Chapter 10
Error-Control Coding

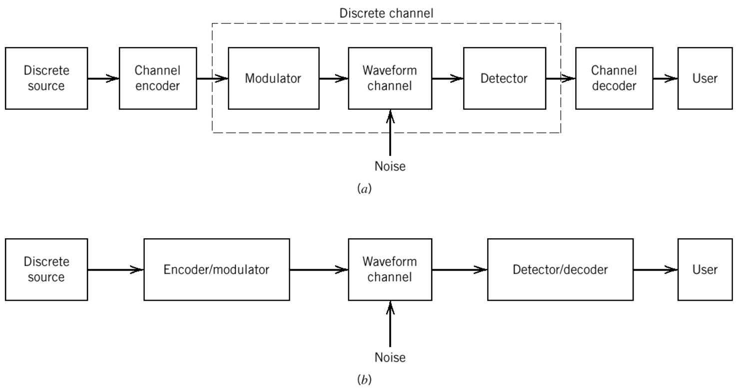
Dr. Samir Alghadhban
EE 417

KFUPM 1

Content

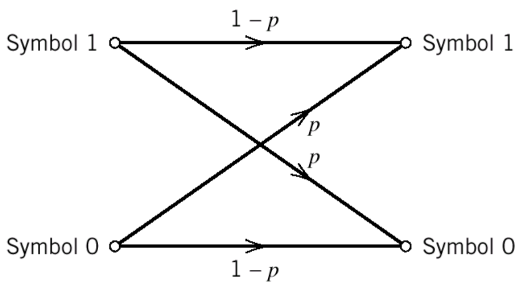
2

Discrete Channel Model



KFUPM 3

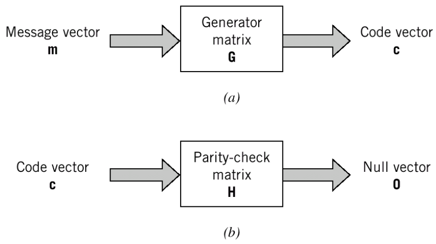
Binary Symmetric Channels



4

Linear Block Code

The parity bits of linear block codes are linear combination of the message. Therefore, we can represent the encoder by a linear system described by matrices.



(n, k) Linear Block Codes over GF(2)

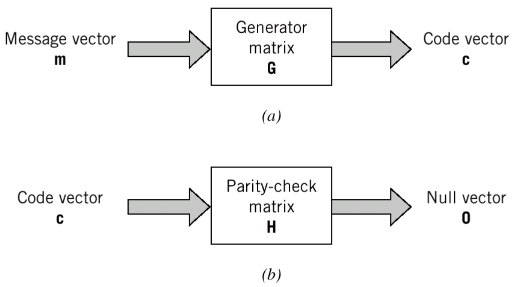
Let the message $m = (m_0, m_1, \ldots\ldots, m_{k-1})$ be an arbitrary k bit

The linear (n, k) code over GF(2) is the set of 2^k codewords of row-vector form

$$c = (c_0, c_1, \ldots\ldots, c_{n-1})$$

where $c_j \in$ GF(2)

The code rate is R=k/n.



linear Encoder.

By linear transformation

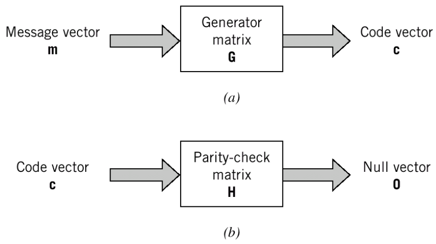
$c = m \cdot G = m_0 g_0 + m_1 g_0 + \ldots\ldots + m_{k-1} g_{k-1}$

The code C is called a k-dimensional subspace.

G is called a generator matrix of the code.

Here G is a $k \times n$ matrix of rank k of elements from GF(2), g_i is the i-th row vector of G.

The rows of G are linearly independent since G is assumed to have rank k.



