ELEC 405
Error Control Coding and Sequences

Hamming Codes and
What is Possible

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

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

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

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

Hamming Codes

- (7,4,3) Hamming code

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

- (7,3,4) dual code

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

Comments about H

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

$$\mathrm{cH}^{\mathrm{T}} = [c_0, c_1, \ldots, c_{\mathrm{n}-1}] \begin{bmatrix} \mathrm{d}_0 \\ \mathrm{d}_1 \\ . \\ \mathrm{d}_{\mathrm{n}-1} \end{bmatrix} = c_0 \mathrm{d}_0 + c_1 \mathrm{d}_1 + \ldots + c_{n-1} \mathrm{d}_{\mathrm{n}-1} = 0$$

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

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

Comments about 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**, i.e., 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 $c\mathbf{H}^T$

Parity Check Matrix of the (7,4,3) Code

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

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 $2^m - 1$.

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

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

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

$m = n - k$

Hamming Code Parameters

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

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 $\mathbf{H}$

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

Example

For the Hamming code given by the parity-check matrix

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

the received word

$$r = 1101011$$

has syndrome

$$S(r) = 110$$

and therefore the error is in the sixth position.

Hamming codes were originally 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 a code can correct?

The Main Coding Theory Problem

A good (n,M,d) code has small n, large M and large d.

The main coding theory problem is to optimize one of the parameters n, M, d for given values of the other two.

For linear codes, a good (n,k,d) code has small n, large k and large d.

The main coding theory problem for linear codes is to optimize one of the parameters n, k, d for given values of the other two.

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

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

n-k is constant

so both n and k are changed

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

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

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

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

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

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

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

Self-Dual Code Example

- C= C$^{\perp}$ ≥ n-k=k $\longrightarrow$ k=n/2
- **G=[I P]   GG^T=0 $\Leftrightarrow$ I+PP^T=0 $\longrightarrow$ PP^T=-I**
- Self-dual code over GF(3) with n=4, k=2, d=3

$$\mathrm{G} = \begin{bmatrix} 1011 \\ 0112 \end{bmatrix}$$

$$(1011)\cdot(1011) = 0$$
$$(1011)\cdot(0112) = 0$$
$$(0112)\cdot(0112) = 0$$

- Codewords

0000 1011 2022 0112 0221

1102 2201 1220 2110

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:

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

- 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 optimal d_{min} = 4 codes are extended Hamming 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 $0 \le t \le n$, the number of words of length *n* a distance at most *t* from *c* is

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{t}$$

Hamming or Sphere Packing Bound

- Consider an (n,k,t) binary code
- 2^k codewords, 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 $1+7=8=2^3$

codeword   1 bit error patterns

- 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)

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

- A 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

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

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

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)

Hamming Bound for Nonbinary Codes

- For GF(q)

$$\sum_{i=0}^{t} \binom{n}{i} (q-1)^i \le q^{n-k}$$

  - Size of the vector space is q^n
  - The number of codewords is q^k
  - Each error location has q-1 possible error values
- Two of the three classes of perfect binary linear codes also exist for nonbinary alphabets

- Vector space codes

$$\sum_{i=0}^{0} \binom{n}{i} (q-1)^i = q^0 = q^{n-k}$$

- Nonbinary Hamming codes
  - **H** has *m* rows
  - There are $q^m - 1$ possible nonzero *q*-ary *m*-tuples
  - For each *q*-ary *m*-tuple, there are *q*-1 distinct non-zero *m*-tuples that are a multiple of that *m*-tuple

- **H** has dimension $m \times \dfrac{q^m - 1}{q - 1}$

$$n = \frac{q^m - 1}{q - 1} \quad k = n - m \quad d_{\min} = 3$$

- Example: *m*=3, *q*=3, 26 possible nonzero *m*-tuples

only ½ are usable

$$\mathrm{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 2 & 1 & 2 & 2 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\sum_{i=0}^{1} \binom{n}{i} (q-1)^i = 1 + n(q-1) = q^m = q^{n-k}$$

Golay Codes

- Marcel Golay (1902-1989) 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 [Van Lint and Tietäväinen, 1973]

