ELEC 405/ELEC 511
Error Control Coding and Sequences

Hamming Codes and the
Hamming Bound

Single Error Correcting Codes

$$(3,\ 1,\ 3)\ \text{code} \quad \text{rate } 1/3 \quad n-k=2$$

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

$$(5,\ 2,\ 3)\ \text{code} \quad \text{rate } 2/5 \quad n-k=3$$

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

$$(6,\ 3,\ 3)\ \text{code} \quad \text{rate } 1/2 \quad n-k=3$$

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

Hamming Codes

- One form of the (7,4,3) Hamming code is generated by

$$\mathbf{G}' = \left[\mathbf{P}' | \mathbf{I}\right] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

- This is equivalent to the code in Wicker Section 1.3 with

$$\mathbf{G}'' = \left[\mathbf{I} | \mathbf{P}''\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Hamming Codes

- (7,4,3) Hamming code

$$\mathbf{G} = \left[\mathbf{I} \mid \mathbf{P}\right] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- (7,3,4) dual code

$$\mathbf{H} = \left[-\mathbf{P}^{\mathrm{T}} \mid \mathbf{I}\right] = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

- Theorem 4-9 The minimum distance of a code is equal to the minimum number of columns of **H** which sum to zero
- For any codeword *c*

$$c\mathbf{H}^{\mathrm{T}} = [c_0, c_1, \ldots, c_{\mathrm{n}-1}]\begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_{\mathrm{n}-1} \end{bmatrix} = c_0 d_0 + c_1 d_1 + \ldots + c_{n-1} d_{\mathrm{n}-1} = 0$$

where d_0, d_1, …, $d_{n\text{-}1}$ are the column vectors of **H**

- $c\mathbf{H}^{\mathrm{T}}$ is a linear combination of columns of **H**

Significance of H

- For a codeword of weight *w* (*w* ones), c$\mathbf{H}^T$ is a linear combination of *w* columns of **H**.
- Thus we have a one-to-one mapping between weight *w* codewords and linear combinations of *w* columns of **H** that sum to 0.
- The minimum value of *w* which results in $c\mathbf{H}^T$=0, i.e., codeword *c* with weight *w,* determines that $d_{\min} = w$

Example

- For the (7,4,3) code, a codeword with weight $d_{\min} = 3$ is given by the first row of **G**

  $$c = 1000011$$

- The linear combination of the first and last 2 columns in **H** gives

  $$(011)^T+(010)^T+(001)^T = (000)^T$$

- Thus a minimum of 3 columns (= $d_{\min}$) are required to get a zero value for $c\mathbf{H}^T$

Hamming Codes

Definition Let m be an integer and **H** be an $m \times (2^m - 1)$ matrix with columns which are the non-zero distinct words from V_m. The code having **H** as its parity-check matrix is a binary Hamming code of length $2^m - 1$.

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

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

The Hamming codes are $(2^m - 1, 2^m – 1 – m, 3)$ codes

$m = n - k$

Binary Hamming Code Parameters

$$\begin{aligned} C: \; n &= 2^m - 1 \\ k &= 2^m - 1 - m \\ d &= 3 \\ C^{\perp}: \; n &= 2^m - 1 \\ k &= m \\ d &= 2^{m-1} \end{aligned}$$

Coset Leaders for the Hamming Codes

- There are $2^{n-k} = 2^m$ coset leaders or correctable error patterns
- The number of single error patterns is $n = 2^m-1$
- Thus the coset leaders are precisely the words of weight ≤ 1
- The syndrome of the word 0…010…0 with 1 in the *j* th position and 0 otherwise is the transpose of the *j* th column of **H**

Decoding Hamming Codes

For the case that the columns of **H** are arranged in order of increasing binary numbers that represent the column numbers 1 to $2^m - 1$

- **Step 1** Given *r* compute the syndrome $s = r\mathbf{H}^T$
- **Step 2** If $s = 0$, then *r* is assumed to be the codeword sent
- **Step 3** If $s \neq 0$, then assuming a single error, *s* gives the binary position of the error

Example

For the Hamming code given by the parity-check matrix

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

the received word

$$r = 1101011$$

has syndrome

$$s = 110$$

and therefore the error is in the sixth position.

Hamming codes were first used to deal with errors in long-distance telephone calls.

