S-72.341 CODING METHODS

Tutorial 3, Solutions

1. First we notice that for code words $\mathbf{x},\mathbf{y},\mathbf{z}$ the following equalities hold

$$d(\mathbf{x},\mathbf{y}) = \mathrm{w}(\mathbf{x}+\mathbf{y}),$$

and

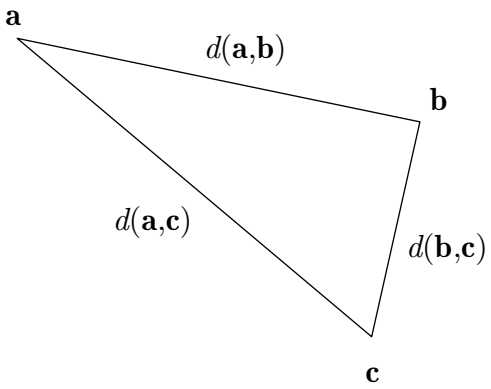
$$d(\mathbf{x}+\mathbf{z},\mathbf{y}+\mathbf{z}) = \mathrm{w}(\mathbf{x}+\mathbf{z}+\mathbf{y}+\mathbf{z}) = \mathrm{w}(\mathbf{x}+\mathbf{y}) = d(\mathbf{x},\mathbf{y}),$$

where $\mathrm{w}(\mathbf{x})$ is the weight (number of ones) of word $\mathbf{x}$. Furthermore,

$$\mathrm{w}(\mathbf{x}+\mathbf{y}) \le \mathrm{w}(\mathbf{x}) + \mathrm{w}(\mathbf{y}).$$

Using these relations we see that

$$\begin{aligned} d(\mathbf{b},\mathbf{c}) &= \mathrm{w}(\mathbf{b}+\mathbf{c}) \\ &= \mathrm{w}(\mathbf{a}+\mathbf{b}+\mathbf{a}+\mathbf{c}) \\ &\le \mathrm{w}(\mathbf{a}+\mathbf{b}) + \mathrm{w}(\mathbf{a}+\mathbf{c}) \\ &= d(\mathbf{a},\mathbf{b}) + d(\mathbf{a},\mathbf{c}). \end{aligned}$$



The key point of this problem is to emphasize that the Hamming distance between two binary words is equal to the weight of their sum. Notice also that $\mathrm{w}(\mathbf{x}+\mathbf{y}) = \mathrm{w}(\mathbf{x}) + \mathrm{w}(\mathbf{y}) - 2\,\mathrm{w}(\mathbf{x}\cdot\mathbf{y})$, $\quad \mathrm{w}(\mathbf{x}\cdot\mathbf{y}) \triangleq \mathrm{w}\Big(\Big[x_1y_1 \quad x_2y_2 \quad \ldots \quad x_ny_n\Big]\Big)$, from which the following observations are made:

- sum of two even-weight words has even weight
- sum of two odd-weight words has even weight
- sum of an even-weight and an odd-weight word has odd weight

2. A code word $\mathbf{c}$ is generated using $\mathbf{c} = \mathbf{uG}$. Also recall that $\mathbf{GH}^T = \mathbf{0}$.

   a) The generator matrix is

$$\mathbf{G} = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] = \left[\mathbf{P}_{4\times 4} \mid \mathbf{I}_{4\times 4}\right].$$

   To satisfy the orthogonality condition the parity-check matrix must be set to $\mathbf{H} = \left[\mathbf{I}_{4\times 4} \mid \mathbf{P}_{4\times 4}^T\right]$.

   b) All rows of $\mathbf{G}$ have even weight, and a sum of two even-weight binary words has also even weight, which results in all code words having an even weight. Since the sum of the first three columns and the fifth column of $\mathbf{H}$ is zero, $\mathbf{I}_{4\times 4}$ is a zero vector, $d_{\min} \leq 4$. Thus, a minimum-weight code word must have weight 2 or 4. A code word cannot have weight two, since all columns of $\mathbf{H}$ are distinct, so $d_{\min} = 4$.

   The code can detect at least $d_{\min} - 1 = 3$ errors, and correct at least $\left\lfloor (d_{\min} - 1)/2 \right\rfloor = 1$ error.

