



Chapter 4. Error Correction Codes

Block Codes

Convolutional Codes

Each k input symbols are mapped into n output symbols
 $n > k$, $\frac{k}{n}$ is the code rate

To see the relationship of block codes and convolutional codes, let us consider real sequences.

$x(l)$: input $\rightarrow$ serial to parallel $\rightarrow k$ subsequences
 $y(l)$: output $\xrightarrow{\text{convolution}}$ $x:(l)$

Let $z_i(l)$ be the z -transform of $x_i(l)$.

$$Y(l) = \begin{pmatrix} Y_1(l) \\ \vdots \\ Y_k(l) \end{pmatrix} = (Z_1(l) \cdots Z_k(l)) \underbrace{\begin{bmatrix} G_{11}(l) & \cdots & G_{1n}(l) \\ G_{21}(l) & \cdots & G_{2n}(l) \\ \vdots & \ddots & \vdots \\ G_{k1}(l) & \cdots & G_{kn}(l) \end{bmatrix}}_{\text{Generator matrix}}$$

$$Y_i(l) = \sum_{j=1}^k Z_j(l) G_{ji}(l)$$

$G(l)$: Generator matrix

When $G(l)$ is an k by N constant matrix, it is called a block code (without memory), otherwise it is a convolutional code (with memory).



Difference between block & convolutional codes

Block codes: $\checkmark$ rates are usually large ($R_c = \frac{k}{n} > \frac{1}{2}$)

$\checkmark$ Sizes are usually large

$\checkmark$ They are hard to search by computers

BCH codes
 $\checkmark$ Decoding algorithms are usually fast (hard decoding) but suboptimal.

RS codes
 $\checkmark$ good for high SNR applications, such as recording systems.

$\checkmark$ good for burst errors

$\checkmark$ Soft decoding is not simple comparing to hard decoding

Convolutional codes
 $\checkmark$ Rates are usually small, ($\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\dots$)

$\checkmark$ Sizes are usually small ($n=3, k=1, \dots$)

$\checkmark$ Optimal codes can be searched by computers

$\checkmark$ Decoding is usually slow but optimal (Viterbi, etc.)

$\checkmark$ Good for low SNR applications (wireless)

$\checkmark$ Not good for burst errors

$\checkmark$ Soft decoding is simple comparing to



Error correction codes are usually defined on finite fields (Galois fields). The simplest example is binary field $\{0, 1\}$.

Why do we need finite fields?

§4-1. Block codes

Map k dimensional vectors into n dimensional vectors that are called codewords and the code is called an (n, k) block code.

An important measure for a code is the minimum distance.

Let c_i and c_j be two codewords in an (n, k) block code. Their Hamming distance is defined as the number of corresponding elements in which they differ.

$$\begin{array}{ll} \text{Ex: } c_1: 11010 & \Rightarrow H(c_1, c_2) = 3 \\ c_2: 10111 & \end{array}$$

The minimum distance $d_{\min}$ of an (n, k) block code is defined as the minimum Hamming distance of all two different codewords in the code

$$\begin{array}{ll} 4 \{ 11010 \}_2 & \\ 4 \{ 01011 \}_2 & \Rightarrow d_{\min} = 2 \\ 4 \{ 10101 \}_2 & \end{array}$$



§4-1-10 Linear block codes

An (n, k) linear block code linearly map all k dimensional vector into n dimensional vectors over the same field, i.e., any codeword can be generated by multiplying a k dimensional vector to the same $k \times n$

matrix: $\underline{y} = \underline{x} \underline{G}$ row operations

where $\underline{y} = (y_1, \dots, y_n)$, $\underline{x} = (x_1, \dots, x_k)$

$$\underline{G} = \begin{pmatrix} g_{11} & \dots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{k1} & \dots & g_{kn} \end{pmatrix}$$

- * Row operation on $\underline{G}$ do not change the code.
- * Column permutations on $\underline{G}$: only permute the components of the codewords and therefore basically don't change the code either.

$\Rightarrow$ A generator matrix $\underline{G}$ can be reduced by row operations and column permutations to the "system form":

$$\underline{G} = [\underline{I}_k \mid \underline{P}] = \begin{bmatrix} 1 & 0 & \dots & 0 & | & p_{11} & \dots & p_{1n-k} \\ 0 & 1 & \dots & 0 & | & p_{21} & \dots & p_{2n-k} \\ \vdots & \vdots & \ddots & \vdots & | & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & | & p_{k1} & \dots & p_{kn-k} \end{bmatrix}$$

information symbols
parity symbols



An (n, k) linear block code with the above systematic generator matrix is called a systematic code. For a systematic code, the first k symbols (bits) are the information symbols (bits) and the rest $n-k$ symbols (bits) are the linear combinations of the k information symbols (bits).