- The (7,4,3) code is an optimal single error correcting code for *n*-*k* = 3
- An (8,5,3) code does not exist
- The (15,11,3) code is an optimal single error correcting code for *n*-*k* = 4

- What is the limit on how many errors an (*n*,*k*) code can correct?

Optimal Codes

$d_{\min} = 1$ $(n, n, 1)$ entire vector space

$d_{\min} = 2$ $(n, n\text{-}1, 2)$ single parity check codes

$d_{\min} = 3$ $n = 2^{m} - 1$ Hamming codes

what about other values of n?

Shortening

- For $2^{m-1} \le n < 2^m-1$, $k = n-m$, use shortening
- To get a (6,3,3) code, delete one column say $(1\ 1\ 1)^T$ from **H**

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

n-*k* is constant

so both *n* and *k* are changed

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

- Next delete $(0\ 1\ 1)^T$ which gives a (5,2,3) code

$$\mathbf{H}^2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{G}^2 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

- Next delete $(1\ 0\ 1)^T$ which gives a (4,1,3) code

$$\mathbf{H}^3 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{G}^3 = \begin{bmatrix} 1 & 1 & 1 & 0 \end{bmatrix}$$

- The (4,1,4) repetition code has larger d_{min}

- Does a (4,2,3) binary code exist?

Extending

- The process of deleting a message coordinate from a code is called shortening

  $(n, k) \longrightarrow (n\text{-}1, k\text{-}1)$

- Adding an overall parity check to a code is called extending

  $(n, k) \longrightarrow (n+1, k)$

- Example:

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

- If d(C) is odd, d(C’) is even
    - In this case, d(C’) = d(C) + 1
- Example (7,4,3) $\longrightarrow$ (8,4,4)

- The extended Hamming codes are optimal d_{min} = 4 codes

Optimal Codes

$d_{\min} = 1$ $(n, n, 1)$ entire vector space

$d_{\min} = 2$ $(n, n\text{-}1, 2)$ single parity check codes

$d_{\min} = 3$ Hamming and shortened Hamming codes

$d_{\min} = 4$ extended $d_{\min} = 3$ codes

Binary Spheres of Radius *t*

- The number of binary words (vectors) of length *n* and distance *i* from a word *c* is

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

- Let *c* be a word of length *n*. For 0 ≤ *t* ≤ *n*, the number of words of length *n* a distance at most *t* from *c* is

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots. + \binom{n}{t}$$

Hamming or Sphere Packing Bound

- Consider an (n,k,d) binary code
- 2^k codewords and spheres of radius t around the codewords must be disjoint
- Volume of a sphere with radius t is the number of vectors in the sphere
- Example: (7,4,3) Hamming code t=1
- Volume of each sphere is $\underset{\substack{\nearrow\\ \text{codeword}}}{1}+\underset{\substack{\nwarrow\\ \text{1 bit error patterns}}}{7}=8=2^3$

- Number of spheres (codewords) is 2^{k} =16
- Volume of all spheres is $2^{k} \cdot 2^{3} = 2^{7} = 2^{n}$
- The spheres completely fill the *n*-dimensional space

- The Hamming bound (binary)

$$2^{k}\left[1+\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{t}\right]\leq 2^{n} \quad \text{or} \quad \sum_{i=0}^{t}\binom{n}{i}\leq 2^{n-k}$$

- A binary code is called perfect if it meets this bound with equality

Hamming Bound Example

- Give an upper bound on the size of a linear code C of length *n*=6 and distance *d*=3

$$|C| = 2^k \le \frac{2^6}{\binom{6}{0}+\binom{6}{1}} = \frac{64}{7}$$

- This gives |C|≤ 9 but the size of a linear code C must be a power of 2 so |C|≤ 8 and k ≤ 3

