITY OF NEW SOUTH WALES SYDNEY • AUSTRALIA



- Map the noisy linear $\mathbb{C}-$ combined signal from the channel

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

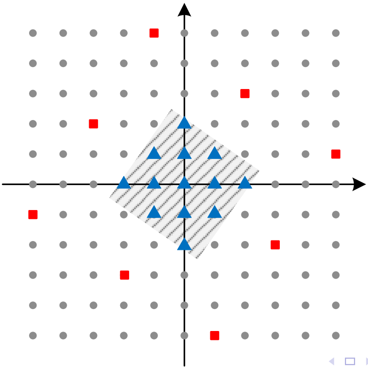
to a linear (integer) function (network coding)

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

- 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 message $\mathbf{u}$ over the finite field.

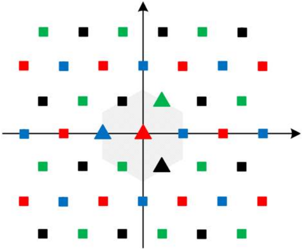
Nested Lattice

- Consider a lattice Λ and a sublattice Λ' of 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 v of the coarse lattice Λ'.



Lattice Partition

- Let R be a discrete subring of $\mathbb{C}$ forming a principle ideal domain *PID* (*e.g.*, integer numbers, Gaussian integers $\mathbb{Z}[i]$).
- Define an **R-lattice** $\Lambda = \{rG_\Lambda : r \in R^n\}$ ($R-$module) and its sublattice of Λ'.
- the set of the cosets of Λ' in Λ, denoted by Λ/Λ', forms an **R-lattice partition** of Λ. The message space $W = \Lambda/\Lambda'$.



Lattice Network Coding (LNC)

- **Encoder:** maps a message $w = \lambda + \Lambda'$ to a coset leader.

$$x_i = \varepsilon(w_i) = \phi(w_i) - D_{\Lambda'}(\phi(w_i))$$

$\Phi : W \rightarrow \Lambda$ embedding each message to a lattice point in the same coset.

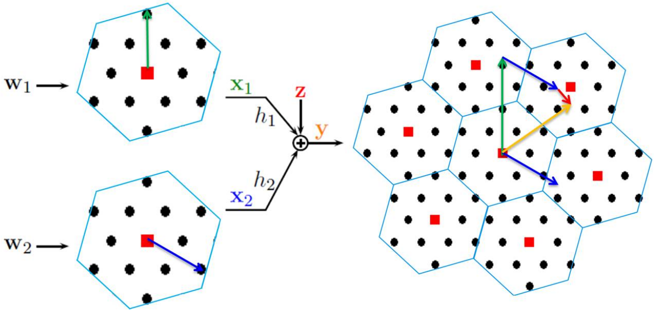
- **Decoder:** estimates an $R-$linear combination from the $\mathbb{C}-$linear signal and maps $R-$linear combination to a coset Λ/Λ' by using **linear labeling**

$$y = \sum_i h_i x_i + z \quad \rightarrow \quad \sum_i a_i w_i = \phi^{-1}(D_\Lambda(\alpha y))$$

$\Phi^{-1} : \Lambda \rightarrow \Lambda/\Lambda'$, taking a lattice point λ in Λ, map to a coset $\lambda + \Lambda'$ of Λ' in Λ.

- R is a subring of $\mathbb{C}$, the linear labeling induces a nature bridge between the $\mathbb{C}-$linear combining and the $R-$linear combining in the message space.

Lattice Network Coding (LNC)

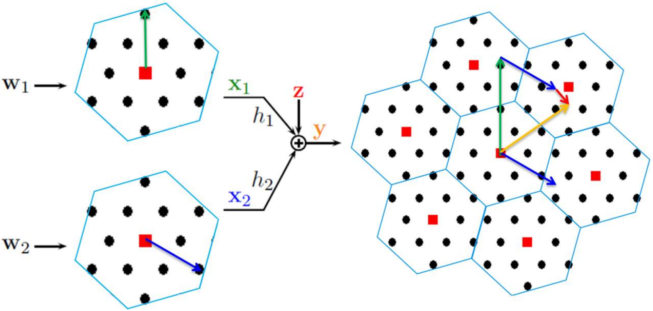


$$\mathrm{h} = [\ 2.1 \quad 1.4\ ]$$
$$\mathrm{a} = [\ 3 \quad 2\ ]$$

Effective Noise: $\mathrm{N} + \mathrm{P}|\mathrm{h} - \mathrm{a}|^2$

From: Nazer/Gastpar

Lattice Network Coding (LNC)

