EE6101   DIGITAL COMMUNICATION SYSTEMS
PART III – ERROR CORRECTION CODES

Assoc Prof Erry Gunawan

Tel: 6790 5392

Office: S1-B1c-80

E-mail: egunawan@ntu.edu.sg

Error Correction Coding

1. LINEAR BLOCK CODES
2. CYCLIC CODES
3. CONVOLUTIONAL CODES
4. INTEGRATED CODING MODULATION TECHNIQUES (will not be examined)
5. TURBO CODES

References

1. E. R. BERLEKAMP
   "Algebraic Coding Theory", McGraw-Hill, 1968.

2. W. W. PETERSON and E. J. WELDON
   "Error-Correcting Codes", MIT Press, 1972.

3. S. LIN, D. J. COSTELLO
   "Error Control Coding: Fundamentals and Applications", Prentice-Hall, 1983.

4. G. C. Jr. CLARK and J. B. CAIN
   "Error-Correction Coding for Digital Communication", Plenum Press, 1981.

5. A. J. VITERBI and J. K. OMURA
   "Principles of Digital Communication and Coding", McGraw-Hill, 1979.

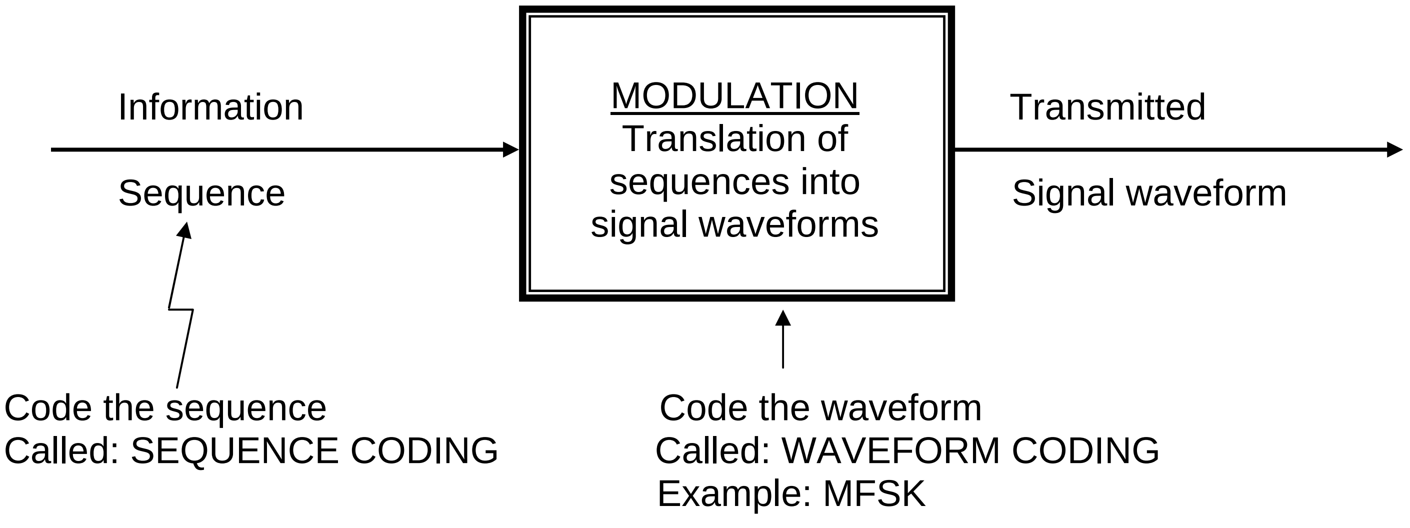
6. P. SWEENEY
   "Error Control Coding: An Introduction", Prentice-Hall, 1991.

TEXT BOOK:

Bernard Sklar, "Digital Communications: Fundamentals and Applications," Second Edition, 2001, Prentice-Hall.

Purpose of Channel Coding

TO IMPROVE COMMUNICATIONS PERFORMANCE BY ENABLING THE TRANSMITTED SIGNALS TO BETTER WITHSTAND THE EFFECTS OF VARIOUS CHANNEL IMPAIRMENTS: NOISE, FADING, JAMMING, ETC.



Application of Sequence Coding

- COMPACT DISC.
  CODING IS USED FOR THE DIGITIZED AUDIO WAVEFORM STORED IN THE DISC.
  PHILIPS’ AND SONY’S STANDARD USES:
  CROSS-INTERLEAVE REED-SOLOMON CODE (CIRC).

- NASA DEEP SPACE AND SATELLITE APPLICATION.
  CONVOLUTIONAL CODE IS USED IN INTELSAT, EUTELSAT AND OTHER SATELLITE SERVICES.
  THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS) STANDARD USES:
  (255, 223) REED-SOLOMON CONCATENATED WITH ½-RATE, CONSTRAINT LENGTH 7, CONVOLUTIONAL CODE.

- COMPUTER APPLICATIONS.
  - COMPUTER MEMORY.
    IBM 7030 USES HAMMING CODE.
  - DISK STORAGE.
    IBM 3370, IBM 3375, IBM 3380E USE: REED-SOLOMON CODES.
  - MAGNETIC TAPE STORAGE.
    IBM 3850 MASS STORAGE SYSTEM (MSS) USES (15, 13) BCH CODE.

Types of Error Control

1. ERROR DETECTION ONLY AND RETRANSMISSION.

   - FOR FULL-DUPLEX OR HALF-DUPLEX AND REQUIRES ARQ.
   - SIMPLER DECODING AND LESS REDUNDANCY THAN FEC.

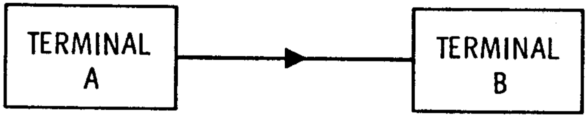
2. ERROR DETECTION AND CORRECTION: FORWARD ERROR CORRECTION (FEC).

   FOR:
   - SIMPLEX CONNECTIVITY ONLY OR DELAY WITH ARQ IS EXCESSIVE
   - REAL TIME DATA TRANSMISSION
   - NOISY CHANNEL WHERE ARQ WILL BE EXCESSIVE.

   MORE COMPLEX DECODING AND REDUNDANCY.

Terminal Connectivity Classifications

SIMPLEX

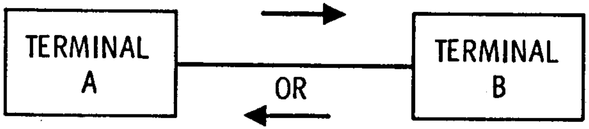


TERMINAL A

TERMINAL B

TRANSMISSION IN ONLY ONE DIRECTION

HALF-DUPLEX



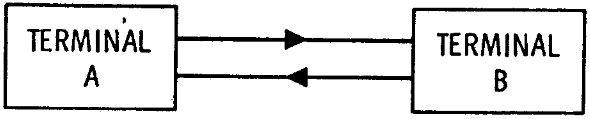
TERMINAL A

OR

TERMINAL B

TRANSMISSION IN EITHER DIRECTION, BUT NOT SIMULTANEOUSLY

FULL-DUPLEX



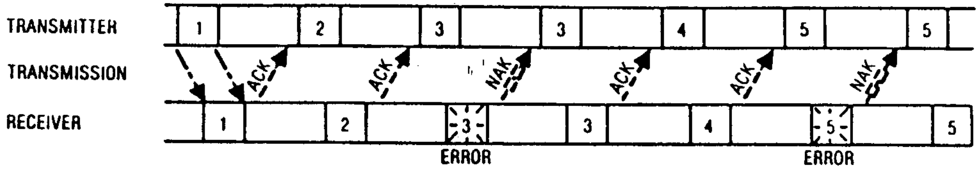
TERMINAL A

TERMINAL B

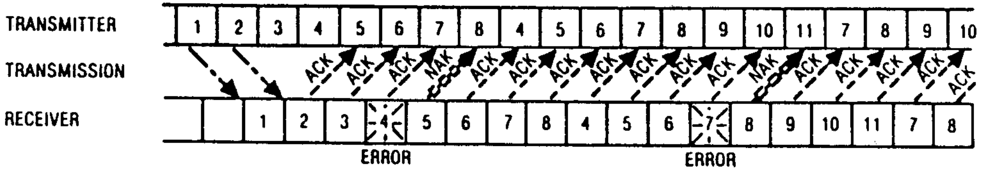
TRANSMISSION IN BOTH DIRECTIONS AT ONCE

Automatic Repeat Request (ARQ)

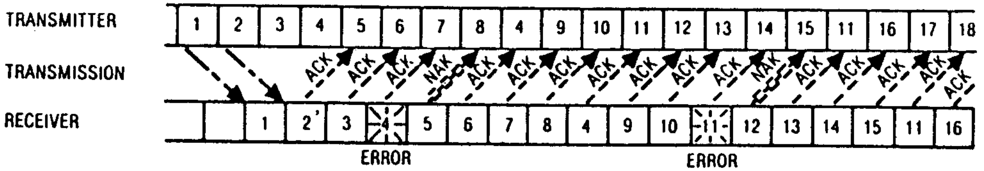
STOP AND WAIT ARQ (HALF-DUPLEX)



CONTINUOUS ARQ, WITH PULLBACK (FULL-DUPLEX)



CONTINUOUS ARQ, WITH SELECTIVE REPEAT (FULL-DUPLEX)



Channel Models

1. DISCRETE MEMORYLESS CHANNEL (DMC)

CHARACTERISTICS:
- ⇨ DISCRETE INPUT ALPHABET, **U**
- ⇨ DISCRETE OUTPUT ALPHABET, **Z**
- ⇨ A SET OF CONDITIONAL PROBABILITY

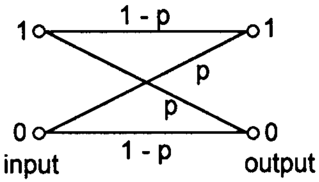
$$P(\mathbf{Z}|\mathbf{U}) = \prod_{m=1}^{N} P(z_m|u_m)$$

