

Construction and Performance of Network Codes.

J. de Curtó i Díaz.

Bellaterra, 2013.

Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

6 Conclusions

Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

6 Conclusions

Physical-layer Network Coding

Introduction

Today

Interference is treated as a destructive phenomenon.

Network Coding Introduced the Idea

Intermediate nodes in a network are able to perform operations to the input packets rather than just forwarding them.

Network Coding at the Physical-layer? PNC

When multiple electromagnetic waves come together within the same physical space, they add. This additive mixing of electromagnetic waves is a form of Network Coding, performed by nature. PNC aims to exploit this fact.

Physical-layer Network Coding

Main ideas

The Source Transmits a Message

$\mathbf{w}_I \in \mathbb{F}_p^k$, where \mathbb{F}_p is a finite field with p elements $\{0, 1, 2, \dots, p-1\}$ and p is a prime number.

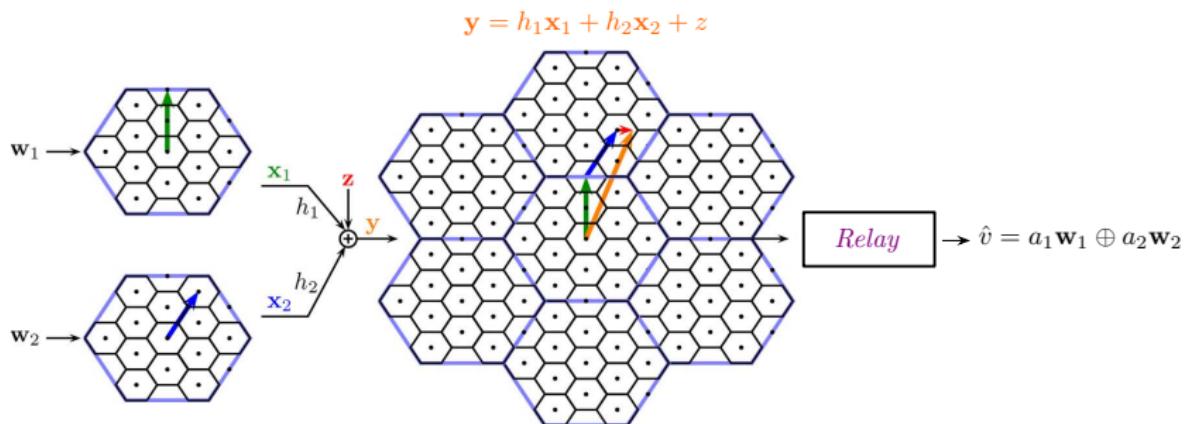
The Relay Decodes a Linear Combination \mathbf{v} of these Messages

$\mathbf{v} = a_1\mathbf{w}_1 \oplus a_2\mathbf{w}_2 \oplus \dots a_L\mathbf{w}_L$, where a_I are coefficients over the finite field \mathbb{F}_p .

The Destination Can Solve For the Original Messages if

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{1L} \\ a_{21} & a_{22} & a_{2L} \\ \vdots & \vdots & \vdots \\ a_{M1} & a_{M2} & a_{ML} \end{bmatrix} \text{ has rank } L.$$

Physical-layer Network Coding Example



Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

6 Conclusions

Lattice Network Codes

Introduction

What Are We Looking For?

If the waveforms at the transmitter are points of a lattice (that is \mathbb{Z} or $\mathbb{Z}[i]$), then every integer combination of these waveforms is itself a point of the same lattice.

The Algebraic Structure Necessary Is

Given a R -lattice Λ (e.g. $\mathbb{Z}[i]$) and a sublattice Λ' of Λ (e.g. $\pi\mathbb{Z}[i]$), the quotient group Λ/Λ' (e.g. $\frac{\mathbb{Z}[i]}{\pi\mathbb{Z}[i]}$) is a R -module. For a Lattice Network Code, the message space is $W = \Lambda/\Lambda'$.

Let's See a Bit More of Insight

The R/aR structure, being R a PID and a prime, forms a field. Thus, we will be able to find an isomorphism between $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ and $\frac{\mathbb{Z}[i]}{\pi\mathbb{Z}[i]}$ if both fields have the same number of elements.

