Mathematics 392 – Seminar in Coding Theory
Final Problem Set Solutions
May 6, 2002

I. A) We have $\alpha = x \bmod h_1(x)$. So α satisfies $\alpha^3 + \alpha + 1 = 0$ in F_1. If $\phi : F_1 \to F_2$ satisfies both properties in (1), then

$$0 = \phi(0) = \phi(\alpha^3 + \alpha + 1) = \phi(\alpha^3) + \phi(\alpha) + \phi(1) = \phi(\alpha)^3 + \phi(\alpha) + 1$$

(where $\phi(1) = 1$ since by the second equation in (1), $\phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1)$, but we dont want $\phi(1) = 0$ – otherwise ϕ cannot be one to one). Hence $\phi(\alpha)$ is a root of the equation $x^3 + x + 1 = 0$ in F_2. The powers of $\beta = y \bmod h_2(y)$ in F_2 are

$$\begin{aligned}
\beta^0 &= 1\\
\beta^1 &= \beta\\
\beta^2 &= \beta^2\\
\beta^3 &= \beta^2 + 1\\
\beta^4 &= \beta^2 + \beta + 1\\
\beta^5 &= \beta + 1\\
\beta^6 &= \beta^2 + \beta\\
\beta^7 &= 1
\end{aligned}$$

Of these we see $(\beta^3)^3 + \beta^3 + 1 = \beta^9 + \beta^3 + 1 = \beta^2 + \beta^2 + 1 + 1 = 0$. Hence β^3 is a root of the equation $x^3 + x + 1 = 0$ in F_2. Similarly β^5 and β^6 are also roots of this equation. These are the only possibilities for $\phi(\alpha)$: $\phi(\alpha) \in \{\beta^3, \beta^5, \beta^6\}$. (Note: $\{3, 5, 6\}$ is the cyclotomic coset of 3 mod $8 - 1 = 7$.)

B) Using the second equation in (1),

$$\phi(\alpha^j) = \phi(\alpha \cdot \alpha \cdot \cdots \cdot \alpha) = \phi(\alpha) \cdot \phi(\alpha) \cdot \cdots \cdot \phi(\alpha) = (\phi(\alpha))^j$$

Hence the choice $\phi(\alpha)$ will determine the values of ϕ on all of the nonzero elements of the field.

C) Any one of the choices $\phi(\alpha) = \beta^3, \beta^5, \beta^6$ will yield an isomorphism between F_1 and F_2, if you extend ϕ to the powers of α using part B. For instance, with $\phi(\alpha) = \beta^3$, we have $\phi(\alpha^j + \alpha^k) = \phi(\alpha^j) + \phi(\alpha^k)$ for all j, k. (You needed to check this case by case. For example with $j = 1, k = 2$:

$$\phi(\alpha + \alpha^2) = \phi(\alpha^4) = (\beta^3)^4 = \beta^{12} = \beta^5$$

And

$$\phi(\alpha) + \phi(\alpha^2) = \beta^3 + (\beta^3)^2 = \beta^3 + \beta^6 = \beta^2 + 1 + \beta^2 + \beta = \beta + 1 = \beta^5$$

II. A) A generator matrix for C is

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

Forming all linear combinations of the rows, we get the following list of words in C:

$$\{0000000, 1101000, 0110100, 0011010, 0001101, 1011100, 0101110, 0010111,$$
$$1110010, 0111001, 1100101, 1000110, 1010001, 1111111, 0100011, 1001011\}$$

From this, we see that there is one word of weight 0, 7 of weight 3, 7 of weight 4, and 1 of weight 7, so $W_C(t) = 1 + 7t^3 + 7t^4 + t^7$.

B) This is just algebra: Since $k = 4$ for C, we substitute in the the McWilliams identity, simplify, and expand using the binomial theorem:

$$\begin{aligned} 2^4 W_{C^\perp}(t) &= (1+t)^7 \left(1 + 7\left(\frac{1-t}{1+t}\right)^3 + 7\left(\frac{1-t}{1+t}\right)^4 + \left(\frac{1-t}{1+t}\right)^7\right) \\ &= (1+t)^7 + 7(1-t)^3(1+t)^4 + 7(1-t)^4(1+t)^3 + (1-t)^7 \\ &= (1 + 7t + 21t^2 + 35t^3 + 35t^4 + 21t^5 + 7t^6 + t^7) \\ &\quad + 7(1 - 3t + 3t^2 - t^3)(1 + 4t + 6t^2 + 4t^3 + t^4) \\ &\quad + 7(1 + 3t + 3t^2 + t^3)(1 - 4t + 6t^2 - 4t^3 + t^4) \\ &\quad + (1 - 7t + 21t^2 - 35t^3 + 35t^4 - 21t^5 + 7t^6 - t^7) \\ &= 16 + 112t^4 \end{aligned}$$

Hence $W_{C^\perp}(t) = 1 + 7t^4$.

