ERROR-DETECTING CODES FOR COMPUTER
DATA COMMUNICATION SYSTEMS.

F. B. Wood

Outline, Abstract, and Illustrations for a talk given December 13, 1962, at a joint meeting of local chapters of the Institute of Radio Engineers Professional Group on Radio Frequency Interference and Professional Group on Space Electronics and Telemetry, Palo Alto, California.

This paper is a survey on the history and application of error-detecting codes for computer data communication systems. The subject is introduced by a non-technical explanation of error-detection and error-correction processes with some historical data on the mathematical concepts such as Galois fields and the electronic technology and computer programming upon which the practical use of codes are dependent. The techniques of choosing a code to match the error statistics are reviewed, first using empirical error statistics and second using a noise model.

The engineer is usually confronted with meager error statistics. Techniques of graphically plotting whatever inadequate error data is available are illustrated as a method of finding a confidence interval for the inadequate data and for determining what further data on error statistics would be useful.

NOTE ON STATUS OF DATA IN THIS PAPER

No new codes or recommendations for standards are included. The codes and circuits used as examples are taken from published references. Where results of computer simulations of error detection using data of American Telephone and Telegraph Co. or from data of M.I.T Lincoln Laboratory, only the material released for publication by the original source is used.

NOTE ON EMPHASIS

Emphasis is upon understanding error detection codes from several different viewpoints such as generating polynomials, from Galois fields, linear equations, binary arithmetic, group theory, shift register logic, and matrix algebra. In the evaluation of codes the emphasis is upon techniques of interpreting error statistics and computer simulation of error detection. A method of replotting data from different sources for different conditions is used to illustrate ways of comparing different codes.

List of Flip Charts.

No.	Title
1. ω	Title
A. ω	Outline
2. ω	Pictorial Sketch
B. ω	Systems
3.	Sample Waveforms: Noise, Signal, S+N.
4.	Noise Probability Curves for : Thermal Noise (Normal) and Impulse Noise (Log-Normal).
5. ω	Noise Model(Gilbert)
C. ω	Outline - Error Detection
6.	List of Major Steps in Cyclic Code Theory.
D. ω	Outline - Mathematical Concepts
7. ω	Analogy Between Error Correcting Code and Linear Equations.
8. ω	(cont. of 7) and Example of Hamming Code.
9. ω	Hamming Distance
10.	Galois and GF(p)
11.	GF(3) and Definition of GF(p^m)
12. ω	GF(3^2) $j^2+1=0$
13. ω	GF(3^2) $j^2-j-1=0$(mod 3)
14. ω	Multiplication Vector Q in GF(2^3) for $Q+1=Q^3$
15. ω	Binary Multiplication $Q^3=Q+1$
16. ω	Feedback Shift Register Logic $Q^3=aQ^2+bQ+c$
17. ω	Transposition of Hamming Code to Fit Cyclic Code on FSR.
18. ω	Matrix Code Generator
19. ω	Circuit Realization of Matrix Generator
20. ω	Alternative Realization Defined by Reduced Linear Equations.
21. ω	Mutiply and Divide Circuits.
22. ω	Non-Systematic Coding
23.	Systematic Coding Circuit.
24.	Sample Runs of: Coding, Checking and Error Location.
25.	Major Cyclic Codes: Characteristic Equations.
E. ω	Outline: Questions
26. ω	Questions on Code Selection.

27. ω Outline of Procedure.

28. ω Plotting Error Statistics.

29. ω Replotting of Data from AIEE CP61-1130

30. ω Replotting of Data from MIT Lincoln Laboratory Proc.I.R.E. v. 49, p. 1059-

31. ω Sample of an Incomplete Test (Illustrates What Features From Theory Can Be Used To Limit Extrapolations From Incomplete Data)