Gilbert Bound

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

$$M = \left\lceil \frac{2^n}{\sum_{j=0}^{d-1} \binom{n}{j}} \right\rceil$$

- The bound also holds for linear codes
  - Let *k* be the largest integer such that

$$2^k < \frac{2^n}{\sum_{j=0}^{d-1} \binom{n}{j}}$$

then an (*n,k,d*) code exists

Gilbert-Varshamov Bound

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

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

  - Proof: construct a parity check matrix based on this condition
  - Thus if *k* is the largest integer such that

$$2^k < \frac{2^n}{\sum_{j=0}^{d-2}\binom{n-1}{j}}$$

then an (*n,k,d*) code exists

Examples

- Does there exist a linear code of length n=9, dimension k=2, and distance d=5? Yes, because

$$\binom{8}{0}+\binom{8}{1}+\binom{8}{2}+\binom{8}{3}=93<128=2^{9-2}$$

- Give a lower and an upper bound on the dimension, k, of a linear code with n=9 and d=5
- G-V lower bound: $2^{\mathrm{k}}<\dfrac{2^9}{93}=5.55$ but |C| is a power of 2 so |C| ≥ 4

Examples (Cont.)

- Hamming upper bound:

$$|C| \leq \frac{2^9}{\binom{9}{0}+\binom{9}{1}+\binom{9}{2}} = \frac{512}{1+9+36} = 11.13$$

  but |C| is a power of 2 so |C| ≤ 8
- From the tables, the optimal codes are
  - (9,2,6)
    - the G-V bound is exceeded so it is sufficient but not necessary for a code to exist
  - (9,3,4)
    - the Hamming bound is necessary but not sufficient for a code to exist

G-V Bound and Codes

- Does a (15,7,5) linear code exist?
  - Check the G-V bound

$$\binom{n-1}{0}+\binom{n-1}{1}+\ldots+\binom{n-1}{d-2}=\binom{14}{0}+\binom{14}{1}+\binom{14}{2}+\binom{14}{3}$$
$$=1+14+91+364=470>2^{15-7}=2^{n-k}=256$$

  - G-V bound does not hold, so it does not tell us whether or not such a code exists.

  - Actually such a code does exist - the (15,7,5) BCH code

- Check with the Hamming bound

- A (15,7,5) BCH code has sphere volume

$$1+15+\binom{15}{2}=121$$

- The total volume of the spheres is

$$121\times 2^{7}=15488<2^{15}$$

The Nordstrom-Robinson Code

- Adding an overall parity check to the (15,7,5) code gives a (16,7,6) linear code
  - This is an optimal linear code
  - The G-V bound says a (16,5,6) code exists
- A (16,256,6) nonlinear code exists
  - Twice as many codewords as the optimal linear code

Bounds for Nonbinary Codes

- For nonlinear codes, there exists a code of length *n*, dimension *k* and distance *d* if

$$M=\left\lceil \frac{q^n}{\sum_{j=0}^{d-1}\binom{n}{j}(q-1)^j} \right\rceil$$

  - For linear codes, let k be the largest integer such that

$$q^k < \frac{q^n}{\sum_{j=0}^{d-2}\binom{n-1}{j}(q-1)^j}$$

  is satisfied, then an (*n*,*k*,*d*) code exists

Singleton Bound

- Theorem 4-10 Singleton bound (upper bound)

  For any (n,k,d) linear code, $d-1 \leq n-k$

  $k \leq n-d+1$ or $|C| \leq 2^{n-d+1}$

  Proof: the parity check matrix **H** of an (n,k,d) linear code is an $n-k$ by n matrix such that every $d-1$ columns of **H** are independent Since the columns have length $n-k$, we can never have more than $n-k$ independent columns. Hence $d-1 \leq n-k$.

- For an (n,k,d) linear code C, the following are equivalent:
  - $d = n-k+1$
  - Every $n-k$ columns of the parity check matrix are linearly independent
  - Every k columns of the generator matrix are linearly independent
  - C is Maximum Distance Separable (MDS) (definition: $d=n-k+1$)
  - $C^{\perp}$ is MDS

Example

- (255,223,33) RS code over GF(2^8)

$$\frac{\text{\# of codewords} \times \text{volume}}{\text{size of vector space}} = 2.78 \times 10^{-14}$$

- Singleton bound:

$$d_{\min} \leq n\text{-}k+1$$

- (255,223,33) RS code meets the Singleton bound with equality