WHERE $\mathbf{U} = u_1, u_2, \ldots\ldots\ldots, u_\mathrm{m}, \ldots\ldots\ldots, u_\mathrm{N}$
$\mathbf{Z} = z_1, z_2, \ldots\ldots\ldots\ldots, z_\mathrm{m}, \ldots\ldots\ldots\ldots, z_\mathrm{N}$

MEMORYLESS MEANS THE EVENTS ARE INDEPENDENT ~~MUTUALLY EXCLUSIVE,~~ HENCE THE COMPOUND PROBABILITY OF THE TOTAL SEQUENCE IS JUST A MULTIPLICATION OF THE INDIVIDUAL ELEMENT PROBABILITY

2. BINARY SYMMETRIC CHANNEL (BSC)

A SPECIAL CASE OF DMC WHERE THE INPUT AND OUTPUT ALPHABET SETS CONSISTS OF BINARY ELEMENT (0 AND 1)



P(0 / 1) = P(1 / 0) = p

P(1 / 1) = P(0 / 0) = 1 - p

$p = Q(\sqrt{\frac{2Ec}{No}})$

3. ADDITIVE WHITE GAUSSIAN NOISE CHANNEL (AWGN)

- GENERALIZE DEFINITION OF DMC - CONTINUOUS CHANNEL
- NOISE CAN BE ADDED TO THE SIGNALS

EXAMPLE: CHANNEL WITH DISCRETE INPUT ALPHABET AND A CONTINUOUS OUTPUT ALPHABET OR IN PRACTICE THIS CONTINUOUS OUTPUT USUALLY IS ITS QUANTIZED APPROXIMATION

- DECODING WITH GAUSSIAN CHANNEL IS CALLED SOFT-DECISION DECODING

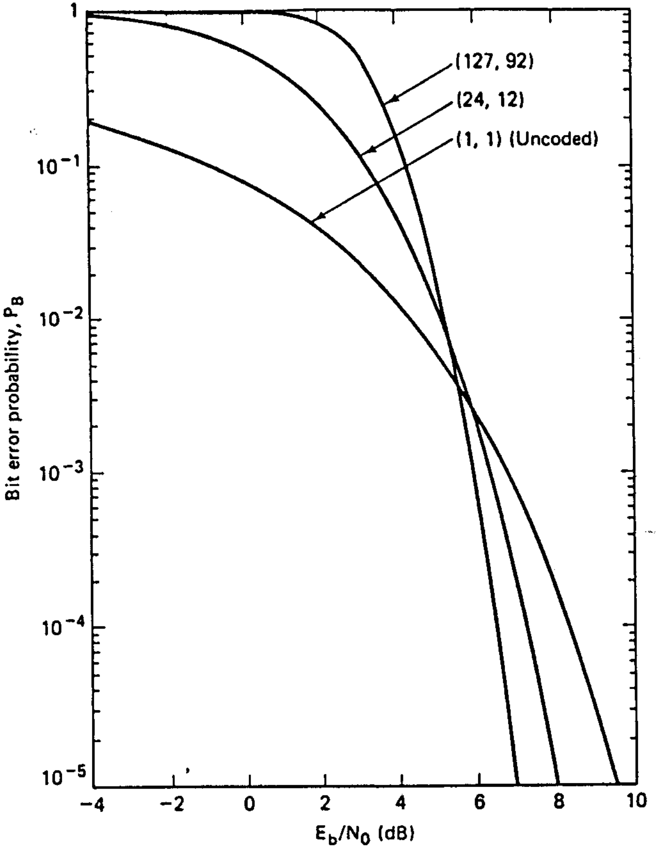


Figure 5.12 Coded versus uncoded bit error performance for coherent PSK with various (n, k) codes.

Linear Block Codes

- ENCODER TRANSFORMS BLOCK OF k SUCCESSIVE BINARY DIGITS INTO LONGER BLOCK OF n $(n > k)$ BINARY DIGITS
- CALLED AN (n, k) CODE
- REDUNDANCY $= \frac{n - k}{k}$; CODE RATE $R = \frac{k}{n}$
- THERE ARE 2^k POSSIBLE MESSAGES
- THERE ARE 2^k POSSIBLE CODE WORDS CORRESPONDING TO THE MESSAGES
- CODE WORD (or code vector) IS AN n-TUPLE FROM THE SPACE V_n OF ALL n-TUPLES
- STORING THE 2^k CODE VECTORS IN A DICTIONARY IS PROHIBITIVE FOR LARGE k

Coding Idea

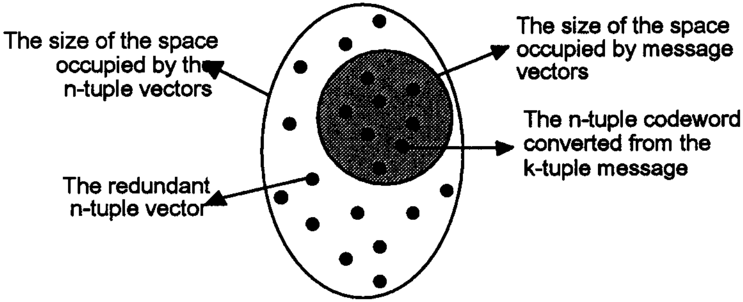
☞ TAKE 3-BIT MESSAGES:

000
001
$\boxed{010}$ ⟶ 3-digit sequence is called 3-tuples
011
100
101
110
111

☞ THE INFORMATION CONTAINED IN EACH SEQUENCE IS 3 BITS BECAUSE ALL THE BITS CARRY INFORMATION (MESSAGE) ⟶ NO REDUNDANCY.

☞ A CHANGE OF ONE BIT IN A PARTICULAR SEQUENCE CONVERTS TO ANOTHER VALID SEQUENCE ⟶ NO WAY OF DETECTING OR CORRECTING ERROR.

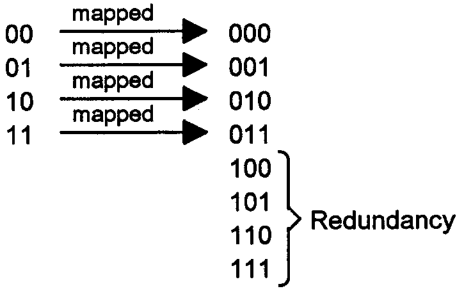
☞ REDUNDANCY IS NEEDED:
IF WE REPRESENT THE SEQUENCE OF DIGITS AS A VECTOR WHICH OCCUPIES A SPACE, THEN THIS MEANS WE NEED A LARGER SPACE THAN THE SPACE OCCUPIED BY THE MESSAGE SEQUENCES.


The size of the space occupied by the n-tuple vectors
The size of the space occupied by message vectors
The n-tuple codeword converted from the k-tuple message
The redundant n-tuple vector

WE HAVE NOW THE PROBLEM OF MAPPING: HOW TO MAP THE 2^k SET OF MESSAGES TO A LARGER 2^n SET OF SEQUENCES SUCH THAT THE REDUNDANCY CAN PROVIDE EXTRA INFORMATION FOR DETECTING OR CORRECTING ERRORS.

Mapping Problem and Rules

- EXAMPLE, MAP 2-BIT MESSAGES TO 3-BIT CODEWORDS.



00 mapped 000

01 mapped 001

10 mapped 010

11 mapped 011

100, 101, 110, 111 Redundancy

- THIS WAY OF MAPPING DOES NOT PRODUCE REDUNDANCY THAT GIVES EXTRA INFORMATION FOR DETECTING/CORRECTING OF ERRORS.

- HENCE, THERE ARE 3 FUNDAMENTAL PROBLEMS FACED BY THE DESIGNER OF ERROR DETECTION/CORRECTION (EDC) SYSTEMS:

  1. TO SYNTHESISE A CODE WITH THE DESIRED REDUNDANCY OR EDC PROPERTIES,

  2. TO FIND A REASONABLY SIMPLE DECODER, AND

  3. TO MAKE THE OVERALL CODING SYSTEM AS EFFICIENT AS POSSIBLE, SO THAT THE MINIMUM AMOUNT OF REDUNDANT INFORMATION IS TRANSMITTED.

Finite Field Number System

☞ NORMAL NUMBERING SYSTEM:

-∞,......, -100,....., -10,......, 0,....., 10,......., 100,......., +∞

THE FIELD OF THIS SYSTEM IS FROM +∞ TO -∞ (INIFINITE FIELD).

☞ GALOIS FIELD NUMBER SYSTEM:

IS A FINITE FIELD ELEMENTS NUMBERING SYSTEM

GF(2) - HAS 2 ELEMENTS ONLY (0 AND 1)
- RESULTS OF ALL OPERATIONS (ADDITION AND MULTIPLICATION) MUST BE IN THE SAME FIELD:

$0 + 0 = 0$	$0 . 0 = 0$
$0 + 1 = 1$	$0 . 1 = 0$
$1 + 1 = 0$	$1 . 1 = 1$

GF(3) - HAS 3 ELEMENTS (0, 1, AND 2)
- RESULTS OF ALL OPERATIONS MUST BE IN THE SAME FIELD:

$1 + 1 = 2$	$0 . 0 = 0$
$1 + 2 = 0$	$1 . 2 = 2$
$2 + 2 = 1$	$2 . 2 = 1$

Vector Spaces and Subspaces

- THE SET OF ALL BINARY N-TUPLES, V_n, IS CALLED A VECTOR SPACE OVER GF (2)
- TWO OPERATIONS ARE DEFINED
  - ADDITION: $\underline{V} + \underline{U} = v_1 + u_1, v_2 + u_2, \cdots v_n + u_n$
  - SCALAR MULTIPLICATION: $a\underline{V} = av_1, av_2, \cdots av_n$
- EXAMPLE: VECTOR SPACE V_4

  0000 0001 0010 0011 0100 0101 0110 0111
  1000 1001 1010 1011 1100 1101 1110 1111

  $(0101) + (1110) = (0+1,\ 1+1,\ 0+1,\ 1+0) = 1011$
  $1 \cdot (0101) = (1 \cdot 0,\ 1 \cdot 1,\ 1 \cdot 0,\ 1 \cdot 1) = 0101$
- A SUBSET S OF V_n IS A SUBSPACE IF
  - THE ALL-ZERO VECTOR IS IN S
  - THE SUM OF ANY TWO VECTORS IN S IS ALSO IN S

  } CONDITIONS FOR LINEAR BLOCK CODES
- EXAMPLE OF S: $\underline{V}_0 = 0000$

  $\underline{V}_1 = 0101$

  $\underline{V}_2 = 1010$

  $\underline{V}_3 = 1111$

Mapping Rules (cont'd)

- SUMMARISING THE RULES OF MAPPING:

  FROM k-TUPLE MESSAGES TO k-DIMENSIONAL SUBSPACE OF n-TUPLE VECTOR SPACE

  1. THE ALL-ZERO VECTOR IS IN THE SUBSPACE
  2. THE SUM OF ANY TWO VECTORS IN THE SUBSPACE IS ALSO IN THE SUBSPACE

- WHEN k IS SMALL, THE MAPPING CAN BE DONE USING TABLE LOOK UP. BUT FOR LARGE k, THE SIZE OF THE REQUIRED MEMORY WILL BE THE LIMITATION.

