EE/Ma 127a Error-Correcting Codes - Final Exam

Ling Li, ling@cs.caltech.edu

December 1, 2000

F.1 *Code designing.* Let H be one parity-check matrix for this (n, k) code. H has n columns, denoted by h_i ($i = 1, 2, \ldots, n$), and each is a vector of length $r = n - k$.

In order to correct all error patterns described in the problem, we must ensure

$$0, h_n, h_n + h_{n-1}, \ldots, \sum_{i=k}^{n} h_i, \ldots, \sum_{i=1}^{n} h_i \tag{1}$$

are $n + 1$ distinct vectors of length r. Thus $2^r \geq n + 1$.

When $2^r \geq n + 1$, we can choose n distinct non-zero vectors of length r, denoted by v_i, and let ($k = 1, 2, \ldots, n$)

$$\sum_{i=k}^{n} h_i = v_k,$$

or equivalently, ($k = 1, 2, \ldots, n - 1$)

$$h_n = v_n, h_k = v_k - v_{k+1}. \tag{2}$$

With such H, the $n + 1$ vectors in (1) are all distinct and then the code can correct all error patterns in the problem.

Thus, the smallest possible r is $\lceil \log_2(n + 1) \rceil$, and the largest possible k for the code is

$$k = n - \lceil \log_2(n + 1) \rceil .$$

The parity-check matrix H can be designed from (2). For $n = 7$, $k = 7 - \lceil \log_2(7 + 1) \rceil = 4$, $r = 3$. Let v_i be the binary representation of number i. We can get the H from (2) is

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

F.2 *Lost syndrome.* One parity-check matrix for the cyclic $(7, 3)$ Abramson code is

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

where α is a primitive root in $GF(2^3)$ and $\alpha^3 = \alpha + 1$. For an error pattern $R = R_0 R_1 \ldots R_6$, the syndrome is

$$S = \sum_{i=0}^{6} R_i \begin{pmatrix} \alpha^i \\ 1 \end{pmatrix}. \tag{3}$$

(a) The syndrome for error pattern of length 0 (no errors) is $\binom{0}{0}$; The syndrome for burst error pattern $(1, i)$ is $\binom{\alpha^i}{1}$, $i = 0, 1, \ldots, 6$; And the syndrome for burst error pattern $(11, i)$ is

$$\begin{pmatrix}\alpha^i\\1\end{pmatrix} + \begin{pmatrix}\alpha^{i+1}\\1\end{pmatrix} = \begin{pmatrix}\alpha^i(1+\alpha)\\0\end{pmatrix} = \begin{pmatrix}\alpha^{i+3}\\0\end{pmatrix},$$

$i = 0, 1, \ldots, 6$. Since $\alpha^i \neq 0$, the syndrome $\binom{0}{1}$ is not included in the above syndromes. Furthermore, since α^i and α^{i+3} both go over all the non-zero vectors of length 3 when $i = 0, 1, \ldots, 6$, $\binom{0}{1}$ is also the only syndrome not included in the above syndromes.
Note that the sum of column #1, #2, and #4 of H is

$$\begin{pmatrix}1\\1\end{pmatrix} + \begin{pmatrix}\alpha\\1\end{pmatrix} + \begin{pmatrix}\alpha^3\\1\end{pmatrix} = \begin{pmatrix}1+\alpha+\alpha^3\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}.$$

So $R = 1101000$ or $R(x) = 1 + x + x^3$ is one error pattern that produces syndrome $\binom{0}{1}$. Thus the polynomial of the syndrome $\binom{0}{1}$ is

$$S(x) = R(x) \bmod g(x) = 1 + x + x^3.$$

(b) From (a), any error pattern of weight 0 or 1 can not produce syndrome $\binom{0}{1}$. For any error pattern of an even weight, from (3), the syndrome has the form $\binom{\beta}{0}$, where $\beta = \sum_{i=0}^{6} R_i\alpha^i$, thus is not equal to $\binom{0}{1}$. So the error patterns with syndrome $\binom{0}{1}$ can only have weights 3, 5, or 7. Since in (a) we've found an error pattern 1101000 that produces syndrome $\binom{0}{1}$, the minimum weight of an error pattern that produces syndrome $\binom{0}{1}$ is 3.

(c) To find all the error patterns with syndrome $\binom{0}{1}$, we only need to study the error patterns of weights 3, 5, or 7.

- The only error pattern of weight 7 is 1111111, which produces syndrome

$$\sum_{i=0}^{6}\begin{pmatrix}\alpha^i\\1\end{pmatrix} = \begin{pmatrix}1+\alpha+\cdots+\alpha^6\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}.$$

- For any error pattern R of weight 5, there are exactly two 0's in R, say, at location j and k ($0 \leq j, k \leq 6$ and $j \neq k$). Thus the syndrome is

$$\sum_{i \neq j,k}\begin{pmatrix}\alpha^i\\1\end{pmatrix} = \sum_{i=0}^{6}\begin{pmatrix}\alpha^i\\1\end{pmatrix} + \begin{pmatrix}\alpha^j\\1\end{pmatrix} + \begin{pmatrix}\alpha^k\\1\end{pmatrix} = \begin{pmatrix}\alpha^j+\alpha^k\\1\end{pmatrix}.$$

  Since $\alpha^j \neq \alpha^k$ when $0 \leq j, k \leq 6$ and $j \neq k$, the syndrome is not $\binom{0}{1}$. Thus there's no error patterns of weight 5 can produce syndrome $\binom{0}{1}$.