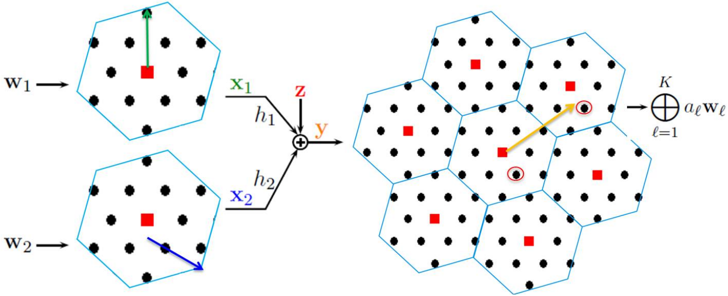


$$\alpha \mathrm{h} = [\ \alpha 2.1 \quad \alpha 1.4\ ]$$
$$\mathrm{a} = [\ 3 \quad 2\ ]$$

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

From: Nazer/Gastpar

Lattice Network Coding (LNC)

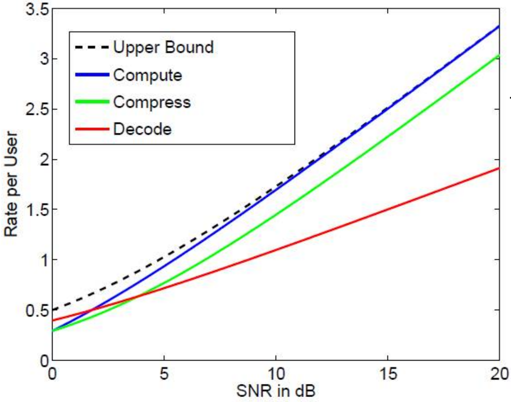


$$\alpha \mathrm{h} = [\ \alpha 2.1 \quad \alpha 1.4\ ]$$
$$\mathrm{a} = [\ 3 \quad 2\ ]$$

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

From: Nazer/Gastpar

Lattice Network Coding (LNC)



The computation rate :

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

LNC Construction From Linear Code

How to construct LNC from linear code?

Complex Construction A

Algorithm 1 : Let π be a prime element in a PID $R \subset \mathbb{C}$. Consider a linear code C of length n over the finite field $R/\pi R$. An LNC Λ/Λ' can be constructed by Complex Construction A via

$$\Lambda = \{\boldsymbol{\lambda} \in R^n : \sigma(\boldsymbol{\lambda}) \in C\},$$

where σ is the natural projection from R^n to $(R/\pi R)^n$, and $\Lambda' = (\pi^r R)^n$, where $r \geq 1$.

LNC Construction From Linear Code

Proposition 1 : Let Λ/Λ' be the LNC constructed by Algorithm 1 over $R/\pi R$. Let $[I_k \;\; B_{k\times(n-k)}]$ be a $k \times n$ matrix over R such that $\sigma([I_k \;\; B_{k\times(n-k)}])$ is a generator matrix for C. The respective generator matrices $\mathbf{M}_\Lambda$ for Λ and $\mathbf{M}_{\Lambda'}$ for Λ' can be described by $\mathbf{M}_\Lambda = \begin{bmatrix} I_k & B_{k\times(n-k)} \\ \mathbf{0} & \pi I_{n-k} \end{bmatrix}$ and $\mathbf{M}_{\Lambda'} = \begin{bmatrix} \pi^r I_k & \pi^r B_{k\times(n-k)} \\ \mathbf{0} & \pi^r I_{n-k} \end{bmatrix}$.

Since $\mathbf{M}_{\Lambda'} = \begin{bmatrix} \pi^r I_k & \mathbf{0} \\ \mathbf{0} & \pi^{r-1} I_{n-k} \end{bmatrix} \mathbf{M}_\Lambda$, we have

$$\Lambda/\Lambda' \cong (R/\pi^r R)^k \oplus (R/\pi^{r-1} R)^{n-k},$$

where $\oplus$ represents the direct sum of two R-modules.

For $R = \mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$,

$$d^2(\Lambda/\Lambda') = \begin{cases} w_E^{min}(C), & \text{when } r = 1 \\ d^2(\Lambda) = \min(|\pi|^2, w_E^{min}(C)), & \text{when } r > 1 \end{cases},$$

$K(\Lambda/\Lambda') = K(\Lambda)$ for $r > 1$, $K(\Lambda)$ is the number of shortest nonzero vectors in Λ.

