CRC-Enabled Lattices for Multiuser Communication

Jiajie Xue and Brian M. Kurkoski

Japan Advanced Institute of Science and Technology

February 16, 2023
2023 Information Theory and Applications (ITA) Workshop

Motivation

Cyclic redundancy check (CRC) codes are widely used in communications

- If a CRC code check passes, received data is assumed valid, and is forwarded for further processing
- If check fails, the receiver requests retransmission, or other corrective action

In lattice-based communications:

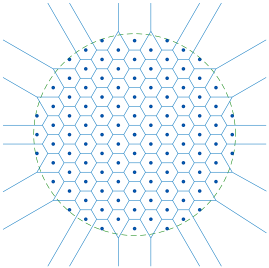
- Decoder has one or more parameters
- If lattice decoding fails, **try decoding again with a different parameter**
- Beneficial if retransmission is more expensive than re-try decoding.

We are particularly interested in the finite-length domain.

Outline

1. Background on lattices for communications
2. Genie-aided decoder for computing a bound on probability of decoder error for point-to-point AWGN channel
3. CRC-enabled lattices for the point-to-point channel
4. CRC-enabled lattices for compute-forward multiple access

Maximum Likelihood Decoding of Lattices

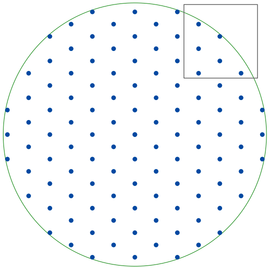


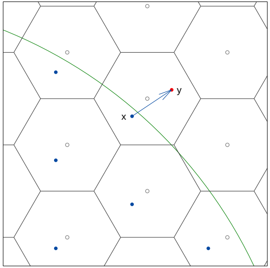
An n-dimensional lattice code is the intersection of a lattice Λ and a shaping region:

- Candidate for high-rate coded modulation. Practical to achieve shaping gain.
- Lattice codes with maximum likelihood decoding achieve the capacity of the AWGN channel [1]
- Unfortunately, Maximum likelihood decoding of lattices is not efficient

[1] Rudiger Urbanke and Bixio Rimoldi, "Lattice codes can achieve capacity on the AWGN channel", IT Trans, 1998

Motivation — Lattice Decoding Achieves Capacity





- Lattice codes with low-complexity lattice decoding can also achieve capacity
- **Lattice decoding** This is possible if scale by α_{MMSE} [2] :

$$\alpha_{MMSE} = \frac{P}{P + \sigma^2}$$

- Intuition: noise moves $\mathbf{y}$ away from the origin, so "expand" the decoding lattice

[2] Uri Erez and Ram Zamir, "Achieving $\frac{1}{2}\log(1+\mathrm{SNR})$ on the AWGN Channel With Lattice Encoding and Decoding," IT Trans, October 2004.

Scaling for Finite-Dimension Lattices

α_{MMSE} is optimal when $n \to \infty$

- How to choose scaling α when n is finite?
- Actually, α_{MMSE} is not a bad choice[3] for $n \geq 100$

What if we could try many different α? Introduce a **genie-aided decoder**

- Genie tells decoder if estimated lattice point is correct or not
- If not, decoder retries decoding using different scaling α
- Genie may be implemented using CRC codes

Goal: quantify how much the decoding can be improved by re-try decoding.

