Oliver Tonnesen
V00885732

Assignment 5

MATH 413
April 3, 2020

1

$$\begin{aligned} L_1(x) &= (q-1)\binom{n-x}{1}\binom{x-1}{0} + (-1)\binom{n-x}{0}\binom{x-1}{1} \\ &= (q-1)(n-x) - (x-1) \end{aligned}$$

$$\begin{aligned} \sum_{s=0}^{1} K_s(x) &= [1] + \left[(q-1)\binom{x}{0}\binom{n-x}{1} - \binom{x}{1}\binom{n-x}{0}\right] \\ &= 1 + (q-1)(n-x) - x \\ &= (q-1)(n-x) - (x-1) \end{aligned}$$

So when $t = 1$, it is the case that $L_t(x) = \sum_{s=0}^{t} K_s(x)$, as desired.

2

Let C be such a code, and let $w \in C$. If w is non-constant, then it produces at least two distinct cyclic shifts: w itself, and w shifted left by one. We can view these cyclic shifts of w as a cyclic group generated by the left shift operation. For $w = w_1 \cdots w_p$, consider the list of its cyclic shifts:

$$\begin{gathered} w_1 \cdots w_{p-1} w_p \\ w_2 \cdots w_p w_1 \\ \vdots \\ w_{p-1} \cdots w_1 w_2 \end{gathered}$$

For any w, any repetitions in this list would imply the existence of a proper subgroup of the above mentioned cyclic group. The above cyclic group has prime order, so its only subgroups are itself and the trivial subgroup, so all non-constant words must have full order p. Each set of p cyclic shifts in C does not change $|C| \pmod{p}$, so we need only consider the remaining constant words in C. C is in particular a linear code, so if one nonzero constant word is in C, then all of them are, in which case $|C| \equiv q \pmod{p}$. Otherwise, the only constant word is 0, in which case $|C| \equiv 1 \pmod{p}$.

3

We know that if $C = \langle g(x) \rangle$ has length n, then $g(x)$ divides $x^n - 1$. $x^7 + x + 1$ divides $x^{127} - 1$, and in fact one can verify that $x^7 + x + 1$ does not divide $x^i - 1$ for any i less than 127, so the smallest length binary code with generator polynomial $x^7 + x + 1$ has length 127.

4

4.a

$\dim C = n - \deg(g) = 11 - 5 = 6$, so $G = \begin{pmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ x^3 g(x) \\ x^4 g(x) \\ x^5 g(x) \end{pmatrix}$.

We get $G = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

4.b

We know that if C is a nontrivial linear cyclic code with generator polynomial $g(x)$, then $C^\perp$ is also a linear cyclic code with generator polynomial $g^*(x)$.

So the generator polynomial for $C^\perp$ is

$$g^*(x) = 1 + 2x^2 + x^3 + 2x^4 + 2x^5$$

From here, we know that if the generator polynomial is $g(x)$, then the check polynomial is $h(x) = \frac{x^n - 1}{g(x)}$, so the check polynomial for $C^{\perp}$ is

$$
\begin{aligned}
h(x) &= \frac{x^{11} - 1}{g^*(x)} \\
&= \frac{x^{11} - 1}{1 + 2x^2 + x^3 + 2x^4 + 2x^5} \\
&= 2x^6 + x^5 + x^4 + x^3 + 2x^2 + 2
\end{aligned}
$$

5

In this case, $q = 2$ and $r = 3$, so $n = q^r - 1 = 2^3 - 1 = 7$, and $2 \leq d \leq 7$. To find β, a primitive element of $\mathbb{F}_8$, we can simply take $\mathbb{F}_8 \cong \mathbb{F}_2[x] / \langle x^3 + x + 1 \rangle$ and let $\beta^3 + \beta + 1 = 0$.

We now find the minimal polynomials of $\beta, \ldots, \beta^7$:

$$
\begin{aligned}
m_{\beta}(x) &= x^3 + x + 1 \\
m_{\beta^2}(x) &= x^3 + x + 1 \\
m_{\beta^3}(x) &= x^3 + x^2 + 1 \\
m_{\beta^4}(x) &= x^3 + x + 1 \\
m_{\beta^5}(x) &= x^3 + x^2 + 1 \\
m_{\beta^6}(x) &= x^3 + x^2 + 1 \\
m_{\beta^7}(x) &= x + 1
\end{aligned}
$$

Since $C = \langle g(x) \rangle$, where $g(x) = \operatorname{lcm}(m_{\beta}(x), \ldots, m_{\beta^{d-1}}(x))$, we can now find C for each possible distance d.

For $d = 2$, we have $C = \left\langle x^3 + x + 1 \right\rangle$. For $d = 3, 4, 5, 6$, we have $C = \left\langle (x^3 + x + 1)(x^3 + x^2 + 1) \right\rangle$. For $d = 7$, we have $C = \left\langle (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1) \right\rangle$.