- HOWEVER, WE DO NOT NEED THE WHOLE k-DIMENSIONAL SUBSPACE CODEWORD VECTORS TO BE STORED IN MEMORY TO DO THE MAPPING. RULE 2 STATES THAT ALL OTHER VECTORS IN THE SUBSPACE CAN BE OBTAINED FROM CERTAIN VECTORS IN THIS SUBSPACE → VECTORS WHICH ARE *LINEARLY INDEPENDENT* FROM EACH OTHER.

- THIS LINEARLY INDEPENDENT SET CHOSEN FROM ALL THE VECTORS IN THE k-DIMENSIONAL SUBSPACE WILL THEN BE A *GENERATOR* FOR THE OTHER CODEWORD VECTORS.

Reducing Encoding Complexity

- KEY FEATURE OF LINEAR BLOCK CODES: THE 2^k CODE VECTORS FORM A k-DIMENSIONAL SUBSPACE OF ALL n-TUPLES

- EXAMPLE: $k = 3$, $2^k = 8$, $n = 6$, (6, 3) CODE

MESSAGE	CODE WORD
0 0 0	0 0 0 0 0 0
1 0 0	1 1 0 1 0 0
0 1 0	0 1 1 0 1 0
1 1 0	1 0 1 1 1 0
0 0 1	1 0 1 0 0 1
1 0 1	0 1 1 1 0 1
0 1 1	1 1 0 0 1 1
1 1 1	0 0 0 1 1 1

A 3-DIMENSIONAL SUBSPACE OF THE VECTOR SPACE OF ALL 6-TUPLES

- IT IS POSSIBLE TO FIND A SET OF k LINEARLY INDEPENDENT n-TUPLES $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_k$ SUCH THAT EACH n-TUPLE OF THE SUBSPACE IS A LINEAR COMBINATION OF $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_k$

- CODE WORD $\underline{u} = m_1 \underline{v}_1 + m_2 \underline{v}_2 + \ldots + m_k \underline{v}_k$

WHERE $m_i = 0$ OR 1

$i = 1, \ldots, k$

Generator Matrix

$$G = \begin{bmatrix} \underline{v}_1 \\ \underline{v}_2 \\ \vdots \\ \underline{v}_k \end{bmatrix} = \begin{bmatrix} v_{11} & v_{12} & v_{13} & \cdots & v_{1n} \\ v_{21} & v_{22} & v_{23} & \cdots & v_{2n} \\ \vdots & & & & \\ v_{k1} & v_{k2} & v_{k3} & \cdots & v_{kn} \end{bmatrix}$$

k x n
GENERATOR MATRIX

- THE 2^k CODE VECTORS CAN BE DESCRIBED BY A SET OF k LINEARLY INDEPENDENT CODE VECTORS
- LET $\underline{m} = [m_1, m_2, \ldots, m_k]$ BE A MESSAGE (row vectors are standard in the coding literature)
- CODE WORD CORRESPONDING TO MESSAGE m: $\underline{u} = \underline{m}\, G$

$$\underline{u} = [m_1, m_2, \ldots, m_k] \begin{bmatrix} \underline{v}_1 \\ \underline{v}_2 \\ \vdots \\ \underline{v}_k \end{bmatrix}$$

$$\underline{u} = m_1 \underline{V}_1 + m_2 \underline{V}_2 + \ldots + m_k \underline{V}_k$$

Generator Matrix

(cont'd)

- STORAGE IS GREATLY REDUCED
- THE ENCODER NEEDS TO STORE THE k ROWS OF G INSTEAD OF THE 2^k CODE VECTORS OF THE CODE

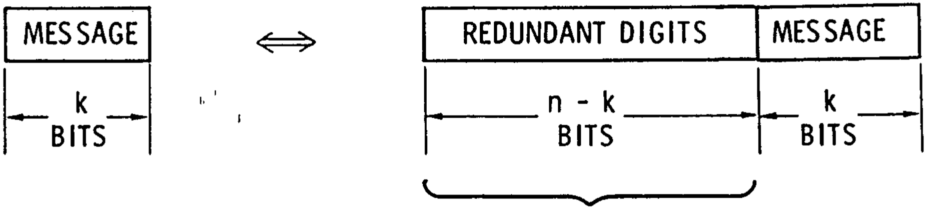
EXAMPLE

LET $G = \begin{bmatrix} \underline{v}_1 \\ \underline{v}_2 \\ \underline{v}_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$ AND $\underline{m} = [1\ 1\ 0]$

THEN

$$\underline{u} = [1\ 1\ 0]\begin{bmatrix} \underline{v}_1 \\ \underline{v}_2 \\ \underline{v}_3 \end{bmatrix} \begin{aligned} &= 1 \cdot \underline{v}_1 + 1 \cdot \underline{v}_2 + 0 \cdot \underline{v}_3 \\ &= 1 \cdot [1\ 1\ 0\ 1\ 0\ 0] + 1 \cdot [0\ 1\ 1\ 0\ 1\ 0] + 0 \cdot [1\ 0\ 1\ 0\ 0\ 1] \\ &= 1\ 0\ 1\ 1\ 1\ 0 \quad \text{CODE VECTOR FOR } \underline{m} = [1\ 1\ 0] \end{aligned}$$

Systematic Code



MESSAGE ⟺ REDUNDANT DIGITS | MESSAGE

k BITS

n - k BITS

k BITS

USED TO COMBAT ERRORS
INTRODUCED DURING
TRANSMISSION

THE ENCODING PROBLEM: FORM THE REDUNDANT DIGITS

$$G = \begin{bmatrix} p_{11} & p_{12} \cdots, & p_{1,n-k} & 1\ 0\ 0\ 0 \ldots 0 \\ p_{21} & p_{22} \cdots, & p_{2,n-k} & 0\ 1\ 0\ 0 \ldots 0 \\ p_{31} & p_{32} \cdots, & p_{3,n-k} & 0\ 0\ 1\ 0 \ldots 0 \\ & & & \vdots \qquad \vdots \\ p_{k1} & k_{k2} & p_{k,n-k} & 0\ 0\ 0\ 0 \ldots 1 \end{bmatrix}$$

WHERE p_{ij} = 0 OR 1

AND I_k IS THE k x k IDENTITY MATRIX

Systematic Code
(cont'd)

$G = [P\ I_k]$ GENERATOR MATRIX

$\underline{u} = \underline{m}\ G$

$$[u_1, u_2, \ldots u_n] = [m_1, m_2, \ldots, m_k] \begin{bmatrix} p_{11}\, p_{12} \cdots, p_{1,n-k} & 1\,0\,0\,0 \ldots \\ p_{21}\, p_{22} \cdots, p_{2,n-k} & 0\,1\,0\,0 \ldots \\ p_{31}\, p_{32} \cdots, p_{3,n-k} & 0\,0\,1\,0 \ldots \\ \vdots & \vdots \end{bmatrix}$$

- $u_i = m_1 p_{1i} + m_2 p_{2i} + \ldots + m_k p_{ki}$

  FOR $i = 1, \ldots, n - k$

- THE LAST k DIGITS OF THE CODE WORD ARE THE DATA DIGITS

Systematic Code (cont'd)

☞ IF WE EXPRESS THE SYSTEMATIC CODE VECTOR AS:

$$\underline{U} = p_1, p_2, \ldots\ldots\ldots, p_{n-k}, m_1, m_2, \ldots\ldots\ldots, m_k$$

THEN

$$\begin{aligned}
p_1 &= m_1 p_{11} + m_2 p_{21} + \ldots\ldots\ldots + m_k p_{k1} \\
p_2 &= m_1 p_{12} + m_2 p_{22} + \ldots\ldots\ldots + m_k p_{k2} \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
p_{n-k} &= m_1 p_{1,\,(n-k)} + m_2 p_{2,\,(n-k)} + \ldots\ldots\ldots + m_k p_{k,\,(n-k)}
\end{aligned}$$

Systematic Code

(cont'd)

- STORAGE REQUIREMENTS FURTHER REDUCED: STORE k x (n-k) DIGITS OF THE P MATRIX INSTEAD OF k x n DIGITS OF THE G MATRIX

EXAMPLE: (6, 3) CODE

$$\underline{u} = [u_1, u_2, \ldots, u_6]$$

$$\underline{u} = [m_1, m_2, m_3] \left[\begin{matrix} \underbrace{\begin{matrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{matrix}}_{P} & \underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{I_k} \end{matrix}\right]$$

$$\underline{u} = \underbrace{m_1 + m_3}_{u_1},\ \underbrace{m_1 + m_2}_{u_2},\ \underbrace{m_2 + m_3}_{u_3},\ \underbrace{m_1}_{u_4},\ \underbrace{m_2}_{u_5},\ \underbrace{m_3}_{u_6}$$

Parity Check

☞ IT IS DESIRED TO HAVE A METHOD OF CHECKING THE CORRECTNESS OF THE PARITY BITS IN THE MESSAGE RECEIVED IN THE RECEIVER.

