1 Construction A

Construction A forms a lattice from a finite-field code. The code's finite field must be of prime size.

When the code is binary, the lattices's squared minimum distance and kissing number can be found from the properties of the code, but the squared minimum distance can be no greater than 4. For this reason, binary Construction A lattices are primarily of interest in small dimension n, although lattices based on binary convolutional codes are also of importance due to their high normalized second moment.

1.1 Definition and Properties

Two integers a and b are *congruent modulo* p if $a - b$ is divisible by p. Equivalently, a and b are congruent if a mod p is equal to b mod p. For example, 13 is congruent to 33, taken modulo 10. Congruence is extended to vectors componentwise. For example $(10, 5, 9, 2, 5, 10)$ is congruent to $(0, 1, 1, 0, 1, 0)$, taken modulo 2.

Definition 1.1. *Construction A* Let $\mathcal{C}$ be an (n, k) linear code over the field $\mathbb{F}_p$, where p is a prime number. A vector $\mathbf{x}$ is a point of lattice Λ_{A} if and only if $\mathbf{x}$ is congruent modulo p to a codeword of $\mathcal{C}$.

If $\mathbf{x} \in \Lambda_{\mathrm{A}}$, then we can write $\mathbf{x} = \mathbf{c} + p\mathbf{z}$ where $\mathbf{c} \in \mathcal{C}$ and $\mathbf{z} \in \mathbb{Z}^n$, so that $\mathbf{x}$ mod p is $\mathbf{c}$. The lattice can be represented by embedding the code $\mathcal{C}$ with elements $\mathbb{F}_p$ in the real space, and then shift it by multiples of p:

$$\Lambda = \mathcal{C} + p\mathbb{Z}^n \tag{1.1}$$

For p is prime number, the elements of $\mathbb{F}_p$ are $\{0, 1, \ldots, p-1\}$ and they are embedded directly in the real space.

The volume of a Construction A lattice is:

$$V(\Lambda) = p^{n-k}. \tag{1.2}$$

The hypercube with sides $0 \le x_i < p$ has volume p^n and contains 2^k codewords from $\mathcal{C}$. The volume per lattice point is $2^n/2^k$.

Example 1.1. Consider the $(2, 1)$ parity-check code defined over $\mathbb{F}_3$ with codewords

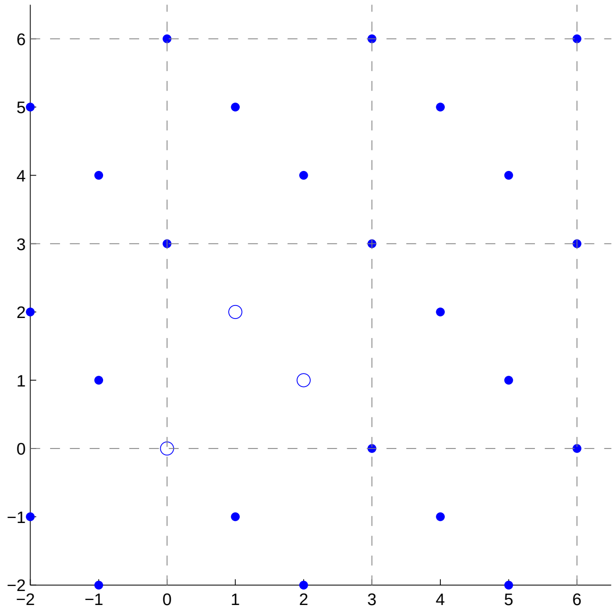

Figure 1.1: Construction A lattice obtained from the code $\mathcal{C} = \{00, 12, 21\}$ over the ternary field $\mathbb{F}_3$.

$\mathcal{C} = \{00, 12, 21\}$. Then, the lattice consists of the points:

$$\{00, 12, 21\} + 3\mathbb{Z}^2. \tag{1.3}$$

The volume is $V(\Lambda) = 3$. This lattice is shown in Fig. 1.2, where the original codebook is shown with open circles.