Lattice Network Codes

The Lattice $\mathbb{Z}[i]$

GAUSSIAN Integers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Prime Factorization Used

If $p \equiv 1 \pmod{4}$ then $p = \pi\pi^*$ is a product of two conjugate primes π, π^* .

Example

The prime $p = 5$ satisfies $5 \equiv 1 \pmod{4}$, so 5 has two conjugate GAUSSIAN prime factors.

Since $5 = 1^2 + 2^2$, $5 = (1 + 2i)(1 - 2i)$.

Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

6 Conclusions

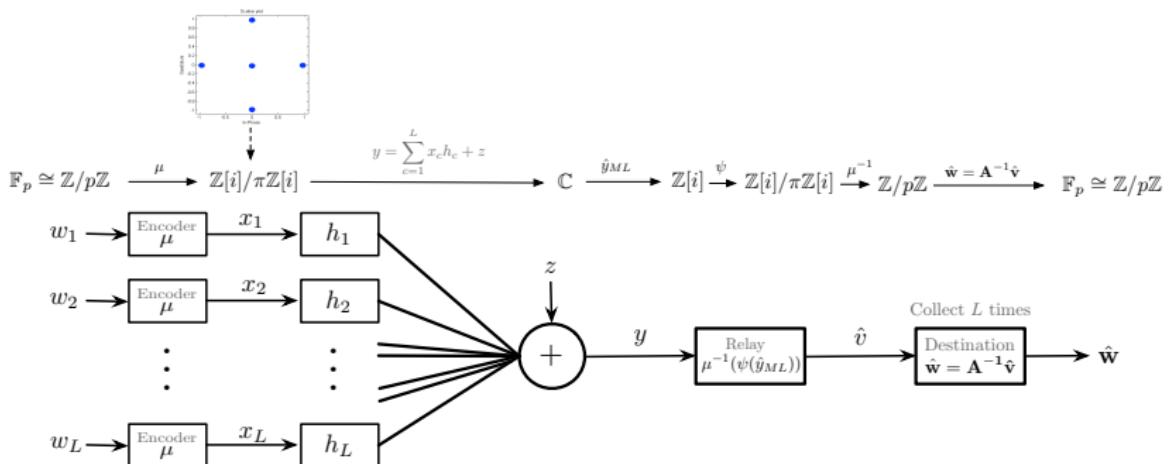
Outline

3 C&F

- C&F System: Scalar Case
- C&F System: Vectorial Case

C&F System: Scalar Case

System Model



$$\mu(w_l) = w_l \bmod \pi = w_l - \left[\frac{w_l \pi^*}{\pi \pi^*} \right] \pi$$

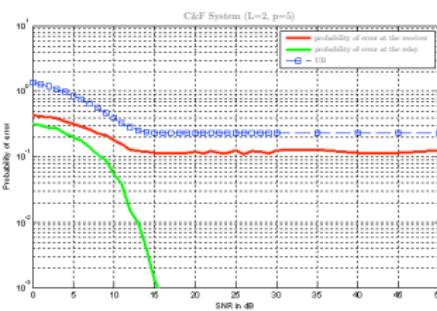
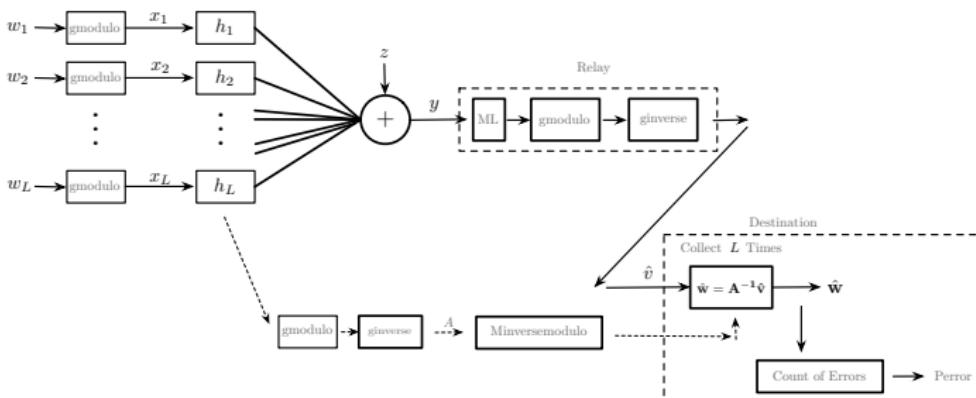
$$\mu^{-1}(z) = z \bmod p = (z^* u \pi + z v \pi^*) \bmod p$$