[3] N. S. Ferdinand, M. Nokleby, B. M. Kurkoski, and B. Aazhang, "MMSE scaling enhances performance in practical lattice codes," in Asilomar Conference on Signals, Systems, and Computers, November 2014

Background — Lattices

Definition (Lattices)

Lattices are additive subgroup in real number space. An n-dimension lattice Λ can be formed as:

$$\Lambda = \{\mathbf{G}\mathbf{b} : \mathbf{b} \in \mathbb{Z}^n\}$$

where $\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_n] \in \mathbb{R}^{n \times n}$ and $\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_n \in \mathbb{R}^n$ are linear independent. Voronoi region $\mathcal{V}$ is the set of points closer to $\mathbf{0}$ than any other lattice point, with volume:

$$V(\Lambda) = |\det(\mathbf{G})|$$

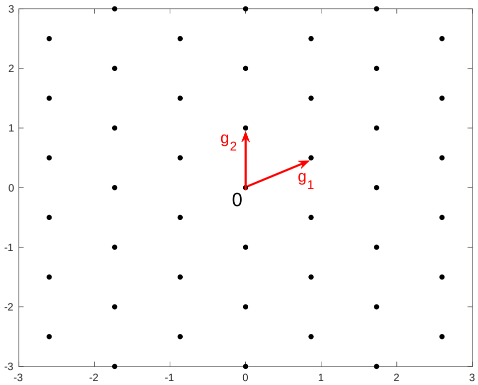


Figure 1: Example of 2-dimensional lattice spanned by $\mathbf{g}_1 = [\frac{\sqrt{3}}{2}, \frac{1}{2}]^T$ and $\mathbf{g}_2 = [0, 1]^T$.

Background — Nested Lattice Codes

Let two lattices Λ_c and Λ_s satisfy $\Lambda_s \subseteq \Lambda_c$ and form a quotient group Λ_c/Λ_s. A nested lattice code $\mathcal{C}$ is defined as:

$$\mathcal{C} = \{\mathbf{x} \bmod \Lambda_s : \mathbf{x} \in \Lambda_c\}$$

have code rate:

$$R = \frac{1}{n} \log \frac{V(\Lambda_s)}{V(\Lambda_c)}.$$

Nested lattice codes:

- Allow lattices to satisfy a power constraint
- Possess certain algebraic properties

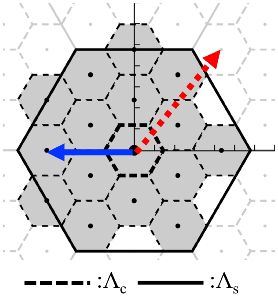
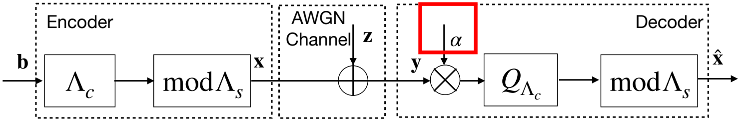


Figure 2: Nested lattice code formed using a coding lattice Λ_c and a shaping lattice Λ_s.

Background—Single-User System

Encoding and decoding scheme is given as:



Let n-dimensional lattice code $\mathcal{C} = \Lambda_c/\Lambda_s$ and $\mathbf{G}$ is generator matrix of Λ_c,

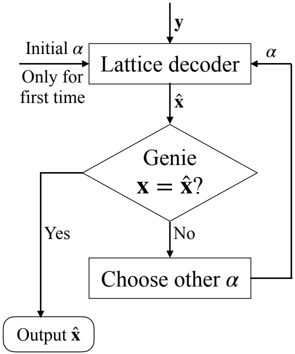
Encoder: $\mathbf{x} = \mathbf{G}\mathbf{b} \bmod \Lambda_s$, with $E[\|\mathbf{x}\|^2] = nP_x$

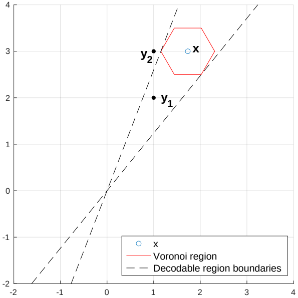
Channel: $\mathbf{y} = \mathbf{x} + \mathbf{z}$, with $\mathbf{z} \sim \mathcal{N}(0, \sigma^2\mathbf{I})$

Decoder: $\hat{\mathbf{x}} = Q_{\Lambda_c}(\alpha\mathbf{y}) \bmod \Lambda_s$, with $\alpha \in \mathbb{R}$

Genie-Aided Decoder

The genie-aided exhaustive search decoder is allowed to use all $\alpha \in \mathbb{R}$





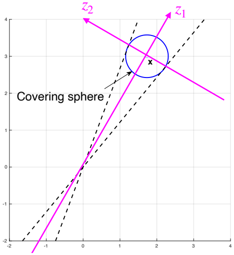
Cone region is the “decodable region”.

