

In Search Of the Best Dimension 128 Lattice: Construction A

Jiajie Xue ¹, Brian M. Kurkoski ¹ and Emanuele Viterbo ²

¹Japan Advanced Institute of Science and Technology

²Monash University

February 2025

2025 Information Theory and Applications (ITA) Workshop

Outline

Backgrounds

Truncated union bound based design

Design examples

Comparison with classic design rules

Conclusions

Motivations

This research focuses on finite dimensional construction A lattice design.

For dimension $n \rightarrow \infty$,

- ▶ lattice codes **achieve AWGN channel capacity** [UR98], [EZ04];
- ▶ construction A lattices can be good for **AWGN channel coding** [ELZ05].

Motivations

This research focuses on finite dimensional construction A lattice design.

For dimension $n \rightarrow \infty$,

- ▶ lattice codes **achieve AWGN channel capacity** [UR98], [EZ04];
- ▶ construction A lattices can be good for **AWGN channel coding** [ELZ05].

How about lattices with finite dimensional?

Motivations

This research focuses on finite dimensional construction A lattice design.

For dimension $n \rightarrow \infty$,

- ▶ lattice codes **achieve AWGN channel capacity** [UR98], [EZ04];
- ▶ construction A lattices can be good for **AWGN channel coding** [ELZ05].

How about lattices with finite dimensional?

- ▶ $n = 128$ construction D lattices using extended BCH codes [MKO18] and polar codes [LLAK21].
- ▶ Construction D lattices use multiple component codes, while construction A lattices only need one component code.
- ▶ Lower decoding complexity can be achieved by construction A.

Background – Lattices

A lattice is a discrete additive subgroup of the real number space \mathbb{R}^n .

Definition (Lattices)

Let $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n \in \mathbb{R}^n$ be n linearly independent column vectors and a generator matrix

$\mathbf{G} = [\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_n]$. A lattice Λ is defined as:

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

Voronoi region $\mathcal{V}(\mathbf{x})$ is the set of points closer to $\mathbf{x} \in \Lambda$ than any other lattice point, with volume:

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

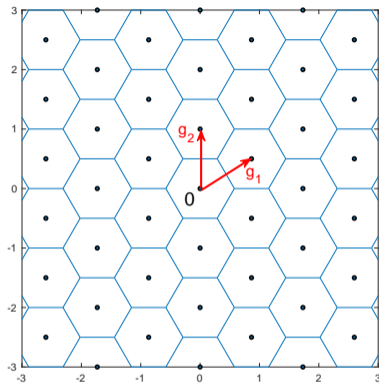


Figure 1: Example of 2-dimensional lattice spanned by $\mathbf{g}_1 = [\frac{\sqrt{3}}{2}, \frac{1}{2}]^T$ and $\mathbf{g}_2 = [0, 1]^T$ with Voronoi region \mathcal{V} .

Background – VNR and theta series

A lattice has an infinite constellation thus is power unconstrained.

Volume-to-noise ratio (VNR) is applied to evaluate error performance, defined as:

$$\text{VNR} = \frac{V(\Lambda)^{(2/n)}}{2\pi e\sigma^2},$$

where σ^2 is the per-dimensional Gaussian noise variance.

Background – VNR and theta series

A lattice has an infinite constellation thus is power unconstrained.

Volume-to-noise ratio (VNR) is applied to evaluate error performance, defined as:

$$\text{VNR} = \frac{V(\Lambda)^{(2/n)}}{2\pi e\sigma^2},$$

where σ^2 is the per-dimensional Gaussian noise variance.

Definition (Theta series)

The theta series is the weight enumerator function of a lattice Λ in the Euclidean space considering the squared length of $\mathbf{x} \in \Lambda$, given as

$$\theta = 1q^0 + \sum_{i=1}^{\infty} \tau_{d_i^2} q^{d_i^2},$$

where $\tau_{d_i^2}$ is the number of \mathbf{x} having $\|\mathbf{x}\|^2 = d_i^2$ and q is a dummy variable.