ERROR-DETECTING CODES FOR COMPUTER DATA COMMUNICATION SYSTEMS

COMPUTER

COMMUNICATION

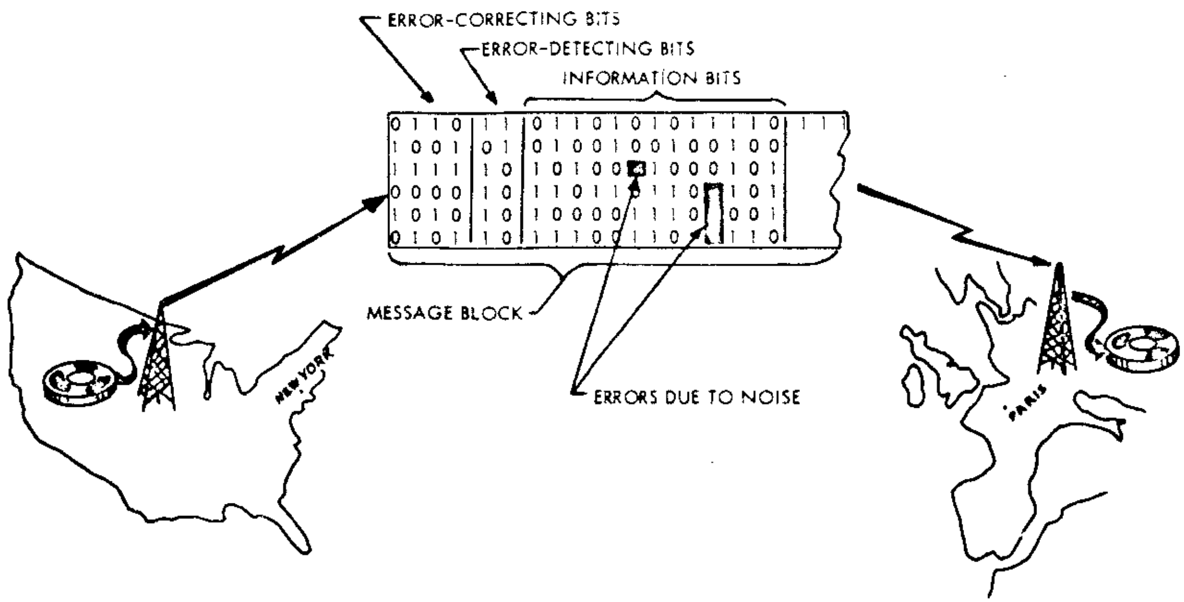
SYSTEMS & ERRORS

ERROR DETECTION

ALTERNATIVE MATH

CONCEPTS IN CYCLIC CODE THEORY

QUESTIONS ON CODE SELECTION



EVALUATION OF CODES REQUIRED TO GUARANTEE RELIABILITY OF TRANSMISSION

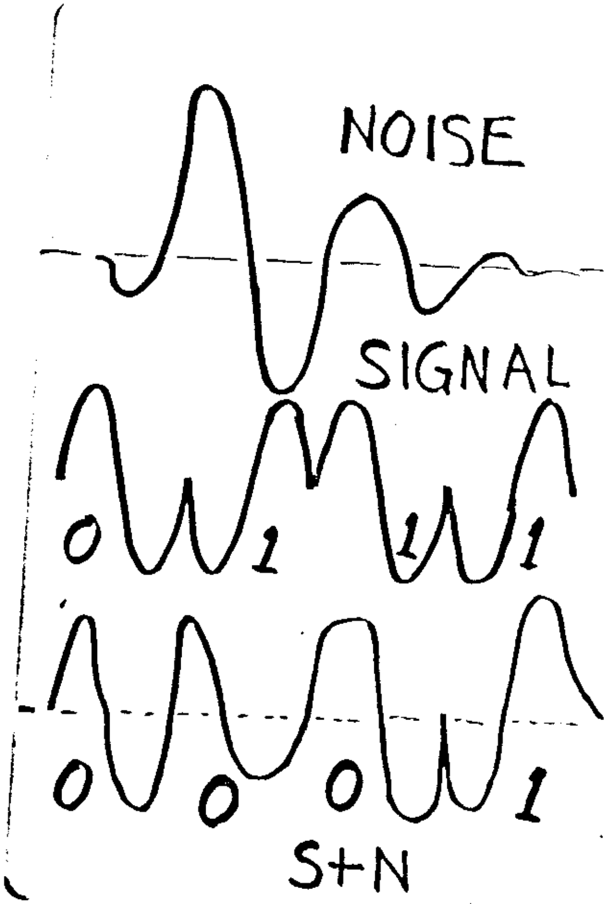
No. 2

COMPUTER
COMMUNICATION
SYSTEMS

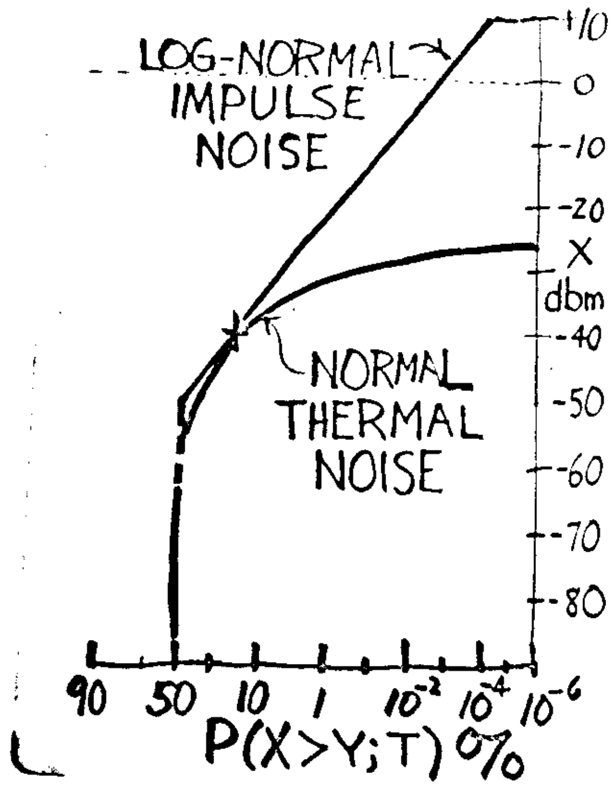
SIGNAL & NOISE

NOISE PROBABILITY

ERROR PROBABILITY MODEL

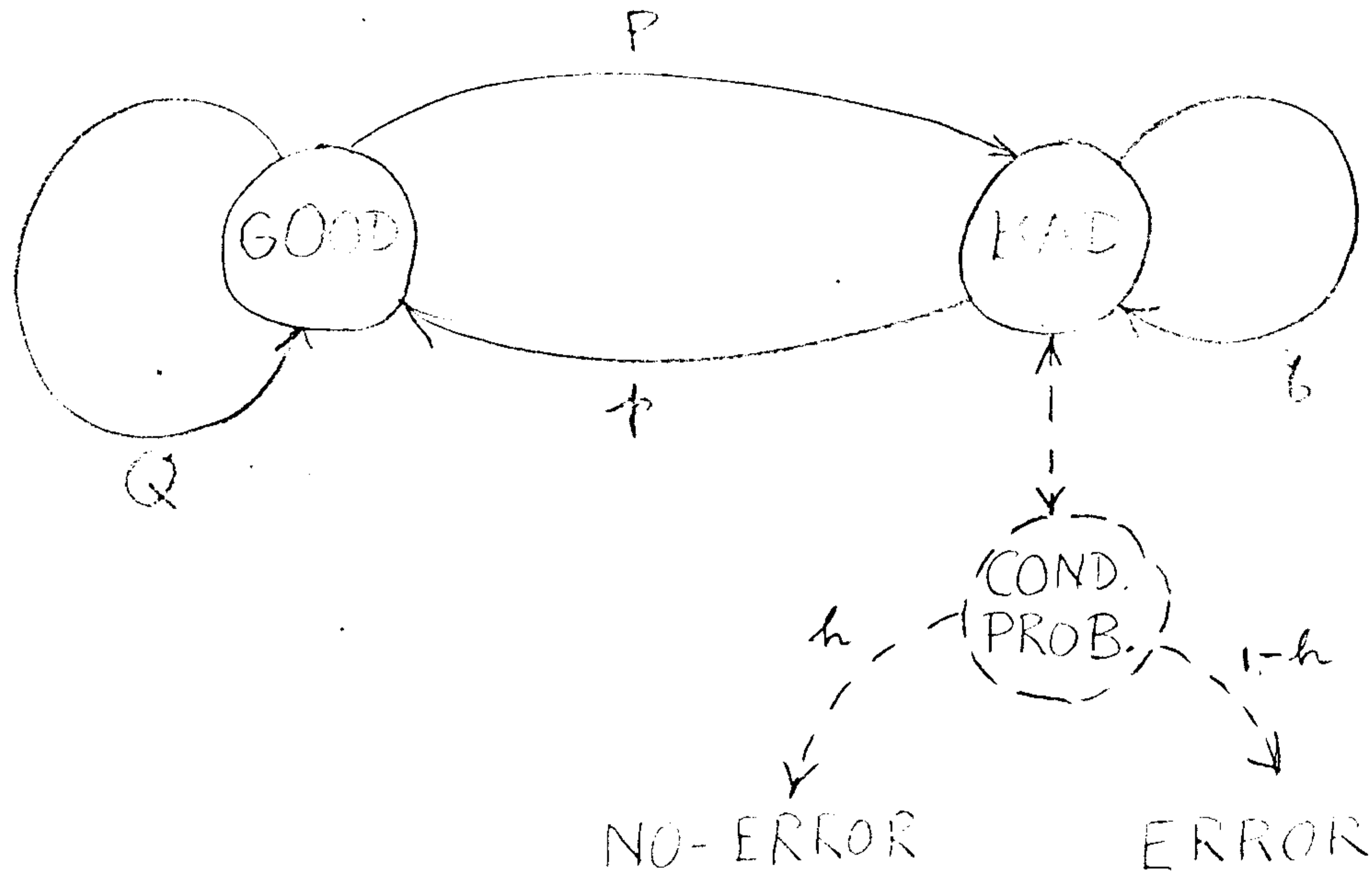

NOISE
SIGNAL
0 1 1 1
0 0 0 1
S+N

No. 3


LOG-NORMAL
IMPULSE
NOISE
NORMAL
THERMAL
NOISE
+10
0
-10
-20
X
dbm
-40
-50
-60
-70
-80
90 50 10 1 10^-2 10^-4 10^-6
P(X>Y;T) %

No. 4

GILBERT, E. N. [illegible]



SLIDE [illegible]