☞ LET $\mathbf{U}$ BE THE VALID CODEWORD GENERATED BY $\mathbf{G}$, THEN IT IS OBVIOUS THAT IF WE CAN FIND A VECTOR/MATRIX $\mathbf{V}$ SUCH THAT

$$\mathbf{U.V} = \mathbf{0}$$

THEN $\mathbf{V}$ CAN BE USED AS CHECKING MATRIX. BECAUSE WHEN $\mathbf{U'}$ ($\neq \mathbf{U}$) IS NOT A VALID CODEWORD, THEN

$$\mathbf{U'.V} \neq \mathbf{0}$$

☞ THE PARITY CHECK MATRIX CAN BE FOUND AS FOLLOWS:

$$\mathbf{U.V} = \mathbf{m.G.V} = \mathbf{0}$$

OR

$$\mathbf{G.V} = \mathbf{0}$$

BUT

$$\mathbf{G} = [\,\mathbf{P}\ \ \mathbf{I}_k\,]$$

HENCE

$$\mathbf{V} = \mathbf{H}^T = \begin{bmatrix} \mathbf{I}_{n-k} \\ \mathbf{P} \end{bmatrix}$$ OR $$\mathbf{H} = [\,\mathbf{I}_{n\text{-}k}\ \ \mathbf{P}^T\,]$$

Parity Check Matrix and Syndrome

- IN A SYSTEMATIC CODE WITH $G = \left[P \; I_k\right]$

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

- $$\underbrace{\underline{r}}_{\text{RECEIVED VECTOR}} = \underbrace{\underline{u}}_{\text{CODE VECTOR}} + \underbrace{\underline{e}}_{\text{ERROR VECTOR}}$$

- SYNDROME OF $\underline{r}$ USED FOR ERROR DETECTION AND CORRECTION

  $$\underline{s} = \underline{r} \, H^T$$

- $$\text{SYNDROME } \underline{s} \begin{cases} = \underline{0} & \text{IF } \underline{r} \text{ IS A CODE VECTOR} \\ \neq \underline{0} & \text{OTHERWISE} \end{cases}$$

- $\underline{s} = \underline{r} \, \underline{H}^T = (\underline{U} + \underline{e}) \, \underline{H}^T = \underline{U} \, \underline{H}^T + \underline{e} \, \underline{H}^T$

  BUT $\underline{U} \, \underline{H}^T = \underline{0}$, HENCE

  $$\underline{s} = \underline{r} \, \underline{H}^T = \underline{e} \, \underline{H}^T$$

A Standard Array for the (6, 3) Code

COSET LEADER							
000000	110100	011010	101110	101001	011101	110011	000111
000001	110101	011011	101111	101000	011100	110010	000110
000010	110110	011000	101100	101011	011111	110001	000101
000100	110000	011110	101010	101101	011001	110111	000011
001000	111100	010010	100110	100001	010101	111011	001111
010000	100100	001010	111110	111001	001101	100011	010111
100000	010100	111010	001110	001001	111101	010011	100111
010001	100101	001011	111111	111000	001100	100010	010110

- THE 2^{n-k} COSET LEADERS ARE THE CORRECTABLE ERROR PATTERNS
- THE DECODING IS CORRECT IF AND ONLY IF THE ERROR PATTERN CAUSED BY THE CHANNEL IS A COSET LEADER
- THE 2^k n-TUPLES OF A COSET HAVE THE SAME SYNDROME. THE SYNDROME FOR DIFFERENT COSETS ARE DIFFERENT

Procedure for Error Correction Decoding

☞ CALCULATE SYNDROME

$$\mathbf{S} = \mathbf{r}.\mathbf{H}^T$$

☞ LOCATE THE ERROR PATTERN, $\mathbf{e}_j$, WHOSE SYNDROME IS $\mathbf{S} = \mathbf{r}.\mathbf{H}^T$

☞ THE CORRECTED RECEIVED VECTOR OR CODE VECTOR IS

$$\mathbf{U} = \mathbf{r} + \mathbf{e}_j$$

Error Correction Example

$$G = \begin{bmatrix} 110100 \\ 011010 \\ 101001 \end{bmatrix} \qquad H = \begin{bmatrix} 100101 \\ 010110 \\ 001011 \end{bmatrix}$$

COSET LEADER	SYNDROME
0 0 0 0 0 0	0 0 0
0 0 0 0 0 1	1 0 1
0 0 0 0 1 0	0 1 1
0 0 0 1 0 0	1 1 0
0 0 1 0 0 0	0 0 1
0 1 0 0 0 0	0 1 0
1 0 0 0 0 0	1 0 0
0 1 0 0 0 1	1 1 1

- ASSUME $\underline{v}$ = 1 0 1 1 1 0 IS TRANSMITTED
  AND $\underline{r}$ = 0 0 1 1 1 0 IS RECEIVED
- THE SYNDROME IS: $\underline{r}\,H^T$ = 1 0 0
- THE COSET LEADER IS: 1 0 0 0 0 0
- THEREFORE THE CORRECTED RECEIVED VECTOR IS:

  0 0 1 1 1 0 + 1 0 0 0 0 0 = 1 0 1 1 1 0

Weight and Distance of Binary Vectors

- HAMMING WEIGHT OF A VECTOR

  $W(\underline{v})$ = NUMBER OF NON-ZERO COMPONENTS IN THE VECTOR

- HAMMING DISTANCE BETWEEN 2 VECTORS

  $d(\underline{u}, \underline{v})$ = NUMBER OF COMPONENTS IN WHICH THEY DIFFER

  FOR EXAMPLE

  $$\underline{u} = 1\,0\,0\,1\,0\,1\,1\,0\,0\,0\,1$$
  $$\underline{v} = 1\,1\,0\,0\,1\,0\,1\,0\,1\,0\,1$$

  $$d(\underline{u}, \underline{v}) = 5$$

- $\underline{u} + \underline{v} = 0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,0$

- $d(\underline{u}, \underline{v}) = w(\underline{u} + \underline{v})$ THE HAMMING DISTANCE BETWEEN 2 VECTORS IS EQUAL TO THE HAMMING WEIGHT OF THEIR VECTOR SUM

- THE STRENGTH OF A CODE DEPENDS ON THE DISTANCES (HAMMING DISTANCE FOR BINARY CODES) BETWEEN EACH OF THE CODE VECTORS

Minimum Distance of a Linear Code

- THE SET OF ALL CODE VECTORS OF A LINEAR CODE FORM A SUBSPACE OF THE n-TUPLE SPACE

- IF $\underline{u}$ AND $\underline{v}$ ARE 2 CODE VECTORS, THEN $\underline{u} + \underline{v}$ MUST ALSO BE A CODE VECTOR (closure property)

- THEREFORE, THE DISTANCE $d(\underline{u}, \underline{v})$ BETWEEN 2 CODE VECTORS EQUALS THE WEIGHT OF A THIRD

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

- THUS, THE MINIMUM DISTANCE OF A LINEAR CODE EQUALS THE MINIMUM WEIGHT OF ITS CODE VECTORS

- A CODE WITH MINIMUM DISTANCE d_{min} CAN BE SHOWN TO HAVE ERROR-CORRECTING CAPABILITY $(d_{min} - 1)/2$ OR ERROR-DETECTING CAPABILITY $(d_{min} - 1)$

Decoding Strategy

Maximum Likelihood Decoding

CHOOSE THE MOST LIKELY = MAXIMUM PROBABILITY:

$$P(\mathbf{Z}|\mathbf{U}^{(m')}) = \max_{all\mathbf{U}^{(m)}} P(\mathbf{Z}|\mathbf{U}^{(m)})$$

WHERE $\mathbf{Z} = (\mathbf{Z}_1, \mathbf{Z}_2, \ldots\ldots, \mathbf{Z}_i)$ IS THE RECEIVED SEQUENCE

$\mathbf{U}^{(m)} = (\mathbf{U}_1^{(m)}, \mathbf{U}_2^{(m)}, \ldots\ldots, \mathbf{U}_i^{(m)})$ IS ONE OF THE POSSIBLE TRANSMITTED SEQUENCES.

(HENCE, IF THERE IS N-BIT CODEWORD SEQUENCE { i = N}, THEN THERE ARE 2^N POSSIBLE SEQUENCES FOR $\mathbf{U}^{(m)}$.)

FOR **MEMORYLESS** CHANNEL:

$$P(\mathbf{Z}|\mathbf{U}^{(m)}) = \prod_{i=1}^{N} P(Z_i|U_i^{(m)})$$

$$\log P(\mathbf{Z}|\mathbf{U}^{(m)}) = \sum_{i=1}^{N} \log P(Z_i|U_i^{(m)})$$

Why Hamming Distance for BSC Channel?

RECALL:

$$P(\mathbf{Z}|\mathbf{U}^{(m')}) = \max_{all\mathbf{U}^{(m)}} P(\mathbf{Z}|\mathbf{U}^{(m)})$$

WHERE $P(\mathbf{Z}|\mathbf{U}^{(m)})$ IS THE PROBABILITY OF RECEIVING $\mathbf{Z}$ SEQUENCE WHEN THE POSSIBLE TRANSMITTED SEQUENCE IS $\mathbf{U}^{(m)}$.

IF $\mathbf{Z}$ AND $\mathbf{U}^{(m)}$ ARE EACH N-BIT LONG AND DIFFER IN d_m POSITIONS, THEN

$$P(\mathbf{Z}|\mathbf{U}^{(m)}) = p^{d_m}(1-p)^{N-d_m}$$

OR

$$\log P(\mathbf{Z}|\mathbf{U}^{(m)}) = -d_m \log\left(\frac{1-p}{p}\right) + N\log(1-p)$$

$$= -A.d_m - B$$

HENCE,

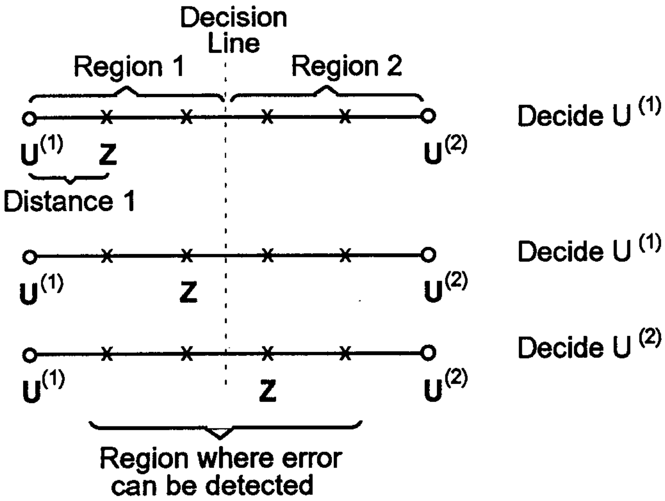
$$Max\left[\log P(\mathbf{Z}|\mathbf{U}^{(m)})\right] = -A \times Min\left[d_m\right] - B$$

AND d_m IS THE HAMMING DISTANCE BETWEEN $\mathbf{Z}$ AND $\mathbf{U}^{(m)}$.