Background – Construction A

A construction A lattice consists of a q -ary code \mathcal{C} and an integer lattice $q\mathbb{Z}^n$.

Here, we consider $q = 2$.

Definition (Modulo-2 construction A lattice)

Given an (n, k, d_c) linear block code $\mathcal{C} \in \mathbb{F}_2^n$, a modulo-2 lattice is:

$$\Lambda_a = \mathcal{C} + 2\mathbb{Z}^n.$$

Properties of construction A lattices:

- ▶ $V(\Lambda_a) = 2^{n-k}$;
- ▶ $d_{min}^2 = \min(4, d_c)$, where d_c is the minimum Hamming distance of \mathcal{C} .

Example: construction A lattice (duplicated with next page)

- ▶ Consider a $n = 2$ repeat code with codebook $\mathcal{C} = \{[0, 0], [1, 1]\}$.
- ▶ Λ_a consists of vectors shifted by \mathcal{C} as $[0, 0] + 2\mathbf{z}$ and $[1, 1] + 2\mathbf{z}$ for $\mathbf{z} \in \mathbb{Z}^2$.
- ▶ The volume is $V(\Lambda_a) = 2^{n-k} = 2$.
- ▶ Theta series is $\theta = 1q^0 + 4q^2 + 4q^4 + \dots$.

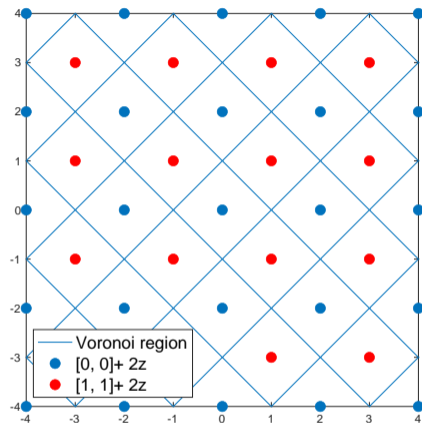


Figure 2: An example of construction A lattice.

Example: construction A lattice (duplicated with previous page)

- ▶ Consider a $n = 2$ repeat code with codebook $\mathcal{C} = \{[0, 0], [1, 1]\}$.
- ▶ Λ_a consists of vectors shifted by \mathcal{C} as $[0, 0] + 2\mathbf{z}$ and $[1, 1] + 2\mathbf{z}$ for $\mathbf{z} \in \mathbb{Z}^2$.
- ▶ The volume is $V(\Lambda_a) = 2^{n-k} = 2$.
- ▶ Theta series is $\theta = 1q^0 + 4q^2 + 4q^4 + \dots$.

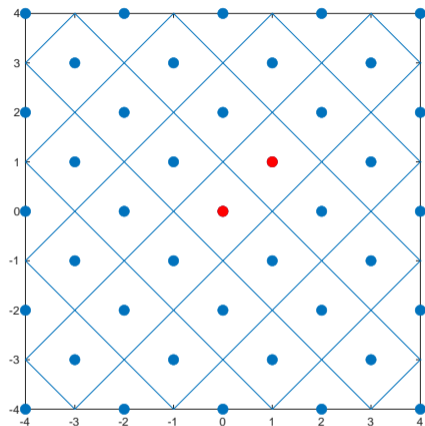


Figure 3: Construction A lattice using $n = 2$ repeat code as the component code \mathcal{C} . Consisting of $[0, 0] + 2\mathbf{z}$ and $[1, 1] + 2\mathbf{z}$ for $\mathbf{z} \in \mathbb{Z}^2$.