A generator matrix is called equivalent to a generator matrix of the systematic form if one can be obtained from the other by elementary row operations and column permutations.

The two (n, k) linear block codes generated by two equivalent generator matrices are called equivalent, and one can be obtained from another by a permutation of the places of every element.

Every linear (n, k) code is equivalent to a linear systematic (n, k) code.

Example

$$G = \begin{bmatrix} 11101 \\ 01110 \\ 10111 \end{bmatrix}$$

$$\text{row 1} + \text{row 3} \quad \begin{bmatrix} 11101 \\ 01110 \\ 11101 \end{bmatrix}$$



$$\rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Associated with any linear (n, k) code is the dual code of dimension $n-k$. The dual code is a linear $(n, n-k)$ code, which is the null space of the (n, k) code.

Let H denote the generator matrix of the dual code of C . Then $GH' = 0$ when H' is the transpose of H .

Assume $G = [I_k \mid P]$

Then, the dual code

$$H = [-P' \mid I_{n-k}]$$

Ex:

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

$$\Rightarrow H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

H is called parity matrix.

An ~~any~~ vector $\mathbf{r}$ is a codeword of the code G iff $\mathbf{r}H' = 0$

no other check



For a received ~~vector~~ ^{rxn} vector r ,

its syndrome: $S \triangleq r \cdot H'$

r is a codeword $\iff$ its syndrome $S=0$

The syndrome S of r is caused purely by the error.

Let $r = c + e$ with a codeword c and error vector e . Then

$$S = (c + e)H' = cH' + eH' = \underline{eH'}$$

We now consider binary linear block codes

A. Minimum distance d_{min}

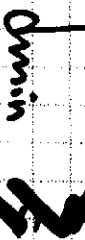
Consider an (n, k) linear block code C . There are 2^k codewords. Let its minimum distance d_{min} is reached by two codewords c_1 and c_2 , i.e., there are d_{min} positions in c_1 and c_2 that are different. (cand only)

Consider the new codeword $c = c_1 + c_2$ (linear)

Clearly $d_{min} = \underline{\text{the weight of } c}$

$\hookrightarrow$ the number of 1's in c .

Thus



the minimum weight of all



Let $\underline{c}_0$ be the codeword with the minimum weight w .

Consider $\underline{c}_0$ and $\underline{0} = (0, 0, \dots, 0)$. Then the Hamming distance between $\underline{c}_0$ and $\underline{0}$ is w .

$$\Rightarrow d_{\min} \leq w.$$

$\Rightarrow$ $d_{\min}$ is the minimum weight of all nonzero codewords.

Thm. Let $\mathcal{C}$ be a linear code with parity-check matrix H . The minimum weight (or the minimum distance) of $\mathcal{C}$ is equal to the smallest number of columns of H that sum to $\underline{0}$.

Ex:

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

$$\Rightarrow H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Consider all sums of two different columns, which are clearly not zero

Consider all the sum of three different columns,



B. Error-detecting and Error-Correcting Capabilities of a block code

Let $\mathcal{C}$ be a linear block code with minimum distance $d_{\min}$. It means that any two distinct codewords of $\mathcal{C}$ differ in at least $d_{\min}$ places. Thus, no error pattern of $d_{\min} - 1$ or fewer errors can change one codeword to another codeword

$$c_1 + e \neq c_2 \quad \text{as long as } |e| \leq d_{\min} - 1$$

Hamming weight

This implies that any error pattern of $d_{\min} - 1$ or fewer errors will result in a received vector $\mathbf{r}$ that is not a codeword in $\mathcal{C}$.

When the receiver detects that the received vector is not a codeword of $\mathcal{C}$, we say that errors are detected.

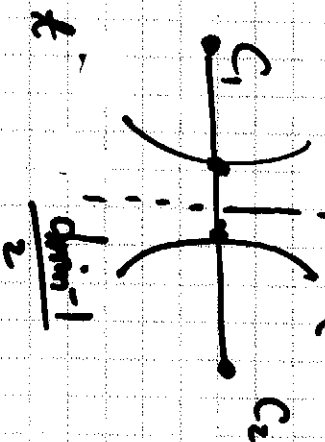
Using the syndrome detection, any error pattern of $d_{\min} - 1$ or fewer errors can be detected.

Thus,

* For minimum distance d_{min} , the error detection capability is $d_{min} - 1$.

(dmin errors can not be detected because there is at least a pair of codewords that differ dmin positions).

* The error-correction capability is $\left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$



$$2t+1 \leq d_{\min}$$

C. Standard Array and Syndrome Decoding

Consider an (n, k) linear code and let $C_1, \dots, C_k$ be all the codewords.

The received vector $\underline{r} = \underline{C} + \underline{e}$ is one of 2^n binary $n \times 1$ vectors.

