Introduction to Linear Block Codes

Talk at B. K. Birla College, Kalyan

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

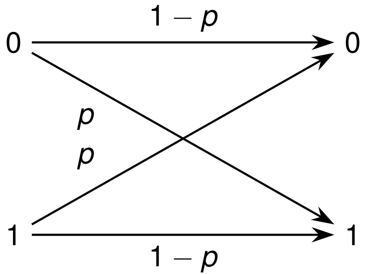
Department of Electrical Engineering
Indian Institute of Technology Bombay

March 8, 2025

Error Correction

The Setting

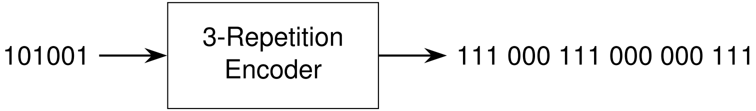
- A transmitter wishes to communicate a string of bits to a receiver
  - For example, a transmitter may wish to send the string 1010
- The transmission occurs over a noisy channel which flips each bit with a probability $p < \frac{1}{2}$



- The transmitter adds redundancy to the transmitted message to correct errors

3-Repetition Code

- Each message bit is repeated 3 times



- How many errors can it correct?
- How many errors can the following code correct?

$$0 \to 101, 1 \to 010$$

- What about this code?

$$0 \to 101, 1 \to 110$$

- **Takeaway**: Error correcting capability depends on the distance between the codewords

Issues with Repetition Coding

- The 3-repetition code cannot correct more than one error
- To correct two errors, we can use a 5-repetition code
- To correct three errors, we can use a 7-repetition code
- But this increases the number of redundancy bits sent
- Can we do better?

Binary Block Codes

Binary Block Code

Let $\mathbb{F}_2$ be the set $\{0, 1\}$.

Definition

An (n, k) binary block code is a subset of $\mathbb{F}_2^n$ containing 2^k elements

Example

$n = 3$, $k = 1$, $C = \{000, 111\}$

Example

$n \geq 2$, C = Set of vectors of **even Hamming weight** in $\mathbb{F}_2^n$
$k = n - 1$
$n = 3$, $k = 2$, $C = \{000, 011, 101, 110\}$
This code is called the **single parity check code**

Definition

The **rate** of an (n, k) binary block code is $\frac{k}{n}$

Encoding Binary Block Codes

The encoder maps k-bit information blocks to codewords.

Definition

An encoder for an (n, k) binary block code C is an injective function from $\mathbb{F}_2^k$ to C

Example (3-Repetition Code)

$0 \to 000, 1 \to 111$
or
$1 \to 000, 0 \to 111$

Decoding Binary Block Codes

The decoder maps n-bit received blocks to codewords

Definition

A decoder for an (n, k) binary block code is a function from $\mathbb{F}_2^n$ to C

Example (3-Repetition Code)

$n = 3$, $C = \{000, 111\}$

$$
\begin{array}{ll}
000 \to 000 & 111 \to 111 \\
001 \to 000 & 110 \to 111 \\
010 \to 000 & 101 \to 111 \\
100 \to 000 & 011 \to 111
\end{array}
$$

Since encoding is injective, information bits can be recovered as $000 \to 0, 111 \to 1$

Optimal Decoder for Binary Block Codes

- **Optimality criterion**: Maximum probability of correct decision
- Let $\mathbf{x} \in C$ be the transmitted codeword
- Let $\mathbf{y} \in \mathbb{F}_2^n$ be the received vector
- Maximum a posteriori (MAP) decoder is optimal

$$\hat{\mathbf{x}}_{MAP} = \text{argmax}_{\mathbf{x} \in C} \Pr(\mathbf{x}|\mathbf{y})$$

- Over a BSC with $p < \frac{1}{2}$, the minimum distance decoder is optimal if the codewords are equally likely

$$\hat{\mathbf{x}} = \text{argmin}_{\mathbf{x} \in C} d(\mathbf{x}, \mathbf{y})$$

Error Correction Capability of Binary Block Codes

Definition

The **minimum distance** of a block code C is defined as

$$d_{min} = \min_{\mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y})$$

Example (3-Repetition Code)

$C = \{000, 111\}$, $d_{min} = 3$

Example (Single Parity Check Code)

C = Set of vectors of even weight in $\mathbb{F}_2^n$, $d_{min} = 2$

Theorem

For a binary block code with minimum distance d_{min}, the minimum distance decoder can correct upto $\lfloor \frac{d_{min}-1}{2} \rfloor$ errors.

