EE/Ma 127a Error-Correcting Codes - Homework Assignment 5

Ling Li, ling@cs.caltech.edu

November 9, 2000

5.1 Use the parity-check matrix in *Example 8.21*,

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

where α is a primitive root (thus $\alpha^7 = 1$) satisfying $\alpha^3 = \alpha + 1$ in GF(8). From

$$\alpha^i \left(1 + \alpha + \alpha^2\right) = \alpha^i \left(\alpha^3 + \alpha^2\right) = \alpha^{i+2} \left(\alpha + 1\right) = \alpha^{i+5} = \alpha^{(i+5) \bmod 7},$$

we know that the syndrome of any error pattern $(111, i)$, which is $\binom{\alpha^i(1+\alpha+\alpha^2)}{1}$, is the same with that of the error pattern $(1, (i+5) \bmod 7)$, which is $\binom{\alpha^{(i+5) \bmod 7}}{1}$.

5.2 The Abramson bounds r_A and Reiger bounds r_R for $n = 31$ and $b = 1, 2, \ldots, 15$ are:

b	r_A	r_R	$\max\{r_A, r_R\}$
1	5	2	5
2	6	4	6
3	7	6	7
4	8	8	8
5	9	10	10
6	10	12	12
7	11	14	14
8	12	16	16
9	13	18	18
10	14	20	20
11	15	22	22
12	16	24	24
13	17	26	26
14	18	28	28
15	19	30	30

5.3 For $n = 31$ and $b = 3$, the Abramson and Reiger bounds hint that $r \geq 7$. From *Table 8.1*, the irreducible factors of $\left(x^{31} - 1\right)$ consist of $(x + 1)$ and 6 other polynomials of degree 5. Thus if polynomial $g(x) \,\middle|\, \left(x^{31} - 1\right)$, the degree of $g(x)$ must be $5t$ or $5t + 1$, where $t = 0, 1, \ldots, 6$. So we cannot construct a polynomial $g(x)$ of degree 7 such that $g(x) \,\middle|\, \left(x^{31} - 1\right)$, which means there's no cyclic code that meets the bound $r = 7$.

5.4 The desired generator polynomial has the form $g(x) = \left(x^{2b-1}-1\right) f(x)$, where $b \geq 11$ and $f(x)$ is an irreducible polynomial which is not a divisor of $\left(x^{2b-1}-1\right)$. Let $f(x)$ be one primitive polynomial of degree m. Thus the period of $f(x)$ is $n_0 = 2^m - 1$. When $n_0 > 2b-1$, $f(x)$ is not a divisor of $\left(x^{2b-1}-1\right)$.

For the code generated by $g(x)$, $n = \operatorname{lcm}(2b-1, n_0)$, and $k = n-(2b-1)-m$. $k \geq 100{,}000$ requires

$$\begin{aligned} & 10^5 \leq n-(2b-1)-m < (2b-1)n_0 - (2b-1) \\ \Rightarrow \quad & n_0 = 2^m - 1 > \frac{10^5}{2b-1} + 1 \\ \Rightarrow \quad & m > \log_2\left(\frac{10^5}{2b-1} + 2\right). \end{aligned}$$

$b \geq 11$ gives $m \geq 13$. Let $b = 11$, $m = 13$ and $f(x) = 1 + x^9 + x^{10} + x^{12} + x^{13}$ is a primitive polynomial. Thus

$$\begin{aligned} g(x) &= \left(x^{21}-1\right)\left(1+x^9+x^{10}+x^{12}+x^{13}\right) \\ &= 1+x^9+x^{10}+x^{12}+x^{13}+x^{21}+x^{30}+x^{31}+x^{33}+x^{34}, \end{aligned}$$

and $n = \operatorname{lcm}\left(21, 2^{13}-1\right) = 172011$, $k = n - 21 - 13 = 171977$.

5.5 The period of $f_m(x)$ is $n_0 = 2^m - 1$. $2b - 1 = 5$.

(a) Write m as $m = 4t + i$, where $t = \lfloor \frac{m}{4} \rfloor$ and $i = m \bmod 4$. Thus

$$2^m - 1 = 16^t 2^i - 1 \equiv 2^i - 1 \pmod 5.$$

For $i = 0, 1, 2, 3$, only $i = 0$ satisfies $5 \,\big|\, \left(2^i - 1\right)$. So $n_0 = 2^m - 1$ is a multiple of 5 if and only if m is a multiple of 4. Thus

$$\begin{aligned} n_m &= \operatorname{lcm}(2b-1, n_0) = \begin{cases} 2^m - 1, & \text{when } 4|m; \\ 5\left(2^m - 1\right), & \text{otherwise.} \end{cases} \\ k_m &= n_m - (2b-1) - m = \begin{cases} 2^m - 6 - m, & \text{when } 4|m; \\ 5\left(2^m - 2\right) - m, & \text{otherwise.} \end{cases} \end{aligned}.$$

(b) Since $2^{m+2} < 5\left(2^m - 1\right) + 1 < 2^{m+3}$ when $m \geq 3$, the "weak" Abramson bound is

$$r_A^{(m)} \geq \lceil \log_2(n_m + 1) \rceil + (b-1) = \begin{cases} m+2, & \text{when } 4|m; \\ m+5, & \text{other } m \geq 3. \end{cases}$$

The actual redundancy is $r_m = n_m - k_m = (2b-1) + m = m + 5$, bigger than or equal to the bound. When $m \to \infty$, r_m is the same as or very close to $r_A^{(m)}$, which shows that the "weak" bound here is really a tight bound.