Linear Block Codes

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

July 28, 2014

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

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

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

- If all codewords are equally likely to be transmitted, then maximum likelihood (ML) decoder is optimal

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

- 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
- $\hat{\mathbf{x}}_{ML} = \text{argmax}_{\mathbf{x} \in C} \Pr(\mathbf{y}|\mathbf{x})$
- Worst case storage requirement = $O(n2^k)$
- Time complexity = $O(n2^k)$

Need more structure to reduce complexity