Construction A lattices have a generator matrix derived from the generator matrix of the code $\mathcal{C}$. Let $\mathbf{G}_c$ be a full-rank generator matrix for (n, k) code $\mathcal{C}$, which is over $\mathbb{F}_p^n$. If the following $n \times n$ matrix $\widetilde{\mathbf{G}}$ over $\mathbb{F}_p^n$ is a basis for $\mathbb{F}_p^n$:

$$\widetilde{\mathbf{G}} = \begin{array}{l} \left[\begin{array}{ccccccc} | & | & & | & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_k & \mathbf{g}_{k+1} & \cdots & \mathbf{g}_n \\ | & | & & | & | & & | \end{array}\right] \\ \xleftrightarrow{\hspace{6cm}} \\ \underset{\mathbf{G}_c}{\xleftrightarrow{\hspace{3cm}}} \qquad \mathbb{F}_p^n \end{array}, \tag{1.4}$$

(where columns 1 to k are the columns of $\mathbf{G}_c$), then the generator matrix $\mathbf{G}$ for the lattice Λ_A is:

$$\mathbf{G} = \left[\begin{array}{ccccccc} | & | & & | & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_k & p\mathbf{g}_{k+1} & \cdots & p\mathbf{g}_n \\ | & | & & | & | & & | \end{array}\right]. \tag{1.5}$$

This is a matrix over the reals, including the product $p\mathbf{g}$.

The following guarantees that this condition is satisfied. Let $\mathbf{G}_\mathrm{c}'$ be a generator matrix for $\mathcal{C}$ in lower-triangular form with 1's on the diagonal. A generator matrix $\mathbf{G}$ for Λ_A can be formed using $\mathbf{G}_\mathrm{c}'$ as:

$$\mathbf{G} = \begin{bmatrix} \mathbf{G}_\mathrm{c}' & \begin{matrix} \mathbf{0} \\ p\mathbf{I}_{n-k} \end{matrix} \end{bmatrix}. \tag{1.6}$$

where $\mathbf{0}$ is the k-by-k matrix of zeros. Since $\mathbf{G}_\mathrm{c}'$ is lower-triangular, $\mathbf{G}$ is also lower triangular.

Example 1.2. Continuing Example 1.1, there two generator matrices for $\mathcal{C}$ are $\begin{bmatrix}1 & 2\end{bmatrix}^\mathrm{t}$ and $\begin{bmatrix}2 & 1\end{bmatrix}^\mathrm{t}$, corresponding to matrices over $\mathbb{F}_p^n$:

$$\begin{bmatrix}1 & 0\\ 2 & 1\end{bmatrix} \text{ and } \begin{bmatrix}2 & 0\\ 1 & 1\end{bmatrix}. \tag{1.7}$$

While the former is a basis for $\mathbb{F}_n^2$, the latter is not. Using the former, a lattice generator matrix is

$$\mathbf{G} = \begin{bmatrix}1 & 0\\ 2 & 3\end{bmatrix}. \tag{1.8}$$

Example 1.3. Consider the $(6, 3)$ code over $\mathbb{F}_{11}$ with generator matrix:

$$\begin{bmatrix}6 & 0 & 0\\ 7 & 2 & 0\\ 3 & 0 & 7\\ 5 & 4 & 6\\ 9 & 0 & 0\\ 9 & 5 & 6\end{bmatrix} \tag{1.9}$$

This matrix is in lower-triangular form, but the diagonal elements are not 1. Another generator matrix can be found by multiplying the three columns by 6^{-1}, 2^{-1} and 7^{-1} over $\mathbb{F}_{11}$ respectively. Then the corresponding generator matrix for Λ_A is:

$$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0\\ 3 & 1 & 0 & 0 & 0 & 0\\ 6 & 0 & 1 & 0 & 0 & 0\\ 10 & 2 & 4 & 11 & 0 & 0\\ 7 & 0 & 0 & 0 & 11 & 0\\ 7 & 8 & 4 & 0 & 0 & 11\end{bmatrix} \tag{1.10}$$

A lattice check matrix $\mathbf{H}$ for Λ_A may be obtained from the code parity-check matrix. Let $\mathbf{H}_\mathrm{c}'$ be a lower-triangular full-rank $(n-k)$-by-n parity-check matrix for $\mathcal{C}$, with 1s on the diagonal. Then an n-by-n lattice check matrix $\mathbf{H}$ for Λ_A is:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_k \quad \mathbf{0} \\ \frac{1}{p}\mathbf{H}_\mathrm{c} \end{bmatrix}, \tag{1.11}$$

where **0** is the k-by-$(n-k)$ matrix of zeros.