CONCLUSION: FOR BSC CHANNEL THE MAXIMUM PROBABILITY IS INVERSELY PROPORTIONAL TO THE DISTANCE BETWEEN $\mathbf{Z}$ AND $\mathbf{U}^{(m)}$:

DECIDE IN FAVOUR OF $\mathbf{U}^{(m')}$ IF

$$d(\mathbf{Z},\mathbf{U}^{(m')}) = \underset{all\,\mathbf{U}^{(m)}}{Min}\; d(\mathbf{Z},\mathbf{U}^{(m)})$$



Relation of Minimum Distance to Parity Check Matrix

IF $\mathbf{c} = (c_0, c_1, \ldots\ldots, c_{n-1})$ IS A CODEWORD, AND $\mathbf{H} = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & & \vdots \\ h_{n-k,1} & h_{n-k,2} & \cdots & h_{n-k,n} \end{bmatrix}$ IS THE PARITY CHECK MATRIX, THEN

$$\mathbf{cH}^{\mathrm{T}} = (c_0 \quad c_1 \quad \cdots \quad c_{n-1}) \begin{bmatrix} h_{11} & h_{21} & \cdots & h_{n-k,1} \\ h_{12} & h_{22} & \cdots & h_{n-k,2} \\ \vdots & \vdots & & \vdots \\ h_{1n} & h_{2n} & \cdots & h_{n-k,n} \end{bmatrix}$$

$$= (c_0 h_{11} + c_1 h_{12} + \ldots + c_{n-1} h_{1n}, \cdots\cdots, c_0 h_{n-k,1} + c_1 h_{n-k,2} + \ldots + c_{n-1} h_{n-k,n}) = \mathbf{0}$$

HENCE,

$$c_0 h_{11} + c_1 h_{12} + \ldots\ldots + c_{n-1} h_{1n} = 0$$

$$\vdots$$

$$c_0 h_{n-k,1} + c_1 h_{n-k,2} + \ldots\ldots + c_{n-1} h_{n-k,n} = 0$$

THIS SHOWS THAT THE COLUMN VECTORS OF $\mathbf{H}$ IS LINEARLY DEPENDENT.

IF **c** IS A MINIMUM WEIGHT CODEWORD WITH WEIGHT, $w_{\min} = \mathrm{m}$, THEN THERE ARE m NON-ZERO COMPONENTS, AND (n-m) ZERO COMPONENTS:

$$c_j,\ c_{j+1},\ \ldots\ldots\ldots,\ c_{j+m-1} = 1$$

AND

$$h_{1,j+1} + h_{1,j+2} + \ldots\ldots + h_{1,j+m} = 0$$
$$\vdots$$
$$h_{n-k,j+1} + h_{n-k,j+2} + \ldots\ldots + h_{n-k,j+m} = 0$$

OR

$$\begin{pmatrix} h_{1,j+1} \\ h_{2,j+1} \\ \vdots \\ h_{n-k,j+1} \end{pmatrix} + \begin{pmatrix} h_{1,j+2} \\ h_{2,j+2} \\ \vdots \\ h_{n-k,j+2} \end{pmatrix} + \ldots\ldots\ldots\ldots + \begin{pmatrix} h_{1,j+m} \\ h_{2,j+m} \\ \vdots \\ h_{n-k,j+m} \end{pmatrix} = \mathbf{0}$$

SINCE $w_{\min} = d_{\min}$, THE POSSIBLE MINIMUM DISTANCE OF A CODE CAN BE DETERMINED BY COUNTING THE MINIMUM NUMBER OF LINEARLY DEPENDENT COLUMNS OF **H**.

EXAMPLE:

THE MINIMUM DISTANCE OF A CODE WITH PARITY CHECK MATRIX:

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

IS THREE.

THE LINEARLY DEPENDENT COLUMNS ARE COLUMNS 1, 2, 6 OR COLUMNS 3, 6, 7, ETC.

NO LESS THAN THREE COLUMNS ARE LINEARLY DEPENDENT.

Bit Error Probability

CONSIDER A CODE WITH: $n=6$
$t=2$ (TWO BIT ERROR CORRECTABLE)

SO THE DECODER WILL MAKE ERRONEOUS DECODING WHEN IT RECEIVES ERRORS MORE THAN t:

$(t+1)$ TO n BITS

USING BINOMIAL DISTRIBUTION:
THE PROBABILITY OF 3 BIT ERRORS IN 6 BIT CODE IS

$$\binom{6}{3}p^3(1-p)^{6-3}$$

WHERE p = PROBABILITY OF CHANNEL ERROR (1 BIT)

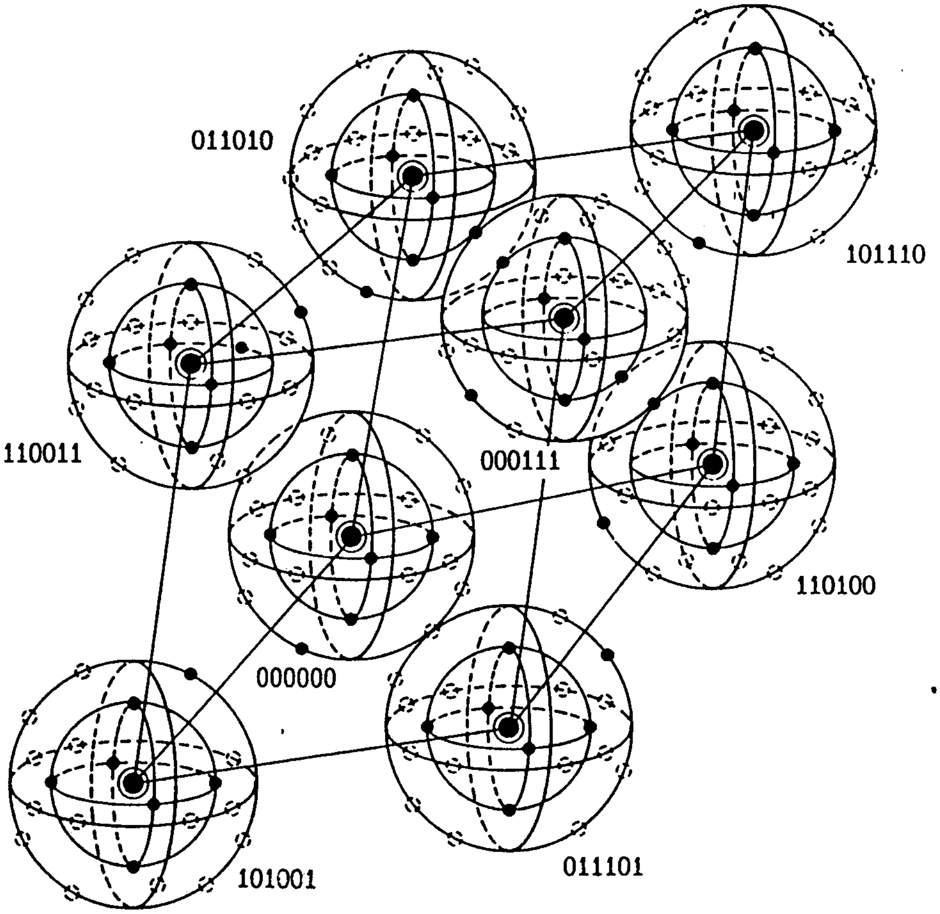
HENCE, PROBABILITY THAT n-BIT BLOCK IS DECODED IN ERROR IS

$$P_M \le \sum_{j=t+1}^{n}\binom{n}{j}p^j(1-p)^{n-j}$$

BIT-ERROR-PROBABILITY OF THE DECODER CAN BE APPROXIMATED AS:

$$P_B \approx \frac{1}{n}\sum_{j=t+1}^{n} j\binom{n}{j}p^j(1-p)^{n-j}$$

Example of 8 Codewords in a 6 - Tuple Space



Binary Cyclic Codes

Limitations of Linear Block Codes

- THE GENERATOR MATRIX COULD BE VERY LARGE.
  FOR (127, 92) CODE, WE NEED TO GENERATE 92x127 MATRIX
  TO GET A GOOD PERFORMANCE CODE, WE USUALLY NEED A VERY LARGE n AND k

- DIFFICULT TO IMPLEMENT IN HARDWARE

Binary Cyclic Codes

- A SUBCLASS OF LINEAR BLOCK CODES
- EASILY IMPLEMENTED VIA FEEDBACK SHIFT REGISTERS
- SYNDROME CALCULATION EASILY ACCOMPLISHED WITH FB SHIFT REGISTER
- ALGEBRAIC STRUCTURE LENDS ITSELF TO EFFICIENT DECODING METHODS

Description of Cyclic Codes

IF AN n-TUPLE

$V = (v_0, v_1, v_2, \ldots, v_{n-1})$ IS A CODE VECTOR OF C,

THEN $V^{(1)} = (v_{n-1}, v_0, v_1, \ldots, v_{n-2})$ IS ALSO A CODE VECTOR OF C

OR, IN GENERAL:

$V^{(i)} = (v_{n-i}, v_{n-i+1}, \ldots, v_{n-1}, v_0, v_1, \ldots, v_{n-i-1})$

IS A CODE VECTOR OF C

Cyclic Codes (Cont'd)