Background – Encoding/decoding construction A and system model

► **Encoder:**

$$\mathbf{x} = \text{Enc}(\mathbf{u}) + 2\mathbf{z}.$$

► **Channel:** given noise $\mathbf{n} \sim \mathcal{N}(0, \sigma^2 \mathbf{I})$

$$\mathbf{y} = \mathbf{x} + \mathbf{n}.$$

► **Decoder:**

$$\diamond \mathbf{y}_c = \text{mod}^*(\mathbf{y}) = |\text{mod}_2(\mathbf{y} + 1) - 1|,$$

$$\diamond [\hat{\mathbf{x}}_c, \hat{\mathbf{u}}] = \text{Dec}(\mathbf{y}_c),$$

$$\diamond \hat{\mathbf{z}} = \text{round}((\mathbf{y} - \hat{\mathbf{x}}_c)/2).$$

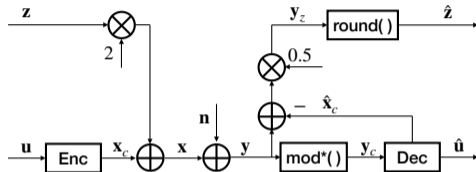


Figure 4: Encoding and decoding construction A lattices for AWGN transmission.

“Enc” and “Dec” are the encoder and decoder of the binary component code \mathcal{C} .

Goal and assumptions

This research considers design of construction A lattices using binary codes $\mathcal{C} \in \mathbb{F}_2^n$.

Goal:

- ▶ Obtain truncated union bound from truncated theta series to estimate word error rate P_e of construction A lattices under maximum likelihood (ML) decoding.
- ▶ Find the \mathcal{C} that minimizes required VNR to achieve a target P_e to design the best $n = 128$ construction A lattice.

Goal and assumptions

This research considers design of construction A lattices using binary codes $\mathcal{C} \in \mathbb{F}_2^n$.

Goal:

- ▶ Obtain truncated union bound from truncated theta series to estimate word error rate P_e of construction A lattices under maximum likelihood (ML) decoding.
- ▶ Find the \mathcal{C} that minimizes required VNR to achieve a target P_e to design the best $n = 128$ construction A lattice.

Assumptions:

- ▶ Modulo-2 construction A lattice for the AWGN transmission.
- ▶ $\mathcal{C} \in \mathbb{F}_2^n$ is an (n, k, d_c) linear block code with known:
 1. minimum Hamming distance d_c ;
 2. codeword multiplicity τ_c , the number of minimum weight codeword.

Truncated theta series of Λ_a

To give the truncated theta series θ' , we first have the following.

1. For $d^2 < d_c$, only the $2\mathbb{Z}^n$ lattice contributes to the theta series of Λ_a .

Truncated theta series of Λ_a

To give the truncated theta series θ' , we first have the following.

1. For $d^2 < d_c$, only the $2\mathbb{Z}^n$ lattice contributes to the theta series of Λ_a .
2. The theta series of $2\mathbb{Z}^n$ lattice can be obtained exactly by

$$\theta_{2\mathbb{Z}^n} = (\theta_{2\mathbb{Z}})^n = (1q^0 + 2q^4 + 2q^{16} + 2q^{36} + \dots)^n.$$

Truncated theta series of Λ_a

To give the truncated theta series θ' , we first have the following.

1. For $d^2 < d_c$, only the $2\mathbb{Z}^n$ lattice contributes to the theta series of Λ_a .
2. The theta series of $2\mathbb{Z}^n$ lattice can be obtained exactly by

$$\theta_{2\mathbb{Z}^n} = (\theta_{2\mathbb{Z}})^n = (1q^0 + 2q^4 + 2q^{16} + 2q^{36} + \dots)^n.$$

3. Binary codeword with weight d_c corresponds to 2^{d_c} construction A lattice points by adding '-' at each position with '1'.
(Example: a binary codeword (0, 1, 1, 0) corresponds to 4 lattice points: (0, 1, 1, 0), (0, -1, 1, 0), (0, 1, -1, 0), (0, -1, -1, 0).)

Truncated theta series of Λ_a

To give the truncated theta series θ' , we first have the following.