Codes that meet the Hamming Bound

- Binary Hamming codes

$$\binom{n}{0}+\binom{n}{1}=1+2^m-1=2^m=2^{n-k}$$

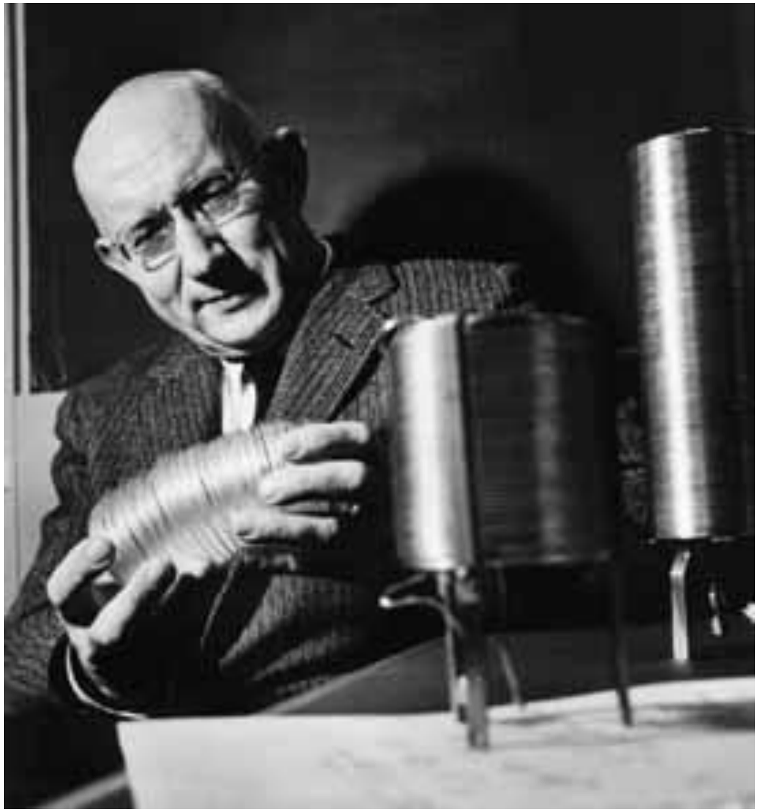
- Odd binary repetition codes (2*m*+1, 1, 2*m*+1)

  t=m

  Sphere volume = $\sum_{i=0}^{m}\binom{2m+1}{i}=2^{2m}=2^{n-k}$

- (*n*, *n*, 1) codes (all vectors in V_n are codewords)

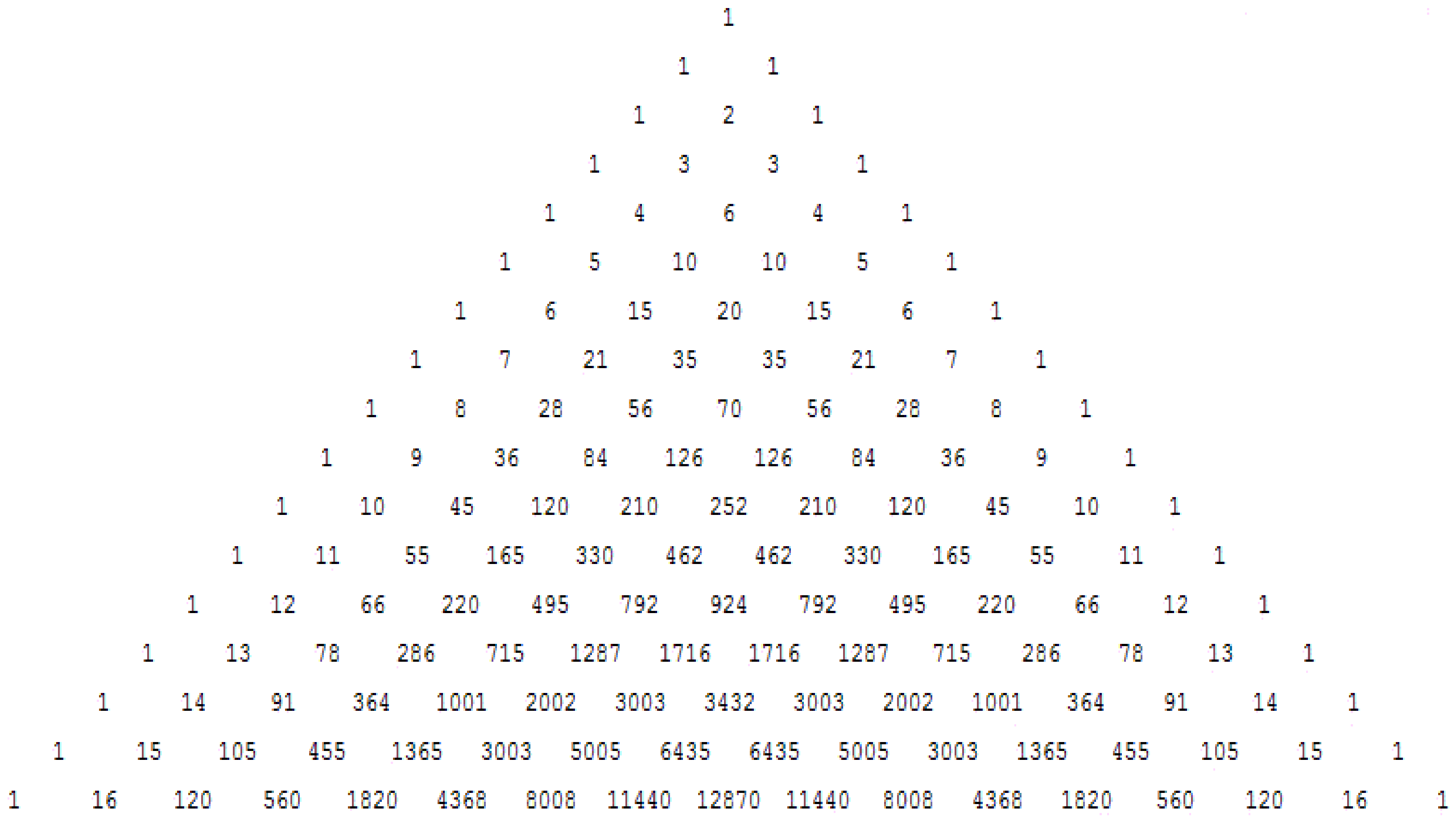
Marcel Golay (1902-1989)