- Let i, j, and k denote the locations of 1's in an error pattern of weight 3. The syndrome of that error pattern is $\binom{0}{1}$ if and only if

$$\begin{pmatrix}\alpha^i\\1\end{pmatrix} + \begin{pmatrix}\alpha^j\\1\end{pmatrix} + \begin{pmatrix}\alpha^k\\1\end{pmatrix} = \begin{pmatrix}\alpha^i+\alpha^j+\alpha^k\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix},$$

  i.e., $\alpha^i = \alpha^j + \alpha^k$.

For any combination of j, k that $0 \le j, k \le 6$ and $j \ne k$, $\alpha^j + \alpha^k \ne 0$. Thus there must be one i such that $0 \le i \le 6$ and

$$\alpha^i = \alpha^j + \alpha^k.$$

And from $a^j, a^k \ne 0$ we know $i \ne j, k$. Thus the error pattern with 1's at locations i, j, and k has the syndrome $\binom{0}{1}$. And the number of such error patterns is

$$\frac{\binom{7}{2}}{\binom{3}{2}} = 7.$$

In fact, from $\alpha^i = \alpha^j + \alpha^k$, we get

$$\alpha^{k-i} = \alpha^{j-i} + 1. \tag{4}$$

Without loss of generality, assume $i < j < k$. Thus (4) can only be one of

$$\alpha^3 = \alpha^1 + 1, \alpha^6 = \alpha^2 + 1, \alpha^5 = \alpha^4 + 1.$$

Note that the 2nd and 3rd equations are "cyclic" versions of the first one, by multiplying both sides of the 1st equation by α^6 and α^4, respectively. So the 7 error patterns of weight 3 that produce syndrome $\binom{0}{1}$ are $(1101, i)$, $i = 0, 1, \ldots, 6$.

Summarizing above, the error patterns that produce syndrome $\binom{0}{1}$ are 1111111 and $(1101, i)$, $i = 0, 1, \ldots, 6$.

F.3 *Decoder errors.* Let $d(C, C')$ denote the Hamming distance between C and C'. For error pattern R, the decoder will make a decoder error if and only if there exists a non-zero codeword C such that $d(R, C) \le 2$. When such C exists, it must be unique since the minimum distance of the $(15, 7)$ "Hex-BCH" code is ≥ 5 and thus for another codeword C',

$$d(R, C') \ge d(C, C') - d(R, C) \ge 5 - 2 = 3.$$

So I say that R is *associated* to C when $d(R, C) \le 2$, and we can count the error patterns that will result in decoder error by counting the error patterns associated to some non-zero codeword.

(a) When the weight of R is 3, the weight of C that satisfying $d(R, C) \le 2$ can only be 5, according to the code's weight enumerator

$$A(z) = 1 + 18z^2 + 30z^6 + \cdots.$$

And the difference between C and R can only happen at two bits that are 1's in C. Thus, the number of error patterns associated to C is

$$\binom{5}{2} = 10.$$

There are 18 codewords of weight 5, so the total number of error patterns of weight 3 that will result in decoder error is $18 \times 10 = 180$.

(b) When the weight of R is 4, the weight of C that satisfying $d(R, C) \leq 2$ can be 5 or 6. Similarly to (a), the number of error patterns associated to codewords of weight 5 is

$$18 \times \binom{5}{1} = 90,$$

and the number of error patterns associated to codewords of weight 6 is

$$30 \times \binom{6}{2} = 450.$$

So the total number of error patterns of weight 4 that will result in decoder error is $90 + 450 = 540$.

F.4 *Hamming codes.* The columns of the parity-check matrix H for a $(2^m - 1, 2^m - m - 1)$ Hamming code are $2^m - 1$ distinct non-zero vectors of length m. Thus the number of different H is $(2^m - 1)!$. However, for one code, H is not unique. The number of different H for one code is

$$\prod_{i=0}^{m-1} (2^m - 2^i).$$

So the number of different $(2^m - 1, 2^m - m - 1)$ Hamming codes is

$$\frac{(2^m - 1)!}{\prod_{i=0}^{m-1} (2^m - 2^i)}.$$

For $m = 3$, the number is

$$\frac{7!}{7 \times 6 \times 4} = 30.$$

F.5 *Common entries.* If the "x" row of the addition table and the "y" row of the multiplication table are common in the "t" entry, we have $x + t = y \cdot t$, or equivalently,

$$(y - 1) \cdot t = x. \tag{5}$$

- If $y \neq 1$, then $(y - 1)^{-1}$ exists. So $t = (y - 1)^{-1} \cdot x$ is unique. Thus those two rows have exactly one entry in common.
- If $y = 1$ and $x \neq 0$, then no t satisfies (5). Thus those two rows have no entries in common.
- If $y = 1$ and $x = 0$, then any $t = 0, 1, \ldots, F$ satisfies (5). That is, those two rows, which are the "0" row of the addition table and the "1" row of the multiplication table, are common in all 16 entries.