1. For $d^2 < d_c$, only the $2\mathbb{Z}^n$ lattice contributes to the theta series of Λ_a .
2. The theta series of $2\mathbb{Z}^n$ lattice can be obtained exactly by

$$\theta_{2\mathbb{Z}^n} = (\theta_{2\mathbb{Z}})^n = (1q^0 + 2q^4 + 2q^{16} + 2q^{36} + \dots)^n.$$

3. Binary codeword with weight d_c corresponds to 2^{d_c} construction A lattice points by adding '-' at each position with '1'.
(Example: a binary codeword $(0, 1, 1, 0)$ corresponds to 4 lattice points:
 $(0, 1, 1, 0)$, $(0, -1, 1, 0)$, $(0, 1, -1, 0)$, $(0, -1, -1, 0)$.)
4. The minimum weight codewords of \mathcal{C} contribute $\tau_{\mathcal{C}} 2^{d_c}$ lattice points at $d^2 = d_c$.

Truncated theta series of Λ_a

Let $L = \lfloor d_c/4 \rfloor$ and $\theta_{2\mathbb{Z}^n, 4L}$ be truncated theta series of $2\mathbb{Z}^n$ with $d^2 \leq 4L$.

The truncated theta series of Λ_a is given for $d^2 \leq d_c$ as:

$$\theta' = \begin{cases} 1q^0 + \tau_c 2^{d_c} q^{d_c} & d_c < 4 \\ 1q^0 + (2n + \tau_c 2^{d_c}) q^{d_c} & d_c = 4 \\ \theta_{2\mathbb{Z}^n, 4L} + \tau_c 2^{d_c} q^{d_c}, & d_c > 4, d_c \bmod 4 \neq 0 \\ \theta_{2\mathbb{Z}^n, 4(L-1)} + (\tau_{2\mathbb{Z}^n, d_c} + \tau_c 2^{d_c}) q^{d_c}, & d_c > 4, d_c \bmod 4 = 0, \end{cases}$$

Truncated theta series of Λ_a

Let $L = \lfloor d_c/4 \rfloor$ and $\theta_{2\mathbb{Z}^n, 4L}$ be truncated theta series of $2\mathbb{Z}^n$ with $d^2 \leq 4L$.

The truncated theta series of Λ_a is given for $d^2 \leq d_c$ as:

$$\theta' = \begin{cases} 1q^0 + \tau_c 2^{d_c} q^{d_c} & d_c < 4 \\ 1q^0 + (2n + \tau_c 2^{d_c}) q^{d_c} & d_c = 4 \\ \theta_{2\mathbb{Z}^n, 4L} + \tau_c 2^{d_c} q^{d_c}, & d_c > 4, d_c \bmod 4 \neq 0 \\ \theta_{2\mathbb{Z}^n, 4(L-1)} + (\tau_{2\mathbb{Z}^n, d_c} + \tau_c 2^{d_c}) q^{d_c}, & d_c > 4, d_c \bmod 4 = 0, \end{cases}$$

Example

Consider a Λ_a using the (32, 11, 12) extended BCH code, which has $d_c = 12$ and $\tau_c = 496$. Here, $L = 3$ and the truncated theta series contains $L + 1$ terms as:

$$\theta' = \underbrace{1q^0 + 64q^4 + 1984q^8}_{\theta_{2\mathbb{Z}^n, 4(L-1)}} + \underbrace{(39680)}_{\tau_{2\mathbb{Z}^n, d_c}} + \underbrace{496 * 2^{12}}_{\tau_c 2^{d_c}} q^{12}.$$

Truncated union bound and optimization metric

- ▶ The truncated theta series θ' are decided by the binary code \mathcal{C} .
⇒ The truncated union bound is also a function of \mathcal{C} and VNR:

$$P_e = f(\mathcal{C}, \text{VNR}) \approx \sum_{i=1}^m \tau_{d_i^2} \cdot Q \left(\sqrt{\frac{d_i^2 \cdot 2\pi e \cdot \text{VNR}}{4 \cdot 4^{1-k/n}}} \right),$$

with $d_m^2 = d_c$.

