Lecture 3: encoding and decoding with linear codes

Let $C \leq \mathbb{Z}_2^n$ be a linear code. By Lagrange's theorem $|C| \mid 2^n$. Thus $|C| = 2^k$ for some $1 \leq k \leq n$.

The rate of such a code is $\frac{k}{n}$.

k is the dimension of C

To describe a non-linear code, we have to list all its codewords. To describe a linear code, it is enough to list the elements of a basis.

If $C \leq \mathbb{Z}_2^n$ is a k-dimensional code, a $k \times n$ matrix whose rows form a basis for C is called a generator matrix of the code. If G is such a matrix then we may define the encoding function from messages to codewords $\mathbb{Z}_2^k \to \mathbb{Z}_2^n$ by

$$\underline{u} \longmapsto \underline{u}G.$$

Observe that $\underline{u}G$ is simply a linear combination of the rows of G and so belongs to the code whose basis is G

<u>Example</u> Let $C = \{0000, 1100, 0011, 1111\}$.

We first show that C is a linear code.

	0000	1100	0011	1111
0000	—	1100	0011	1111
1100		—	1100	0011
0011			—	1100
1111				—

Next we find a basis. There are a number to choose from. The set $\{1100, 0011\}$ works since every element of C can be written $\alpha(1100) + \beta(0011)$ for some $\alpha, \beta \in \mathbb{Z}_2$.

Thus a possible generator matrix is

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

This defines an encoding function $\mathbb{Z}_2^2 \longrightarrow \mathbb{Z}_2^4$ by

$\underline{u} \longmapsto \underline{u}\, G$.

message	codeword
00	0000
10	1100
01	0011
11	1111

We shall now turn to the question of how to decode linear codes. To explain how, I shall need some new ideas.

Let $\underline{u}, \underline{v} \in \mathbb{Z}_2^n$. We define the <u>inner product</u> of $\underline{u}$ and $\underline{v}$, denoted by $\underline{u} \cdot \underline{v}$, to be

$$\underline{u} \cdot \underline{v} = u_1 v_1 + \dots + u_n v_n$$

where $\underline{u} = (u_1, \dots, u_n)$ and $\underline{v} = (v_1, \dots, v_n)$.

<u>Lemma 1</u>

(i) $\underline{u} \cdot \underline{v} = \underline{v} \cdot \underline{u}$.

(ii) $(\underline{u} + \underline{v}) \cdot \underline{w} = \underline{u} \cdot \underline{w} + \underline{v} \cdot \underline{w}$

If $\underline{u} \cdot \underline{v} = 0$, we say that $\underline{u}$ and $\underline{v}$ are <u>ortogonal</u>.

Let $C \leqslant \mathbb{Z}_2^n$ be a k-dimensional linear code.

The <u>dual code</u> of C is

$$C^{\perp} = \{ \underline{v} \in \mathbb{Z}_2^n : \ \underline{v} \cdot \underline{u} = 0 \ \forall \underline{u} \in C \}$$

__Theorem 2__ $C^\perp \leqslant \mathbb{Z}_2^n$ is a linear code with dimension $n-k$.

__Proof__

$\underline{v} \in C^\perp \iff \underline{v}$ is orthogonal to every vector in C

$\iff \underline{v}$ is orthogonal to every vector in a basis for C

$\iff \underline{v}\, G^T = \underline{0}$

G^T = the transpose of G

$\iff G\, \underline{v}^T = \underline{0}$.

Let $C' = \{ \underline{v}^T : G\underline{v}^T = \underline{0} \}$.

Then $\underline{v} \in C^\perp \iff \underline{v}^T \in C'$.

It is clear that C' is a subspace of $\mathbb{Z}_2^n$ where the elements are regarded as __column__ vectors.

Thus $C^\perp$ is a __linear__ code.

$$\dim(C') = \dim(\text{nullspace } G)$$
$$= n - \text{rank}(G)$$
$$= n-k \quad (\text{since rows of } G \text{ are lin. indep})$$

by the Rank-Nullity Theorem ■

A <u>parity check matrix</u> H for the linear code C is a generator matrix for the linear code $C^\perp$.