ERROR DETECTION

- SIMPLE PARITY
- INTERLACED PARITY CHECKS
- CYCLIC GROUP CODES
- SHORT HISTORY

MAJOR STEPS IN CYCLIC CODE THEORY

1950	Hamming	Error Correction
1956	Huffman	Linear Circuits
	Slepian	Unified Theory
1957	Prange	Ideals = Cyclic
1958	Green & San Soucie	K-Stage
1958	Prange	Shift Registers
1959	Abramson	Systematic Daec
	Fire	Burst Codes
	Melas	Dependent E. C.
	Kautz	Geometric Int.
	Elspas	Linear Seq. NTW.
1960	Meggitt	Matrix Der. Ckt.
	Peterson	n-k Shift Reg.
		Alternative Ckts.
		Organized Theorems
1960	Bose-Chandhuri	Generalized MTPL
(1959)	Hocquenghem	Error Correction
1961	Brown & Peterson	Add'tl Theorems

EXAMPLE OF
CYCLIC CODE

EQUIV.
HAMMING
CODE

ALTERNATIVE
MATHEMATICAL
CONCEPTS

REDUNDANT LINEAR,
EQUATIONS

GALOIS FIELDS

GENERATING
POLYNOMIAL

VECTOR MPY

BINARY MPY

SWITCHING CKT = FSR

MATRIX GEN (T)

REDUCED LIN EQ.

ENCODE
$\Updownarrow$
MULTIPLY

DECODE
$\Updownarrow$
DIVIDE

1 1 0 1

(1) $a_{11}w + a_{12}x + a_{13}y + d_{14}z = S_1$ $\quad w = 1$

(2) $a_{21}w + b_2x + c_2y + d_2z = S_2$ $\quad x = 1$

(3) $a_{31}w + b_3x + c_3y + d_3z = S_3$ $\quad y = 0$

(4) $a_{41}w + b_4x + c_4y + d_4z = S_4$ $\quad z = 1$

(5) $= (1)+(2)+(3)$ $a_{51}w + b_5x + c_5y + d_5z = S_5$

(6) $= (1)+(2)+(4)$ $a_{61}w + b_6x + c_6y + d_6z = S_6$

(7) $= (1)+(3)+(4)$ $a_{71}w + b_7x + c_7y + d_7z = S_7$

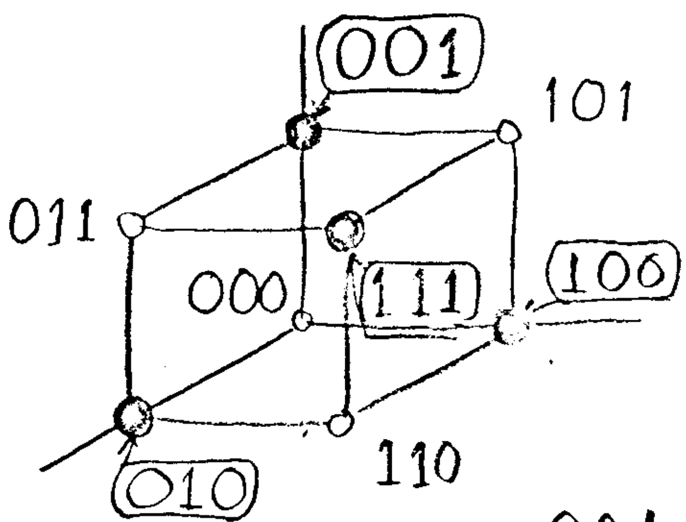
SLIDE 7

$a_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ for $i, j = 1, 2, 3, 4$

$$
\begin{array}{ccccccccc}
w & & & & = & S_1 & & \\
 & x & & & = & S_2 & & \\
 & & y & & = & S_3 & & \\
 & & & z & = & S_4 & & \\
S_1 & + S_2 & + S_3 & & = & S_5 & & \\
S_1 & + S_2 & & + S_4 & = & & S_6 & \\
S_1 & & + S_3 & + S_4 & = & & & S_7
\end{array}
$$

	D_1	D_2	D_3	D_4	P_1	P_2	P_3
P_1	X	X	X		X		
P_2	X	X		X		X	
P_3	X		X	X			X

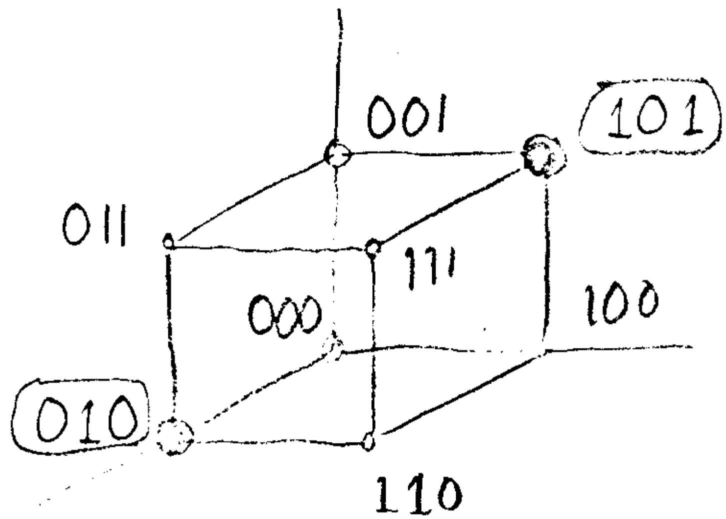
No. 9



001
010
100
111

D = 2

SED



D = 3

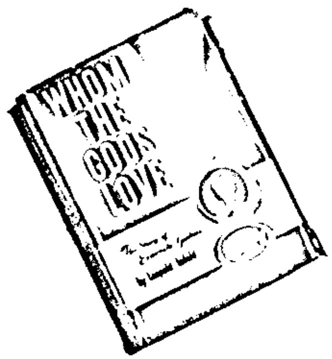
SEC
DED

101
010

No. 9

ÉVARISTE GALOIS

(1811 — 1832)



RESIDUE CLASSES OF INTEGERS MODULO ANY PRIME NUMBER p FORM A FIELD OF p ELEMENTS CALLED the GALOIS FIELD GF(p).

Example of GF(3):

$$\begin{array}{ccccccccc} -4 & -3 & -2 & -1 & 0 & +1 & +2 & +3 & +4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ -1 & 0 & +1 & -1 & 0 & +1 & -1 & 0 & +1 \end{array}$$

Example of GF(2)

$$\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ \downarrow & & \downarrow & & \downarrow & \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

THE FIELD OF POLYNOMIALS OVER GF(p) MODULO AN IRREDUCIBLE POLYNOMIAL OF DEGREE m IS CALLED THE GALOIS FIELD OF p^m ELEMENTS OR GF(p^m), I.E. A VECTOR SPACE OF DIMENSION m OVER GF(p).