- ▶ The inverse function is found numerically as:

$$\text{VNR} = f^{-1}(\mathcal{C}, P_e).$$

- ▶ The best component code \mathcal{C}_b is found according to:

$$\mathcal{C}_b = \arg \min_{\mathcal{C}} f^{-1}(\mathcal{C}, P_e).$$

Design examples using $n = 128$ EBCH codes

- ▶ $d_c = 4, 6, 8, 10$ are considered.
- ▶ τ_c are found in [TAK]¹.
- ▶ The estimate P_e is evaluated by simulation, which becomes accurate when $P_e \leq 10^{-4}$.
- ▶ At $10^{-7} \lesssim P_e \lesssim 10^{-4}$, $(128, 106, 8)$ EBCH code lattice has the lowest P_e .
- ▶ At $P_e \lesssim 10^{-7}$, $(128, 113, 6)$ EBCH code lattice has the lowest P_e .

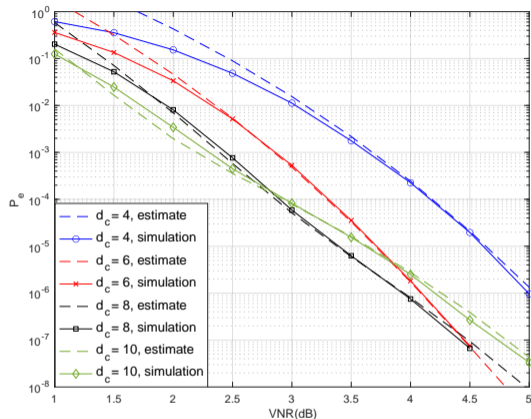


Figure 5: Design examples using $n = 128$ EBCH codes. Order-2 OSD is applied to decode EBCH codes.

¹M. Terada, J. Asatani and T. Koumoto, <https://isec.ec.okayama-u.ac.jp/home/kusaka/wd/index.html>

Design examples using polar codes

Information set \mathcal{I} is selected to satisfy the partial order property [RDV23], for which

1. bit-channels are ordered based on their reliability through BI-DMC,
2. τ_c can be calculated analytically,
3. τ_c only depends on rows of polar code generator matrix with weight d_c .

For a desired code parameter (n, k, d_c) , the information set \mathcal{I} consists of:

- ▶ all rows with weight $> d_c$;
- ▶ rows with weight d_c , such that:
 1. the partial order property is satisfied;
 2. the desired k is achieved.

Design examples using polar codes

- ▶ $d_c = 4, 8, 16$ are considered.
- ▶ If multiple polar codes have same (n, k, d_c) , the one with the lowest τ_c is evaluated.
- ▶ The estimate P_e is evaluated by simulation, which becomes accurate when $P_e \leq 10^{-4}$.
 - A mismatch at $P_e \approx 10^{-3}$ occurs, where the best code by estimation and simulation are different.
- ▶ Order-2 OSD algorithm is used in simulation to evaluate the estimate.

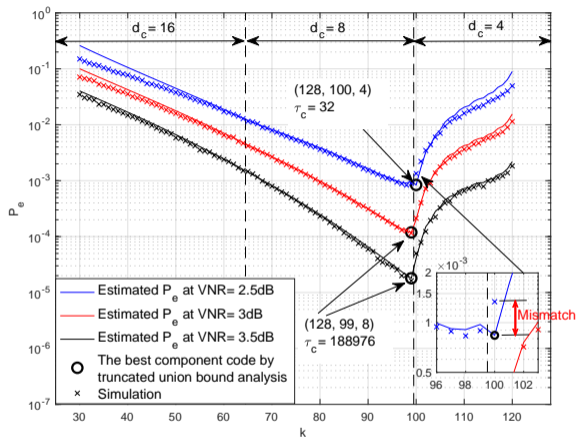


Figure 6: Design examples using $n = 128$ polar codes.

Summary of the best component codes for $P_e = 10^{-4}$ to 10^{-8}

P_e	EBCH code lattices			Polar code lattices		
	VNR(dB)	Code parameter	τ_c	VNR(dB)	Code parameter	τ_c
10^{-4}	2.86	(128, 106, 8)	774192	3.05	(128, 99, 8)	188976
10^{-5}	3.38			3.67		
10^{-6}	3.95			4.27		
10^{-7}	4.45	(128, 113, 6)	341376	4.82		
10^{-8}	4.81			5.31		

Table 1: Component EBCH codes and polar codes for construction A with the required VNR to achieve given target P_e .

