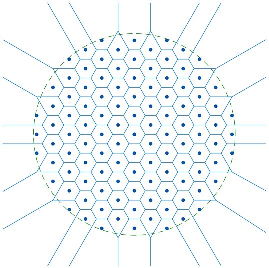
Lower Bound on the Error Rate of Genie-Aided Lattice Decoding

Jiajie Xue and Brian M. Kurkoski

Japan Advanced Institute of Science and Technology

July 1, 2022
2022 IEEE International Symposium on Information Theory

Motivation — ML Decoding of Lattices

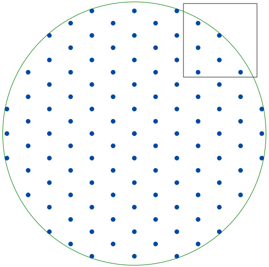


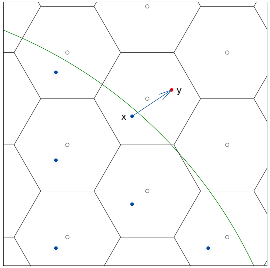
An n-dimensional lattice code is the intersection of a lattice and a shaping region:

- 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 $_{MMSE}$[2]:

$$_{MMSE} = \frac{P}{P + N}$$

- Intuition: noise moves **y** away from the origin, so "expand" the decoding lattice

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

Preview — Scaling for Finite-Dimension Lattices

$_{MMSE}$ is optimal when n ! 1

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

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

- Genie tells decoder if estimated lattice point is correct or not
- If not, decoder retries decoding using different scaling
- 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

Preview — Main Results

Consider a genie-aided exhaustive search decoder which is allowed to use all 2 R.

Clearly, genie-aided decoding achieves lower word error rate (WER) than one-shot decoder using $_{MMSE}$ only.

1. Give a lower bound on WER for this decoder
2. Give an estimate of the WER. Not a bound, but empirically accurate for lattices with sphere-like Voronoi regions.
3. Asymptotic error expression when power $P \; ! \; 1$
4. Implement genie by using CRC. Shows a 0.1 dB gain on $n = 128$ polar code lattices.

Background — Lattices (1)

Definition (Lattices)

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

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

where $\mathbf{G} = [\mathbf{g}_1; \mathbf{g}_2; \quad ; \mathbf{g}_n] \in \mathbb{R}^{n \quad n}$ and $\mathbf{g}_1; \mathbf{g}_2; \quad ; \mathbf{g}_n \in \mathbb{R}^n$ are linear independent.

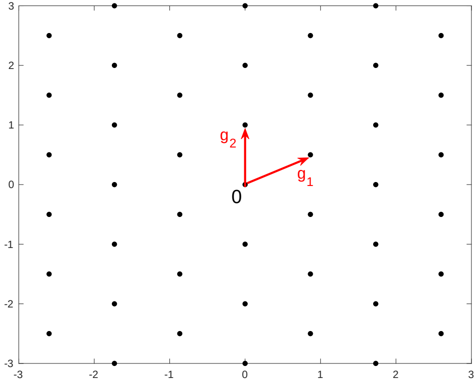


Figure 1: Example of 2-dimensional lattice spanned by $\mathbf{g}_1 = [\frac{\sqrt{3}}{2}; \frac{1}{2}]^T$ and $\mathbf{g}_2 = [0; 1]^T$.

Background — Lattices (2)

Definition (Voronoi region, covering sphere and effective sphere)

Given lattice and $\mathbf{x} \in$, we can define:

- Voronoi region $V(\mathbf{x})$: set of $\mathbf{y} \in \mathbb{R}^n$ closer to $\mathbf{x}$ than any other lattice point;
- Covering sphere $S_c(\mathbf{x})$: sphere with minimal radius r_c that covers V, i.e. $V \quad S_c$;
- Effective sphere $S_e(\mathbf{x})$: sphere with radius r_e that has same volume as V, i.e. $V(V) = V(S_e)$.

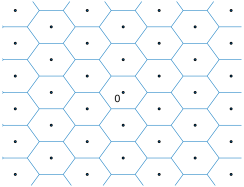


Figure 2: Voronoi region.