There exists some α such that $\mathbf{y}_1$ will be correctly decoded.

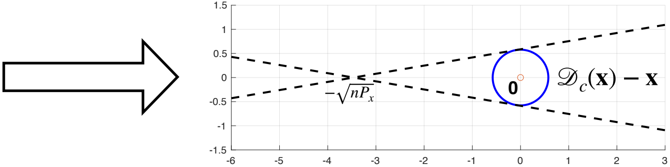
Idea: Bound the probability of decoding error by integrating noise over the cone.

Probability of Decoding Error: Lower Bound and Estimate

(1) Form a lower bound on probability of decoding error using the lattice **covering sphere**. Using this approximation because the Voronoi region is irregular.



※Draw coordinate of $\mathbf{z}$ based on rotationally invariant property.



(2) Form an estimate on the probability of decoder error using the lattice **equivalent sphere**. While not a bound, it is numerically close for some lattices.

Lower Bound on Error Rate

Theorem (1)

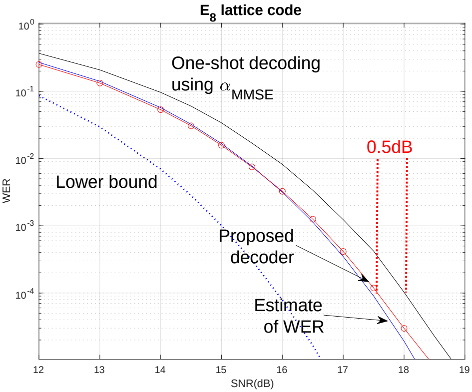
Let non-zero $\mathbf{x}$ be a lattice point of an $n \geq 2$ dimensional lattice Λ having covering radius r_c and per-dimensional power $P_{\mathbf{x}} = \|\mathbf{x}\|^2/n$. With the restriction of $r_c^2 < nP_{\mathbf{x}}$, the probability of word error for the genie-aided decoder on the AWGN channel with noise variance σ^2 is lower bounded by:

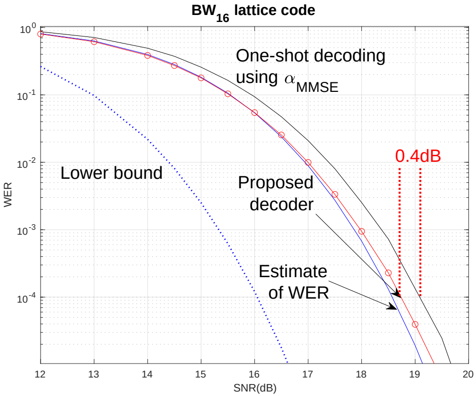
$$P_{e,Dec} > 1 - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{z^2}{2\sigma^2}} (1 - h(z)) dz$$

where[1] $h(z) = e^{-t} \left(\sum_{k=0}^{(n-3)/2} \frac{t^k}{k!} \right)$ for odd n;
$h(z) = erfc(t^{1/2}) + e^{-t} \left(\sum_{k=1}^{(n-2)/2} \frac{t^{k-1/2}}{(k-1/2)!} \right)$ for even n, with $t = f^2(z)/(2\sigma^2)$
and $f(z) = \left| r_c z / \sqrt{nP_{\mathbf{x}} - r_c^2} + \sqrt{nP_{\mathbf{x}} r_c^2/(nP_{\mathbf{x}} - r_c^2)} \right|$.