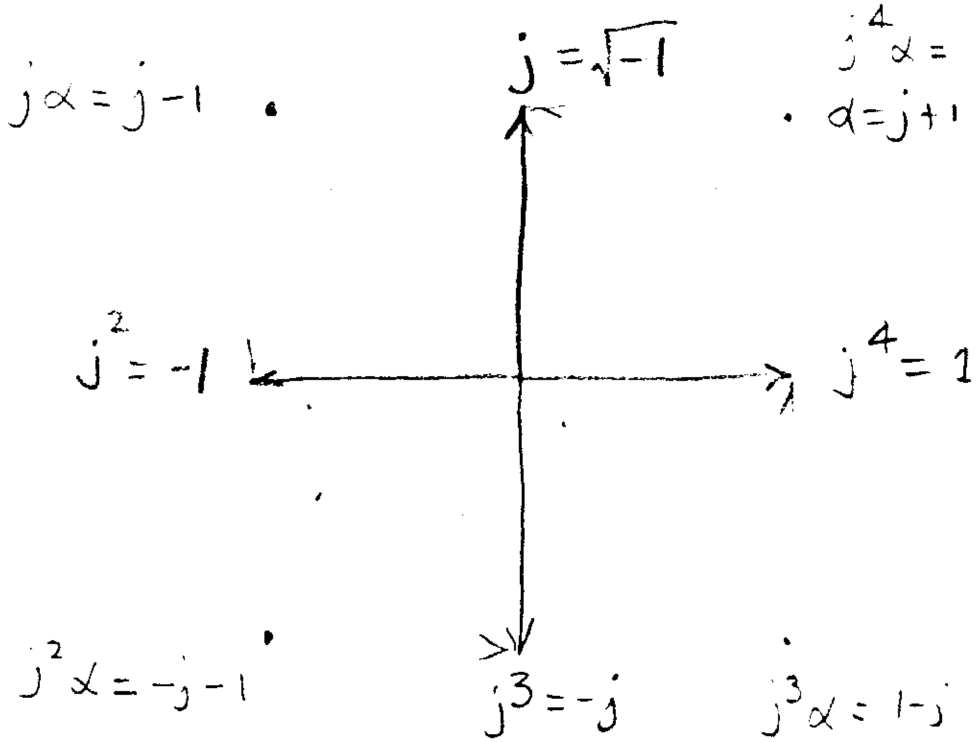
$0 = 0 \pmod 3$

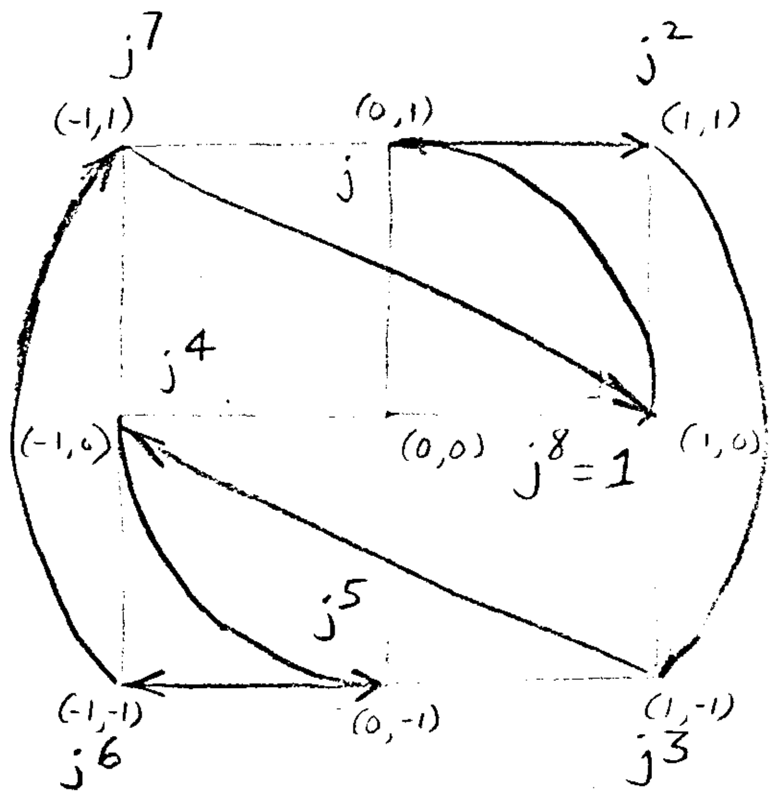
$1 = +1 \pmod 3$

$2 = -1 \pmod 3$

$3 = 0 \pmod 3$

$4 = +1 \pmod 3$



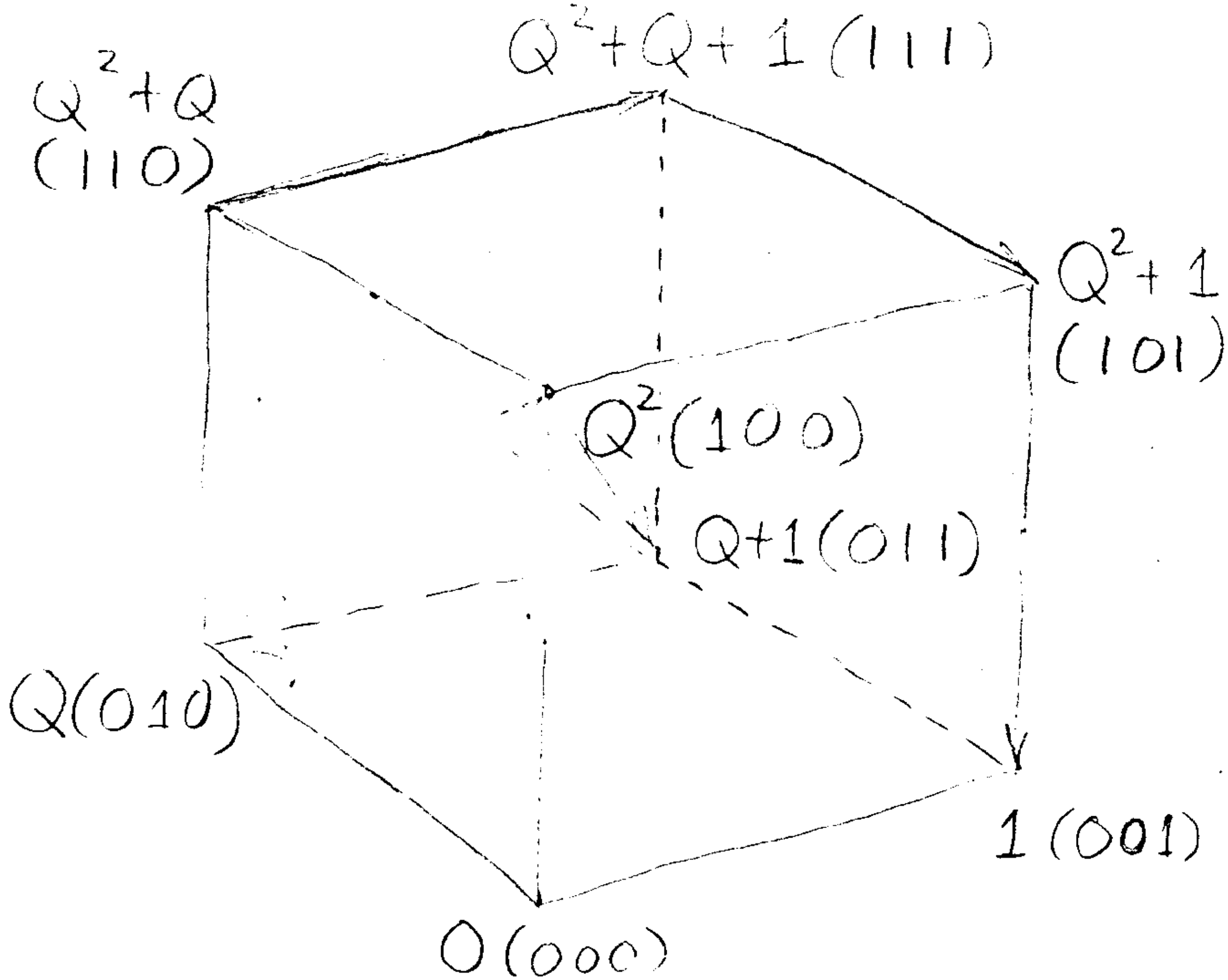


COMPLEX NUMBERS

$j^2 + 1 = 0$

ALGEBRAIC NUMBER FIELD

$GF(3^2)$ $j^2 - j - 1 = 0 \pmod 3$



$$Q^0 = 1$$
$$Q^1 = Q$$
$$Q^2 = Q^2$$
$$Q^3 = Q + 1$$
$$Q^4 = Q^2 + Q$$
$$Q^5 = Q^3 + Q^2 = Q^2 + Q + 1$$
$$Q^6 = Q^3 + Q^2 + Q = Q^2 + 1$$
$$Q^7 = Q^3 + Q = 1$$

$[aQ^2 + bQ + c]$ $\quad Q^3 + Q + 1 = 0$

$GF(2^3)$

No. 14

$$Q^0 = 001$$

$$Q^1 = 010$$

$$Q^2 = 010 \times 010 = 100$$

$$Q^3 = 010 \times 100 = 1000 \equiv 011$$

$$Q^4 = 010 \times 011 = 110$$

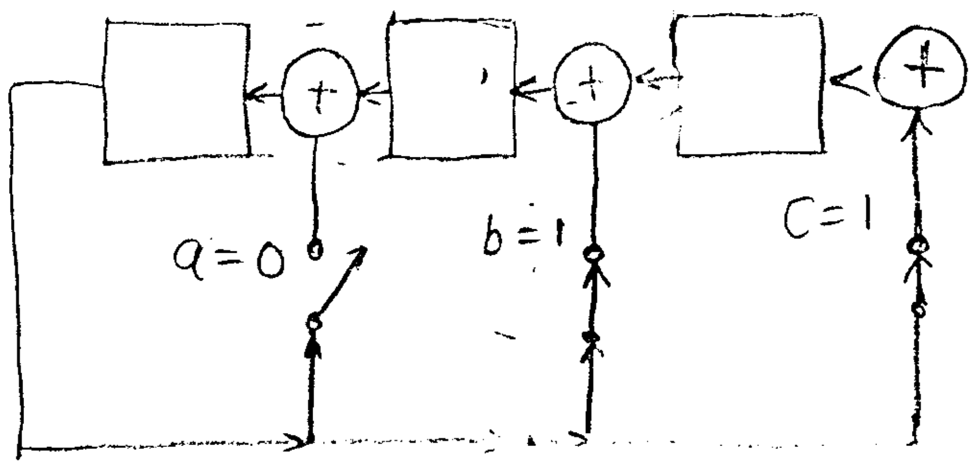
$$Q^5 = 010 \times 110 = 1100 = 011 + 100$$
$$= 111$$

$$Q^6 = 010 \times 111 = 1110 = 011 + 110$$
$$= 101$$

$$Q^7 = 010 \times 101 = 1010 = 011 + 010$$
$$= 001$$

$$Q^3 = Q + 1$$

$Q^3 = aQ^2 + bQ + c$



$Q^3 + Q + 1 = 0$

0	0	1	$= Q^0 = 1$
0	1	0	$= Q^1$
1	0	0	$= Q^2$
0	1	1	$= Q^3$
1	1	0	$= Q^4$
1	1	1	$= Q^5$
1	0	1	$= Q^6$
0	0	1	$= Q^7 = 1$

FEEDBACK SHIFT REGISTER

	P_3	P_2	P_1
D_1	1	1	1
D_2	0	1	1
D_3	1	0	1
D_4	1	1	0
P_1	0	0	1
P_2	0	1	0
P_3	1	0	0

D_2	0	1	1	$\longrightarrow Q^3$
D_4	1	1	0	$\longrightarrow Q^4$
D_1	1	1	1	$\longrightarrow Q^5$
D_3	1	0	1	$\longrightarrow Q^6$
P_1	0	0	1	$\longrightarrow Q^7 = Q^0$
P_2	0	1	0	$\longrightarrow Q^1$
P_3	1	0	0	$\longrightarrow Q^2$

MODIFIED HAMMING CODE
TABLE & FSR STAGES

IRREDUCIBLE POLYNOMIAL:

$$Q^k + c_{k-1}Q^{k-1} + c_{k-2}Q^{k-2} + \cdots + c_1 Q + c_0 = 0$$