THE COMPONENTS OF A CODE VECTOR CAN BE TREATED AS THE COEFFICIENTS OF A POLYNOMIAL AS FOLLOWS:

$$V = (v_0, v_1, v_2, \ldots, v_{n-1}) \Longleftrightarrow V(X) = v_0 + v_1 X + v_2 X^2 + \ldots + v_{n-1} X^{n-1}$$

IN GENERAL, THE CODE POLYNOMIAL CORRESPONDING TO THE CODE VECTOR $V^{(i)}$ IS:

$$V^{(i)}(X) = v_{n-i} + v_{n-i+1} X + v_{n-i+2} X^2 + \ldots + v_{n-1} X^{i-1}$$
$$+ v_0 X^i + v_1 X^{i+1} + \ldots + v_{n-i+1} X^{n-1}$$

Cyclic Codes (Cont'd)

IT CAN BE SHOWN THAT $V^{(i)}(X)$ IS THE REMAINDER RESULTING FROM DIVIDING

$X^i V(X)$ BY $X^n + 1$

OR $$X^i V(X) = q(X)(X^n + 1) + \underbrace{V^{(i)}(X)}_{\text{REMAINDER}}$$

EXAMPLE

LET $V = 1101 \; (n = 4)$

$V(X) = 1 + X + X^3 \Big\}$ POLYNOMIAL IS WRITTEN LOW-ORDER TO HIGH-ORDER

LET $i = 3$; $X^3 V(X) = X^3 + X^4 + X^6$

DIVIDE BY $X^4 + 1$:

$$\begin{array}{r l}
 & X^2 + 1 \\
X^4 + 1 \,\big)\!\!\! & \overline{X^6 + X^4 + X^3} \\
 & \underline{X^6 \qquad\qquad\quad + X^2} \\
 & \qquad X^4 + X^3 + X^2 \\
 & \qquad \underline{X^4 \qquad\qquad + 1} \\
 & \qquad\qquad \left. X^3 + X^2 + 1 \right\} V^{(3)}(X) \text{ REMAINDER}
\end{array}$$

CODEWORD $\underline{V}^{(3)} = 1011$ IS 3 CYCLIC SHIFTS OF $\underline{V} = 1101$

Cyclic Code Properties

- IN AN (n, k) CYCLIC CODE THERE EXISTS ONE, AND ONLY ONE GENERATOR POLYNOMIAL g(X) OF DEGREE n - k

- COEFFICIENT g_0 OF g(X) MUST = 1

- $\underline{V}$ IS A CODEWORD iff g(X) DIVIDES INTO V(X) WITHOUT A REMAINDER

  $$V(X) = m(X)\,g(X)$$

  $$V(X) = (m_0 + m_1X + m_2X^2 + \cdots + m_{k-1}X^{k-1})\,g(X)$$

- g(X) IS A FACTOR OF $X^n + 1$

  $X^n + 1 = g(X)\,h(X)$ WHERE h(X) IS THE PARITY CHECK POLYNOMIAL

- IF g(X) IS A POLYNOMIAL OF DEGREE n - k AND IS A FACTOR OF $X^n + 1$, THEN, g(X) GENERATES AN (n, k) CYCLIC CODE

Cyclic Code Example

- g (X) IS A FACTOR OF $X^n + 1$
  $X^7 + 1 = (X^3 + X + 1)\ (X^4 + X^2 + X + 1)$

- USING $g(X) = X^3 + X + 1$ A POLYNOMIAL OF DEGREE $n - k$
  WE CAN GENERATE AN $(n, k) = (7, 4)$ CYCLIC CODE

- OR, USING $g(X) = X^4 + X^2 + X + 1$
  WE CAN GENERATE A (7, 3) CYCLIC CODE

Encoding in Systematic Form

MESSAGE POLYNOMIAL:

$$m(X) = m_0 + m_1X + m_2X^2 + \cdots + m_{k-1}X^{k-1}$$

MULTIPLYING m(X) BY X^{n-k}:

$$X^{n-k}\,m(X) = m_0X^{n-k} + m_1X^{n-k+1} + \cdots + m_{k-1}X^{n-1}$$

DIVIDING $X^{n-k}m(X)$ BY g(X)

$$X^{n-k}\,m(X) = q(X)\,g(X) + r(X)$$

$$\text{WHERE } r(X) = r_0 + r_1X + r_2X^2 + \cdots + r_{n-k-1}X^{n-k-1}$$

$$\underbrace{r(X) + X^{n-k}\,m(X)} = q(X)\,g(X)$$

A MULTIPLE OF g(X) WITH DEGREE n - 1 OR LESS
HENCE, A CODE POLYNOMIAL GENERATED BY g(X)

$$r(X) + X^{n-k}\,m(X) = r_0 + r_1X + \ldots + r_{n-k-1}X^{n-k-1} + m_0X^{n-k} + m_1X^{n-k+1} + \cdots + m_{k-1}X^{n-1}$$

CORRESPONDS TO CODE WORD:

$$(\underleftrightarrow{r_0, r_1, \cdots, r_{n-k-1},}\ \underleftrightarrow{m_0, m_1, \cdots, m_{k-1}})$$

n - k PARITY CHECK DIGITS — k INFORMATION DIGITS

Example: (7,4) Cyclic Code in Systematic Form

LET $g(X) = 1 + X + X^3$

$\underline{m} = 1011$

THEN $m(X)\ 1 + X^2 + X^3$

DIVIDE $X^{n-k}\, m(X)$ BY $g(X)$

$$\frac{X^3(1 + X^2 + X^3)}{1 + X + X^3} = \frac{X^3 + X^5 + X^6}{1 + X + X^3}$$

$q(X) = 1 + X + X^2 + X^3$ (quotient)

$r(X) = 1$ (remainder)

$V(X) = r(X) + X^3\, m(X)$

$$V(X) = 1 + X^3 + X^5 + X^6$$

$$\underline{V} = \underbrace{1\ 0\ 0}_{\text{PARITY}}\quad \underbrace{1\ 0\ 1\ 1}_{\text{MESSAGE}}$$

Polynomial Divisor Circuit

LET

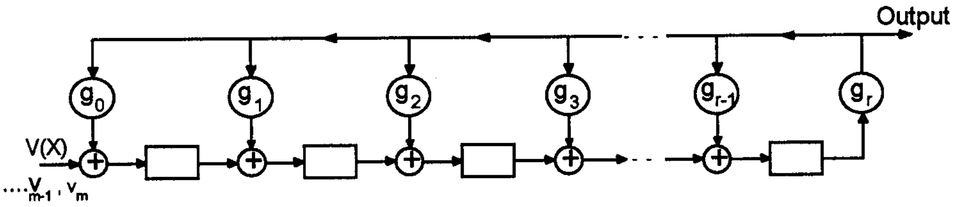
$$V(X) = v_0 + v_1X + v_2X^2 + \ldots\ldots\ldots\ldots + v_mX^m$$

$$g(X) = g_0 + g_1X + g_2X^2 + \ldots\ldots\ldots\ldots + g_rX^r$$

WE WANT TO

$$\frac{V(X)}{g(X)} = q(X) + \frac{r(X)}{g(X)}$$

USE CIRCUIT:



NOTE: g_r REPRESENTS EITHER CONNECTION OR NO CONNECTION DEPENDING ON g_r IN THE POLYNOMIAL g(X) EITHER A 1 OR 0 RESPECTIVELY.

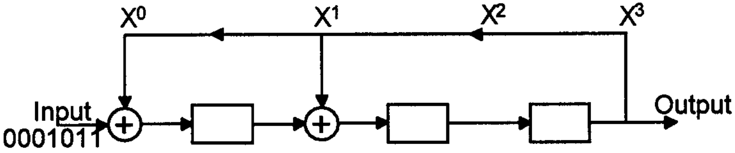
AT THE LAST SHIFT OF V(X) BITS INTO THE SHIFT REGISTERS, THE CONTENTS OF THE SHIFT REGISTERS ARE THE REMAINDER r(X).

EXAMPLE:

$$V(X) = X^3 + X^5 + X^6 \qquad (V = 0001011)$$

$$g(X) = 1 + X + X^3$$

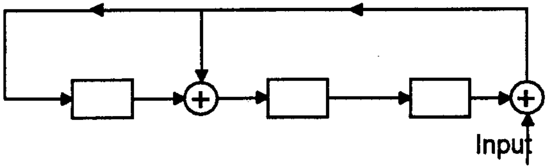
$g(X)$ IS OF DEGREE 3, SO WE NEED 3 REGISTERS:



PROBLEM WITH THIS CONFIGURATION:

THE FIRST 3 SHIFTS ARE JUST TO FILL THE 3 REGISTERS WITH THE FIRST 3 BITS OF $V(X)$. WE DO NOT HAVE ANY FEEDBACK HERE.