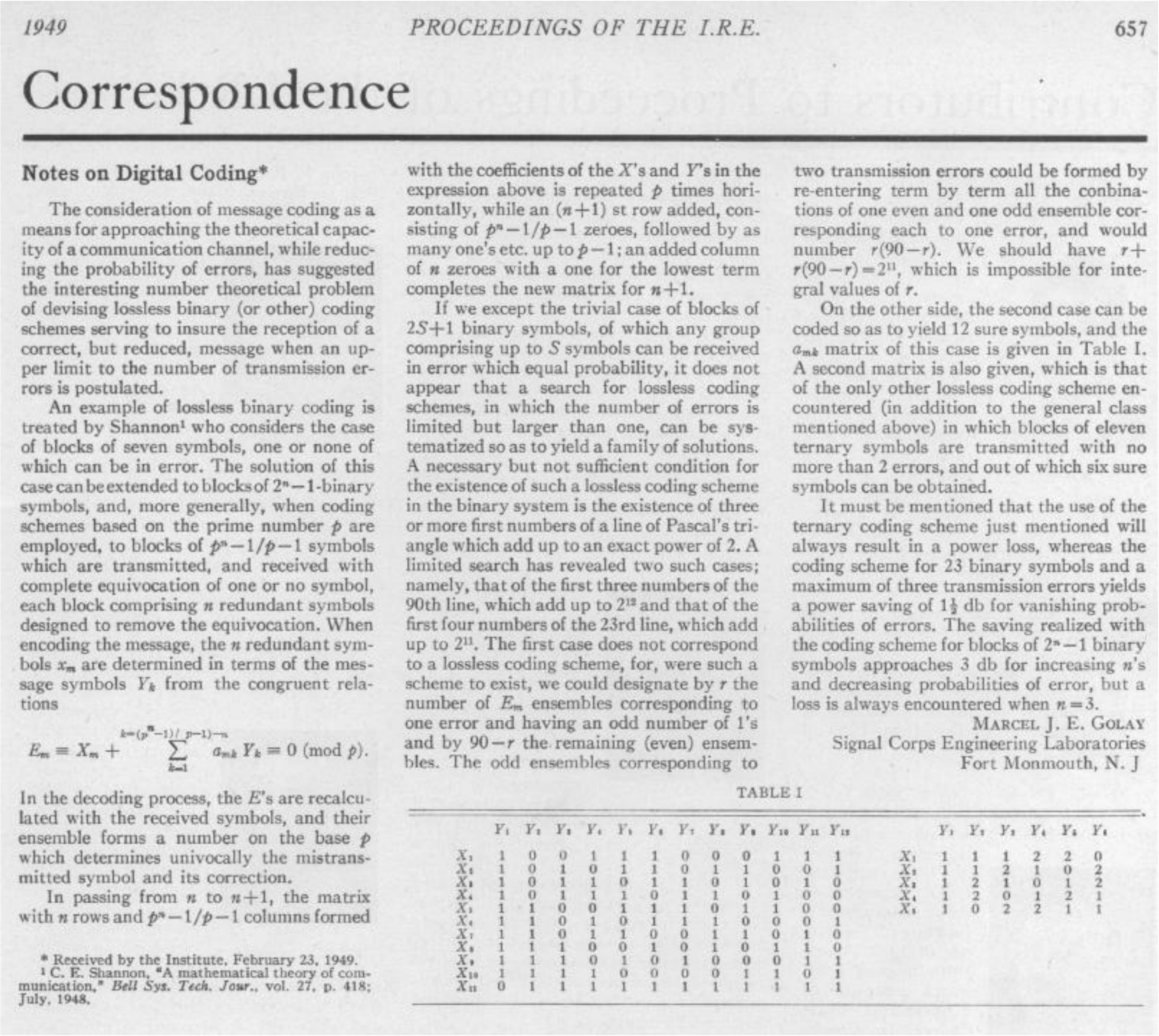
Blaise Pascal (1623-1662)