- ▶ For different target P_e , the best lattice could be different.
- ▶ At $P_e = 10^{-4}$ to 10^{-8} , EBCH code lattices outperform polar code lattices for $n = 128$.

Comparison with classic design rules – lattices without shaping

Comparison of WER performance is applied for:

1. truncated union bound based design rule using codes suggested in Table 1:
 - (128, 106, 8) EBCH code and (128, 99, 8) polar code
2. balanced distance rule:
 - $d_c = d_{min, 2\mathbb{Z}}^2 = 4$,
 - applied for EBCH codes and polar codes
3. equal error probability rule:
 - design based on [LLAK21]
 - applied for polar codes only

The order-2 OSD is used to decode binary codes for construction A lattices.

Comparison with classic design rules – lattices without shaping

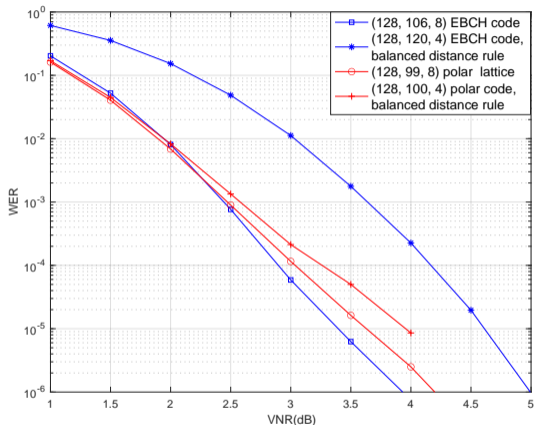


Figure 7: Comparison for lattices using the balanced distance rule.

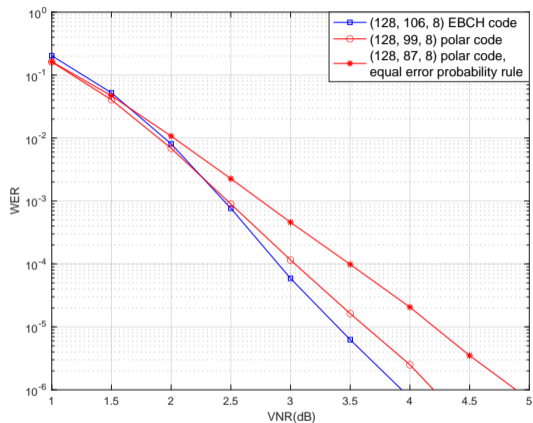


Figure 8: Comparison for lattices using the equal error probability rule (only applied for polar code lattice).

Lattice codes with power constraint

- ▶ To evaluate the WER performance in power-constrained communications, SNR_{norm} introduced in [TVZ99] is applied:

$$\text{SNR}_{norm} = \frac{P}{(2^{2R_L} - 1) \cdot \sigma^2}.$$

P and R_L are message power and code rate of lattice code.

- ▶ SNR_{norm} allows us to compare lattice codes of different rates on the same scale.
 - Asymptotically, arbitrary small P_e can be achieved if $R_L \rightarrow C$ at $\text{SNR}_{norm} \rightarrow 0\text{dB}$.
- ▶ The relationship between SNR_{norm} and VNR is found as:

$$\begin{aligned} \text{SNR}_{norm}(\text{dB}) = & \text{VNR}(\text{dB}) + 10 \log_{10}(2\pi e \cdot P) \\ & - \underbrace{10 \log_{10}[(2^{2R_L} - 1) \cdot V(\Lambda)^{2/n}]}_{\text{affected by code rate}}. \end{aligned}$$