[1] Tarokh, Vardy and Zeger, "Universal Bound on the Performance of Lattice Codes", IT Transactions, 1999

Numerical Evaluation of Bound for E8 and BW16 Lattices





- Genie-aided decoder gives gain over one-shot decoding
- Estimate of error-rate is quite accurate

Implementation of Genie Using CRC

- The genie may be implemented using a CRC code.
- In a typical communications system, failed CRC is used to request re-transmission.
- In this case, a failed CRC is used to adjust α. Repeating decoding is more efficient than re-transmission.

CRC-Enabled Lattice Code Λ'

Embed a codeword of $\mathcal{C}_b$ in the LSB of the lattice integer $\mathbf{b}$, where $\mathcal{C}_b$ is a block code of length n.

The original lattice Λ is:

$$\Lambda = \{\mathbf{G}\mathbf{b} \mid \mathbf{b} \in \mathbb{Z}^n\}$$

The CRC-enabled structure Λ' is:

$$\Lambda' = \{\mathbf{G}\mathbf{b} \mid \mathbf{b} \in \mathbb{Z}^n, \mathbf{b}_{\mathrm{LSB}} \in \mathcal{C}_b\}$$

$$\begin{array}{cccccc} b_1 & b_2 & b_3 & & b_n & \\ \boxed{1} & \boxed{1} & \boxed{1} & \cdots & \boxed{1} & 2^2 \\ \boxed{0} & \boxed{1} & \boxed{1} & \cdots & \boxed{1} & 2^1 \\ \boxed{1} & \boxed{1} & \boxed{0} & \cdots & \boxed{0} & 2^0 \end{array}$$

codeword of $\mathcal{C}$

Theorem

If $\mathcal{C}_b$ is an (n, k) linear block code then Λ' is a lattice.

We use a CRC as the linear block code $\mathcal{C}_b$.

CRC-Enabled Lattice Code Λ'

Λ' is a lattice with generator matrix:

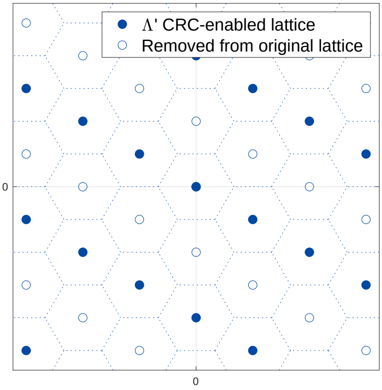
$$\mathbf{G}' = \mathbf{G} \cdot \underbrace{\begin{bmatrix} \mathbf{I}_k & \mathbf{0} \\ \mathbf{P} & 2\mathbf{I}_{n-k} \end{bmatrix}}_{\mathrm{CA}}$$

CA is the Construction A generator matrix for $\mathcal{C}$.

Volume is $V(\Lambda') = 2^{n-k} V(\Lambda)$.

With N bits/codeword on AWGN channel, we must pay:

$$\mathrm{Rate\ penalty} = 10 \log \frac{N}{N-(n-k)} \ \mathrm{dB}$$



Original Λ is A_2 hexagonal lattice.

Using single-parity check code $\mathcal{C}_b$, points are removed to form Λ'.

Polar Code Lattices Using CRC-Enabled Genie

- Dimension $n = 128$ polar code lattice[1].
- $R = 1.74$ with 223 bits per codeword; 4 CRC bits.
- 3 decoding attempts.
- (SC decoding in standard Construction D multilevel decoder)
- 0.1 dB improvement in WER.
  - Includes SNR penalty 0.078 dB due to CRC bits

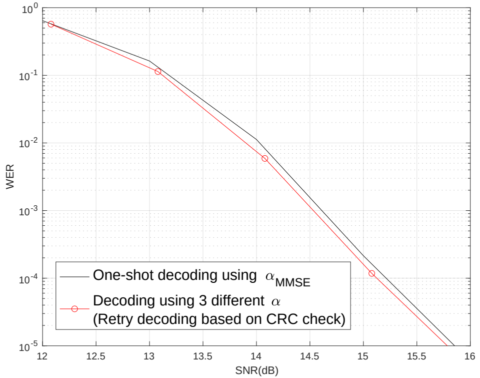


Figure 3: SNR vs WER of 128-dim polar code lattice with one-shot decoding and 3-times decoding.