- French religious philosopher, physicist, and mathematician
- Thoughts on Religion (1655)
- Syringe, and Pascal’s Law for fluid dynamics (1647-1654)
- First mechanical calculator (1642-1644)
- Modern Theory of Probability with Pierre de Fermat (1654)
- Pascal’s triangle was discovered by Chinese mathematician Yanghui, 500 years before Pascal and in the Eleventh century by Persian mathematician and poet Omar Khayam

Pascal’s Triangle



```
                                                                1
                                                            1       1
                                                        1       2       1
                                                    1       3       3       1
                                                1       4       6       4       1
                                            1       5       10      10      5       1
                                        1       6       15      20      15      6       1
                                    1       7       21      35      35      21      7       1
                                1       8       28      56      70      56      28      8       1
                            1       9       36      84      126     126     84      36      9       1
                        1       10      45      120     210     252     210     120     45      10      1
                    1       11      55      165     330     462     462     330     165     55      11      1
                1       12      66      220     495     792     924     792     495     220     66      12      1
            1       13      78      286     715     1287    1716    1716    1287    715     286     78      13      1
        1       14      91      364     1001    2002    3003    3432    3003    2002    1001    364     91      14      1
    1       15      105     455     1365    3003    5005    6435    6435    5005    3003    1365    455     105     15      1
1       16      120     560     1820    4368    8008    11440   12870   11440   8008    4368    1820    560     120     16      1
```



Correspondence

Notes on Digital Coding*

The consideration of message coding as a means for approaching the theoretical capacity of a communication channel, while reducing the probability of errors, has suggested the interesting number theoretical problem of devising lossless binary (or other) coding schemes serving to insure the reception of a correct, but reduced, message when an upper limit to the number of transmission errors is postulated.

An example of lossless binary coding is treated by Shannon[1] who considers the case of blocks of seven symbols, one or none of which can be in error. The solution of this case can be extended to blocks of 2^n-1-binary symbols, and, more generally, when coding schemes based on the prime number p are employed, to blocks of $p^n-1/p-1$ symbols which are transmitted, and received with complete equivocation of one or no symbol, each block comprising n redundant symbols designed to remove the equivocation. When encoding the message, the n redundant symbols x_m are determined in terms of the message symbols Y_k from the congruent relations

$$E_m \equiv X_m + \sum_{k=1}^{k=(p^n-1)/p-1)-n} a_{mk} Y_k \equiv 0 \pmod{p}.$$

In the decoding process, the E's are recalculated with the received symbols, and their ensemble forms a number on the base p which determines univocally the mistransmitted symbol and its correction.

In passing from n to $n+1$, the matrix with n rows and $p^n-1/p-1$ columns formed with the coefficients of the X's and Y's in the expression above is repeated p times horizontally, while an $(n+1)$ st row added, consisting of $p^n-1/p-1$ zeroes, followed by as many one's etc. up to $p-1$; an added column of n zeroes with a one for the lowest term completes the new matrix for $n+1$.