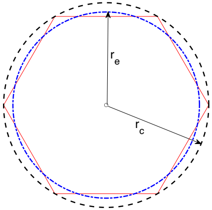


Figure 3: Relationship among V, S_c and S_e.

Background — Lattice codes

Definition (Lattice quantize and $\mathrm{mod}\,\Lambda$)

Given lattice , we can define lattice quantizer Q and mod as:

$$Q\ (\mathrm{y}) = \arg\min_{\mathbf{x}2} ky \quad xk^2$$

$$\mathrm{y} \bmod \quad = \mathrm{y} \quad Q\ (\mathrm{y})$$

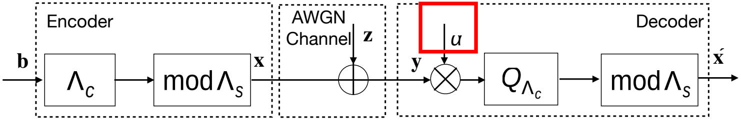
Definition (Nested lattice codes)

Let two lattices $_c$ and $_s$ satisfy $_s$ $_c$ and form a quotient group $_c$= $_s$. A nested lattice code C is defined as:

$$C = f\mathrm{x} \bmod \ _s : \mathrm{x}\ 2\ \ _c g$$

Background—Encoding and decoding

Encoding and decoding scheme is given as:



Let n-dimensional lattice code $C = \ _c = \ _s$ and G is generator matrix of $\ _c$,

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

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

Decoder: $\hat{\mathbf{x}} = Q \ _c(\ \mathbf{y}) \bmod \ _s$, with $\ 2 \ \mathrm{R}$

Decoder Design

The **genie-aided exhaustive search decoder** is allowed to use all *2* R for scaling as shown in Fig. 4

- For practical implementation with finite complexity, *finite search range* and *search step* can be considered.

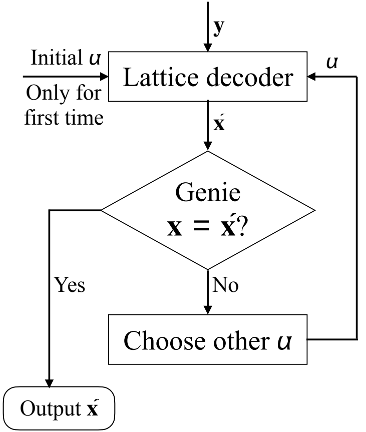


Figure 4: Genie-aided decoding

Decodable Region

Given $\mathbf{x}$, what is region that decoder can correctly decode the message?
This is equivalent to the region of $\mathbf{y}$ that:

- Example $\mathbf{y}_1$: there exists an such that $Q(\ \mathbf{y}_1) = \mathbf{x}$.
- Example $\mathbf{y}_2$: there is no such that $Q(\ \mathbf{y}_2) = \mathbf{x}$.

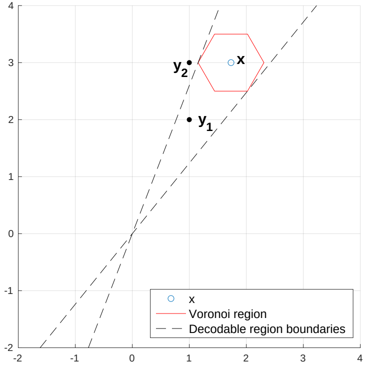


Figure 5: Decodable region of A_2 lattice given $\mathbf{x} = [\sqrt{3}; 3]^T$.

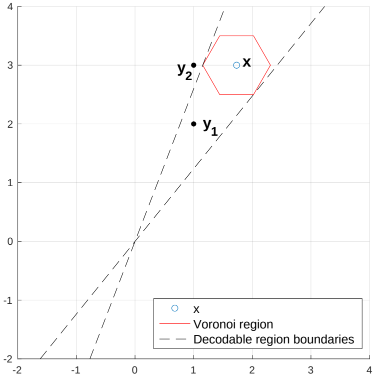
Decodable region

Definition (Decodable region)

Let Λ be n-dimensional lattice. Given $\mathbf{x} \in \Lambda$ and $V(\mathbf{x})$ be the Voronoi region of $\mathbf{x}$, decodable region of $\mathbf{x}$ is defined as:

$$D(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n : \exists \alpha \in \mathbb{R}, Q_\Lambda(\alpha \mathbf{y}) = \mathbf{x}\}$$

Or equivalently, the decodable region is the closure of the lines connecting 0 and any point inside V.