To see this is a check matrix, consider only the lattice points inside the hypercube $0 \leq s_i < p$. There are p^k lattice points which correspond to codewords $\mathbf{c} \in \mathcal{C}$. Let $\mathbf{h}$ be an arbitrary row of $\mathbf{H}_{\mathrm{c}}$. Then the corresponding row of $\mathbf{H}$ is $\frac{\mathbf{h}}{p}$ and parity check $\mathbf{h} \cdot \mathbf{c}/p$ is an integer, since $\mathbf{c}$ satisfies $\mathbf{h} \odot \mathbf{c} = 0$ (over $\mathbb{F}_p$). Since the determinant of $\mathbf{H}$ is p^{k-n}, the corresponding number of points satisfying $\mathbf{Hx}$ inside the hypercube is $p^{k-n}p^n = p^k$. Thus, this $\mathbf{H}$ describes all the points of Λ_{A} inside the hypercube and is a check matrix.

Example 1.4. Consider the following $n = 8, k = 2$ code over $\mathbb{F}_5$ with check matrix:

$$\mathbf{H}_{\mathrm{c}} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 3 & 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 0 & 2 & 0 & 0 & 1 \end{bmatrix}. \tag{1.12}$$

Then, the Construction A lattice has check matrix $\mathbf{H}$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{5} & \frac{1}{5} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{5} & 0 & 0 & 0 & 0 \\ \frac{4}{5} & 0 & 0 & 0 & \frac{1}{5} & 0 & 0 & 0 \\ 0 & 0 & \frac{4}{5} & 0 & 0 & \frac{1}{5} & 0 & 0 \\ \frac{4}{5} & 0 & 0 & \frac{3}{5} & 0 & 0 & \frac{1}{5} & 0 \\ 0 & \frac{3}{5} & 0 & 0 & \frac{2}{5} & 0 & 0 & \frac{1}{5} \end{bmatrix}. \tag{1.13}$$

1.2 Construction A with Binary Codes

1.2.1 Properties

When the code $\mathcal{C}$ is binary, the squared minimum distance and kissing number can be determined from the codes minimum distance. The lattice kissing number can be determined from the codeword multiplicity. For non-binary codes, the minimum Hamming distance cannot be used, since Hamming distance only tells how many positions disagree, and not how far apart they are.

All Construction A lattices are integer codes, and for binary codes we have $2\mathbb{Z}^n \subset \Lambda_{\mathrm{A}} \subset \mathbb{Z}^n$.

Example 1.5. Consider the repeat code for $n = 2$, with $\mathcal{C} = \{00, 11\}$. The Construction A lattice is shown in Fig. 1.2, where the two codewords are shown using open circles. The remaining lattice points, the closed circles, can be obtained by shifts of the codewords.

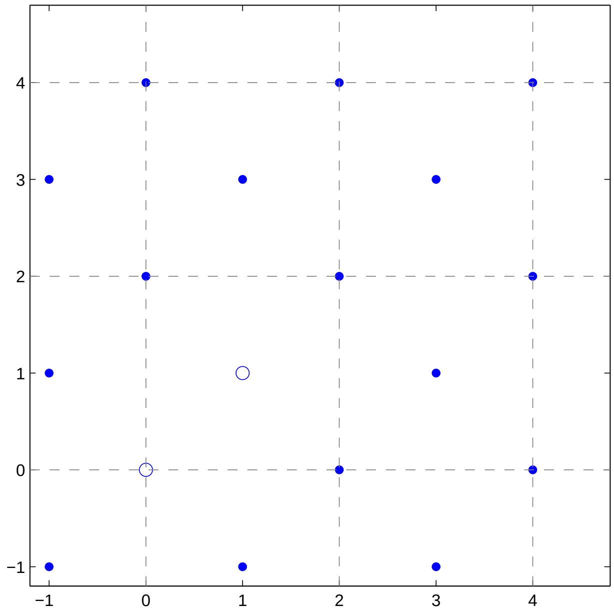

Figure 1.2: Construction A lattice obtained from the $n = 2$ repeat code $\mathcal{C} = \{00, 11\}$ over the binary field $\mathbb{F}_2$.