Complexity of Encoding and Decoding

Encoder

- Map from $\mathbb{F}_2^k$ to C
- Worst case storage requirement = $O(n2^k)$

Decoder

- Map from $\mathbb{F}_2^n$ to C
- $\hat{\mathbf{x}}_{ML} = \operatorname{argmax}_{\mathbf{x} \in C} \Pr(\mathbf{y}|\mathbf{x})$
- Worst case storage requirement = $O(k2^n)$
- Time complexity = $O(n2^k)$

Need more structure to reduce complexity

Binary Linear Block Codes

Vector Spaces

Let V be a set with a binary operation $+$ (addition) defined on it. Let F be a field. Let a multiplication operation, denoted by $\cdot$, be defined between elements of F and V. The set V is called a **vector space** over F if

- V is a commutative group under addition
- For any $a \in F$ and $\mathbf{v} \in V$, $a \cdot \mathbf{v} \in V$
- For any $\mathbf{u}, \mathbf{v} \in V$ and $a, b \in F$

$$\begin{aligned} a \cdot (\mathbf{u} + \mathbf{v}) &= a \cdot \mathbf{u} + b \cdot \mathbf{v} \\ (a + b) \cdot \mathbf{v} &= a \cdot \mathbf{v} + b \cdot \mathbf{v} \end{aligned}$$

- For any $\mathbf{v} \in V$ and $a, b \in F$

$$(ab) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$$

- Let 1 be the unit element of F. For any $\mathbf{v} \in V$, $1 \cdot \mathbf{v} = \mathbf{v}$

Vector Spaces over $\mathbb{F}_2$

- Define the following operations on $\mathbb{F}_2$
- Addition $+$
  - $0 + 0 = 0$
  - $0 + 1 = 1$
  - $1 + 0 = 1$
  - $1 + 1 = 0$
- Multiplication $\times$
  - $0 \times 0 = 0$
  - $0 \times 1 = 0$
  - $1 \times 0 = 0$
  - $1 \times 1 = 1$
- $\mathbb{F}_2$ is a field

Fact

The set $\mathbb{F}_2^n$ is a vector space over $\mathbb{F}_2$

Binary Linear Block Code

Definition

An (n, k) binary linear block code is a k-dimensional subspace of $\mathbb{F}_2^n$

Theorem

Let S be a nonempty subset of $\mathbb{F}_2^n$. Then S is a subspace of $\mathbb{F}_2^n$ if $\mathbf{u} + \mathbf{v} \in S$ for any two $\mathbf{u}$ and $\mathbf{v}$ in S.

Example (3-Repetition Code)

$C = \{000, 111\} \neq \phi$

$000 + 000 = 000$, $000 + 111 = 111$, $111 + 111 = 000$

Example (Single Parity Check Code)

C = Set of vectors of even weight in $\mathbb{F}_2^n$

$\mathrm{wt}(\mathbf{u} + \mathbf{v}) = \mathrm{wt}(\mathbf{u}) + \mathrm{wt}(\mathbf{v}) - 2\,\mathrm{wt}(\mathbf{u} \cap \mathbf{v})$

Encoding Binary Linear Block Codes

Definition

A generator matrix for a k-dimensional binary linear block code C is a $k \times n$ matrix $\mathbf{G}$ whose rows form a basis for C.