TO SHORTEN THE SHIFTING CYCLE:



THIS WORK PROVIDED: $g_0 = 1$ AND $g_r = 1$

Encoding with an (n-k) Stage Shift Register

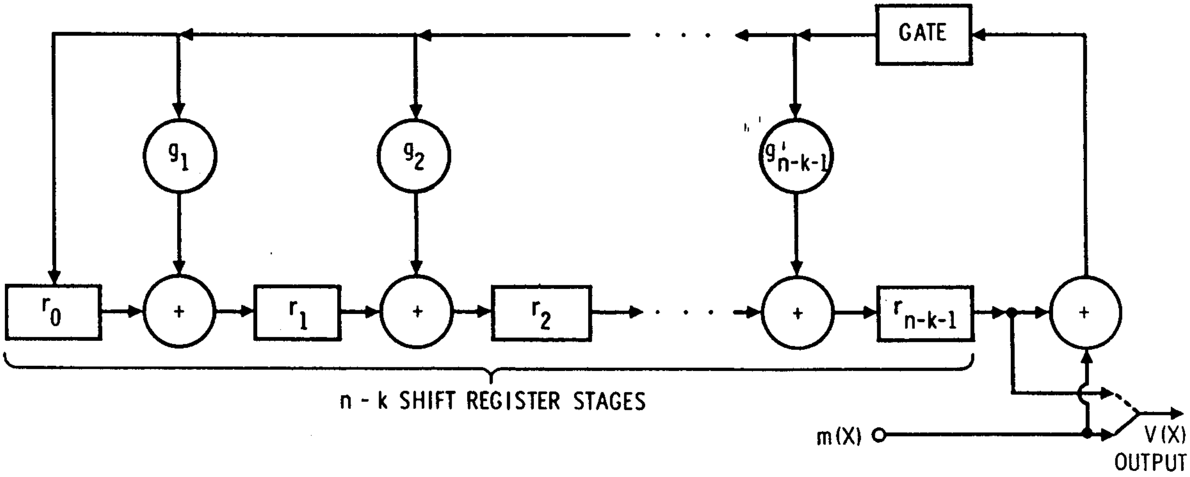
- ENCODING HAS BEEN SHOWN TO BE THE REMAINDER OF DIVIDING $X^{n-k}\, m(X)$ BY $g(X)$

- THIS IS ACCOMPLISHED BY A DIVIDING CIRCUIT (FB shift register)

- THE FEEDBACK CONNECTIONS CORRESPOND TO THE GENERATOR POLYNOMIAL

$$g(X) = 1 + g_1X + g_2X^2 + \ldots + g_{n-k-1}X^{n-k-1} + X^{n-k}$$

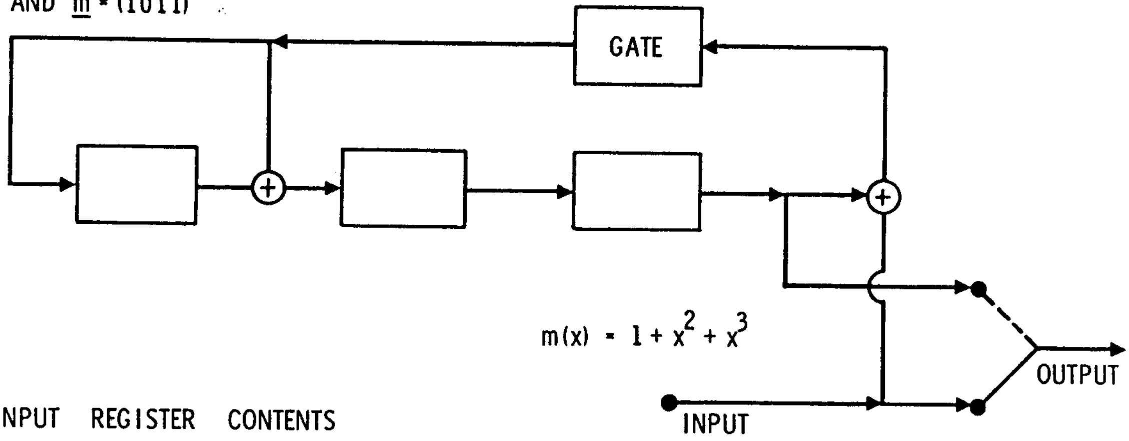
Encoding with an (n-k) Stage Shift Register



- WITH GATE ON, THE k INFORMATION DIGITS ARE SHIFTED INTO THE REGISTER AND SIMULTANEOUSLY TO THE OUTPUT
- THE GATE IS TURNED OFF (feedback disabled)
- THE CONTENTS OF THE SHIFT REGISTER ARE SHIFTED TO THE OUTPUT
- THE OUTPUT CODE POLYNOMIAL IS: $V(X) = r(X) + X^{n-k} m(X)$

Example: Encoding a (7,4) Code with an (n-k) Stage Shift Register

ASSUME: $g(X) = 1 + X + X^3$
AND $\underline{m} = (1011)$



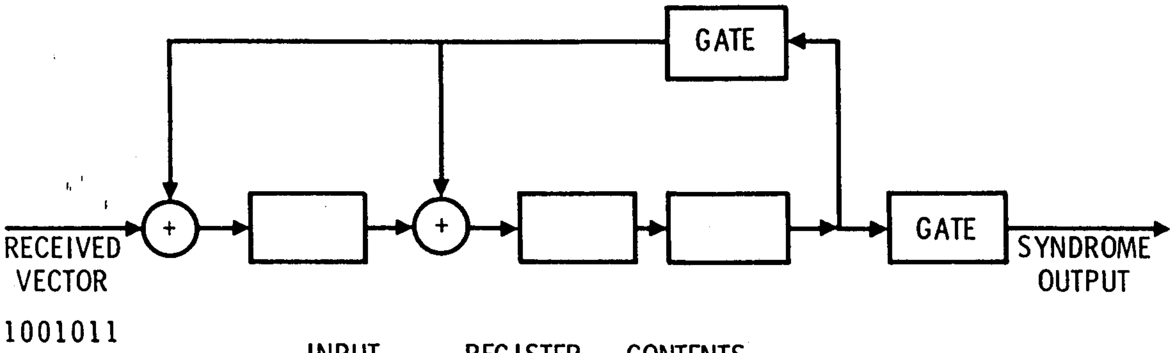
$m(x) = 1 + x^2 + x^3$

INPUT	REGISTER	CONTENTS
	0 0 0	INITIAL STATE
1	1 1 0	1ST SHIFT
1	1 0 1	2ND SHIFT
0	1 0 0	3RD SHIFT
1	$\boxed{1\ 0\ 0}$	PARITY DIGITS (4th shift)

THE OUTPUT CODEWORD IS: 1 0 0 1 0 1 1

THE CODE POLYNOMIAL IS: $1 + X^3 + X^5 + X^6$

Example: Syndrome Calculation with an (n-k) Shift Register



INPUT	REGISTER CONTENTS	
	0 0 0	INITIAL STATE
1	1 0 0	1ST SHIFT
1	1 1 0	2ND SHIFT
0	0 1 1	3RD SHIFT
1	0 1 1	4TH SHIFT
0	1 1 1	5TH SHIFT
0	1 0 1	6TH SHIFT
1	$\boxed{0\ 0\ 0}$	SYNDROME (7th shift)

AFTER THE ENTIRE RECEIVED VECTOR HAS BEEN ENTERED INTO THE SHIFT REGISTER, THE FINAL VALUE IS THE SYNDROME

WELL KNOWN BLOCK CODES

HAMMING CODES

$(N, K) = (2^M - 1,\ 2^M - 1 - M)$, WHERE $M = 2, 3, \ldots,$ AND $D_{MIN} = 3$

$P_B = P - P(1 - P)^{N-1}$, WHERE P IS THE PROBABILITY OF CHANNEL SYMBOL ERROR

EXTENDED GOLAY CODE

$(N, K) = (24, 12)$, WHERE $D_{MIN} = 8$

FORMED BY ADDING A PARITY BIT TO THE PERFECT GOLAY (23, 12) CODE

$$P_B = \frac{1}{24} \sum_{J=4}^{24} J \binom{24}{J} P^J (1 - P)^{24-J}$$

BCH CODES

FOR ANY POSITIVE INTEGERS M AND t, WHERE $M \geq 3$, AND $t \leq 2^{M-1}$, THERE EXISTS A BCH CODE WITH $N = 2^M - 1$, $(N - K) \leq Mt$, AND $D_{MIN} \geq 2t + 1$