LNC Construction From Linear Code

Corollary 1 : Let Λ/Λ' be the LNC constructed by Algorithm 1 from a linear code C over $R/\pi R$. When $R = \mathbb{Z}[\omega]$, the nominal coding gain of Λ/Λ' is

$$\gamma_c(\Lambda/\Lambda') = \begin{cases} \frac{w_E^{min}(C)}{\frac{\sqrt{3}}{2}|\pi|^{2(1-k/n)}}, & \text{when } r = 1 \\ \frac{\min(|\pi|^2, w_E^{min}(C))}{\frac{\sqrt{3}}{2}|\pi|^{2(1-k/n)}}, & \text{when } r > 1 \end{cases}$$

The UBE on the decoding error probability can be written as

$$P_e(\mathbf{u} \to \hat{\mathbf{u}} \mid \mathbf{h}, \mathbf{a}) \lessapprox \begin{cases} K(\Lambda/\Lambda') \exp\left(-\frac{9}{5}\frac{w_E^{min}(C)}{|\pi|^{2(1-k/n)}}\mathrm{SENR}_{\mathrm{norm}}\right), & \text{when } r = 1 \\ K(\Lambda) \exp\left(-\frac{9}{5}\frac{\min(|\pi|^2, w_E^{min}(C))}{|\pi|^{2(1-k/n)}}\mathrm{SENR}_{\mathrm{norm}}\right), & \text{when } r > 1 \end{cases}$$

LNC Construction From Linear Code

Example Codes

Rate-1/2 convolutional codes C over $\mathbb{Z}[i]/(2+3i)\mathbb{Z}[i]$ ($\cong \mathbb{F}_{13}$) with maximum $w_E^{min}(C)$, and the corresponding LNCs Λ/Λ' with Λ constructed from C by Algorithm 1 and $\Lambda' = ((2+3i)\mathbb{Z}[i])^n$

v	$\mathbf{g}(D)$	$\gamma_c(\Lambda/\Lambda')$	$w_E^{min}(C)$	$K(\Lambda/\Lambda')$
1	$1+2D$ $2+(1+i)D$	2.22 (3.46dB)	8	4
2	$1+D+(2i)D^2$ $(-1-i)+(-1+i)D+(-1-i)D^2$	3.33 (5.22dB)	12	4
3	$2+(1-i)D+(2i)D^2+(-2)D^3$ $1+(1+i)D+iD^2+iD^3$	4.44 (6.47dB)	16	8
4*	$(-2i)+(-i)D+(2i)D^2+(-1)D^3+(i)D^4$ $(-1)+2D+0D^2+(-1+i)D^3+(1-i)D^4$	4.99 (6.98dB)	18	4
5*	$(-2)+(-i)D^2+(-1)D^3+(1-i)D^4+D^5$ $(-1+i)+(2i)D+(-2)D^3+(-1+i)D^4+(-1-i)D^5$	5.82 (7.65dB)	21	16

∗ not exhaustive search

LNC Construction From Linear Code

Example Codes

Rate-1/2 convolutional codes C over $\mathbb{Z}[\omega]/(4+3\omega)\mathbb{Z}[\omega](\cong \mathbb{F}_{13})$ with maximum $w_E^{min}(C)$, and the corresponding convolutional LNCs Λ/Λ' with Λ constructed from C by Algorithm 1 and $\Lambda' = ((4+3\omega)\mathbb{Z}[\omega])^n$

v	$\mathbf{g}(D)$	$\gamma_c(\Lambda/\Lambda')$	$w_E^{min}(C)$	$K(\Lambda/\Lambda')$
1	$1+D$	2.56 (4.09dB)	8	12
	$(-1+w)+(2+w)D$			
2	$1+D+(-1+w)D^2$	3.85 (5.85dB)	12	24
	$(-1+w)+(1-w)D+(1+w)D^2$			
3	$(2+w)+(1+2w)D+(1+2w)D^2+(-1-2w)D^3$	5.13 (7.10dB)	16	96
	$(-w)+(w)D+(w)D^2+(1+w)D^3$			
4*	$(-1)+(-w)D+(1-w)D^2+(-2-w)D^3+(1-w)D^4$	5.76 (7.61dB)	18	30
	$(2+w)+(1+w)D+(-1-w)D^2+(-1-2w)D^3+D^4$			
5*	$(1+w)+(1+w)D+(-1+w)D^2+(-1-2w)D^3+(-1-2w)D^4+(-w)D^5$	5.76 (7.61dB)	18	6
	$(1+w)+(-1+w)D+(0)D^2+(1+w)D^3+(-2-w)D^4+(1-w)D^5$			

$*$ not exhaustive search

LNC Construction From Linear Code

Complex Construction B

Algorithm 2 : Consider a linear code C of length n over $R/\pi R$ subject to $\sum_{1\leq i\leq n} c_i = 0$ for each $(c_1, \cdots, c_n) \in C$. Define

$$\Lambda = \{\boldsymbol{\lambda} \triangleq (\lambda_1, \cdots, \lambda_n) \in R^n : \sigma(\boldsymbol{\lambda}) \in C, \sum_{i=1}^{n} \lambda_i \equiv 0 \mod \pi^2\}$$

where σ is the natural projection from R to $(R/\pi R)^n$, and $\Lambda' = (\pi^r R)^n$, where $r \geq 2$. In this way, Λ is an n-dimensional R-lattice and Λ' is a sublattice of Λ. An LNC Λ/Λ' is thus constructed from C by Complex Construction B.