$$y = h_1 x_1 + h_2 x_2 + \dots + h_L x_L + z$$

$$\hat{v} = a_1 w_1 \oplus a_2 w_2 \oplus \dots \oplus a_L w_L$$

C&F System: Scalar Case

Performance



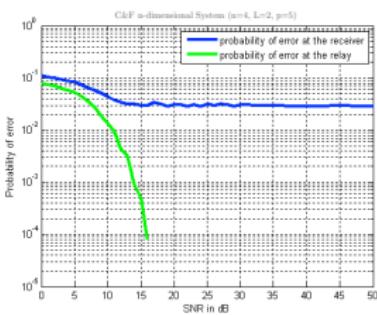
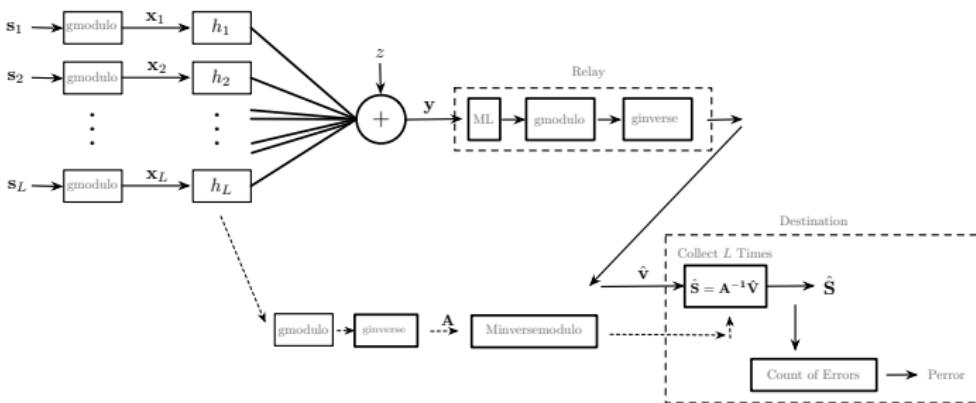
Outline

3 C&F

- C&F System: Scalar Case
- C&F System: Vectorial Case

C&F System: Vectorial Case

Performance



Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

6 Conclusions

HAMMING q -ary Codes

Generating Matrix

$$C = uG : u \in \mathbb{F}_p^k.$$

We say that G is systematic if $G = (I_k | -P^T)$.

Parity Check Matrix

$$C = \{v \in \mathbb{F}_p^n : Hv^T = 0\}.$$

If G is systematic, a parity check matrix is $H = (P|I_{n-k})$.

C&F HAMMING q -ary Coded System

Construction

HAMMING q -ary Code

Given an integer $r \geq 2$, let $n = \frac{q^r - 1}{q - 1}$. The HAMMING q -ary code is a linear $[n, n - r]$ code in \mathbb{F}_q^n , whose parity check matrix H is such that

$$H = (v_1 | v_2 | \dots | v_n)$$

where $v_1, \dots, v_r \in \mathbb{F}_q^r$ is a list of nonzero vectors satisfying the condition that no two vectors are scalar multiples of each other.