Shaping using $8\mathbb{Z}^n$ lattice

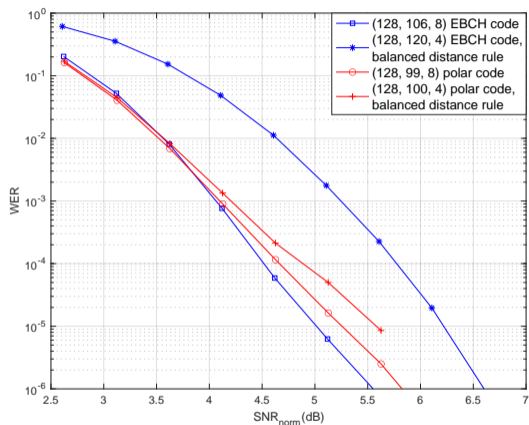


Figure 9: Comparison for lattice codes using the balanced distance rule.

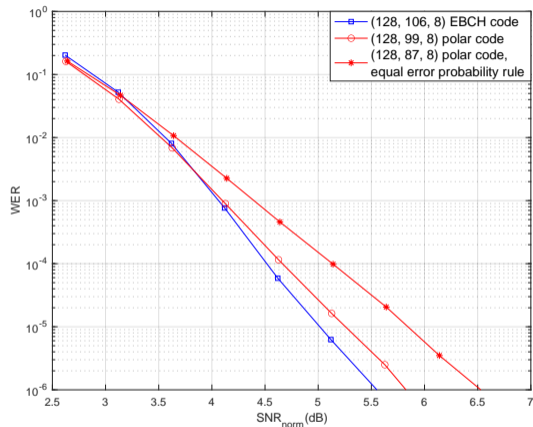


Figure 10: Comparison for lattice codes using the equal error probability rule (only applied for polar code lattice).

Conclusion and future works

Conclusion

1. The truncated union bound based design gives the best lattice under ML decoding, verified by the OSD algorithm.
2. At $P_e = 10^{-5}$, **the best-known** $n = 128$ **construction A lattice** is formed by the $(128, 106, 8)$ EBCH code and achieves $P_e = 10^{-5}$ at $VNR \approx 3.38\text{dB}$.
3. For polar code lattices, the best component code is also the $RM(4, 7)$ code.

Future works

1. Apply the design rule for $n > 128$ polar codes satisfying the partial order property. For high dimensional lattice design, the capacity rule can be applied.
2. Can we extend the design method to construction D lattices?

Reference

- [ELZ05] Uri Erez, Simon Litsyn, and Ram Zamir. “Lattices which are good for (almost) everything”. In: *IEEE Transactions on Information Theory* 51.10 (2005), pp. 3401–3416.
- [EZ04] Uri Erez and Ram Zamir. “Achieving $1/2 \log(1+\text{SNR})$ on the AWGN channel with lattice encoding and decoding”. In: *IEEE Transactions on Information Theory* 50.10 (2004), pp. 2293–2314.
- [LLAK21] Obed Rhesa Ludwiniananda et al. “Design of Polar Code Lattices of Finite Dimension”. In: *2021 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2021, pp. 1011–1016.
- [MKO18] Toshiki Matsumine, Brian M Kurkoski, and Hideki Ochiai. “Construction D lattice decoding and its application to BCH code lattices”. In: *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE. 2018, pp. 1–6.
- [RDV23] Mohammad Rowshan, Son Hoang Dau, and Emanuele Viterbo. “On the formation of min-weight codewords of polar/PAC codes and its applications”. In: *IEEE Transactions on Information Theory* 69.12 (2023), pp. 7627–7649.
- [TAK] M. Terada, J. Asatani, and T. Koumoto. *Weight Distribution of extended BCH codes*. <https://isec.ec.okayama-u.ac.jp/home/kusaka/wd/index.html>.
- [TVZ99] Vahid Tarokh, Alexander Vardy, and Kenneth Zeger. “Universal bound on the performance of lattice codes”. In: *IEEE Transactions on Information Theory* 45.2 (1999), pp. 670–681.
- [UR98] Rüdiger Urbanke and Bixio Rimoldi. “Lattice codes can achieve capacity on the AWGN channel”. In: *IEEE Transactions on Information Theory* 44.1 (1998), pp. 273–278.