LNC Construction From Linear Code

Theorem 1 : Let Λ/Λ' be an LNC constructed from an $[n,k]$ linear code C over $R/\pi R$ by Algorithm 2. There exists a generator matrix $\mathbf{M}_\Lambda$ for Λ and $\mathbf{M}_{\Lambda'}$ for Λ' in the form

$$\mathbf{M}_\Lambda = \begin{bmatrix} I_k & & B_{k\times(n-k)} & & & \\ & \pi & -\pi & 0 & \dots & 0 \\ \mathbf{0} & & & \ddots & & \\ & 0 & \dots & 0 & \pi & -\pi \\ & 0 & 0 & \dots & 0 & \pi^2 \end{bmatrix}, \mathbf{M}_{\Lambda'} = \begin{bmatrix} \pi^r I_k & & \pi^r B_{k\times(n-k)} & & & \\ & \pi^r & -\pi^r & 0 & \dots & 0 \\ \mathbf{0} & & & \ddots & & \\ & 0 & \dots & 0 & \pi^r & -\pi^r \\ & 0 & 0 & \dots & 0 & \pi^r \end{bmatrix} \quad (1)$$

Consequently, $\mathbf{M}_{\Lambda'} = \begin{bmatrix} \pi^r I_k & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \pi^{r-1} I_{n-k-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \pi^{r-2} \end{bmatrix} \mathbf{M}_\Lambda$, and hence

$$\Lambda/\Lambda' \cong (R/\pi^r R)^k \oplus (R/\pi^{r-1}R)^{n-k-1} \oplus (R/\pi^{r-2}R).$$

Moreover, in the special case that $R = \mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$,

$$\begin{aligned} d^2(\Lambda/\Lambda') &= d^2(\Lambda) = \min(2|\pi|^2, w_E^{min}(C)) \\ K(\Lambda/\Lambda') &= K(\Lambda), \text{ when } |\pi|^2 \neq 2 \end{aligned}$$

LNC Construction From Linear Code

Corollary 2 : When $R = \mathbb{Z}[\omega]$, the nominal coding gain of the LNC Λ/Λ' constructed from a linear code over $R/\pi R$ by Algorithm 2 is