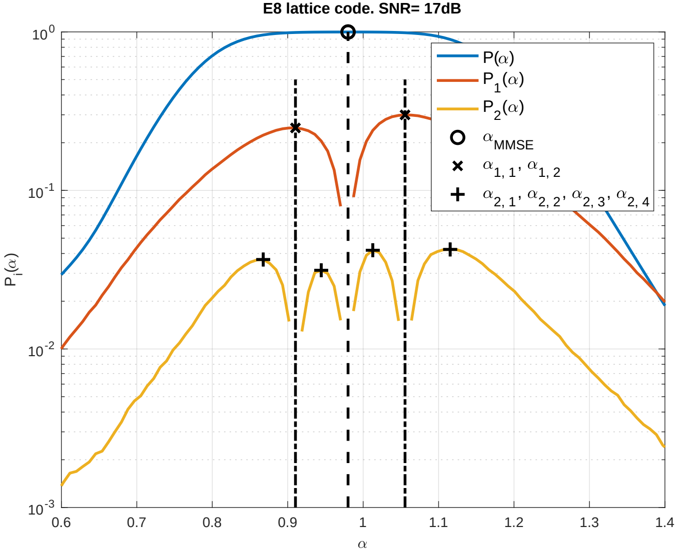
[1] Ludwiniananda, Liu, Anwar, and Kurkoski, "Design of polar code lattices of small dimension," ISIT 2021.

α for Successive Attempts

On the first decoding attempt, choose $\alpha = \alpha_{\text{MMSE}}$.

If we need to re-attempt, which value of α should be used?

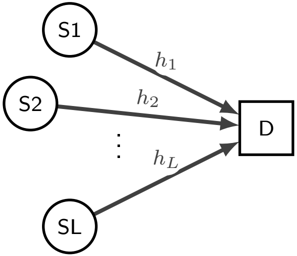
$P_1(\alpha)$ is the probability of correct on second try, given first try failed.
$\Rightarrow$ The local optimums $\alpha_{1,1}, \alpha_{1,2}$ are next candidates.



Multiple-Access Using Compute-Forward Relaying[1]

L transmitters transmit $\mathbf{x}_i \in \mathcal{C}$ over channel with fading coefficient h_i.

One receiver with one linear combination shown; need L independent linear combinations.



$$h_1\mathbf{x}_1 + \cdots h_L\mathbf{x}_L + \mathbf{z} \qquad h \in \mathbb{R}$$

decoder should produce

$$a_1\mathbf{x}_1 + \cdots a_L\mathbf{x}_L \in \Lambda \qquad a_i \in \mathbb{Z}$$

Receiver must determine $a_i \in \mathbb{Z}$. Usual strategy is to maximize computation rate:

$$\mathbf{a} = \arg\max \log^+ \left(||\mathbf{a}||^2 - \frac{P|\mathbf{h}^t\mathbf{a}|^2}{\sigma^2 + P||\mathbf{h}||^2}\right)$$

a_i is considered to be an integer approximation of real h_i.