Example

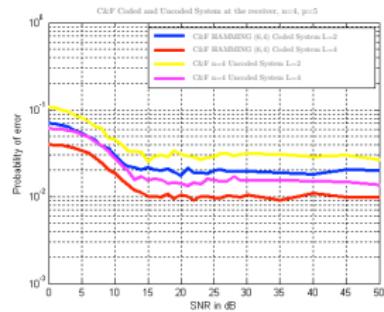
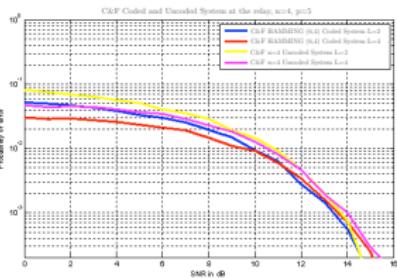
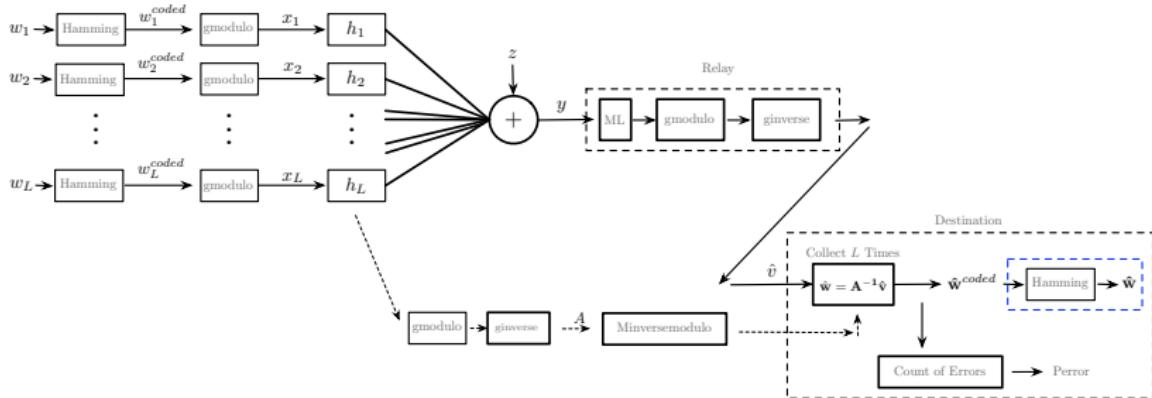
Let \mathbb{F}^5 and $r = 2$, $n = \frac{5^2 - 1}{5 - 1} = 6$. So, $k = n - r = 4$. A straightforward way to generate a systematic HAMMING q -ary code is generating the matrix P as a $r \times k$ matrix with columns

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{bmatrix}.$$

And then generate H and G using $G = (I_k | P^T)$ and $H = (P | I_{n-k})$.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 1 \end{bmatrix} \quad \text{and} \quad G = \begin{bmatrix} 1 & 0 & 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 0 & 4 & 3 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 1 \end{bmatrix}.$$

C&F HAMMING q -ary Coded System Performance



Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

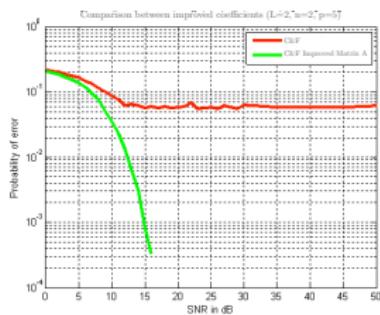
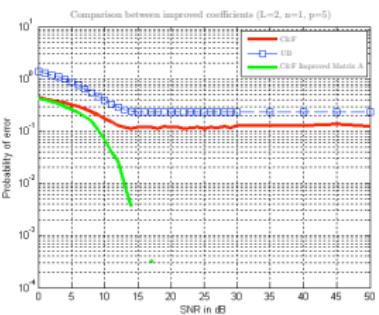
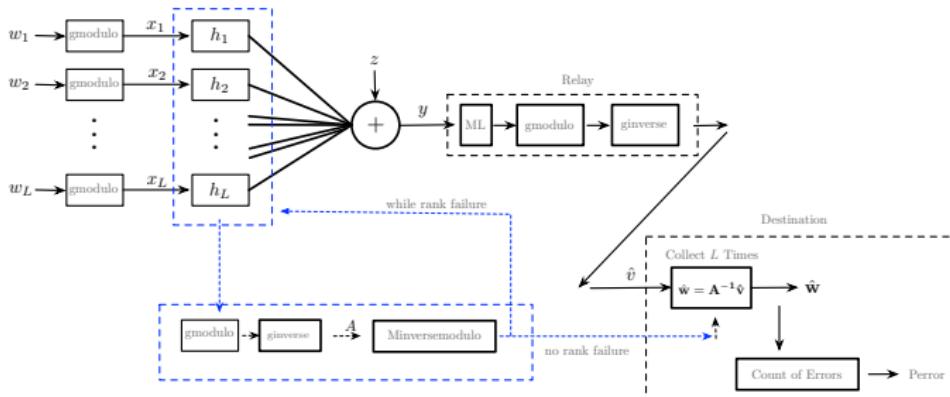
6 Conclusions

Outline

5 Improvement of the Coefficients

- Improvement of the Coefficients: Improved Matrix **A**
- Improvement of the Coefficients: Optimum Matrix **A**
- Improvement of the Coefficients: Improved Optimum Matrix **A**