Let the binary code $\mathcal{C}$ have minimum distance d and let the codeword multiplicity at distance d be A_d (that is, A_d is the number of codewords at minimum distance d).

Proposition 1.1. Let the (n, k) binary code $\mathcal{C}$ have minimum distance d and let the codeword multiplicity at distance d be A_d. For the corresponding Construction A lattice, the squared minimum distance d^2_{min} of Λ_{A} is:

$$d^2_{\text{min}} = \min(d, 4). \tag{1.14}$$

and the kissing number τ is:

$$\tau = \begin{cases} A_d 2^d & \text{if } d < 4 \\ A_d 2^d + 2n & \text{if } d = 4 \\ 2n & \text{if } d > 4 \end{cases} \tag{1.15}$$

Also, the volume is $V(\Lambda) = 2^{n-k}$.

Proof of d^2_{min} (If two distinct centers are congruent to the same codeword their distance apart is at least 2. If they are congruent to different codewords then they differ by at least 1 in at least d places, so there are at least $\sqrt{d}$ apart. Thus we make take the radius of the spheres to be:).

Proof 1 of τ Recall lattice points are $\mathbf{x} = \mathbf{c} + 2\mathbf{z}$ with $\mathbf{c} \in \mathcal{C}$ and $\mathbf{z} \in \mathbb{Z}^n$. Consider lattice points near $\mathbf{0}$, which has two types of neighbors. (a) another lattice point of the form $(\pm 2 0^{n-1})$; there are $2n$ points at squared distance 4. (b) There are A_d codewords at Hamming distance d from **0**, so there are 2^d lattice points of the form $((\pm 1)^d 0^{n-d})$, at a squared distance d from **0**. If $d > 4$ then the points in (a) are closer to **0** and contribute to the kissing number. If $d < 4$ then the points in (b) are closer to **0** and contribute to the kissing number. If $d = 4$, then both contribute.

Proof 2 of τ (Let S be a sphere with center x, where x is congruent to the codeword c. Candidates for centers closets to x are as follows. (a) there are $2n$ centers of the type $x + ((\pm 20^{n-1}))$ at a distance of 2 from x. (b) Let A_i be the weight distribution of C with respect to c. Since there are A_d codewords at a distance of d from c, there are $2^d A_d$ centers of the type $x + ((\pm 1)^d 0^{n-d})$ at a distance $\sqrt{d}$ from x. Therefore the number of spheres touching S, the kissing number of S, is:)

In addition, the Construction A lattice Λ_{A} has coding gain:

$$\gamma_c = \frac{d^2_{\text{min}}}{4^{(n-k)/n}}. \tag{1.16}$$

The well-known lattice D_n is obtained by applying Construction A to the single-parity check code. Similarly the E_7 and E_8 lattices are obtained from the $(7,4)$ Hamming code and the $(8,4)$ extended Hamming code, respectively.

1.2.2 Checkerboard lattice D_n

The checkerboard D_n lattice is obtained by applying the single-parity check code of block length n to Construction A. It is called the “checkerboard” lattice, because it consists of all the points where the sum of the coordinates is even:

$$D_n = \{\mathbf{x} \in \mathbb{Z}^n | \sum_{i=1}^{n} x_i \text{ is even}\}. \tag{1.17}$$

A generator matrix for D_n is:

$$\mathbf{G}_n = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ & \vdots & & & & \vdots & \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & -1 & 2 \end{bmatrix} \tag{1.18}$$

Since the minimum distance of the single parity check code is $d = 2$, the D_n lattice has $d^2_{\text{min}} = 2$. For the n-dimensional D_n lattice, the volume is $V(\Lambda) = 2$, the squared minimum distance is $d^2_{\text{min}} = 2$ and the kissing number is $2n(n-1)$. For $n = 4$, and the D_4 generator matrix is:

$$\mathbf{G}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 2 \end{bmatrix}. \tag{1.19}$$