Example:

(7, 4) Hamming code over GF(2)

The encoding equation for this code is given by

$c_0 = m_0$
$c_1 = m_1$
$c_2 = m_2$
$c_3 = m_3$
$c_4 = m_0 + m_1 + m_2$
$c_5 = m_1 + m_2 + m_3$
$c_6 = m_0 + m_1 + m_3$

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

KFUPM 8

Hamming Distance

- The Hamming distance is the most important measure in block codes. The Hamming distance is a measure of the distance between two codewords and is *defined as the number of different bits between two codewords*.
-
- For **example**, the distance between codeword 000 and codeword 011 is two bits.

9

Example repetition code of length 4

- We can make a repetition code of length 4 that correct single-bit error and detect two-bit errors. This is an error detection and correction code. There are two valid codewords {0000, 1111}.
- **Decoding rule**:
- Find the Hamming distance between the received codeword and the two valid codewords which are {0000, 1111}.
- If Hamming distance ≤ 1, then decode received codeword to the closest valid codeword.
- If Hamming distance = 2, then declare an error

10

Example repetition code of length 4

Received Word	Error Detection Decoder Output	Error Correction Decoder Output
0 0 0 0	0	0
0 0 0 1	Error	0
0 0 1 0	Error	0
0 0 1 1	Error	Error
0 1 0 0	Error	0
0 1 0 1	Error	Error
0 1 1 0	Error	Error
0 1 1 1	Error	1
1 0 0 0	Error	0
1 0 0 1	Error	Error
1 0 1 0	Error	Error
1 0 1 1	Error	1
1 1 0 0	Error	Error
1 1 0 1	Error	1
1 1 1 0	Error	1
1 1 1 1	1	1

Hamming Distance and Code Capability

For every pair , we can calculate a non-zero, Hamming Distance

$$d_{\min} = \min_{AllCodeWords} \left\{ d_H(\bar{c}_i, \bar{c}_j) \right\}$$

- If a code has a minimum hamming distance of $d_{\min}$, then;
- It can detect up to $t \leq d_{\min} - 1$ errors.
- It can correct up to $t \leq \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$ errors.
- It can correct $t_c \leq \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$ and detect $t_d \leq d_{\min} - t_c - 1$ errors.

definition:

An (*n, k) block code is said to be linear if the vector sum of two* codeword is a codeword.

Zero vector must be a codeword.

Ex.

C0 = 0 0 0 0　　　　C2= 1 0 1 0

C1= 0 1 0 1　　　　C3= 1 1 1 1

C0 +C1 =C1, C1 +C2=C3, C3+C2=C1 ………..etc.

Ci+Cj ϵ C so it is a linear code.

Linear Systematic Block Code:

In systematic from the codeword C *is comprised of an* information segment and a set of *n-k symbols that are linear* combinations of certain information symbols, determined by the *P matrix.*

$b_0, b_1, \ldots, b_{n-k-1}$	$m_0, m_1, \ldots, m_{k-1}$
Parity bits	Message bits

Linear Systematic Block Code:

That is

$$c_i = m_i \text{; for } 0 \le i < k$$

$$c_i = \sum_{j=0}^{k-1} m_j p_{j,n-k-i} \text{; for } k \le i < n$$

message codeword

($m_0, m_1, \ldots\ldots, m_{k-1}$) ↔($m_0, m_1, \ldots\ldots, m_{k-1}$, $c_k, c_{k+1}, \ldots, c_{n-1}$) The second set of equations, given above, is called the set of parity-check equations.