FIND MATRIX $\underline{T}$

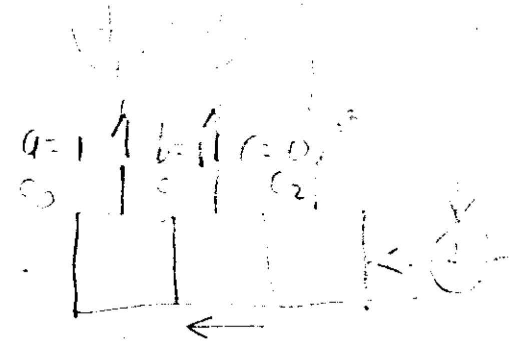
$$\phi(\underline{T}) = \underline{T}^k + c_{k-1}\underline{T}^{k-1} + c_{k-2}\underline{T}^{k-2} + \cdots + c_1\underline{I} + c_0 = 0$$

IF PRIMITIVE: $\underline{T}^{e} = \underline{I}$, $e = 2^k - 1$

$$\underline{T} = \left\| \begin{matrix} c_{k-1} & c_{k-2} & \cdots & c_1 & c_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{matrix} \right\|$$

$$Q^3 = Q + 1$$

$$\underline{T} = \left\|\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{matrix}\right\| \qquad \underline{x}_1 = \begin{Bmatrix} 1 \\ 0 \\ 0 \end{Bmatrix}$$



$$Q^3 = \underset{c_0}{a} + \underset{c_1}{b}Q + \underset{c_2}{c}Q^2$$

$$\begin{array}{ccccl} 0 & 0 & 1 & = & \underline{x}_1 \\ 0 & 1 & 0 & = & \underline{T}^1 \underline{x}_1 \\ 1 & 0 & 1 & = & \underline{T}^2 \underline{x}_1 \\ 0 & 1 & 1 & = & \underline{T}^3 \underline{x}_1 \\ 1 & 1 & 1 & = & \underline{T}^4 \underline{x}_1 \\ 1 & 1 & 0 & = & \underline{T}^5 \underline{x}_1 \\ 1 & 0 & 0 & = & \underline{T}^6 \underline{x}_1 \\ \hline 0 & 0 & 1 & = & \underline{T}^7 \underline{x}_1 = \underline{x}_1 \end{array}$$

$$\left|\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{matrix}\right| \times \left|\begin{matrix} 1 \\ 0 \\ 0 \end{matrix}\right| = \left|\begin{matrix} 0 \\ 1 \\ 0 \end{matrix}\right|$$

$$\left|\begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{matrix}\right| \times \left|\begin{matrix} 0 \\ 1 \\ 0 \end{matrix}\right| = \left|\begin{matrix} 1 \\ 0 \\ 1 \end{matrix}\right|$$

etc.