Linear Block Code Encoder

Let $\mathbf{u}$ be a $1 \times k$ binary vector of information bits. The corresponding codeword is

$$\mathbf{v} = \mathbf{uG}$$

Example (3-Repetition Code)

$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$

$$\begin{aligned} \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} &= \begin{bmatrix} 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} &= \begin{bmatrix} 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \end{aligned}$$

Encoding Binary Linear Block Codes

Example (Single Parity Check Code)

$n = 3$, $k = 2$, $C = \{000, 011, 101, 110\}$

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\begin{aligned}
\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \\
\begin{bmatrix} 0 & 1 & 1 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \\
\begin{bmatrix} 1 & 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \\
\begin{bmatrix} 1 & 1 & 0 \end{bmatrix} &= \begin{bmatrix} 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}
\end{aligned}$$

Encoding Complexity of Binary Linear Block Codes

- Need to store **G**
- Storage requirement = $O(nk) \ll O(n2^k)$
- Time complexity = $O(nk)$
- Complexity can be reduced further by imposing more structure in addition to linearity
- Decoding complexity? What is the optimal decoder?

Decoding Binary Linear Block Codes

- Equally likely codewords and channel is BSC $\Rightarrow$ Minimum distance decoder is optimal

$$\hat{\mathbf{x}}_{ML} = \text{argmin}_{\mathbf{x} \in C} d(\mathbf{x}, \mathbf{y})$$

- To exploit linear structure to reduce decoding complexity, we need to study the **dual code**

Inner Product of Vectors in $\mathbb{F}_2^n$

Definition

Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$ belong to $\mathbb{F}_2^n$. The inner product of **u** and **v** is given by

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i$$

$\mathbf{u} \cdot \mathbf{v} = 0 \Rightarrow$ **u** and **v** are orthogonal.

Examples

- $\begin{pmatrix}1 & 0 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & 1 & 1\end{pmatrix} = 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 1 = 0$
- $\begin{pmatrix}1 & 1 & 0\end{pmatrix} \cdot \begin{pmatrix}0 & 1 & 1\end{pmatrix} = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 1$
- $\begin{pmatrix}1 & 1 & 1\end{pmatrix} \cdot \begin{pmatrix}0 & 1 & 1\end{pmatrix} = 1 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0$
- $\begin{pmatrix}0 & 1 & 1\end{pmatrix} \cdot \begin{pmatrix}0 & 1 & 1\end{pmatrix} = 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 1 = 0$

Nonzero vectors can be self-orthogonal

Dual Code of a Linear Block Code

Definition

Let C be an (n, k) binary linear block code. Let $C^\perp$ be the set of vectors in $\mathbb{F}_2^n$ which are orthogonal to all the codewords in C.

$$C^\perp = \left\{ \mathbf{u} \in \mathbb{F}_2^n \middle| \ \mathbf{u} \cdot \mathbf{v} = 0 \ \text{ for all } \ \mathbf{v} \in C \right\}$$

$C^\perp$ is a linear block code and is called the **dual code** of C.

Example (3-Repetition Code)

$C = \{000, 111\}$, $C^\perp = ?$

$$\begin{array}{ll} 000 \cdot 111 = 0 & 111 \cdot 111 = 1 \\ 001 \cdot 111 = 1 & 110 \cdot 111 = 0 \\ 010 \cdot 111 = 1 & 101 \cdot 111 = 0 \\ 100 \cdot 111 = 1 & 011 \cdot 111 = 0 \end{array}$$

$C^\perp = \{000, 011, 101, 110\}$ = Single Parity Check Code

Dimension of the Dual Code

Example (3-Repetition Code and SPC Code)

$C = \{000, 111\}$, $\dim C = 1$
$C^{\perp} = \{000, 011, 101, 110\}$, $\dim C^{\perp} = 2$
$\dim C + \dim C^{\perp} = 1 + 2 = 3$

Theorem

$\dim C + \dim C^{\perp} = n$

Corollary

C is an (n, k) binary linear block code $\Rightarrow$ $C^{\perp}$ is an $(n, n-k)$ binary linear block code

Parity Check Matrix of a Code

Definition

Let C be an (n, k) binary linear block code and let $C^\perp$ be its dual code. A generator matrix $\mathbf{H}$ for $C^\perp$ is called a parity check matrix for C.

Example (3-Repetition Code)

$C = \{000, 111\}$
$C^\perp = \{000, 011, 101, 110\}$

A generator matrix of $C^\perp$ is $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

$\mathbf{H}$ is a parity check matrix of C.