$b_0, b_1, \cdots, b_{n-k-1}$	$m_0, m_1, \cdots, m_{k-1}$
Parity bits	Message bits

Linear Systematic Block Code:

An (*n, k) linear systematic code is completely specified by a k × n* generator matrix of the following form.

$$G = \begin{bmatrix} \bar{g}_0 \\ \bar{g}_1 \\ \vdots \\ \bar{g}_{k-1} \end{bmatrix} = [I_k P]$$

where I_k *is the k × k identity matrix.*

KFUPM 16

Parity-check matrix

An *(n, k) linear code can also be specified by an (n - k) × k* matrix *H.*

$$H = \left[P^T I_{n\text{-}k}\right]$$

G $\cdot$ H^T ***= 0 .***
where P^T *is the transpose of P*

KFUPM 17

Linear Encoder

c=m G

c:1x16 codeword
m: 1x9 message bits
G: 9x16 generator matrix

At the receiver we need to find the syndrome bits.
Syndrome vector s=[s_0 s_1 s_2 s_3 s_4 s_5 s_6]

KFUPM 18

Decoding

At the receiver we need to find the syndrome bits.

Syndrome vector $s=[s_0\ s_1\ s_2\ s_3\ s_4\ s_5\ s_6]$

$$S= v\ H^T$$

The matrix H is called the parity check matrix and in the above example it has size 7x16

note: the superscript T stand for matrix transpose

KFUPM 19

Linear Block Codes

- the number of codeworde is 2^k since there are 2^k distinct messages.
- The set of vectors $\{g_i\}$ are linearly independent since we must have a set of unique codewords.
- linearly independent vectors mean that no vector g_i can be expressed as a linear combination of the other vectors.
- These vectors are called bases vector of the vector space C.
- The dimension of this vector space is the number of the basis vector which are k.
- G_i ϵ C→ the rows of G are all valid codewords.

KFUPM 20

Hamming Codes

- The Hamming Codes are family of single-error correcting codes.
- They are perfect codes => redundant bit is equal to the Hamming bound.
- A Hamming code exists for every r ≥ 3.
- The Block length is $n=2^r-1$, r ≥ 3.
- and the rate is: $R = \frac{2^r - r - 1}{2^r - 1}$
- $(n,k)=(2^r-1, 2^r-r-1)$
- So, Hamming code can be (7,4),(15,11),(31,26),...,etc.21

21

Hamming Codes

- To specify a Hamming Code of length 2^r-1:
  – begin with the systematic parity check matrix H_{rxn}.
  – Start by the identity Matrix I_{rxr}, then fill the remaining k columns with remaining nonzero binary vectors of length r.

KFUPM 22

Example1: (7,4) systematic Hamming code

- n=7, k=4 → r = 7-4 =3
  parity check matrix (H):

$$H(r\ x\ n) = \left[I_{r\ x\ r} \,|\, -P^T \right]_{r\ x\ n}$$

$$H(r\ x\ n) = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}_{3x\ 7}$$

KFUPM 23

Example1: continue

- Now the generator matrix (G)

$$G(k\ x\ n) = \left[P \ \ |I_{k\ x\ k} \right]_{k\ x\ n}$$

$$G(4x\ 7) = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}_{4x\ 7}$$

KFUPM 24

Error Correction and detection

- For all Hamming codes, d_{min}=3.

So, we have single error correction or double error detection.

- The codes may be decoded using a syndrome table.

$$\bar{s} = \bar{e}H^T$$

e	s
1000000	100
0100000	010
0010000	001
0001000	110
0000100	101
0000010	011
0000001	111

For correcting correctable error pattern:

- Evaluate the syndrom s, from s= v*H^T
- Look up the corresponding e in the syndrom table.
- Then, the correct codeword, c= v + e

- *** notice that the syndrome is just the i^{th} column of H**

Error Rate Performance

- The probability of an uncorrected error in a block is:

$$P_B = 1 - \sum_{j=0}^{t} \binom{n}{j} P^j (1-P)^{n-j}$$

- For large values of n, this calculation maybe difficult. However, we can use the following approximation:

Block error probability: $$P_B \approx 1 - e^{-np} \sum_{j=0}^{t} \frac{(nP)^j}{j!}$$

Notes on the crossover probability

- In order to correctly evaluate the crossover probability of the coded system, we have to take into account the Energy distribution of the information bits over the coded bits.