Thank you for listening!

Appendix

Polar codes with same parameter but different τ_c

- ▶ By selecting different \mathcal{I} , there may exist multiple polar code having the same (n, k, d_c) , but different τ_c .
- ▶ For $d_c = 4$, polar code with lower τ_c improves P_e .
- ▶ Such improvement is negligible for $d_c = 8$,

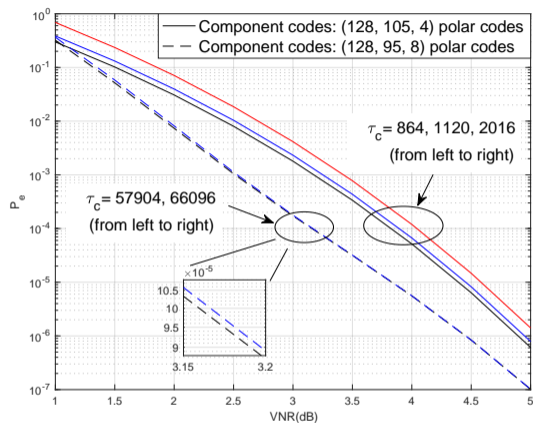


Figure 11: Truncated union bound for polar code having same (n, k, d_c) but different τ_c for $d_c = 4, 8$.

Polar codes not satisfying the partial order property

- ▶ A search for polar codes **not** satisfying the partial order property for $k = 97$ to 103 .
- ▶ τ_c are found by numerical tools.
- ▶ Lower τ_c are found at $k = 97, 101, 102, 103$.
- ▶ The improvement of P_e is non-negligible at $k = 101, 102, 103$ (only at $d_c = 4$).
- ▶ However, component code exceeds the $(128, 99, 8)$ polar code has not been found.

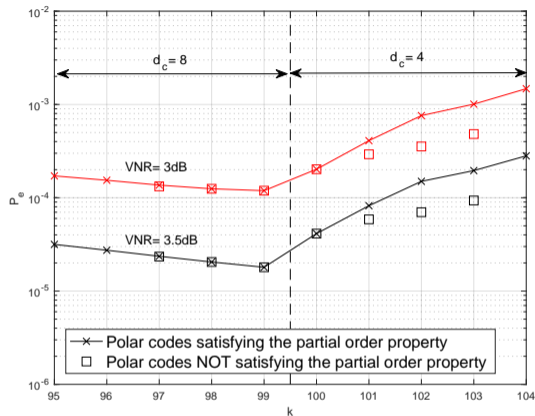


Figure 12: Truncated union bound for polar code not satisfying the partial order property for $k = 97$ to 103 .

Comparison with construction D lattices

- ▶ Lattices for comparison use EBCH codes [MKO18] and polar codes [LLAK21].
- ▶ Construction D lattices have lower WER with the high cost on decoding (EBCH codes) and design (polar codes).
- ▶ Using EBCH codes, the number of OSD computations are
 - construction A: 5671;
 - construction D: 1505702.
- ▶ Using polar codes, lattice design is based on:
 - construction A: analytic truncated union bound based design
 - construction D: Monte-Carlo method.

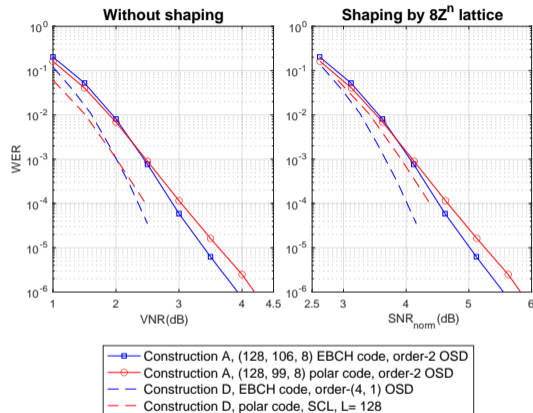


Figure 13: Comparing construction D lattices/lattice codes.