To calculate H given G: find a basis $\underline{v}_1^T, \ldots, \underline{v}_{n-k}^T$ for the nullspace of G. Put

$$H = \begin{pmatrix} \longleftarrow & \underline{v}_1 & \longrightarrow \\ & \vdots & \\ \longleftarrow & \underline{v}_{n-k} & \longrightarrow \end{pmatrix}.$$

Observe that $\underline{x} \in C \iff H\underline{x}^T = \underline{0}$.

<u>Example</u> A linear code has a generator matrix

$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. We shall find a parity check matrix for this code.

We have to solve the equations

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\therefore \quad x_1 + x_3 + x_4 = 0$$
$$x_2 + x_4 + x_5 = 0.$$

The free variables are x_3, x_4 and x_5.

Let $x_3 = \alpha$, $x_4 = \beta$, $x_5 = \gamma$ where $\alpha, \beta, \gamma \in \mathbb{Z}_2$.

Then

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} \alpha + \beta \\ \beta + \gamma \\ \alpha \\ \beta \\ \gamma \end{pmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_2 \right\}$$

$$= \left\{ \alpha \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_2 \right\}$$

Thus we may put

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Which is a parity check matrix for our code.

We have shown how to construct the parity check matrix, we now have to show how it can be used to help us decode received vectors.

We shall now see how the parity check matrix of a linear code can be used in decoding.

Let $C \subseteq \mathbb{Z}_2^n$ be a linear code.

We suppose that $\mathbb{Z}_2^k \to \mathbb{Z}_2^n$ is given by $\underline{u} \longmapsto \underline{u}G$ where G is the generator matrix.

Let H be the parity check matrix.

Then $\underline{x} \in C \iff H\underline{x}^T = \underline{0}$.

Let $\underline{x} \in C$ be transmitted and let $\underline{y}$ be received.

Then $\underline{y} - \underline{x} = \underline{e}$ is called the <u>error vector</u>.

Thus $\underline{y} = \underline{x} + \underline{e}$.

<u>Lemma 3</u> $H\underline{y}^T = H\underline{e}^T$.

<u>Proof</u> $H\underline{y}^T = H(\underline{x}^T + \underline{e}^T) = H\underline{x}^T + H\underline{e}^T$
$= \underline{0} + H\underline{e}^T$
$= H\underline{e}^T$. ∎

$H\underline{y}^T$ is called the <u>syndrome of $\underline{y}$</u> and depends *only* on the error vector $\underline{e}$.

Theorem 4 (Decoding linear codes using the parity check matrix).

Let C be a t-error correcting code. $C \subseteq \mathbb{Z}_2^n$

Let $\underline{e}_1, \ldots, \underline{e}_s$ be all possible vectors in $\mathbb{Z}_2^n$ with weights $\leq t$.

Then all the vectors $H\underline{e}_1, \ldots, H\underline{e}_s$ are different.

Proof Let $\underline{e}_1$ and $\underline{e}_2$ be two vectors each of whose weights $\leq t$. Suppose $\underline{e}_1 \neq \underline{e}_2$, but suppose that $H\underline{e}_1^T = H\underline{e}_2^T$.

Then $H(\underline{e}_1 - \underline{e}_2)^T = \underline{0}$. It follows that $\underline{e}_1 - \underline{e}_2 = \underline{e}_1 + \underline{e}_2 \in C$. We shall now use the result that $w(\underline{x}+\underline{y}) \leq w(\underline{x}) + w(\underline{y})$.

Thus $w(\underline{e}_1 + \underline{e}_2) \leq w(\underline{e}_1) + w(\underline{e}_2) \leq t+t = 2t < d$

which contradicts the fact that the min. weight of an element of C will be d. ■

The result we used above

$$w(\underline{x}+\underline{y}) \leq w(\underline{x}) + w(\underline{y})$$

follows easily:

$$d(\underline{x}+\underline{y}, \underline{0}) \leq d(\underline{x}+\underline{y}, \underline{y}) + d(\underline{y}, \underline{0})$$
$$\qquad\qquad\qquad\qquad\qquad\qquad \shortparallel$$
$$\qquad\qquad\qquad\qquad\qquad\qquad d(\underline{x}, \underline{0}) + d(\underline{y}, \underline{0}).$$

Observe that

$$d(\underline{u}, \underline{v}) = d(\underline{u}+\underline{z}, \underline{v}+\underline{z}).$$

<u>Remark</u> $H\underline{e}^T$ = sum of columns of H

- corresponding to the non-zero elements of $\underline{e}$
- corresponding to the bits in the received vector that were corrupted.