C) (There were a number of different approaches used in the submitted solutions. Here is another one, even more elementary.) In fact the dual code of a cyclic code is always cyclic. *Proof*: Since we assume C is cyclic, the cyclic shift π maps C to itself. If $v \in C$ and $w \in C^\perp$ are arbitary words, then $0 = v \cdot w = \pi(v) \cdot \pi(w)$ (since cyclically shifting the two words simultaneously does not change the dot product). This says that $\pi(w)$ is perpendicular to every word in C, so $\pi(w) \in C^\perp$ and $C^\perp$ is also closed under π. Hence $C^\perp$ is also cyclic. A generator matrix for $C^\perp$ is obtained by taking the transpose of a parity check matrix for C. I applied our usual method to get the H for C then took the transpose to yield:

$$G^\perp = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

The word in $C^\perp$ giving a corresponding codeword polynomial of minimal degree comes from the first row: $g^\perp(x) = 1 + x^2 + x^3 + x^4$. This is the generator polynomial for $C^\perp$.

III. A) The question from Discussion 4 referred to in the problem said: If $C = \langle v_1, \ldots, v_k \rangle$ and $\pi(v_i) \in C$ for all i, then C is cyclic. Here we have the spanning set

$$\{ev(1), ev(t), \ldots, ev(t^{k-1})\},$$

where $ev(t^j) = (1, \beta^j, \beta^{2j}, \ldots, \beta^{(2^r-2)j})$, $1 \leq j \leq k-1$. Applying the cylic shift, we have

$$\begin{aligned}\pi(ev(t^j) &= (\beta^{(2^r-2)j}, 1, \beta^j, \beta^{2j}, \ldots, \beta^{(2^r-3)j}) \\ &= ev(\beta^{(2^r-2)j}t^j)\end{aligned}$$

(using $\beta^{2^r-1} = 1$). The polynomial $\beta^{(2^r-2)j}t^j$ is in the span of $\{1, t, t^2, \ldots, t^{k-1}\}$. So this is also a codeword. Hence the image of ev is a cyclic code.

B) The product

$$(1+x)(1+x+x^2+\cdots+x^{2^r-2}) = 1+x^{2^r-1}$$

Every nonzero element in $\mathbf{F}_{2^r}$ satisfies $1+x^{2^r-1} = 0$, so every nonzero element is a root of one of the two factors on the left side of the last equation. Since $x = 1$ is a root of the first, the roots of $1+x+x^2+\cdots+x^{2^r-2} = 0$ are *all the nonzero elements of* $\mathbf{F}_{2^r}$ *except* $x = 1$. Note: The polynomial $1+x+x^2+\cdots+x^{2^r-2} = 0$ is the codeword polynomial corresponding to $ev(1) = (1, 1, 1, \ldots, 1)$. The next part deals with the $ev(t^j)$ for $j \neq 0$.

C) The codeword polynomial corresponding to $ev(t^j)$ is

$$1+\beta^j x+(\beta^j x)^2+\cdots+(\beta^j x)^{2^r-2}$$

This has the form $1+u+u^2+\cdots+u^{2^r-2}$ with $u = \beta^j x$. By part B, the roots of this last polynomial are all $u \neq 0, 1$ in $\mathbf{F}_{2^r}$, so $\beta^j x \neq 0, 1$. This yields all $x \neq 0, \beta^{-j}$.

D) We must determine the common roots of all the polynomials corresponding to $ev(t^j)$, $j = 0, 1, \ldots, k-1$. Combining parts B and C, we have the sets of roots as follows:

$$\begin{aligned}
ev(1) &\leftrightarrow \text{ all } x \neq 0, 1 \Rightarrow \{\beta, \beta^2, \ldots, \beta^{2^r-2}\} \\
ev(t) &\leftrightarrow \text{ all } x \neq 0, \beta^{-1} = \beta^{2^r-2} \Rightarrow \{1, \beta, \beta^2, \ldots, \beta^{2^r-3}\} \\
ev(t^2) &\leftrightarrow \text{ all } x \neq 0, \beta^{-2} = \beta^{2^r-3} \Rightarrow \{1, \beta, \beta^2, \ldots, \beta^{2^r-4}, \beta^{2^r-2}\} \\
&\vdots \quad \vdots \\
ev(t^{k-1}) &\leftrightarrow \text{ all } x \neq 0, \beta^{-k+1} = \beta^{2^r-k} \Rightarrow \{1, \beta, \beta^2, \ldots, \beta^{2^r-k-1}, \beta^{2^r-k+1}, \ldots, \beta^{2^r-3}\}
\end{aligned}$$

The set of common roots is found by removing $1, \beta^{2^r-2}, \ldots, \beta^{2^r-k}$ from the nonzero elements of the field. The remaining set is

$$\beta, \beta^2, \ldots, \beta^{2^r-k-1} = \beta^{\delta-1}$$

This is the same as the set of roots of the generator polynomial of the Reed-Solomon code $RS(2^r, \delta)$ (with $m = 0$).

IV. A) Let $\beta^{-\ell}$ be any one of the roots of $\sigma(x)$. Of the terms in the sum defining $\omega(x)$, all but the one with $j = \ell$ contain the factor $(1 - \beta^\ell x)$. Hence all those terms will go to zero when we substitute $x = \beta^{-\ell}$. The remaining term is

$$(1) \qquad \omega(-\ell) = e_\ell \beta^\ell \prod_{j \neq \ell} (1 - \beta^j \beta^{-\ell})$$

This is not zero, since the error values are nonzero by definition, $\beta \neq 0$, and $(1 - \beta^{j-\ell}) \neq 0$ if $j \neq \ell$. Hence none of the factors of $\sigma(x)$ divide $\omega(x)$, so the gcd is 1.

B) This follows from (1). Just divide through to solve for e_ℓ.