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

The UBE on the decoding error probability can be written as

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

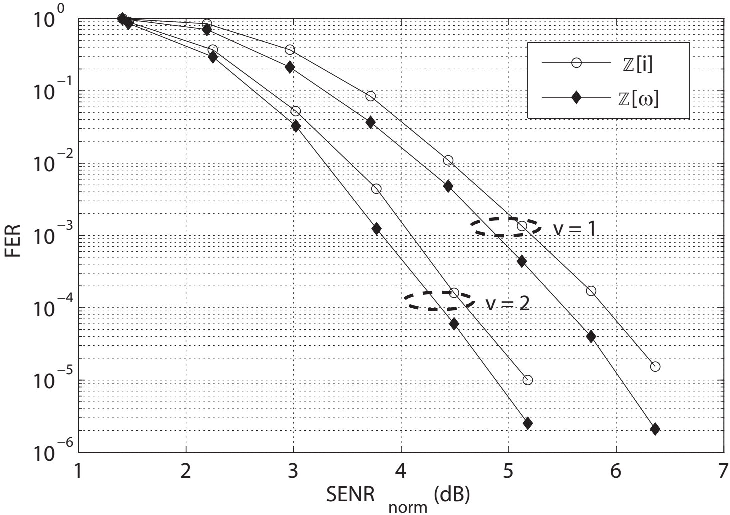
LNC Construction From Linear Code

Example Codes

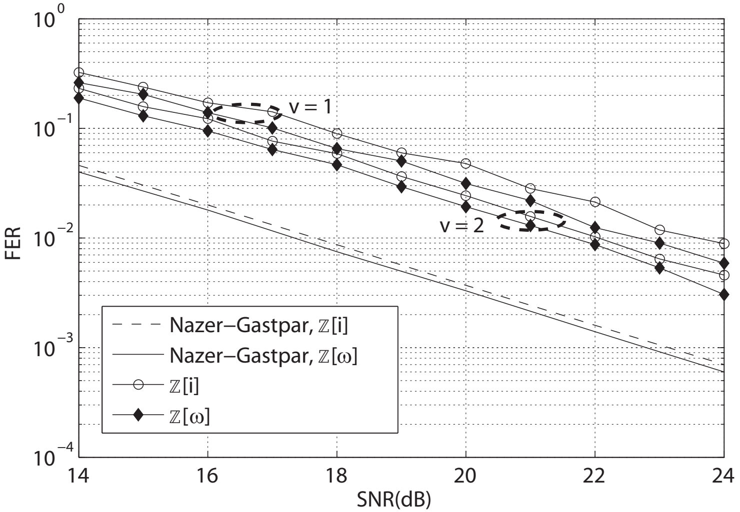
Parameters in various LNCs Λ/Λ' constructed from $[12, 6, 6]$ ternary Golay code over $\mathbb{F}_3 \cong \mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ by different methods. $\pi = 1 + 2\omega$

Λ	By Complex Construction A (Algorithm 1)		By Complex Construction B (Algorithm 2)	Complex Leech Lattice
$\Lambda' =$	$(\mathbb{Z}[w]/\pi\mathbb{Z}[w])^{12}$	$(\mathbb{Z}[w]/\pi^2\mathbb{Z}[w])^{12}$	$(\mathbb{Z}[w]/\pi^2\mathbb{Z}[w])^{12}$	$(\mathbb{Z}[w]/\pi^3\mathbb{Z}[w])^{12}$
$\rho =$	$\frac{1}{2}\log_2 3$	$\frac{3}{2}\log_2 3$	$\frac{17}{12}\log_2 3$	$\frac{3}{2}\log_2 3$
$d^2(\Lambda/\Lambda') =$	6	3	6	3
$\gamma_c(\Lambda/\Lambda') =$	4 (6.02 dB)	2 (3.01 dB)	3.65 (5.62 dB)	4 (6.02 dB)

Simulation Results



Simulation Results



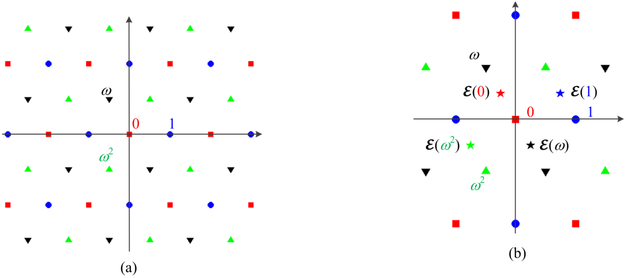
LNC over GF(4)

Motivation

- In practical implementation of communication systems, signal constellations size is always power of 2.
- Lattice partition $R/\pi R$ that is isomorphic to a finite field of size 2^m
- The only finite fields of characteristic 2 that can be represented by $R/\pi R$ are
  - $\mathrm{GF}(2) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$;
  - $\mathrm{GF}(4) \cong \mathbb{Z}[\omega]/2\mathbb{Z}[\omega]$.

LNC over GF(4): Signal Constellation

- In information theory, random dither is required to make the quantization noise to be uniformly distributed and independent of encoded signals.
- For practical systems, a fixed dither is required to minimize the average transmission power.



Proposition 3 : The optimum average power for the baseline LNC is $\frac{1}{2}|\gamma|^2$, which can be obtained by six possible dither vectors $\mathbf{d} = \gamma(d_1, d_2, d_3, \ldots, d_n)$, where $d_j = \{\pm\frac{\omega}{2}, \pm\frac{\omega^2}{2}, \pm\frac{1}{2}\}$.

LNC over GF(4): Code Construction

Let C be an $[n, k]$ linear code over GF(4). Rate-$\frac{2k}{n}$ LNC Λ/Λ' can be constructed from the linear code C by Complex Construction A:

$$\Lambda = \{\boldsymbol{\lambda} \in \gamma\mathbb{Z}[\omega]^n : \sigma(\gamma^{-1}\boldsymbol{\lambda}) \in C\}, \Lambda' = \gamma(2\mathbb{Z}[\omega])^n$$

$$\Lambda/\Lambda' \cong (\mathbb{Z}[\omega]/2\mathbb{Z}[\omega])^k \cong C.$$

- γ: scaling factor to control the transmission power.
- σ: natural projection from $\mathbb{Z}[\omega]^n$ onto $(\mathbb{Z}[\omega]/2\mathbb{Z}[\omega])^n$

Proposition 4 : For the LNC constructed above, we have

$$d^2(\Lambda/\Lambda') = |\gamma|^2 w_H(C) \text{ and } K(\Lambda/\Lambda') = 2^{w_H(C)} K(C),$$

where $w_H(C)$ is the minimum Hamming distance of C and $K(C)$ is the number of codewords with this weight.