Error probability of the decoder can be expressed as: $P_{e;Dec} = 1 - Prob(\mathbf{y} \in D(\mathbf{x}))$.

Unfortunately, $P_{e;Dec}$ depends on $\mathbf{x}$.

Lower Bound on Error Rate

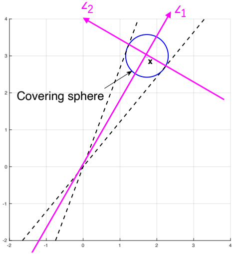
Form a lower bound on $P_{e;Dec}$ using the covering sphere.

Bound will depend on $jjxjj^2$ but not x.

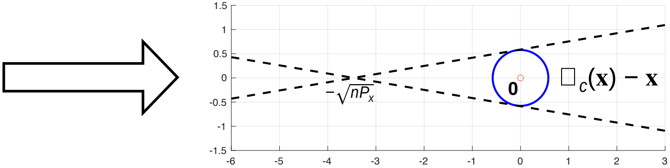
For finite dimension lattices, by the fact $V \quad S_c$, $P_{e;Dec}$ is lower bounded by

$$P_{e;Dec} > P_{e;cover}$$

) Integrate Gaussian noise z over region $D_c(\mathrm{x}) \quad \mathrm{x}$.



※Draw coordinate of **z** based on rotationally invariant property.



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

Sketch of Proof

Denote the probability density function of n-dimension Gaussian be $g(z_1, z_2, \cdots, z_n) \sim N(0, \sigma^2 \mathbf{I}_n)$.

$$
\begin{aligned}
& Prob(\mathbf{z} \in D_c(\mathbf{x}) \mid \mathbf{x}) \\
&= \int_{D_c(\mathbf{x}) \mid \mathbf{x}} g(z_1, z_2, \cdots, z_n) dz \\
&= \int_{-\infty}^{+\infty} dz_1 \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{z_1^2}{2\sigma^2}} \underbrace{\int_{S_{n-1}(r_z)} dz\, g(z_2, z_3, \cdots, z_n)}_{\text{Closed form available}}
\end{aligned}
$$

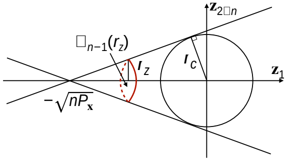


Figure 6: 2-dim image of n-dim cone-like decodable region with known r_c and $\sqrt{nP_{\mathbf{x}}}$.

where $S_{n-1}(r_z)$ is $n-1$ dimensional sphere with radius r_z.

$\int_{S_{n-1}(r_z)} g(z_2, z_3, \cdots, z_n) dz_{2\sim n}$ integral of Gaussian over sphere has closed form.[4]

[4] Tarokh, Vardy and Zeger, "Universal Bound on the Performance of Lattice Codes," IT Trans., March 1999