No. 17

CYCLIC

CODE with digits

K linear equations define K of the a's in terms of other

$$a_1 \underline{x} + a_2 \underline{T}\underline{x} + a_3 \underline{T}^2 \underline{x} + \cdots + a_m \underline{T}^{m-1} \underline{x} = 0$$

$$a_1 \begin{Bmatrix} 1 \\ 0 \\ 0 \end{Bmatrix} + a_2 \begin{Bmatrix} 0 \\ 1 \\ 0 \end{Bmatrix} + a_3 \begin{Bmatrix} 1 \\ 0 \\ 1 \end{Bmatrix} + a_4 \begin{Bmatrix} 1 \\ 1 \\ 0 \end{Bmatrix} + a_5 \begin{Bmatrix} 1 \\ 1 \\ 1 \end{Bmatrix} + a_6 \begin{Bmatrix} 0 \\ 1 \\ 1 \end{Bmatrix} + a_7 \begin{Bmatrix} 0 \\ 0 \\ 1 \end{Bmatrix} = 0$$

$$\boxed{a_5 = a_1 + a_3 + a_4}$$

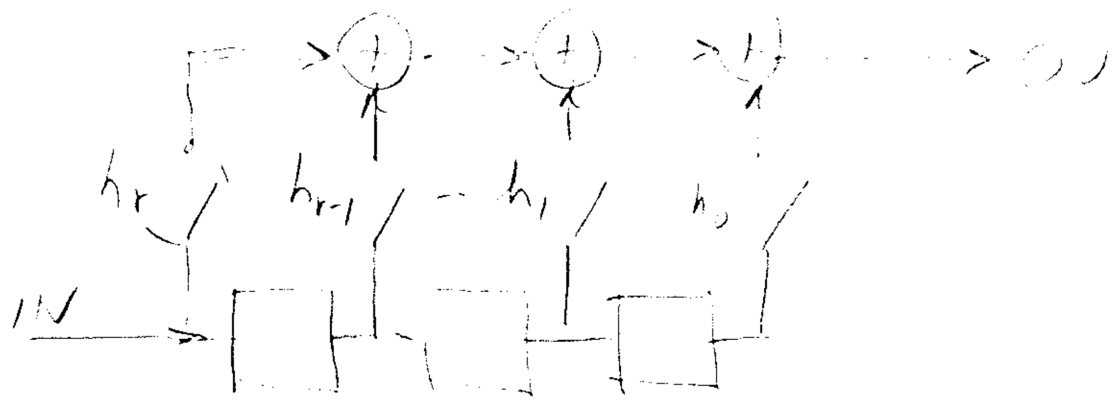
$$a_6 = a_2 + a_4 + a_5$$

$$a_7 = a_3 + a_5 + a_6$$

$$a_i + a_{i+2} + a_{i+3} = a_{i+4}$$

No. 3

MULTIPLY



$a(x) \cdot h(x)$

$a(x) = a_0 + a_1 X_1 + \cdots + a_k X^k$

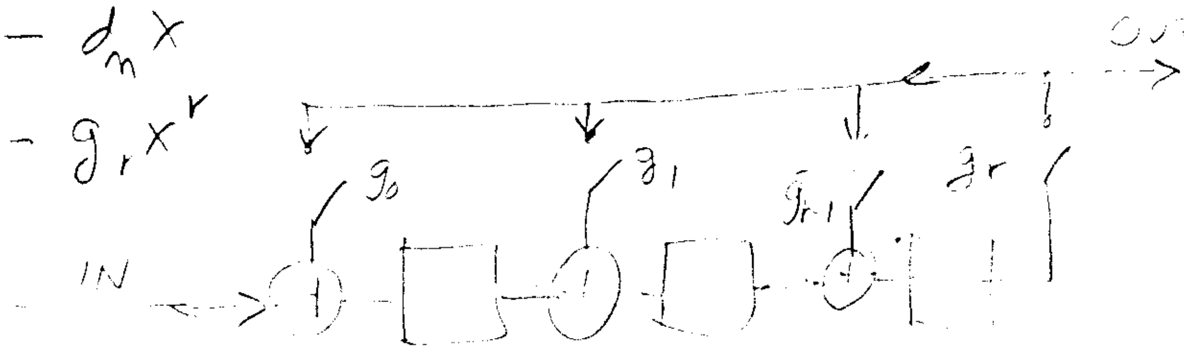
$h(x) = h_0 + hX + \quad + h_r X^r$

DIVIDE

$d(X) = d_0 + d_1 X + \cdots - d_n X^n$

$g(x) = g_0 + g_1 x + \cdots - g_r x^r$

$\frac{d(x)}{g(x)}$



MESSAGE $G(X) = X + X^3 = 0101$

CODE POLYNOMIAL

$P(X) = 1 + X + X^3 = 1101$

MPY:
(CODING)

$$\begin{array}{r} X + X^3 \\ 1 + X + X^3 \\ \hline +X^4 \quad X^6 \\ +X^2 \quad +X^4 \\ +X \quad +X^3 \\ \hline X + X^2 + X^3 \qquad X^6 \end{array}$$

$$\begin{array}{r} 0101 \\ 1101 \\ \hline 0101 \\ 0101 \\ 0101 \\ \hline 0111001 \end{array}$$

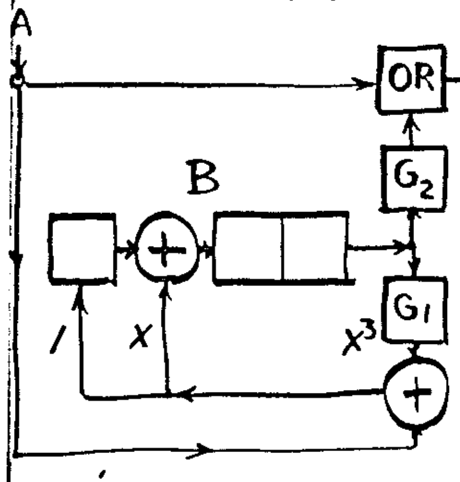
NON-SYSTEMATIC CODING

DIV (DECODING)
(DECODING)

$$\begin{array}{r} 0101 \\ 1101 \overline{)0111001} \\ 1101 \\ \hline 1101 \\ 1101 \\ \hline 0 \end{array}$$

SYSTEMATIC CODING

$$F(x) = \frac{G(x)}{P(x)} + X^{n-K} G(x)$$



001
110
011
111
101
100
010
001

No. 23

t	A	B	G_1	G_2	C
0	1	000	1	0	
1	0	110	1	0	1
2	1	011	1	0	01
3	0	001	1	0	101
4		110	1	0	0101
5		11	0	1	00101
6		1	0	1	100101
7			0	1	1100101

t	A	B	G_1	G_2	C
4	0	110	1	0	0101
5	1	011	0	1	00101
6	1	001	0	1	100101
7		$\boxed{000}$	0	1	1100101

t	A	B	G_1	G_2	C
0	1	000	1	0	
1	1	110	1	0	1
2	1	101	1	0	11
3	0	010	1	0	011
4	0	001	1	0	0111
5	1	110	0	1	00111
6	1	101	0	1	100111
7		010	0	1	1100111

No. 24

MAJOR CYCLIC CODES.