LNC over GF(4): Design Example

Parameters of rate-1/2 convolutional codes over GF(4)

v	$g(D)$	$w_H(C)$	$\gamma_c(\Lambda/\Lambda')$
1	$[1\ 1]$, $[\omega\ 1]$	4	3.63 dB
2	$[1\ 1\ 1]$, $[1\ \omega\ 1]$	6	5.40 dB
3	$[1\ \omega^2\ \omega\ \omega^2]$, $[\omega\ \omega^2\ \omega^2\ \omega^2]$	8	6.65 dB
4	$[\omega\ \omega^2\ \omega^2\ \omega\ \omega^2]$, $[\omega^2\ 0\ 1\ \omega^2\ \omega^2]$	9	7.16 dB
5	$[\omega\ 0\ 1\ \omega^2\ \omega^2\ 1]$, $[\omega\ \omega^2\ \omega^2\ \omega^2\ \omega\ 1]$	11	8.03 dB

Parameters of BCH codes over GF(4)

n	k	$g(X)$	$w_H(C)$	$\gamma_c(\Lambda/\Lambda')$	$K(C)$
15	9	$[1\ \omega^2\ 1\ 1\ \omega\ \omega\ 1]$	5	5.21 dB	189
	7	$[1\ 0\ 1\ \omega^2\ \omega^2\ 1\ \omega^2\ 0\ \omega]$	7	5.86 dB	405
63	54	$[1\ 0\ \omega^2\ 1\ 0\ 1\ 1\ \omega^2\ \omega\ 1]$	5	6.76 dB	8505
	50	$[1\ \omega\ \omega\ 1\ \omega\ \omega^2\ 0\ \ \omega^2\ \omega^2\ \omega^2\ 0\ 1\ 0\ \omega^2]$	7	7.83 dB	3591

LNC over GF(4^m)

An $[n, k]$ linear code C over GF(4^m) can then be expanded to an $[mn, mk]$ code C_e over GF(4) in terms of the basis $\{1, \beta, \cdots, \beta^{m-1}\}$ by $C_\mathrm{e} = \{\phi(\mathbf{c}) : \mathbf{c} \in C\}$.

- β: a primitive element of GF(4^m).
- $\{1, \beta, \cdots, \beta^{m-1}\}$: a natural basis of GF($4^m$) over the subfield GF(4).
- Natural mapping from GF(4^m) onto the m-dimensional vector space $\mathrm{GF}(4)^m$ via
$$\phi(\sum_{j=0}^{m-1} c_j \beta^j) = (c_0, \cdots, c_{m-1}).$$

Proposition 5: An mn-dimensional, rate-$\frac{2k}{n}$ LNC can be constructed from C

$$\begin{aligned} \Lambda &= \{\boldsymbol{\lambda} \in \gamma\mathbb{Z}[\omega]^{mn} : \sigma(\gamma^{-1}\boldsymbol{\lambda}) = \phi(\mathbf{c}) \text{ for some } \mathbf{c} \in C\} \\ \Lambda' &= \gamma(2\mathbb{Z}[\omega])^{mn} \end{aligned}$$

- $\Lambda/\Lambda' \cong \mathrm{GF}(4)^{mk} \cong \phi(C)$
- $|\gamma|^2 w_H(C) \leq d^2(\Lambda/\Lambda') = |\gamma|^2 w_H(C_\mathrm{e}) < |\gamma|^2 m w_H(C)$
- $K(\Lambda/\Lambda') = 2^{w_H(C_\mathrm{e})} K(C_\mathrm{e})$

LNC over GF(4^m)

UNSW
THE UNIVERSITY OF NEW SOUTH WALES
SYDNEY • AUSTRALIA

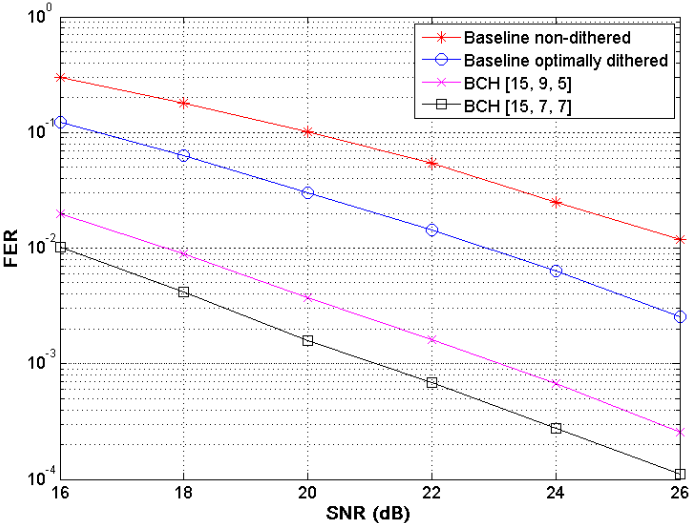
Proposition 6: Consider an LNC Λ/Λ' constructed from a $[4^m - 1, 4^m - d_{RS}]$ narrow-sense RS code over GF(4^m). When $d_{RS} \geq \frac{4^m-1}{3}$, the LNC has rate larger than 4/3, and

$$d^2(\Lambda/\Lambda') \leq \min\left\{\frac{4^m-1}{3}|\gamma|^2, m d_{RS}|\gamma|^2\right\}$$