The dimension $n = 3$ lattice given in Example **??** on page **??** is the D_3 lattice.

```
Algorithm 1.1 Decoding $D_n$ Lattice
Require: noisy input $\mathbf{y}$ of length $n$
Ensure: Element of $D_n$ closest to $\mathbf{y}$
  Compute the following:
      $\mathbf{z}_1 = \lfloor \mathbf{y} \rceil$
      $\mathbf{z}_2 = g(\mathbf{y})$
  Choose the output:
      $\mathbf{x} = \begin{cases} \mathbf{z}_1 & \text{if } \sum_i z_{1,i} \text{ is even} \\ \mathbf{z}_2 & \text{otherwise} \end{cases}$    (1.22)
```

A generator matrix for the binary parity check code (not a lattice) with $n = 4$ is:

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \tag{1.20}$$

and the corresponding D_4 generator matrix is:

$$\mathbf{G}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 2 \end{bmatrix} \tag{1.21}$$

The transpose of the code's generator matrix can be seen in the three left columns of $\mathbf{G}_4$, and the forth column is a linearly independent vector for the Construction A extension (with $p = 2$).

D_n Quantization Recall $\lfloor \mathbf{y} \rceil$ is component-wise integer rounding of $\mathbf{y}$. Wrong-way rounding $g(\mathbf{y})$ of a vector $\mathbf{y}$ rounds the single "worst" position in the opposite direction. For example, if $\mathbf{y} = (5.2, 1.4, -2.3)$ then usual rounding is $(5, 1, -2)$ and wrong-way rounding is:

$$g\big((5.2, 1.4, -2.3)\big) = (5, 2, -2) \tag{1.23}$$

That is, 1.4 is further from its nearest integer than 5.2 or -2.3, so 1.4 is rounded the wrong way, to 2 instead of to 1. If multiple positions tie for the same distance to an integer, then the position with the smallest index is rounded the wrong way. The vectors $\lfloor \mathbf{y} \rceil$ and $g(\mathbf{y})$ agree in all positions except one.

The lattice quantization algorithm for D_n recalls that $\mathbf{x} \in D_n$ if and only if $\sum_{i=1}^{n} x_i$ is even. That is, find both $\lfloor \mathbf{y} \rceil$ and $g(\mathbf{y})$, and choose the one which has an even coordinate sum. This procedure is summarized in Algorithm 1.2.

Example 1.6. Find the point of the D_4 lattice closest to

$$\mathbf{y} = \begin{bmatrix} 0.6, 2.7, -1.1, 0.1 \end{bmatrix}. \tag{1.24}$$

Algorithm 1.2 Quantization of D_n Lattice, $\mathbf{x} = Q_{D_n}(\mathbf{y})$

```
Require: $\mathbf{y} \in \mathbb{R}^n$
Ensure: Element $\mathbf{x}$ of $D_n$ closest to $\mathbf{y}$
  $\mathbf{f} = \lfloor \mathbf{y} \rceil$
  $i = \arg\max(|\mathbf{y} - \mathbf{f}|)$
  $\mathbf{g} \leftarrow \mathbf{f}$
  if $y_i - f_i \geq 0$ then                ▷ position $i$ is wrong-way rounded
      $g_i \leftarrow g_i + 1$
  else
      $g_i \leftarrow g_i - 1$
  end if
  Output:
  $\mathbf{x} = \begin{cases} \mathbf{f} & \text{if } \sum_i f_i \text{ is even} \\ \mathbf{g} & \text{if } \sum_i f_i \text{ is odd} \end{cases}$
```

Compute:

$$\mathbf{f} = \lfloor \mathbf{y} \rceil = \begin{bmatrix} 1, 3, -1, 0 \end{bmatrix} \tag{1.25}$$

$$\mathbf{g} = g(\mathbf{y}) = \begin{bmatrix} 0, 3, -1, 0 \end{bmatrix} \tag{1.26}$$

Then, $\sum_i f_i = 3$. Since the coordinate sum of **f** is odd, **g** is even. The closest point is $\mathbf{x} = \mathbf{g} = \begin{bmatrix} 0, 3, -1, 0 \end{bmatrix}$.