Parity Check Matrix Completely Describes a Code

Theorem

Let C be a linear block code with parity check matrix $\mathbf{H}$. Then

$$\mathbf{v} \in C \iff \mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$$

Example (3-Repetition Code)

$C = \{000, 111\}$, $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

Forward direction: $\mathbf{v} \in C \Rightarrow \mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \end{bmatrix}$$

Parity Check Matrix Completely Describes a Code

Theorem

Let C be a linear block code with parity check matrix **H**. *Then*

$$\mathbf{v} \in C \iff \mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$$

Example (3-Repetition Code)

$C = \{000, 111\}$, $\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

Reverse direction: $\mathbf{v} \in C \Leftarrow \mathbf{v} \cdot \mathbf{H}^T = \mathbf{0}$

$$\mathbf{v} \cdot \mathbf{H}^T = \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} v_1 + v_3 & v_2 + v_3 \end{bmatrix}$$

$$\begin{aligned} \mathbf{v} \cdot \mathbf{H}^T = \mathbf{0} \quad &\Rightarrow \quad v_1 + v_3 = 0, v_2 + v_3 = 0 \\ &\Rightarrow \quad v_1 = v_3, v_2 = v_3 \Rightarrow v_1 = v_2 = v_3 \end{aligned}$$

Decoding Binary Linear Block Codes

- Let a codeword $\mathbf{x}$ be sent through a BSC to get $\mathbf{y}$,

$$\mathbf{y} = \mathbf{x} + \mathbf{e}$$

  where $\mathbf{e}$ is the error vector

- The probability of observing $\mathbf{y}$ given $\mathbf{x}$ was transmitted is given by

$$\begin{aligned}
\Pr(\mathbf{y}|\mathbf{x}) &= p^{d(\mathbf{x},\mathbf{y})}(1-p)^{n-d(\mathbf{x},\mathbf{y})} \\
&= p^{\mathrm{wt}(\mathbf{e})}(1-p)^{n-\mathrm{wt}(\mathbf{e})} \\
&= (1-p)^n \left(\frac{p}{1-p}\right)^{\mathrm{wt}(\mathbf{e})}
\end{aligned}$$

- If $p < \frac{1}{2}$, lower weight error vectors are more likely

Decoding Binary Linear Block Codes

- Optimal decoder is given by

$$\begin{aligned}\hat{\mathbf{x}}_{ML} &= \text{argmin}_{\mathbf{x}\in C} d(\mathbf{x}, \mathbf{y}) \\ &= \mathbf{y} + \hat{\mathbf{e}}_{ML}\end{aligned}$$

  where $\hat{\mathbf{e}}_{ML}$ = Most likely error vector such that $\mathbf{y} + \mathbf{e} \in C$.
- $\mathbf{y} + \mathbf{e} \in C \iff (\mathbf{y} + \mathbf{e}) \cdot \mathbf{H}^T = \mathbf{0} \iff \mathbf{e} \cdot \mathbf{H}^T = \mathbf{y} \cdot \mathbf{H}^T$
- If $\mathbf{s} = \mathbf{y} \cdot \mathbf{H}^T$, the most likely error vector is

$$\hat{\mathbf{e}}_{ML} = \underset{\mathbf{e}\in\mathbb{F}_2^n, \mathbf{e}\cdot\mathbf{H}^T = \mathbf{s}}{\text{argmin}} \ \text{wt}(\mathbf{e})$$

- Time complexity = $O\left(n2^k\right)$
- For each $\mathbf{s}$, the $\hat{\mathbf{e}}_{ML}$ can be precomputed and stored
- $\mathbf{s}$ is $1 \times n - k$ binary vector $\Rightarrow$ Storage required is $O(n2^{n-k})$

Summary

General Block Codes

- Encoding = $O(n2^k)$
- Decoding = $O(n2^k)$

Linear Block Codes

- Encoding = $O(nk)$
- Decoding = $O(n2^k)$

Observations

- Linear structure in codes reduces encoding complexity
- Decoding complexity is still exponential
- Need for codes with low complexity decoders

Thanks for your attention!

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in