Any decoding scheme used at the receiver is a rule to partition all the 2^n possible received vectors into 2^k distinct subsets $D_1, D_2, \dots, D_{2^k}$ such that the



$$D_i \leftrightarrow C_i$$



One-to-one

Correspondence

Then: $r \in D_i \Leftrightarrow r$ is decoded as C_i

↑
decoding rule

Correct decoding is made iff the received vector r is in the subset D_i that corresponds to the actual codeword transmitted.

Standard array is one of the partition methods

Step 1: The 2^k codewords of $\mathcal{C}$ are placed in a row with all-zero codeword $C_1 = (0, \dots, 0)$ at the first element.

Step 2: From the remaining $2^n - 2^k$ $n \times 1$ vectors (n -tuples), an $n \times 1$ vector E_2 is chosen and is placed under the zero vector $C_1 = \underline{0}$. Form a second row by adding E_2 to each codeword C_i in the first row and placing the sum



Steps: From the remainings (un used) $n \times 1$ vectors, $\underline{e}_3$ is chosen and is placed under $\underline{e}_2$. Then similarly the third row can be formed.

Step 4: Continue this process until all $n \times 1$ vectors are used.

Standard Array

$$\begin{array}{ccccccc}
 \underline{e}_{20} & \underline{e}_2 & \dots & \underline{e}_i & \dots & \underline{e}_{2k} & \leftarrow \text{rows are} \\
 \underline{e}_2 & \underline{e}_2 + \underline{e}_2 & \dots & \underline{e}_i + \underline{e}_2 & \dots & \underline{e}_{2k} + \underline{e}_2 & \leftarrow \text{called} \\
 \underline{e}_3 & \underline{e}_2 + \underline{e}_3 & \dots & \underline{e}_i + \underline{e}_3 & \dots & \underline{e}_{2k} + \underline{e}_3 & \leftarrow \underline{\text{cosets}} \\
 \vdots & \vdots & & \vdots & & \vdots & \leftarrow \underline{e}_j \text{ are} \\
 \vdots & \vdots & & \vdots & & \vdots & \text{called} \\
 \vdots & \vdots & & \vdots & & \vdots & \underline{\text{coset}} \\
 \underline{e}_{2nt} & \underline{e}_2 + \underline{e}_{2nt} & \dots & \underline{e}_i + \underline{e}_{2nt} & \dots & \underline{e}_{2k} + \underline{e}_{2nt} & \leftarrow \underline{\text{leaders}}
 \end{array}$$

* No two $n \times 1$ vectors in the same row of a standard array are identical. ? (Homework)
 * Every $n \times 1$ vector appears in one and only one row.

usually
 with
 least
 number
 of
 cosets



A standard array of an (n, k) linear code $\mathcal{C}$ consists of q^k distinct columns. Each column consists of q^{n-k} $n \times 1$ vectors with the topmost one as a codeword in $\mathcal{C}$.

Let $\mathcal{Q}_j = \{c_i, c_{i+q}, \dots, c_{i+q^{n-k}}\}$,
 the j th column in a standard array.

$\{\mathcal{Q}_j, j=1, 2, \dots, 2^k\}$ forms a partition of $n \times 1$ vectors, which can be used as a decoding rule.

Thus, the received vector r is in $\mathcal{Q}_j$ if the error pattern caused by the channel is a coset leader. The received vector r is decoded correctly into the transmitted codeword v_j .

If the error pattern caused by the channel is not a coset leader, an error of the decoding will occur.

Assumption: An error pattern of smaller weight is more probable than an error pattern of larger weight.



Consequence: The coset leader should be chosen to be a vector of least weight from the remaining available vectors.

Then, the decoding based on the standard array is the maximum-likelihood (ML) decoding.

$$\underline{S} = \underline{r}H' = 0 \iff \underline{r} = \underline{S}_i$$

$\Rightarrow$ All the 2^k $n \times 1$ vectors of a coset have the same syndrome.

The syndromes for different cosets are different

Syndrome decoding or table-lookup decoding

Step 1: Compute the syndrome of $\underline{r}$: $\underline{r} \cdot H'$.

Step 2: Locate the coset leader $\underline{e}_\ell$ whose syndrome is equal to $\underline{r} \cdot H'$. Then $\underline{e}_\ell$ is assumed to be the error pattern caused by the channel

Step 3: Decode $\underline{r}$ into the codeword $\underline{c} = \underline{r} + \underline{e}_\ell$.



Homework

1. Consider the $(6,3)$ linear block code with the generator matrix

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

- (a) Find the corresponding parity matrix H
- (b) Find d_{min}
- (c) Generate a standard array.

2. Prove any two elements in the same row of a standard array are not the same (equal).