For example, let E_b be the Energy of information bit m_i. If the coded rate is R, then the energy of each coded bit C_i is RE_b. Since R ≤ 1, notice that the energy of each coded bit will be less than the information bit.

KFUPM 27

Notes on the crossover probability (Continue)

- For example, over a binary systematic channel (BSC), the crossover probability is

$$P_{uncoded} = Q(\sqrt{2\gamma})$$

- if gamma is the SNR for the information bits, then, the crossover probability after coding is

$$P_{coded} = Q(\sqrt{2R\gamma})$$

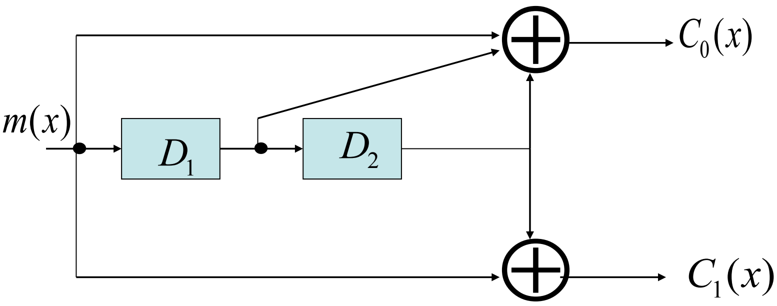
- Notice that the crossover probability for each bit of the coded system will be worse (larger) than the uncoded system since the SNR is reduced. However, with error correction, the overall performance should be better.

KFUPM 28

Convolutional Codes

Example:

$Rate = \frac{1}{2}, M = 2$ **Convolutional Encoder**



KFUPM

29

Continue . . .

In above example ,

- The memory depth of the registrars is M = 2

- For each one bit input , there are two bits outputs.

⟶ **Rate** $R = \frac{k}{n} = \frac{1}{2}$

- Since the effect of any one data input lasts over

$$v = M + 1 = 2 + 1 = 3bits$$

⟶ ***Constraint length = v = M+1***

- The encoder above is a finite impulse response [F I R] encoder.

30

Continue . . .

- The generator polynomials are :

$$g_0(x) = 1 + x + x^2 \quad \Rightarrow c_0(x) = m(x)g_0(x)$$

$$g_1(x) = 1 + x^2 \quad \Rightarrow c_1(x) = m(x)g_1(x)$$

- In general, the memory depth M of a binary convolutional code is:

$$M = \max \deg[g_0(x), \ldots, g_{n-1}(x)]$$

31

Structural Properties of Convolutional Codes

- State Diagram and Trellis Representations.

-- <u>State Diagram:</u>

- There are 2^M states in an encoder with M memory elements.

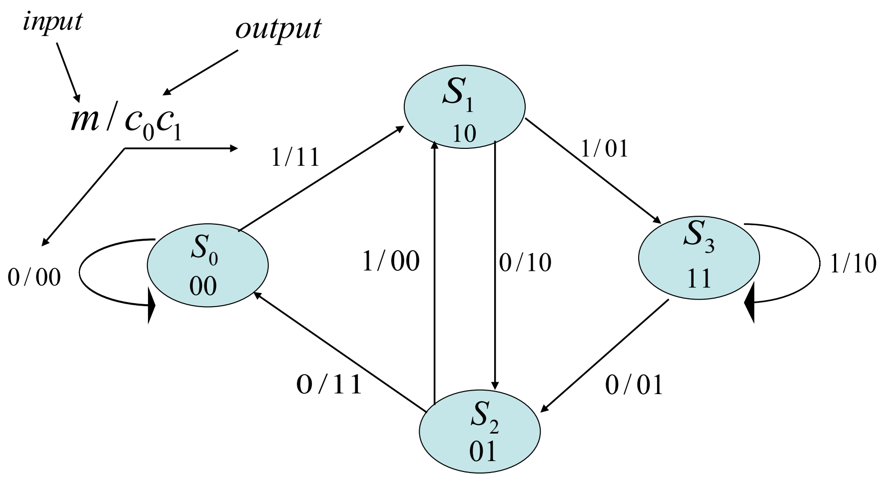
- For the previous example, $2^2 = 4 states$

-- Let us name the states :

$$\left.\begin{aligned} S_0 &= 00 \\ S_1 &= 10 \\ S_2 &= 01 \\ S_3 &= 11 \end{aligned}\right\} \quad \text{Contents of the Shift Regiser}$$

32

- We can draw the state diagram from observing the operation of the Encoder.



