ENEE626. Midterm examination, 10/27/2005 **Instructor:** A. Barg

Solutions of problems

Problem 1. (6pts, 2 each subproblem) Consider a ternary linear code $\mathcal{C}$ with the generator matrix

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 & 2 & 0 \\ 1 & 0 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}$$

(1) Find a parity-check matrix of $\mathcal{C}$

For instance,

$$H = \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(2) What are the parameters $[n, k, d]$ of the code $\mathcal{C}$?

[6,3,3] because, for instance, 200101 is a codeword and no two columns of H are proportional.

(3) How many cosets does $\mathcal{C}$ have? Name 10 coset leaders.

It has $3^{n-k} = 27$ cosets. Since $d(\mathcal{C}) = 3$, all 12 vectors of weight 1 are coset leaders.

Problem 2. (14 pts, 2 each subproblem) Let $f(x) = x^4 + x^3 + 1$ and let α be a root of f.

(1) Is f a primitive polynomial?

Yes because we have shown in class that $f^*(x) = x^4 + x + 1$ is primitive, so if α is a root of f then $\alpha = \gamma^{-1}$ where γ is a root of $f^*(x)$.

Alternatively, let α be a root of f. If $\alpha \neq 1, \alpha^3 \neq 1$, and $\alpha^5 \neq 1$, then $ord(\alpha) = 15$, but the first two are trivial, and for the third, compute

$$\alpha^4 = \alpha^3 + 1$$
$$\alpha^5 = \alpha^3 + \alpha + 1 \neq 1.$$

For future use also compute $\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1, \alpha^7 = \alpha^2 + \alpha + 1, \alpha^8 = \alpha^3 + \alpha^2 + \alpha, \alpha^9 = \alpha^2 + 1, \alpha^{10} = \alpha^3 + \alpha, \alpha^{11} = \alpha^3 + \alpha^2 + 1, \alpha^{12} = \alpha + 1, \alpha^{13} = \alpha^2 + \alpha, \alpha^{14} = \alpha^3 + \alpha^2, \alpha^{15} = 1.$

(2) Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ be the field of 4 elements. Is it a subfield of $\mathbb{F}_{16}$? Write out the addition table of $\mathbb{F}_4$.

It is a subfield because $2^2 - 1 | 2^4 - 1$. The nontrivial entries of the addition table are obtained from the relation $\omega + 1 = \omega^2$.

(3) Is $(1, \omega)$ a basis of $\mathbb{F}_{16}$ over $\mathbb{F}_4$?

No because $1 = \omega^2\omega$, so 1 and ω are proportional.

(4) Let $g(x) = x^2 + \omega x + 1$. Is it irreducible over $\mathbb{F}_4$?

$g(x)$ has no zeros in $\mathbb{F}_4$ so it does not have linear factors. Thus, it is irreducible.

(5) Let β be a root of $g(x)$. Find the order of β. Is it primitive?

Compute $\beta^3 = \omega\beta^2 + \beta = \omega\beta + \omega, \beta^4 = \omega\beta^2 + \omega\beta = \beta + \omega, \beta^5 = \beta^2 + \omega\beta = 1$. Thus $ord(\beta) = 5$, so it is not primitive.

(6) Express β as a power of α.

β is an element of order 5, so we should look among $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$. We claim that $\beta = \alpha^3$ because

$$g(\alpha^3) = \alpha^6 + \omega\alpha^3 + 1 = \alpha^6 + \alpha^8 + 1 = 0.$$

(7) Find the representation of α^7 in the basis $(1, \beta)$ over $\mathbb{F}_4$.

Since $\omega = \alpha^5 = \beta + \alpha + 1$, we obtain $\alpha = \omega + \beta + 1 = \omega^2 + \beta$. Next,

$$\alpha^7 = \alpha^6\alpha = \beta^2\alpha = (\omega\beta + 1)(\omega^2 + \beta) = \omega^2\beta + 1.$$

Thus, the coordinates of α^7 are $1, \omega^2$.

Problem 3. (8 pts each, 2 each subproblem) The polynomial $x^{15} + 1$ factors over F_2 as follows:

$$x^{15} + 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$$

Let $\mathcal{C}$ be a $[15, k, d]$ binary cyclic code $\mathcal{C}$ of length 15 generated by $g = (x + 1)(x^4 + x^3 + 1)$.

(1) What are k and d_{BCH}?

$\dim(\mathcal{C}) = n - \deg g = 10$.

The problem does not state what was the polynomial used to generate $\mathbb{F}_{16}$. Because of uniqueness of $\mathbb{F}_{16}$ is does not matter for the solution, but for definiteness let us assume that the primitive polynomial was $x^4 + x + 1$ and denote its root by α.

Then $g(x) = m_0m_7$, so the zeros of $\mathcal{C}$ are $(0, 7, 11, 13, 14) = (0, -8, -4, -2, -1)$. Among the exponents of the zeros of $\mathcal{C}$ we find $-2, -1, 0$, so $d_{BCH} = 4$.

We could have also taken $x^4 + x^3 + 1$ as the polynomial used to construct the field. Denoting its root by $\beta = \alpha^{-1}$ we would have found the zeros $(0, 1, 2, 4, 8)$, reciprocal to the ones found above.

(2) Is $c(x) = x^{10} + x^9 + x^7 + x^3$ a codeword in $\mathcal{C}$? Is $f(x) = c(x) + 1$?

$c(1) = 0$ and $c(\alpha^7) = \alpha^{10} + \alpha^3 + \alpha^4 + \alpha^6 = \alpha^6(\alpha^4 + 1) + \alpha^4 + \alpha^3 = \alpha^7 + \alpha^4 + \alpha^3 = \alpha^3(\alpha + 1) + \alpha^4 + \alpha^3 = 0$ using $\alpha^4 = \alpha + 1$, so $c \in \mathcal{C}$. The vector f is of odd weight, so $f(1) \neq 0$, $f \notin \mathcal{C}$.

(3) What is the generator polynomial of $\mathcal{C}^\perp$?

We have $g_{\mathcal{C}^\perp}(x) = h^*(x)$, where $h(x) = m_1m_3m_5 = (x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$. Explicitly,

$$g_{\mathcal{C}^\perp}(x) = m_{-1}m_{-3}m_{-5} = m_3m_5m_7 = x^{10} + x^9 + x^8 + x^6 + +x^5 + x^2 + x + 1.$$

(4) What is $d_{BCH}(\mathcal{C}^\perp)$?

The zeros of $\mathcal{C}^\perp$ have the exponents $(-1, -2, -4, -8; -3, -6, -9, -12; -5, -10)$, so the BCH bound gives $d_{BCH}(\mathcal{C}^\perp) = 7$.