[1] Nazer and Gastpar, "Compute-and-forward: Harnessing interference through structured codes," IT Trans 2011

Linear Combinations of CRC-Enabled Lattice

For the unconstrained lattice, the linear combinations preserve the CRC:

Theorem

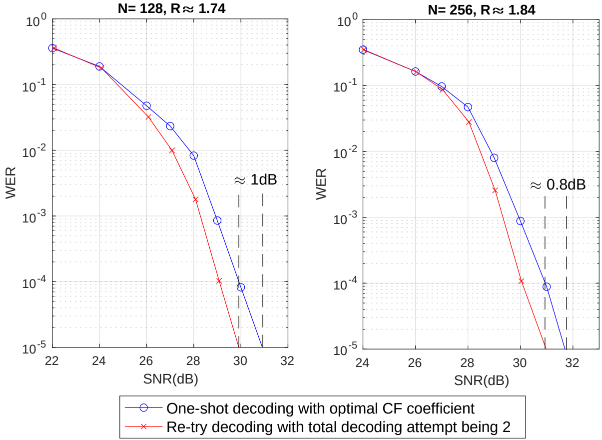
Let $\mathbf{x}_i \in \Lambda'$. Then for any $a_i \in \mathbb{Z}$, the linear combination $\sum_{i=1}^{L} a_i \mathbf{x}_i \in \Lambda'$.

However, for a nested lattice code, there is a minor restriction on the lattice code design for linearity to hold:

Theorem

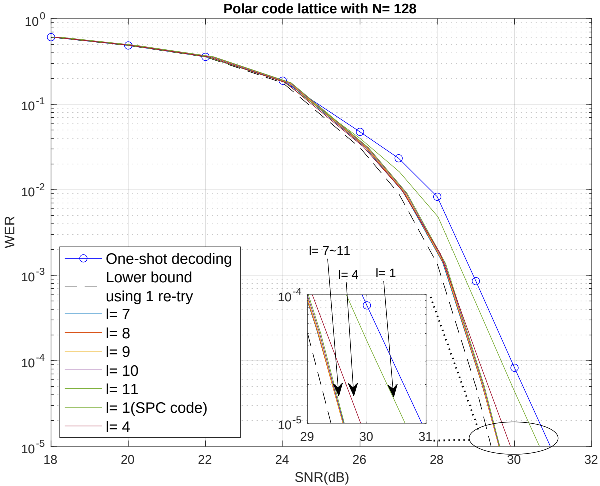
For a nested lattice code $\mathcal{C} = \Lambda'/\Lambda_s$, let Λ' and Λ_s have generator matrices $\mathbf{G}_c$ and $\mathbf{G}_s$, respectively. If $\mathbf{G}_c^{-1}\mathbf{G}_s$ has only even integers, then $\sum_{i=1}^{L} a_i \mathbf{x}_i \in \mathcal{C}$.

Compute-Forward with CRC-Enabled Lattice Codes



- $\mathbf{a}_0$ and $\mathbf{a}_1$ give the maximum and second maximum computation rate.
- 2 decoding attempts using $\mathbf{a}_0$, then $\mathbf{a}_1$.
- 1.0 dB gain with $n = 128, R = 1.74$ polar code lattice
- 0.8 dB gain with $n = 256, R = 1.84$ polar code lattice
- 4 bits CRC.

Optimized CRC Length



- The WER after retry decoding can be estimated analytically as a function of CRC length l.
- CRC length can be optimized by combining the estimated WER after retry decoding and SNR penalty due to CRC bits.
- Gain increased to 1.3 dB for CRC length of $l = 7$ to 11 ($n = 128$ polar code lattice).

Conclusion

Lattice-based decoders have asymptotically-optimal parameters,

but in the finite-length domain, retrying decoding with other parameters can improve error-rate performance.

For the point-to-point channel:

- For genie-aided decoding and CRC-enabled lattices, the benefit of retry decoding is greatest for small dimension n.
- But at small n, the rate penalty due to the CRC is significant.
- For example, an $n = 128$ polar code lattice has a gain of 0.1 dB

For the two-user multiple-access channel using compute-forward:

- Retry decoding allows using second-best $\mathbf{a}$ when first-best fails.
- Shows a benefit of 1.3 and 0.8 dB for $n = 128$ and 256 polar code lattices.