Improved Matrix A Performance



Outline

5 Improvement of the Coefficients

- Improvement of the Coefficients: Improved Matrix **A**
- Improvement of the Coefficients: Optimum Matrix **A**
- Improvement of the Coefficients: Improved Optimum Matrix **A**

Optimum Matrix A Construction

Scalar Factor

$$\beta_{MMSE} = \frac{\text{SNR} \mathbf{h}^T \mathbf{a}_m}{\text{SNR} \|\mathbf{h}_m\|^2 + 1}.$$

Optimum Coefficients

Theorem: For a given vector of coefficients of the channel

$\mathbf{h}_m = [h_{m1}, h_{m2}, \dots, h_{mL}]^T \in \mathbb{R}^L$, the computation rate is maximized by choosing in network coding the vector of coefficients $\mathbf{a}_m \in \mathbb{Z}^L$ as

$$\mathbf{a}_m = \arg \min_{\mathbf{a}_m \in \mathbb{Z}^L, \mathbf{a}_m \neq 0} (\mathbf{a}_m^T \mathbf{G}_m \mathbf{a}_m)$$

where

$$\mathbf{G}_m = \mathbf{I} - \frac{\text{SNR}}{1 + \text{SNR} \|\mathbf{h}_m\|^2} \mathbf{H}_m.$$

Optimum Matrix A Construction

What's Behind this Minimization?

$$\mathbf{a}_m = \arg \min_{\mathbf{a}_m \in \mathbb{Z}^L, \mathbf{a}_m \neq 0} (\mathbf{a}_m^T G_m \mathbf{a}_m).$$

- CHOLESKY factorization.
- Lattice reduction: LLL algorithm.
- Vector search: SCHNORR EUCHNER method.

Optimum Matrix A

Solving the ILS Problem

ILS Problem

$$\min_{z \in \mathbb{Z}^n} \|y - Bz\|^2$$

this problem is analogous to solving

$$\min_{z \in \mathbb{Z}^n} (y - Bz)^T V^{-1} (y - Bz).$$

One can first compute the CHOLESKY factorization $V = R^T R$, then solve two lower triangular linear systems $R^T \bar{y} = y$ and $R^T \bar{B} = B$.

As our real aim is to solve the SVP problem

$$\min_{z \in \mathbb{Z}^n} (z)^T V^{-1} (z)$$

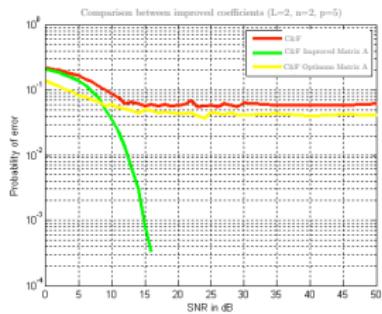
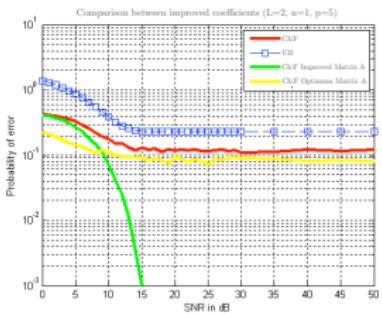
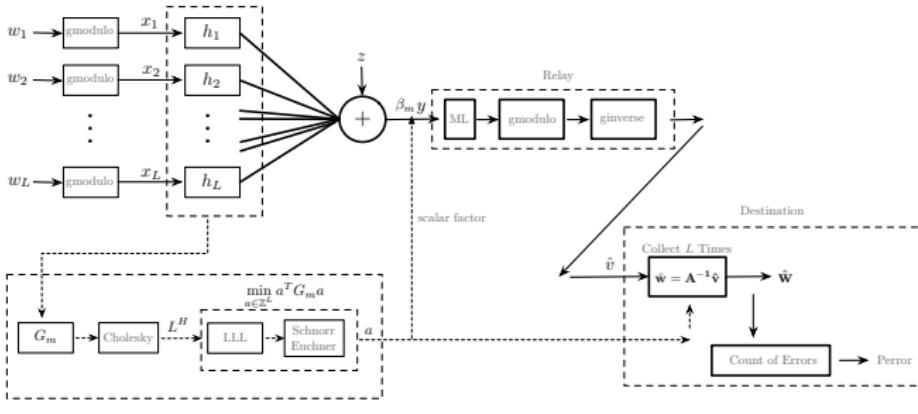
we use $B = -I_n$ and $y = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}_n$ and therefore $\bar{B} = R^T \setminus B$ and $\bar{y} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}_n$.