HAMMING (SEC): m^{th} ord.

$n = 2^m - 1 \quad \phi(\underline{T}) = 0$

SEC;DAEC: $(m-1)^{ST}$ order for $\phi_1[\underline{I}]$ $[\phi_1(\underline{T})][\underline{T}+\underline{I}] = 0$

FIRE BURST:

$$[\phi_1(\underline{T})][\underline{T}^{m_2}+\underline{I}] = 0$$

MELAS BURST: m_1 & m_2

$$\phi(\underline{T}) = \phi_1(\underline{T}) \cdot \phi_2(\underline{T}) = 0$$

BOSE-CHADHURI-HOCQUENGHEM

$$\phi(\underline{T}) = \prod_{i=1}^{t} \phi_i(\underline{T})$$

$\phi_1(\underline{T})$ for $\underline{T}_1$; $\phi_i(\underline{T})$ for $\underline{T}_1^{2i-1}$

No. 25

QUESTIONS ON CODE SELECTION

PROCEDURE

CODE

CHANNEL

UND. ER

HOW TO REPLOT
PUBL'SD DATA TO
SQUEEZE OUT SIG.
FACTS

AIEE (P61-1130)
OCT. 1961 IBM/ATT

PROC. IRE 49:1059
JUNE, 1961 MIT-LINCOLN

SOME INCOMPLETE DATA

CONSIDER COMPUTER
COMMUNICATION SYSTEM,

HOW MANY PARITY BITS?

WHICH CODE?

DETECTION ONLY?

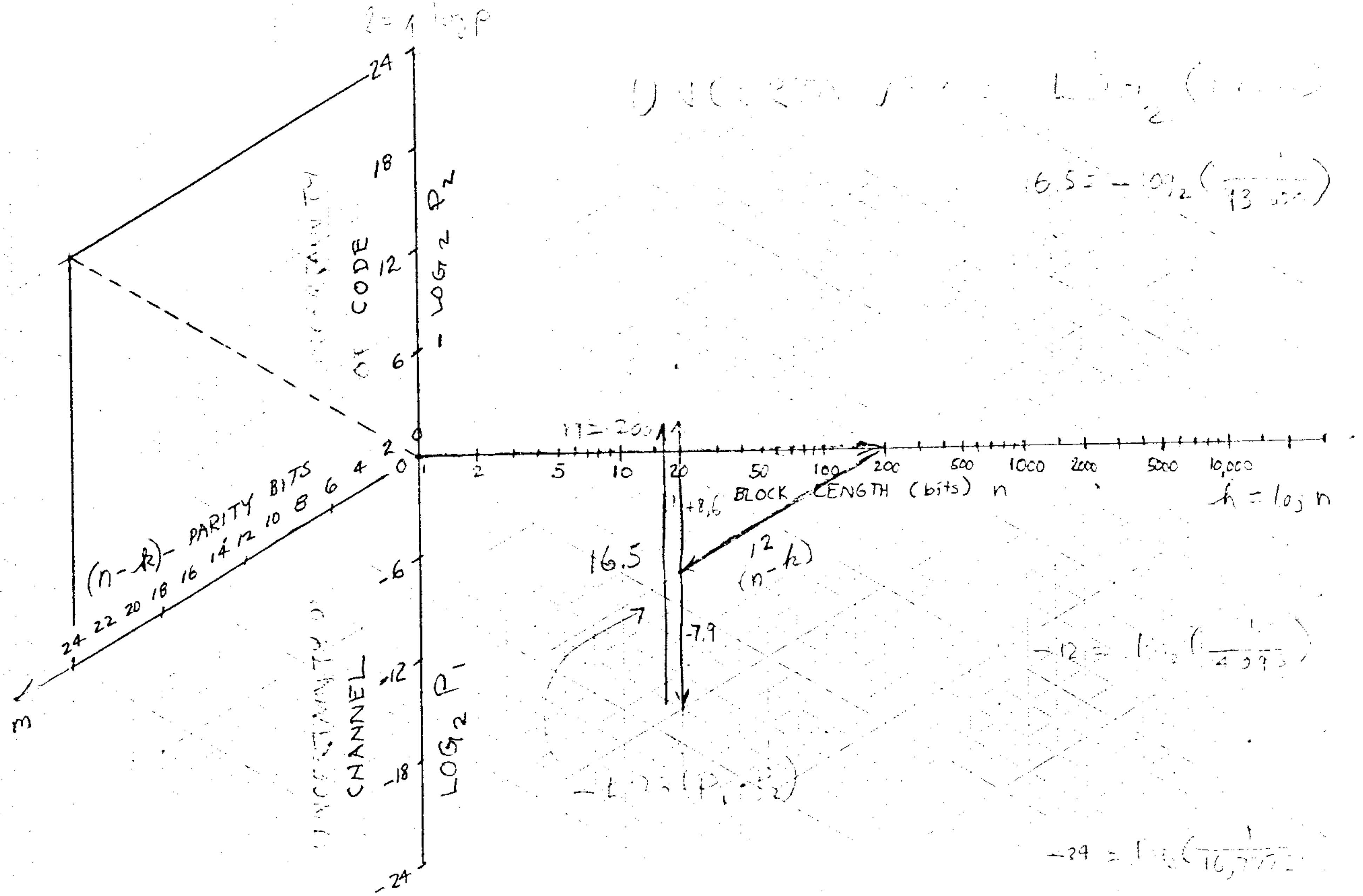
OR CORRECTION?

