Solutions to Homework Assignment 5

Problem 1.

The i-th column of the parity check matrix of the (7,3) Abramson code has the form $(x^i \bmod g(x),\ 1)^T$, where $g(x)$ is a primitive polynomial of degree 3, i.e. is a generator polynomial for a cyclic (7,4) Hamming code. The syndrome of a burst with pattern 111 and location i is gotten by adding the ith, $(i+1)$st and $(i+2)$nd column of the parity check matrix. The syndrome therefore is given by $((x^i + x^{i+1} + x^{i+2}) \bmod g(x),\ 1)^T$. Now we have

$$(x^i + x^{i+1} + x^{i+2}) \bmod g(x) = x^i(1 + x + x^2) \bmod g(x)$$

Note that the right hand side of this equation is nonzero, because $g(x)$ is irreducible (property of a primitive polynomial) and is coprime with both x^i and $1 + x + x^2$ (because it has degree less than the degree of $g(x)$. But any nonzero vector of length 3 (or a polynomial of degree 2) is a power of x modulo $g(x)$, say $x^e \bmod g(x)$. But then the syndrome of the burst with pattern 111 and location i is the same as the syndrome of the burst with pattern 1 and location e.

Therefore every burst having pattern 111 has the syndrome as some burst with pattern 1.

Problem 2.

The Abramson bound gives $r \geq \log_2(n + 1) + b - 1 = b + 4$. The Reiger bound gives $r \geq 2b$. It is easy to see that the Abramson bound is stronger for $b < 4$ and the Reiger bound is stronger for $b > 4$. At $b = 4$ the two bounds coincide.

Problem 3.

For $b = 3$, the Abramson bound gives $r \geq 7$ and the Reiger bound gives $r \geq 6$. So together we have $r \geq 7$. However, from Table 8.1 in the handout, we see that the $x^{31}+1$ has irreducible factors of degrees 1 and 5 only. Thus, it cannot have a factor of degree 7, i.e. there is no (31,24) cyclic code. Therefore for $b = 3$ there is no cyclic code that meets the bound of Problem 2.

Problem 4.

The classical Fire codes have generator polynomial of the form $g(x) = (x^{2b} + 1)f(x) = (x^{21} + 1)f(x)$, since $b = 11$ in this case. Let degree $f(x)$ be m, then n_0, the period of $f(x)$, is at most $2^m - 1$, achieved when $f(x)$ is primitive. Therefore the length of the code is the lcm of $2b - 1$ and n_0 (by the Corollary on Page 30 of the handout), which is at most $21(2^m - 1)$. The code has redundancy equal to the degree of $g(x)$, which is $m + 21$. Therefore the dimension of the code is at most $21(2^m - 1) - (m + 21)$. We require that this is at least 100000, and the smallest m that satisfies this constraint happens to be $m = 13$.

Therefore we pick $f(x)$ to be any primitive polynomial of degree 13 from Appendix A in Wicker, say $f(x) = 1 + x + x^3 + x^4 + x^{13}$. Then check that $m > b$ and $f(x)$ is not a divisor of $x^{21} + 1$. Hence by the Corollary on Page 30 of the handout, the code generated by $g(x) = (x^{21} + 1)f(x)$ is a 11-burst error correcting code.

The code parameters are also given by the same Corollary. n is given by the lcm of 21 and $2^m - 1$ which is 172011. r is $21 + m = 34$, and therefore $k = 171977$, which is bigger than 100000, as required. Therefore we have a 11-burst correcting (172011,171977) code.

Problem 5(a).

By the Fire code construction, n_m is the lcm of $2b - 1$ and $2^m - 1$, i.e. the lcm of 5 and $2^m - 1$. Now notice that the last digit of 2^m cycles through the values 2, 4, 8, 6 periodically. $2^m - 1$ is divisible by 5 only if the last digit of 2^m is 6, and that happens only when m is a multiple of 4.

Therefore $n_m = 2^m - 1$ when m is a multiple of 4, and $5(2^m - 1)$ otherwise.

$k_m = n_m - (m+5)$. Therefore $k_m = 2^m - m - 6$ when m is a multiple of 4, and $5.2^m - m - 10$ otherwise.

Problem 5(b).

Actual redundancy $r_m = m + 5$.
When m is a multiple of 4, the Abramson bound says $r \geq \log_2(n+1) + (b - 1) = \log_2(2^m) + 3 - 1 = m + 2$.
When m is not a multiple of 4, the Abramson bound for large m says $r \geq \log_2(5(2^m - 1) + 1) + 3 - 1 = log_2 5 + m + 2 = m + 4.32$, i.e. $r \geq m + 5$.

Therefore the Fire codes constructed meet the weak Abramson bound when m is not a multiple of 4 in the limit of large m, and differ from it by 3, when m is a multiple of 4.