3.

   a) The dimension of the code is four, since the dimensions of the spaces spanned by the rows of $\mathbf{G}$ and $\mathbf{H}$ must sum to seven.

   b) The number of codewords is $2^4 = 16$.

   c) The sum of the first two columns and the fourth column (for instance) of $\mathbf{H}$ is a zero vector, so $d_{\min} = 3$.

   d) Any codeword $\mathbf{c}$ must satisfy $\mathbf{cH}^T = \mathbf{0}$. The all-one word is a codeword. The other word is not.

   e) The code can correct one error in a received word. It can detect two errors in a received word. For $\mathbf{c} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$, $\mathbf{cH}^T = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$. By examining the parity-check matrix, we notice that the last column is an all-one word. If we flip the final bit in $\mathbf{c}$ over (denote the new word $\mathbf{c}'$), we get a valid codeword: $\mathbf{c}' = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$.

   f) Since $\mathbf{H} = \begin{bmatrix} \mathbf{I}_{3\times 3} & \mathbf{P}_{3\times 4} \end{bmatrix}$, setting $\mathbf{G} = \begin{bmatrix} \mathbf{P}_{3\times 4}^T & \mathbf{I}_{4\times 4} \end{bmatrix}$ yields $\mathbf{GH}^T = \mathbf{0}$. Thus

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

Let $\mathbf{m} = \begin{bmatrix} 0 & 1 & 0 & 1 \end{bmatrix}$, then $\mathbf{mG} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$.

4. Let's use the Hamming bound as lower bound: $r \geq \log_q \left[V_q(n,t) \right]$, where

$$V_q(n,t) = \sum_{j=0}^{t} \binom{n}{j} (q-1)^j$$

is the number of q-ary n-tuples in a Hamming sphere of radius t.

a) $V_2(7,1) = \sum_{j=0}^{1} \binom{7}{j} = \binom{7}{0} + \binom{7}{1} = \frac{7!}{7!0!} + \frac{7!}{6!1!} = 1 + 7 = 8 \qquad \Rightarrow r \geq \log_2 8 = 3.$

b) $V_2(15,1) = \sum_{j=0}^{1} \binom{15}{j} = 1 + 15 = 16 \qquad \Rightarrow r \geq 4.$

c) $V_2(23,1) = \sum_{j=0}^{3} \binom{23}{j} = 1 + 23 + 253 + 1771 = 2048 \qquad \Rightarrow r \geq 11.$

d) $V_4(23,3) = \sum_{j=0}^{3} \binom{23}{j} 3^j = 1 + 23 \cdot 3 + 253 \cdot 9 + 1771 \cdot 27$

$= 50164 \qquad \Rightarrow r \geq 7.807... \qquad$ (or 8)

e) $V_{16}(23,3) = \sum_{j=0}^{3} \binom{23}{j} 15^j = 1 + 23 \cdot 15 + 253 \cdot 225 + 1771 \cdot 3375$

$= 6034396 \qquad \Rightarrow r \geq 5.631... \qquad$ (or 6)

Let's use the Gilbert bound as upper bound: $r \leq \log_q \left[V_q(n,2t) \right]$.

a) $V_2(7,2) = \sum_{j=0}^{2} \binom{7}{j} = 1 + 7 + 21 = 29 \qquad \Rightarrow r \leq \frac{\ln 29}{\ln 2} = 4.857...$

b) $V_2(15,2) = \sum_{j=0}^{2} \binom{15}{j} = 1 + 15 + 105 = 121 \qquad \Rightarrow r \leq 6.918...$

c) $$V_2(23,2) = \sum_{j=0}^{6} \binom{23}{j} = 1 + 23 + 253 + 1771 + 8855 + 33649 + 100947$$
$$= 145499 \qquad \Rightarrow r \leq 17.15...$$

d) $$V_4(23,6) = \sum_{j=0}^{6} \binom{23}{j} 3^j = 1 + 23 \cdot 3 + 253 \cdot 9 + 1771 \cdot 27 + 8855 \cdot 81$$
$$+33649 \cdot 243 + 100947 \cdot 729 = 82534489 \qquad \Rightarrow r \leq 13.149...$$

e) $$V_{16}(23,6) = \sum_{j=0}^{6} \binom{23}{j} 15^j = 1 + 23 \cdot 15 + 253 \cdot 15^2 + 1771 \cdot 15^3 + 8855 \cdot 15^4$$
$$+33649 \cdot 15^5 + 100947 \cdot 15^6 = \text{a big number} \qquad \Rightarrow r \leq 10.02...$$