If we except the trivial case of blocks of $2S+1$ binary symbols, of which any group comprising up to S symbols can be received in error which equal probability, it does not appear that a search for lossless coding schemes, in which the number of errors is limited but larger than one, can be systematized so as to yield a family of solutions. A necessary but not sufficient condition for the existence of such a lossless coding scheme in the binary system is the existence of three or more first numbers of a line of Pascal's triangle which add up to an exact power of 2. A limited search has revealed two such cases; namely, that of the first three numbers of the 90th line, which add up to 2^{12} and that of the first four numbers of the 23rd line, which add up to 2^{11}. The first case does not correspond to a lossless coding scheme, for, were such a scheme to exist, we could designate by r the number of E_m ensembles corresponding to one error and having an odd number of 1's and by $90-r$ the remaining (even) ensembles. The odd ensembles corresponding to two transmission errors could be formed by re-entering term by term all the conbinations of one even and one odd ensemble corresponding each to one error, and would number $r(90-r)$. We should have $r+r(90-r)=2^{11}$, which is impossible for integral values of r.

On the other side, the second case can be coded so as to yield 12 sure symbols, and the a_{mk} matrix of this case is given in Table I. A second matrix is also given, which is that of the only other lossless coding scheme encountered (in addition to the general class mentioned above) in which blocks of eleven ternary symbols are transmitted with no more than 2 errors, and out of which six sure symbols can be obtained.

It must be mentioned that the use of the ternary coding scheme just mentioned will always result in a power loss, whereas the coding scheme for 23 binary symbols and a maximum of three transmission errors yields a power saving of $1\frac{1}{2}$ db for vanishing probabilities of errors. The saving realized with the coding scheme for blocks of 2^n-1 binary symbols approaches 3 db for increasing n's and decreasing probabilities of error, but a loss is always encountered when $n=3$.

Marcel J. E. Golay
Signal Corps Engineering Laboratories
Fort Monmouth, N. J

TABLE I

	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}
X_1	1	0	0	1	1	1	0	0	0	1	1	1
X_2	1	0	1	0	1	1	0	1	1	0	0	1
X_3	1	0	1	1	0	1	1	0	1	0	1	0
X_4	1	0	1	1	1	0	1	1	0	1	0	0
X_5	1	1	0	0	1	1	1	0	1	1	0	0
X_6	1	1	0	1	0	1	1	1	0	0	0	1
X_7	1	1	0	1	1	0	0	1	1	0	1	0
X_8	1	1	1	0	0	1	0	1	0	1	1	0
X_9	1	1	1	0	1	0	1	0	0	0	1	1
X_{10}	1	1	1	1	0	0	0	0	1	1	0	1
X_{11}	0	1	1	1	1	1	1	1	1	1	1	1

	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6
X_1	1	1	1	2	2	0
X_2	1	1	2	1	0	2
X_3	1	2	1	0	1	2
X_4	1	2	0	1	2	1
X_5	1	0	2	2	1	1

* Received by the Institute, February 23, 1949.

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Sys. Tech. Jour.*, vol. 27, p. 418; July, 1948.

Golay Codes

- Marcel Golay considered the problem of perfect codes in 1949
- He found three possible solutions to equality for the Hamming bound
  - $q = 2, n = 23, t = 3$
  - $q = 2, n = 90, t = 2$
  - $q = 3, n = 11, t = 2$
- Only the first and third codes exist

Gilbert Bound

- There exists a code of length *n*, distance *d*, and *M* codewords with

$$M \geq \frac{2^{\mathrm{n}}}{\sum_{j=0}^{d\text{-}1} \binom{n}{j}}$$

- The constructive proof does not result in a linear code

Gilbert-Varshamov Bound

- The Gilbert bound can be improved by considering linear codes
  - There exists a binary linear code of length *n*, dimension *k* and minimum distance *d* if

$$\binom{n\text{-}1}{0}+\binom{n\text{-}1}{1}+\ldots+\binom{n\text{-}1}{d\text{-}2}<2^{\text{n-k}}$$

  - Proof: construct a parity check matrix based on the condition that any combination of up to *d*-1 columns of **H** is linearly independent
  - Thus a binary (*n,k,d*) code exists with

$$k\geq n-\left\lfloor \sum_{j=0}^{d\text{-}2}\binom{n\text{-}1}{j}\right\rfloor-1$$