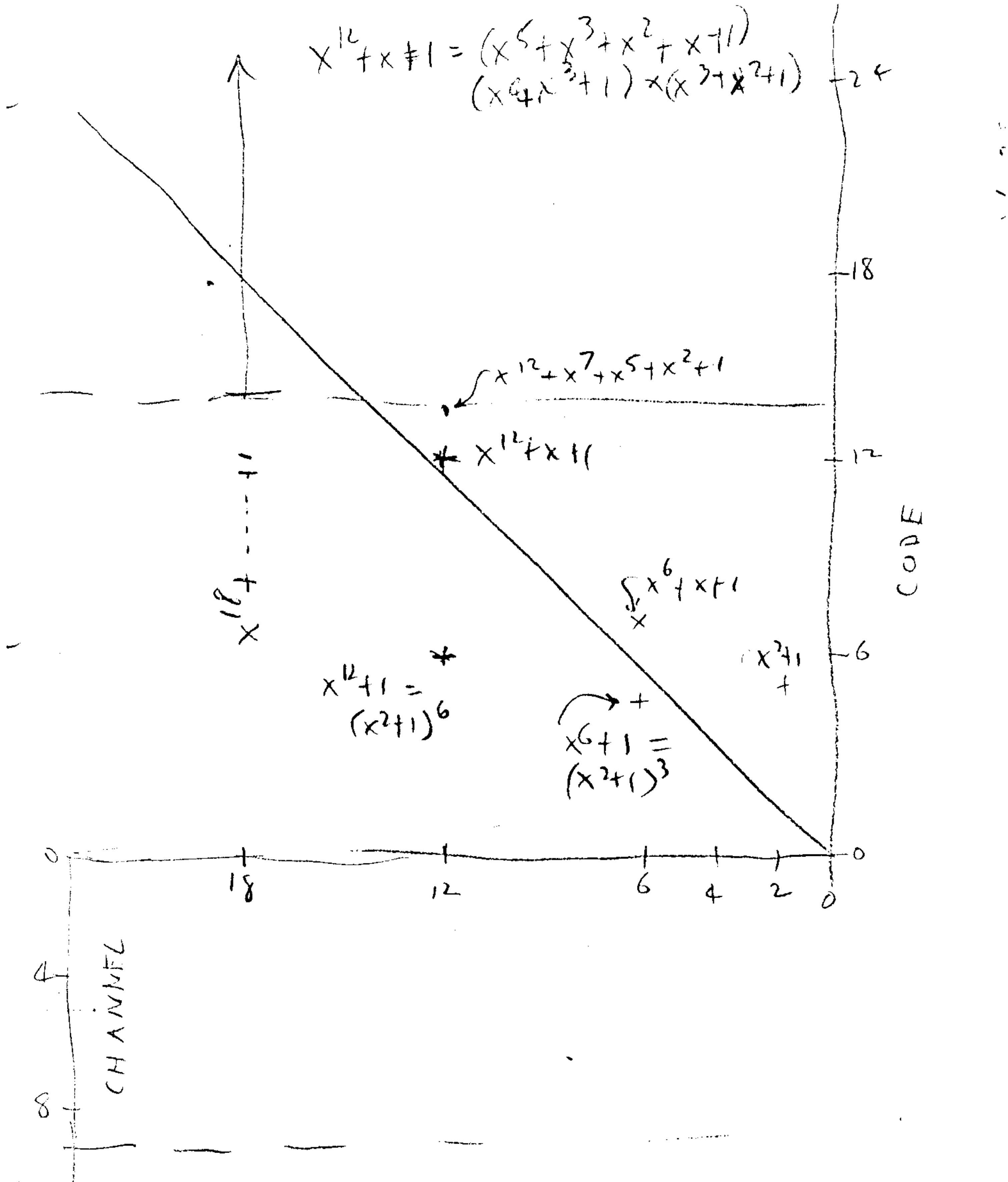
C. C. I. T. T. CONSIDERING
INTERNATIONAL STD'S.

COLLECT ERROR PATTERNS AND
STATISTICAL DATA

SIMULATE ERROR
DETECTION WITH
DIFFERENT CODES
BY DIVIDING E (x)
BY P(x)'s

ERROR MESSAGES
DIVIDED BY P(x) WITH
NO REMAINDER ARE
"UNDETECTED ERRORS."


CODE
$-\log_2 P_2$
CHANNEL
$\log_2 P_1$
$(n-k)$ - PARITY BITS
BLOCK LENGTH (bits) n
$k = \log_2 n$
16.5
+8.6
-7.9
$16.5 = -\log_2\left(\frac{1}{13\ldots}\right)$



I BM & AT & T G
CORBET et al AIEE CP 61-1130

PROC IEEE 1/49

p.159-65

MIT HALL

LAB

$2+X^{16}+1$

$X^{14}+1$

$X^{7}+X^{3}+1$

n=255

n=255

n=127

n=127

C=255

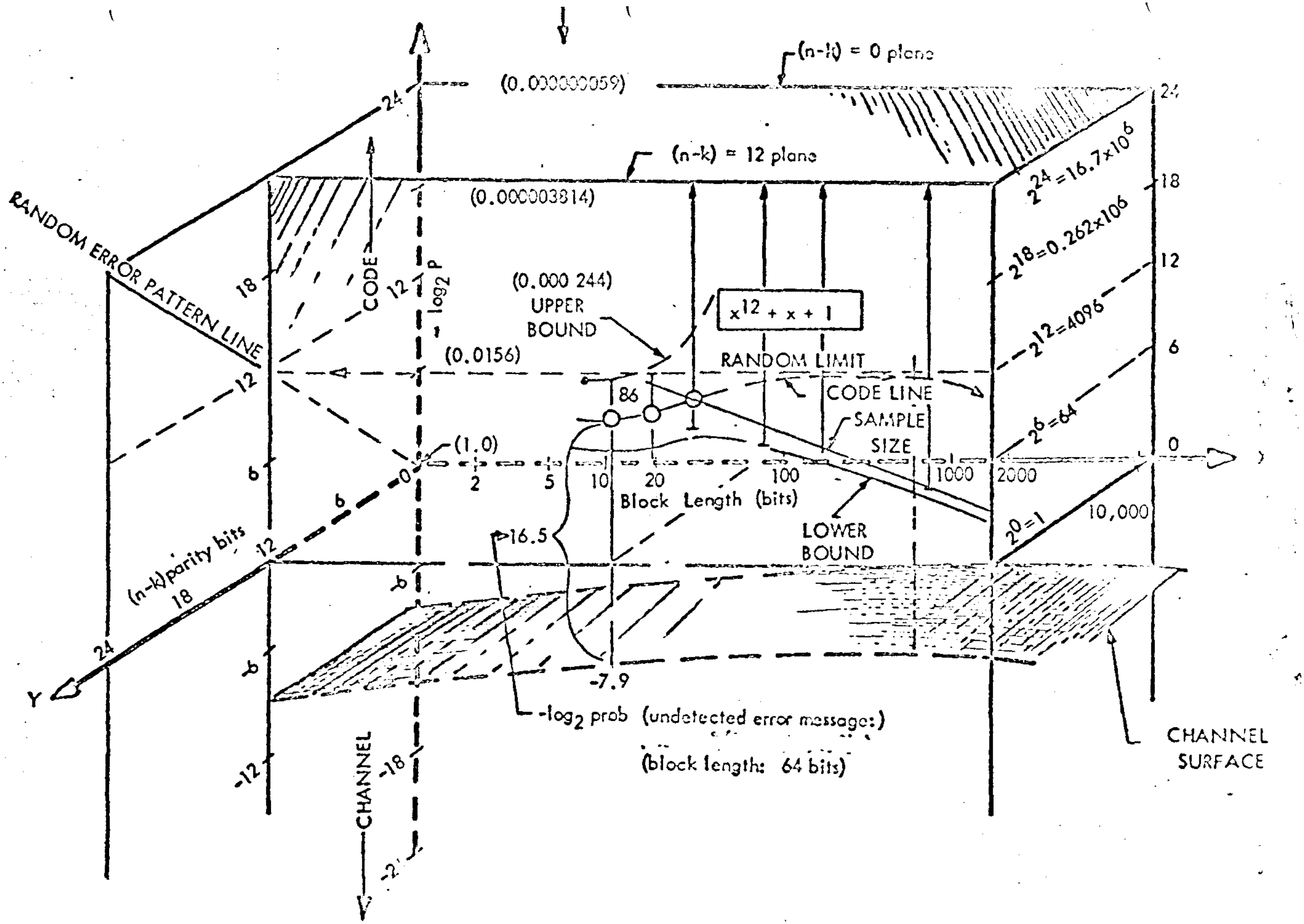


Figure 1 Example of Evaluation of $x^{12} + x + 1$ Code