1.2.3 E_8 Gosset lattice

The E_8, or Gosset lattice is obtained by applying the $(8, 4)$ extended Hamming code to Construction A. It is also the union of the D_8 lattice and a shifted D_8 lattice:

$$E_8 = D_8 \cup \left(D_8 + \frac{\mathbf{1}}{\mathbf{2}} \right) \tag{1.27}$$

where $\frac{\mathbf{1}}{\mathbf{2}} = \left[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right]$. The generator matrix in canonical form is:

$$\mathbf{G} = \begin{bmatrix} 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{bmatrix}. \tag{1.28}$$

For the E_8 lattice, the squared minimum distance is $d^2_{\text{min}} = 4$, the volume is $V(\Lambda) = 1$, and the kissing number is $\tau = 240$.

The E_8 lattice is obtained by applying Construction A to the $(8, 4)$ Hamming code. We call this the $2E_8$ lattice, because it is scaled orthogonally transformed with respect

Algorithm 1.3 Quantization of E_8 Lattice

```
Require: noisy input $\mathbf{y}$ of length 8
Ensure: Element $\mathbf{x}$ of $E_8$ closest to $\mathbf{y}$
  Let $Q_{D8}$ be the quantization function for $D_8$ lattice
  $\mathbf{s} = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right)$
  $\mathbf{z}_1 = Q_{D8}(\mathbf{y})$
  $\mathbf{z}_2 = Q_{D8}(\mathbf{y} - \mathbf{s}) + \mathbf{s}$
  Output:
  $\mathbf{x} = \begin{cases} \mathbf{z}_1 & \text{if } ||\mathbf{z}_1 - \mathbf{y}||^2 \le ||\mathbf{z}_1 - \mathbf{y}||^2 \\ \mathbf{z}_2 & \text{if otherwise} \end{cases}$
```

to the canonical form (1.28). The generator matrix shows the generator matrix of the Hamming code in the first four columns :

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 2 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 2 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 2 \end{bmatrix} \tag{1.29}$$

E_8 *Quantization* Quantization of E_8 uses coset decoding, since E_8 can be written as $D_8 \cup (D_8 + \mathbf{s})$, where

$$\mathbf{s} = \left[\tfrac{1}{2}, \tfrac{1}{2}, \ldots, \tfrac{1}{2}\right]. \tag{1.30}$$

Let $Q_{D8}(\cdot)$ be the quantization function for the D_8 lattice in Algorithm 1.2. Then, the point $\mathbf{x} \in \Lambda_{E8}$ closest to $\mathbf{y} \in \mathbb{R}^8$ can be found by:

1. Find closest point in D_8 as $\mathbf{z}_1 = Q_{D8}(\mathbf{y})$ and
2. Find closest point in $D_8 + \mathbf{s}$ as $\mathbf{z}_2 = Q_{D8}(\mathbf{y} - \mathbf{s}) + \mathbf{s}$. Recall eqn. (**??**).
3. If $\mathbf{y}$ is closer to $\mathbf{z}_1$ than $\mathbf{z}_2$, then $\mathbf{z}_1$ is the point of E_8 closest to $\mathbf{y}$. Otherwise, $\mathbf{z}_2$ is closest.

Algorithm 1.3 gives these steps in detail.

1.2.4 Decoding Binary Construction A

The following is a general-purpose decoder for Construction A lattices, using a usual decoder for the binary code. This decoder is denoted $\text{Dec}(\cdot)$, and $\widehat{\mathbf{c}} = \text{Dec}(\mathbf{y})$ means the decoder finds the binary codeword $\widehat{\mathbf{c}}$ closest to $\mathbf{y} \in \mathbb{R}^n$, in the Euclidean distance sense.