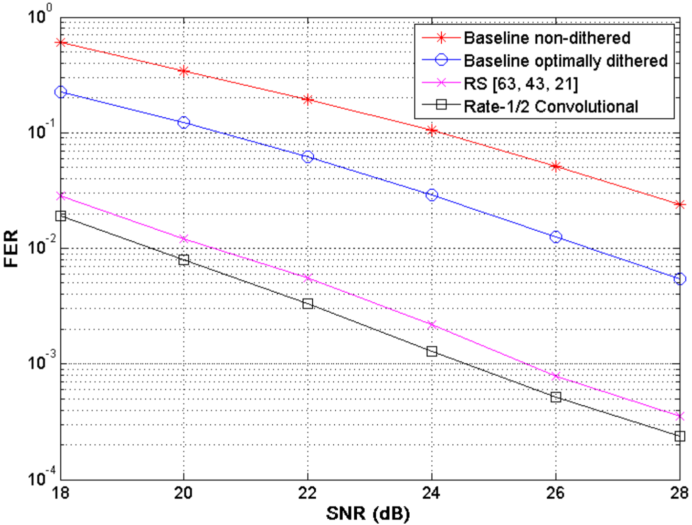
In particular, when $d_{RS} = \frac{4^m-1}{3}$,

$$d^2(\Lambda/\Lambda') = |\gamma|^2 d_{RS}, K(\Lambda/\Lambda') \leq 2^{d_{RS}} \cdot 3m \binom{4^m-1}{d_{RS}}.$$

LNC over GF(4^m): Numerical Results

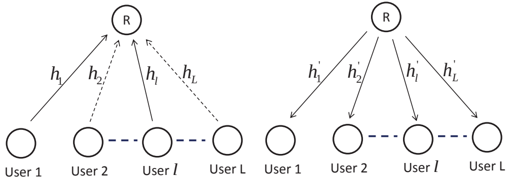


LNC over GF(4^m): Numerical Results



Multi-Way Relay Channel (MWRC)

- System model for both multiple access (MAC) phase and broad-cast (BC) phase.



(a) Multiple access phase (b) Broadcast phase

- L users exchange information via a simple relay.
- No direct link among users.
- Channel remains unchanged during the MAC and BC phases.
- Assume relay knows the Channel State Information (CSI) of all users.

Multi-Way Relay Channel (MWRC)

- MAC phase
  - Two users transmit simultaneously at one time (pair-wise transmission).
  - Relay receives superimposed signal from each pair of users.
  - Relay computes the corresponding network coded messages after each reception.
  - In total $(L-1)$ uplink transmission.
- BC phase
  - Relay broadcasts network coded messages to the users.
  - In total $(L-1)$ downlink transmission.
  - Users need all $(L-1)$ downlink packets to decode all other users's message.

Successive Pair-Wise Transmission

- In a sequential order.
- At $i-$th time slot:

$$y_{(i,i+1)} = h_i x_i + h_{i+1} x_{i+1} + n$$

$$W_{(i,i+1)} = a_i w_i + a_{i+1} w_{i+1}$$

- Total $(L-1)$ uplink transmission.
- In BC phase, each user can retrieve all other user's message after receive all the network coded message from the relay.

Successive Pair-Wise Transmission

- Pair-wise transmission scheduling matrix with size $(L-1) \times L$.

$$\mathbb{S} = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{bmatrix}$$

  - $\mathbb{S}$ has rank of $(L-1)$.
  - $s_{i,j}$: flag for whether user j is activated in time slot i.
  - $s_{i,j} = 1$: active; $s_{i,j} = 0$: silent.
- Transmission rate for each user:

$$R_l < \begin{cases} R^C_{1,2} & \text{if } l = 1 \\ \min\{R^C_{l-1,l}, R^C_{l,l+1}\} & \text{if } l = 2, \cdots, (L-1) \\ R^C_{L-1,L} & \text{if } l = L \end{cases}$$