5. The length of a code is the number of coordinates in code words. Dimension of a linear code is the dimension of the code subspace (Definition 4-10 of the book). The minimum distance of a block code is the minimum Hamming distance between all distinct pairs of code words (Definition 4-4).

   a) The parity-check matrix is a 4×7 matrix so the length of the code is 7. By the dimension theorem (and orthogonality requirement) the dimensions of the subspaces spanned by the rows of the generator matrix and the parity-check matrix must sum to 7, so the dimension of the code subspace must be 3. To find minimum Hamming distance use Theorem 4-9 and notice that sum of columns 1,6,7 or 4,5,7 (and others..) is zero. Since the columns are distinct, no two columns of $\mathbf{H}$ can sum to a zero vector, so $d_{\min} = 3$.

   b) The length is 7 and dimension is 3. To find $d_{\min}$, use Theorem 4-9 directly to the given $\mathbf{H}$, or shuffle the columns to a simpler order, e.g.

$$\mathbf{H}' = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

   No linear combination of two or three colums sums to zero. $d_{\min} = 4$, since the sum of columns 1,2,6,7 is zero. There are also other combinations.

   c) The only primitive polynomial for GF(4) is $f(x) = x^2 + x + 1$, and thus $\alpha^2 + \alpha + 1 = 0$, since roots of the primitive polynomial are primitive elements. The length of the code is 4 and dimension is 2. To find $d_{\min}$ we must again sum columns of $\mathbf{H}$. The parity-check matrix is

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & 0 \end{bmatrix},$$

and we notice that the smallest number of columns that sums to zero vector is 3 (the first three columns). Thus, $d_{\min} = 3$.

6. This problem takes also place in GF(4). In manipulations use $\alpha^3 = 1$ and $\alpha^2 + \alpha + 1 = 0$ like in the previous problem.

   a) To obtain the codewords solve $\mathbf{cH}^T = \mathbf{0}$, where $\mathbf{c} = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 \end{bmatrix}$ is a code word. This produces equations $c_3 = c_1\alpha^2 + c_2\alpha$, and $c_4 = c_1 + c_2$. The 16 code words can be written out by computing c_3, c_4 for all combinations of c_1, c_2.

c_1	c_2	c_3	c_4
0	0	0	0
0	1	α	1
0	α	α^2	α
0	α^2	1	α^2
1	0	α^2	1
1	1	1	0
1	α	0	α^2
1	α^2	α	α
α	0	1	α
α	1	α^2	α^2
α	α	α	0
α	α^2	0	1
α^2	0	α	α^2
α^2	1	0	α
α^2	α	1	1
α^2	α^2	α^2	0

b) To evaluate the Gilbert bound we need to find $d_{\min}$ of the code. Summing the first three columns produces a zero vector, thus $d_{\min} = 3$ and $t = 1$. The Gilbert bound is

$$r \leq \log_4 \sum_{j=0}^{2} \binom{4}{j} 3^j = 3.033... \qquad (3).$$

Redundancy of the code is 2. It does not achieve the Gilbert bound.

c) The Hamming bound is

$$r \geq \log_4 \sum_{j=0}^{1} \binom{4}{j} 3^j = 1.850... \qquad (2).$$

Redundancy of the code exceeds the Hamming bound. The code is not perfect.

d) The Singleton bound is

$$r \leq n - k + 1 = 4 - 2 + 1 = 3 = d_{\min}.$$

The code satisfies the Singleton bound with equality. Such a code is called Maximum-Distance Separable. We shall encounter more MDS codes later in the course (e.g. Reed-Solomon codes).

7. Use equation (4-5) from the book. In our case we get

$$\sum_{j=0}^{1} \binom{n}{j} = 1 + n = 2^r,$$

where $r = n - k$ is redundancy of the code. A necessary condition is $n = 2^r - 1$ for some r. Thus, n must be odd.

For a q-ary code

$$\sum_{j=0}^{1} \binom{n}{j} (q-1)^j = 1 + n(q-1) = q^r,$$

so $n = \dfrac{q^r - 1}{q - 1}$ for some r.