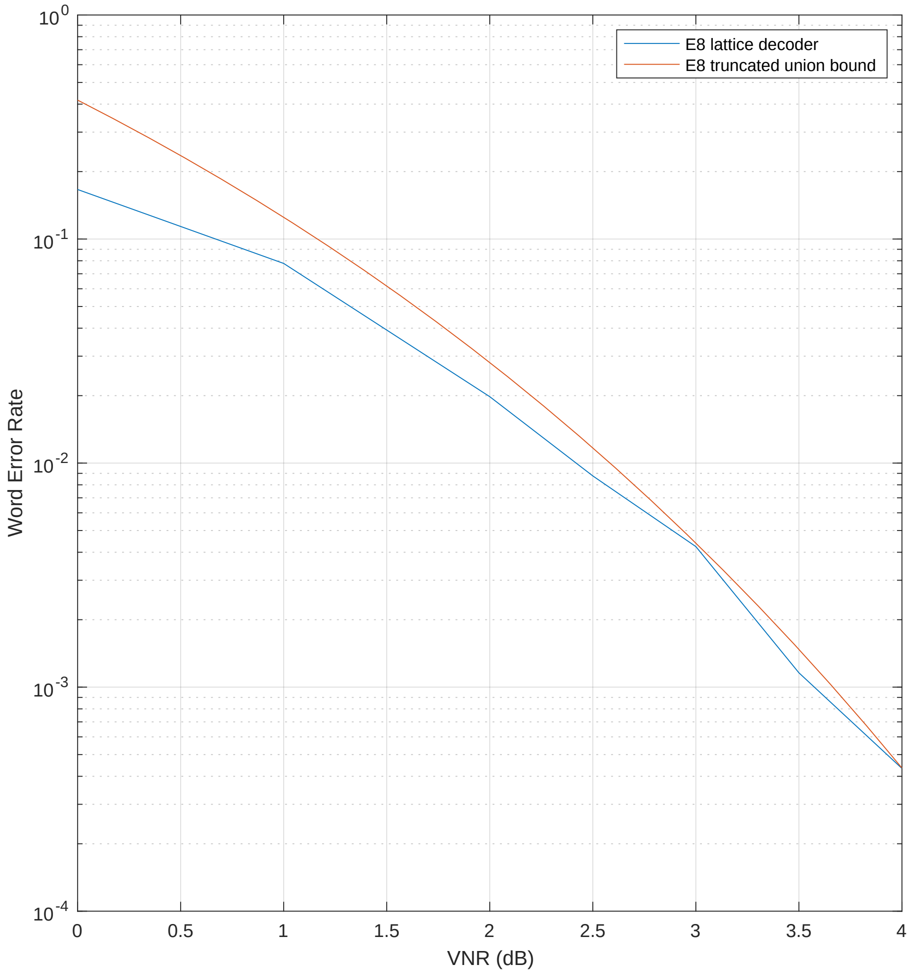

Figure 1.3: Word-error rate versus VNR for the E_8 lattice, and the truncated union bound.

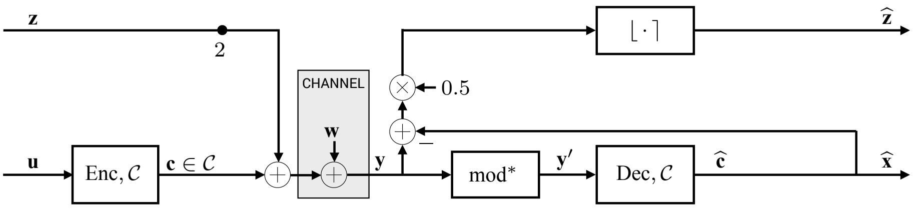

Figure 1.4: Encoder, channel and multistage decoder for Construction D and Construction D'.

Let $\mathbf{x} \in \Lambda_{\mathrm{A}}$ be transmitted over a channel so that $\mathbf{y} = \mathbf{x} + \mathbf{w}$ is received, where $\mathbf{w}$ is noise. Recall that $\mathbf{x} = \mathbf{c} + 2\mathbf{z}$, where $\mathbf{c} \in \mathcal{C}$ and $\mathbf{z} \in \mathbb{Z}^n$. If a modulo-2 operation is applied to $\mathbf{y}$:

$$\mathbf{y} \bmod 2 = \mathbf{c} + \mathbf{w}' \tag{1.31}$$

where $\mathbf{w}'$ is the noise after the modulo operation.

However, the decoder $\mathcal{C}_i$ finds the binary (0,1) codeword closest to $\mathbf{y}_i'$. Even after the modulo operation has been applied, distances to (0,1) should be preserved. The following triangle function preserves these distances[1], and performs the modulo-2 operation as well:

$$\mathrm{mod}^*(y) = \left|\mathrm{mod}_2(y+1) - 1\right|, \tag{1.32}$$

where mod_2 indicates a modulo-2 function. The triangle function is illustrated in Fig. 1.5. Conway and Sloane (page 450) described this function for decoding binary Construction A lattices in a different manner; the mod* function has the advantage it is easy to implement in software.