- Sum-rate for uplink:

$$R_{\mathrm{sum}} = \sum_{l=1}^{L} R_l.$$

Opportunistic Pair-Wise Transmission

- Successive pair-wise transmission is simple, but does not consider the effect of time-varying fading channel.
- Key for the opportunistic pair-wise transmission: At each time slot, a pair of users with the maximum computation rate is selected for transmission.
- For each user to recover all other users' message in broadcasted phase, the scheduled user-pair in these $(L-1)$ time slots should be linearly independent.
- Transmission rate for user l:

$$R_l < \min\{R^C_{j_1,l}, R^C_{j_2,l}, \cdots, R^C_{l,k_1}, R^C_{l,k_2}, \cdots\}$$

  where $1 \le j_1, j_2, \cdots \le l-1$, and $l+1 \le k_1, k_2, \cdots \le L$.
- Sum-rate

$$R_{\mathrm{sum}} = \sum_{l=1}^{L} R_l.$$

Numerical Results

User transmission sum-rate

- Consider 3-user and 4-user MWRCs.

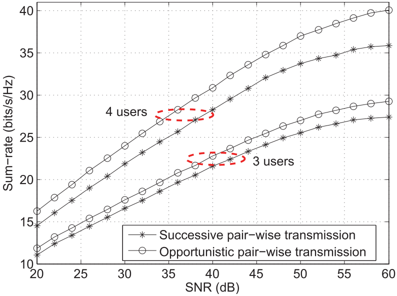


Figure: $\mathbb{Z}[w]$-based LNC.

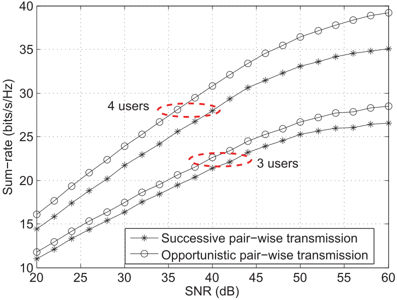


Figure: $\mathbb{Z}[i]$-based LNC.

- At $\rho = 30dB$:
  - 1.25bits/s/Hz improvement for 3-user MWRCs.
  - 2bits/s/Hz improvement for 4-user MWRCs.

Numerical Results

Uncoded system

- SER performance for uncoded $\mathbb{Z}[i]$-based LNC.

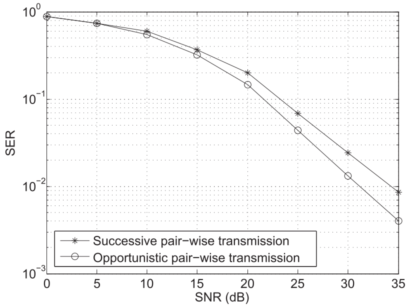


Figure: 3-user MWRC.

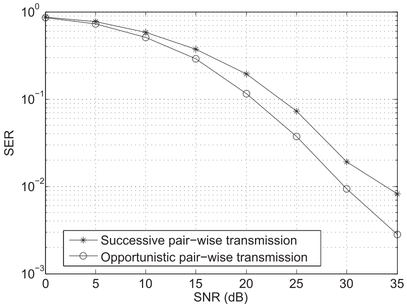


Figure: 4-user MWRC.

- At 10^{-2} SER level:
  - $3dB$ gain for a 3-user MWRC.
  - $4.5dB$ gain for a 4-user MWRC.

Numerical Results

Channel coded system

- Optimized memory order 1 convolutional lattice code at rate $\frac{1}{2}$.
- Information sequence length is 99.

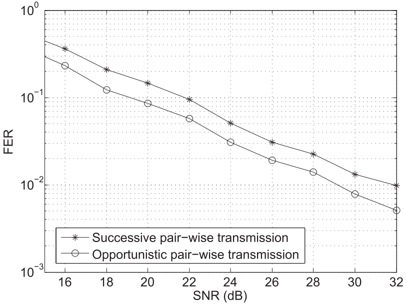


Figure: $\mathbb{Z}[i]$-based 4-user.

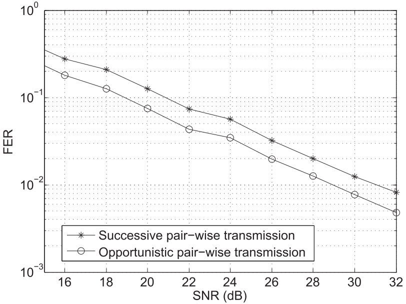


Figure: $\mathbb{Z}[w]$-based 4-user.

- $2.5dB$ gain at 10^{-2} FER level.

Summary

- LNC Construction from linear codes.
- LNC over GF(4)
- Opportunistic Pair-wise Compute-and-Forward

Acknowledgement

Tao Huang, UNSW

Qifu (Tyler) Sun, INC, CUHK

Kenneth W. Shum, INC, CUHK

Thanks!