33

Continue . . .

- So, we can follow the state transition and know the output codeword for an input sequence.
- For example , m=[00101101]

First input

- The output codeword will be (starting from state zero)
- C=[11 10 00 01 0100 10 11]

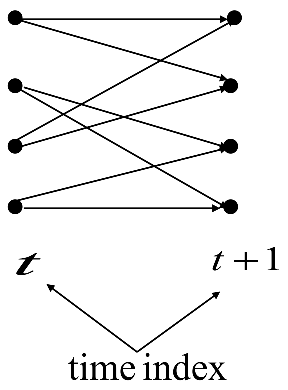
First output

34

Continue . . .

- Trellis Diagram

S_0	$0/00$	$1/11$
S_1	$0/10$	$1/01$
S_2	$0/11$	$1/00$
S_3	$0/10$	$1/10$



35

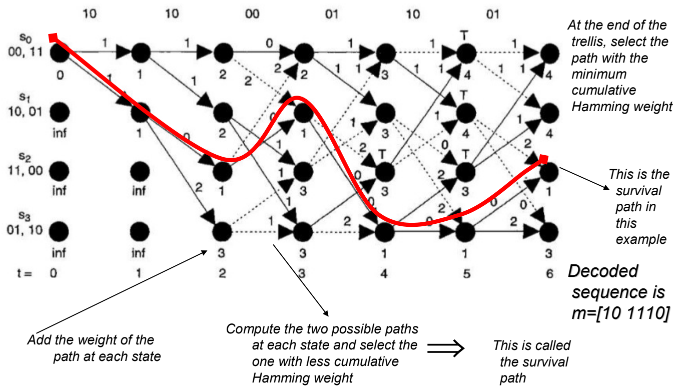
Continue . . .

- **4 – State Trellis Diagram.**
- 2^k **transition branch from each Node [state].**
- **The trellis diagram is very important in analyzing the Hamming distance of the code.**
- **Also, Decoding is based on the Viterbi algorithm which is based on the trellis diagram.**
- **Convolutional Codes are Linear codes.**
- **The Hamming distance properties of any two code sequences in the trellis are equivalent to the Hamming distance properties between some code sequence and the all-zero code sequence.**

36

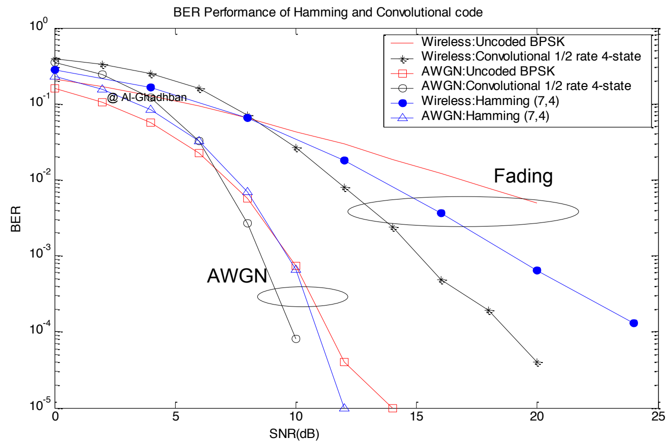
Decoder: The Viterbi Algorithm

Example: For the convolutional code example in the previous lecture, starting from state zero, Decode the following received sequence.



37

Simulation study of coded BPSK over AWGN and Fading channels



38