If the input to the decoder is LLRs, the computation differs from the standard computation since signals are from $\{0, 1\}$ and not $\{-1, +1\}$:

$$LLR \approx \frac{1 - 2y}{2\sigma^2}. \tag{1.33}$$

The above is an approximation — when z is unknown the signal before mod* is periodic, and the exact LLR is:

$$LLR = \log \frac{\sum_{z=-\infty}^{\infty} e^{-\frac{(2z-y)^2}{2\sigma^2}}}{\sum_{z=-\infty}^{\infty} e^{-\frac{(2z+1-y)^2}{2\sigma^2}}} \tag{1.34}$$

However, since all terms are close 0 except in the highest σ^2 cases, it is expected that the exact LLR has no benefit, except possibly for capacity-approaching codes.

1.3 Bibliographic Notes

Leech and Sloane describe Construction A in a 1971 paper "Sphere Packings and Error-Correcting Codes." In 1997, Loeliger shows that Construction A lattices achieve Poltyrev

[1] For example, consider noise $z = -0.1$ and transmitted symbol $x = 0$; applying mod-2 gives $y' = 1.9$. For the binary code, this is incorrectly closer to 1 than to 0. The triangle function maps 1.9 to 0.1, correctly preserving the distances to code symbols 0 and 1. The triangle function is not applicable for asymmetrical noise.

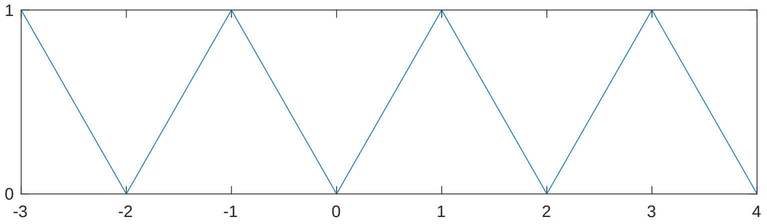

Figure 1.5: The “triangle function” is $|\mathrm{mod}_2(y+1)-1|$, and preserves distances when decoding a (0,1) binary code.

Algorithm 1.4 Decoding binary Construction A Lattice

```
Require: noisy input $\mathbf{y}$, decoder Dec$(\cdot)$ for code $\mathcal{C}$
Ensure: Construction A lattice point $\widehat{\mathbf{x}}$ nearest $\mathbf{y}$
  Compute the following:
```

$$\begin{aligned}
\mathbf{y}' &= \big|\mathrm{mod}_2(\mathbf{y}+1)-1\big| \\
\widehat{\mathbf{c}} &= \mathrm{Dec}(\mathbf{y}') \\
\mathbf{y}'' &= \frac{\mathbf{y}-\widehat{\mathbf{c}}}{2} \\
\widehat{\mathbf{z}} &= \lfloor \mathbf{y}'' \rceil \\
\widehat{\mathbf{x}} &= \widehat{\mathbf{c}} + 2\widehat{\mathbf{z}}
\end{aligned}$$

capacity. In 2012, di Pietro et al construct lattices from non-binary LDPC codes. In 2013, Tunali et al 2013 show that spatially-coupled LDPC codes are close to the Poltyrev limit. Zamir describes the generator matrix for Construction A lattices [**?**, p. 33].

For longer block length, the code C has generally high rate. When the code C is an LDPC code code rate [] Codes using high rates

1.4 Exercises

1.1 Generate a 2-dimensional lattice by applying the repeat code$\{00, 11\}$ to Construction A.

(a) Plot the lattice points within the region $[-5,5]^2$ and plot the Voronoi region.

(b) Using the Construction A decoder, decode $\mathbf{y} = [-3.2, 3.9]$ to the nearest lattice point (use a soft-input decoder for the repeat code).

(c) Randomly generate a large number of samples of $\mathbf{y}$, compute the modulo value $\mathbf{x}_0$ for each one by:

$$\mathbf{x}_0 = \mathbf{y} - Q_\Lambda(\mathbf{y}). \tag{1.35}$$

Make a plot of all $\mathbf{x}_0$, and they should be inside the 0-centered Voronoi region.

(d) Using a large number of $N = 10^5$ samples, estimate the normalized second moment.