REED-SOLOMON CODES

$(N, K) = (2^M - 1,\ 2^M - 1 - 2t)$, WHERE $M = 3, 4, \ldots$

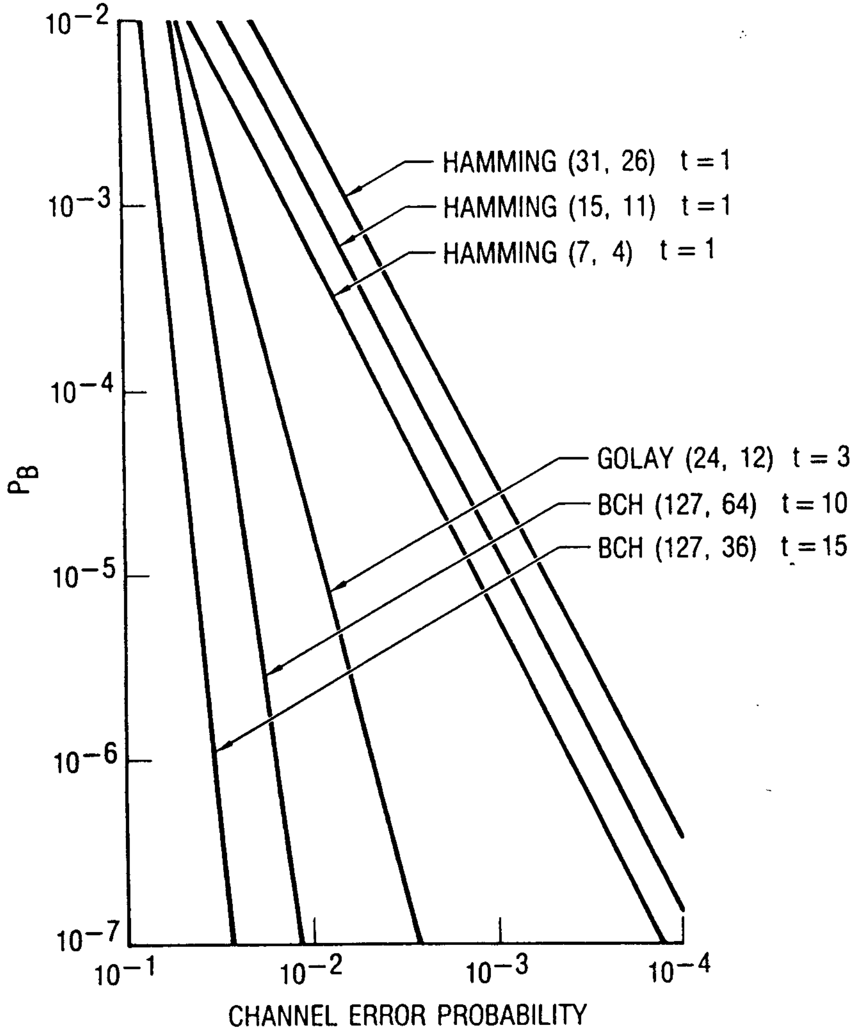
$D_{MIN} = N - K + 1$

$$P_E = \frac{1}{N} \sum_{J=t+1}^{N} J \binom{N}{J} P^J (1 - P)^{N-J}$$

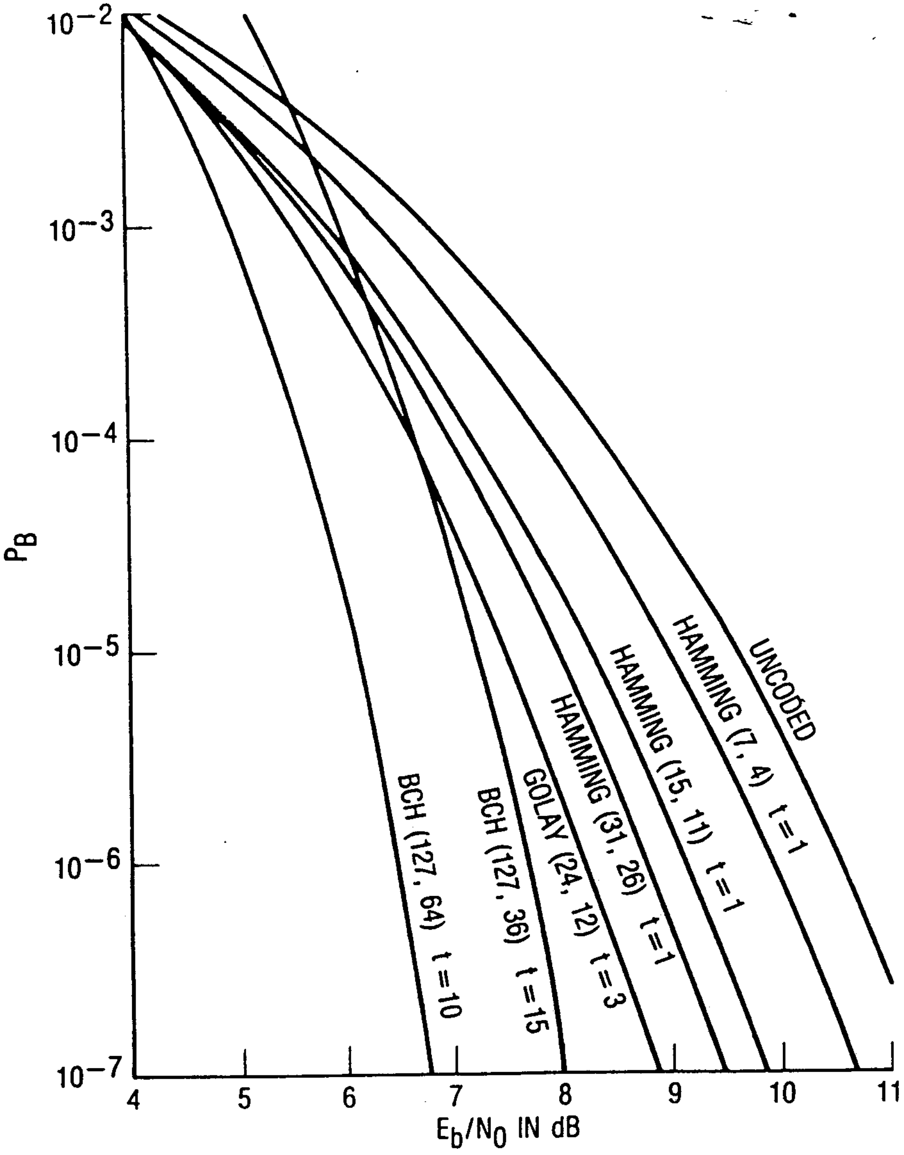
Generators of Primative BCH Codes

n	k	t	g (x)
7	4	1	13
15	11	1	23
	7	2	721
	5	3	2467
31	26	1	45
	21	2	3551
	16	3	107657
	11	5	5423325
	6	7	313365047
63	57	1	103
	51	2	12471
	45	3	1701317
	39	4	166623567
	36	5	1033500423
	30	6	157464165547
	24	7	17323260404441
	18	10	1363026512351725
	16	11	6331141367235453
	10	13	472622305527250155
	7	15	5231045543503271737
127	120	1	211
	113	2	41567
	106	3	11554743
	99	4	3447023271
	92	5	624730022327
	85	6	130704476322273
	78	7	26230002166130115
	71	9	6255010713253127753
	64	10	1206534025570773100045
	57	11	335265252505705053517721
	50	13	54446512523314012421501421
	43	14	17721772213651227521220574343
	36	15	3146074666522075044764574721735
	29	21	403114461367670603667530141176155
	22	23	123376070404722522435445626637647043
	15	27	22057042445604554770523013762217604353
	8	31	7047264052751030651476224271567733130217
255	247	1	435
	239	2	267543
	231	3	156720665
	223	4	75626641375
	215	5	23157564726421
	207	6	16176560567636227
	199	7	7633031270420722341
	191	8	2663470176115333714567
	187	9	52755313540001322236351
	179	10	22624710717340432416300455
255	171	11	15416214212342356077061630637
	163	12	7500415510075602551574724514601
	155	13	3757513005407665015722506464677633
	147	14	1642130173537165525304165305441011711
	139	15	461401732060175561570722730247453567445
	131	18	215713331471510151261250277442142024165471
	123	19	120614052242066003717210326516141226272506267
	115	21	60526665572100247263636404600276352556313472737
	107	22	22205772322066256312417300235347420176574750154441
	99	23	10656667253473174222741416201574332252411076432303431
	91	25	6750265030327444172723631724732511075550762720724344561
	87	26	110136763414743236435231634307172046206722545273311721317
	79	27	66700035637657500020270344207366174621015326711766541342355
	71	29	24024710520644321515554172112331163205444250362557643221706035
	63	30	10754475055163544325315217357707003666111726455267613656702543301
	55	31	7315425203501100133015275306032054325414326755010557044426035473617
	47	42	2533542017062646563033041377406233175123334145446045005066024552543173
	45	43	15202056055234161131101346376423701563670024470762373033202157025051541
	37	45	5136330255067007414177447245437530420735706174323432347644354737403044003
	29	47	3025715536673071465527064012361377115342242324201174114060254757410403565037
	21	55	12562152570603326560017731536076121032273414056530745425211531216144665134737253
	13	59	4641732005052564544426573714250066004330677445476561403174677213570261344605005 47
	9	63	157260252174724632010310432553551346141623672120440745451127661155477055 61677516057

Bit Error Probability vs Channel Error Probability for Several Block Codes



P_B vs E_b/N_0 Coded CBPSK Modulation



SPECIFICATIONS OF THE CROSS-INTERLEAVE REED-SOLOMON CODE (CIRC)

• ERROR CONTROL PROCEDURES:	• ERROR-CORRECTION • ERASURE CORRECTION • INTERPOLATION • MUTING
• MAXIMUM CORRECTABLE BURST LENGTH	~ 4000 BITS (2.5 MM TRACK LENGTH ON THE DISC)
• MAXIMUM INTERPOLATABLE BURST LENGTH	~ 12,000 BITS (8 MM)
• SAMPLE INTERPOLATION RATE	ONE SAMPLE EVERY 10 HOURS AT $P_B = 10^{-4}$ 1000 SAMPLES PER MINUTE AT $P_B = 10^{-3}$
• UNDETECTED ERROR SAMPLES (CLICKS)	LESS THAN ONE VERY 750 HOURS AT $P_B = 10^{-3}$ NEGLIGIBLE AT $P_B \leq 10^{-4}$
• NEW DISCS ARE CHARACTERIZED BY	$P_B \cong 10^{-4}$

Summary of Linear Block Codes

☞ MAP k-TUPLE MESSAGE TO n-TUPLE CODEWORD

☞ RULES OF MAPPING:

- CHOOSE THE n-TUPLES THAT SATISFY THE FOLLOWING:
  1. THE ALL-ZEROS n-TUPLE
  2. THE SUM OF ANY TWO n-TUPLE CODEWORDS MUST ALSO BE ANOTHER n-TUPLE CODEWORD
- THERE ARE ONLY 2^k n-TUPLES CHOSEN FROM TOTAL OF 2^n n-TUPLES BECAUSE THERE ARE ONLY 2^k MESSAGES

☞ TO GENERATE ALL THESE CODEWORDS, WE ONLY NEED TO HAVE THE LINEARLY INDEPENDENT n-TUPLE CODEWORDS (TOTAL NUMBER NEEDED IS k CODEWORDS). AND THE REST OF THE CODEWORDS ARE OBTAINED AS THE SUMS OF ANY 2 OF THESE.

☞ THESE LINEARLY INDEPENDENT CODEWORDS IS CALLED THE GENERATOR MATRIX:

$$\mathbf{G} = [\,\mathbf{P}\ \ \mathbf{I}_k\,]$$

☞ THE PARITY CHECK MATRIX $\mathbf{H}$:

$$\mathbf{H} = [\,\mathbf{I}_{n-k}\ \ \mathbf{P}^T]$$

CONDITION: $\mathbf{G}\mathbf{H}^T = \mathbf{0}$

Summary of Cyclic Codes

- ☞ SUBCLASS OF LINEAR BLOCK CODES WHERE THE STRUCTURE OF THE CODEWORDS CHOSEN FROM THE 2^n n-TUPLES IS CYCLIC
- ☞ CAN REPRESENT THESE CODES USING POLYNOMIAL
- ☞ IMPLEMENTED USING FEEDBACK SHIFT REGISTERS
- ☞ GENERATOR POLYNOMIAL:

$$g(X) = 1 + g_1X + g_2X^2 + \dots\dots\dots + g_{n-k}X^{n-k}$$ is a factor of X^n + 1

- ☞ SINCE CYCLIC CODES ARE BLOCK CODES, THEY SATISFY THE MAPPING RULES JUST DESCRIBED
- ☞ CAN REPRESENT $g(X)$ IN MATRIX FORM G IN THE FOLLOWING WAY:

1. GENERATE ALL CODEWORD: $U(X) = m(X).g(X)$
2. CHOOSE THOSE LINEARLY INDEPENDENT