Finally the problem becomes

$$\min_{z \in \mathbb{Z}^n} \|\bar{y} - \bar{B}z\|^2.$$

Optimum Matrix A

Performance

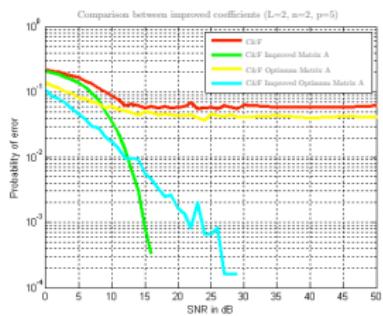
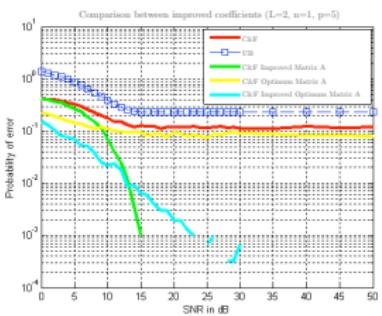
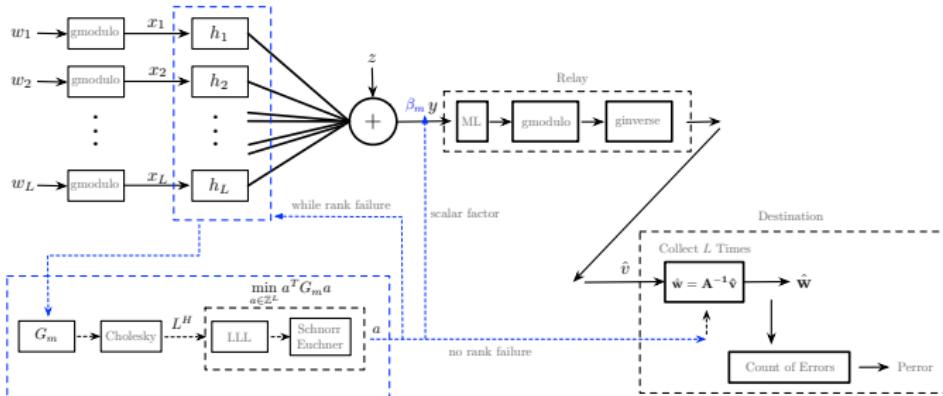


Outline

5 Improvement of the Coefficients

- Improvement of the Coefficients: Improved Matrix **A**
- Improvement of the Coefficients: Optimum Matrix **A**
- Improvement of the Coefficients: Improved Optimum Matrix **A**

Improved Optimum Matrix A Performance



Outline

1 PNC

2 Lattice Network Codes

3 C&F

4 C&F HAMMING

5 Improvement of the Coefficients

6 Conclusions

Conclusions

- Mathematical tools. ✓
- C&F uncoded system model scalar:
 - MATLAB L -dimensional $\forall p$ implementation using a working $L = 2, p = 5$ code base with given ML detector. ✓
- C&F uncoded system model vectorial:
 - MATLAB implementation n -dimensional. ✓
- C&F HAMMING q -ary coded system model:
 - MATLAB implementation C&F HAMMING (6,4) coded system $n = 4$. ✓
- Improvement of the Coefficients:
 - MATLAB implementation improved matrix \mathbf{A} . ✓
 - MATLAB implementation optimum matrix \mathbf{A} . ✓
 - MATLAB implementation improved optimum matrix \mathbf{A} . ✓
- Implementation of sphere decoder for ML detection:
 - Adapting the code used for optimum matrix \mathbf{A} as an efficient sphere decoder. ✓

Conclusions

Obtained Results

- We have explained the lattice theory needed.
- We have provided several MATLAB code implementations for C&F system.
- The results of the improvement of the coefficients show:
 - Improved optimum matrix \mathbf{A} works really well for SNR low.
 - Improved matrix \mathbf{A} has a better slope performance for SNR high.

Thank You

DE CURTÓ I DÍAZ Joaquim.
Thank you.