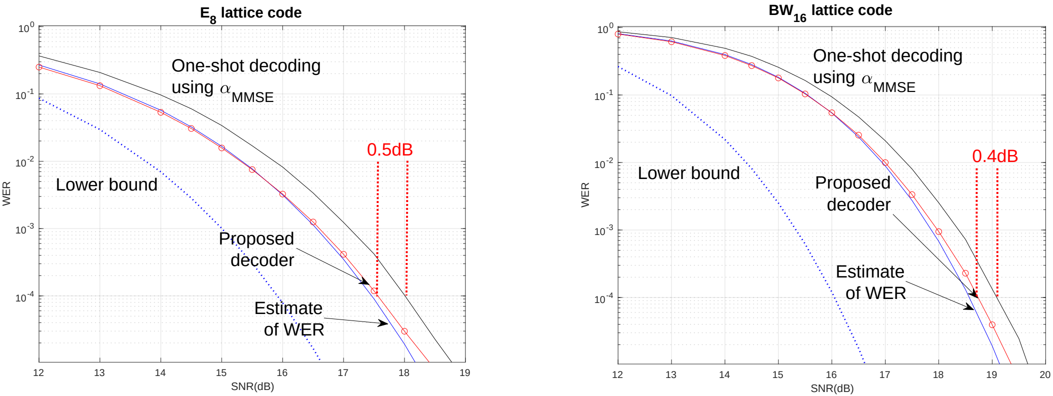
Estimate of Error Rate

- Obtain estimate of error rate (rather than lower bound) on error rate
- Replace covering sphere with effective sphere (sphere of same volume as Voronoi region).
- Use the same expression given in Theorem 1, but replace covering radius r_c with effective radius r_e.

Then we can obtain:

$$1 - Prob(\mathbf{y} \in D(\mathbf{x})) \approx 1 - Prob(\mathbf{y} \in D_e(\mathbf{x}))$$
$$P_{e,Dec} \approx P_{e,effc}.$$

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

Asymptotic analysis when $P_x \to \infty$

When $P_x \to \infty$, cone decodable region becomes cylinder-like in area of interest.

- Radius of S_{n-1} is a constant r and independent of z_1.
- $P_{e,asym}$ is this probability of error, given by:

$$\begin{cases} 1 - e^{-t}\left(1 + \frac{t}{1!} + \frac{t^2}{2!} + \cdots + \frac{t^{(n-3)/2}}{((n-3)/2)!}\right); & n \text{ odd}; \\ 1 - \operatorname{erfc}(t^{1/2}) - e^{-t}\left(\frac{t^{1/2}}{1/2!} + \frac{t^{3/2}}{(3/2)!} + \cdots + \frac{t^{(n-3)/2}}{((n-3)/2)!}\right); & n \text{ even}; \end{cases}$$

With fixed dimension n, noise variance σ^2 and covering (or effective) radius r, the error probability $P_e \to P_{e,asym}$ when $P_{\mathbf{x}} \to +\infty$.

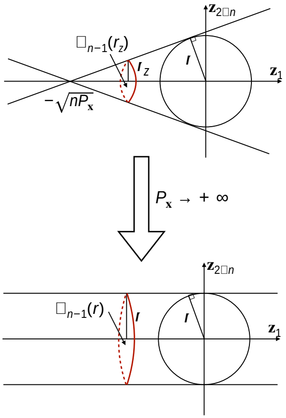


Figure 7: Asymptotic case of the cone-like decodable region.

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 . Repeating decoding is more efficient than re-transmission.

Polar Code Lattices Using CRC-Enabled Genie

- Dimension $n = 128$ polar code lattice.
- $R = 1.74$ 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

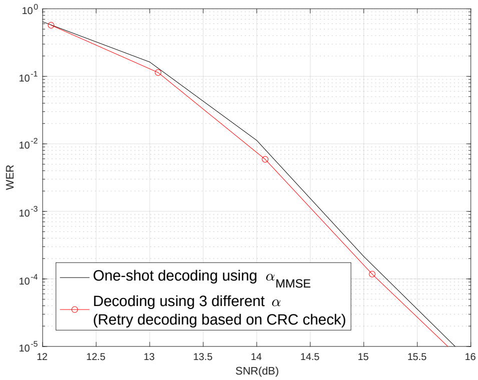


Figure 8: SNR vs WER of 128-dim polar code lattice with one-shot decoding and 3-times decoding.

Preliminary result included to show promise of the method.

Conclusions

1. One-shot lattice decoding fails if $\mathbf{y}$ is outside Voronoi region,
2. Lattice decoding performance can be improved when retries are allowed
3. Retries help significantly when a genie is available, shown through lower bound and estimate expressions.
4. Good for small n, benefit seems to decrease for increasing n.
5. Genies are not practical, so use a CRC instead.
6. Preliminary results for $n = 128$ polar code lattice indicate modest gains in performance.