Math 641, Spring Semester 2001-02 NAME: **Solutions**
R.A. Brualdi

Exam 2: (100 points; 10 per question): Mon. April 19, 2002. Total Points:

Let $p(x)$ be an irreducible polynomial of degree k in $F_2[x]$, and let F_{2^k} be the field obtained by adjoining a root α of $p(x)$ to F_2. **Answer the following short questions:**

(a) How are the elements of F_{2^k} uniquely represented in terms of α?

$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{k-1}\alpha^{k-1}$ where the c_i are in F_2.

(b) Now assume that α is a *primitive element* of F_{2^k}. How can the nonzero elements of F_{2^k} be uniquely represented in terms of α?

$1, \alpha, \alpha^2, \ldots, \alpha^{2^k-2} \quad (\alpha^{2^k-1} = 1)$.

(c) Still assuming α is primitive, what are the elements of F_{2^k} which are conjugate to α? In terms of α, what is $p(x)$?

The following elements are conjugate to α: $\alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{k-1}}$. We have

$$p(x) = \prod_{i=0}^{2^{k-1}} (x - \alpha^i).$$

(d)* Suppose $p(x)$ is *self-reciprocal* (equal to its reciprocal polynomial). Show that α is NOT primitive.

Suppose $p(x)$ is primitive and let α be a primitive root of $p(x)$. Then the roots of $p(x)$ are α^i where $i \in C_1 = \{1, 2, 2^2, \ldots, 2^{k-1}\}$ with 2^k equal to 1 mod $2^k - 1$. If $p(x)$ equals its reciprocal polynomial, then α^{-1} is a root of $p(x)$ (since it is of the reciprocal); this implies that 2^i equals -1 mod $2^k - 1$ for some $i \in C_1$, that is, $2^i = q(2^k - 1) - 1$ mod $2^k - 1$ for some $i \in C_1$. This is clearly impossible.

(e) Suppose that $p(x) = x^4 + x + 1$. What are the (binary) columns of the parity check matrix for the Hamming (15,11,3)-code that correspond to α, α^2, α^4, and α^8?

Using $p(\alpha) = \alpha^4 + \alpha + 1 = 0$, we get

$\alpha = 0 \cdot \alpha^3 + 0 \cdot \alpha^2 + +1 \cdot \alpha + 0 \cdot 1$

$\alpha^2 = 0 \cdot \alpha^3 + 1 \cdot \alpha^2 + +0 \cdot \alpha + 0 \cdot 1$

$\alpha^4 = 0 \cdot \alpha^3 + 0 \cdot \alpha^2 + +1 \cdot \alpha + 1 \cdot 1$

$\alpha^8 = 0 \cdot \alpha^3 + 1 \cdot \alpha^2 + +0 \cdot \alpha + 1 \cdot 1$

The coefficients above give the columns.

(f) Compute the generator polynomial of the even weight subcode of the (15,11,3) Hamming code. What is its dimension? Its minimum distance?

$g(x) = (x-1)p(x) = x^5 + x^4 + x^2 + 1$

(g) What is the encoding of the information word 1000000001 if the even weight subcode of the (15,11,3) Hammimg code is used?

$c(x) = (x^9 + 1)g(x) = x^{14} + x^{13} + x^{11} + x^9 + x^5 + x^4 + x^2 + 1$, so 110101000110101

(h) Compute the column corresponding to α^2 of the full **binary** parity check matrix (i.e. $V_{4,2}$ as a binary matrix) of BCH(4,2).

$[\alpha^2, \alpha^4, \alpha^6, \alpha^8]^T$: We have computed $\alpha^2, \alpha^4, \alpha^8$ above. But $\alpha^6 = \alpha^4 \cdot \alpha^2 = (\alpha+1)\alpha^2 = \alpha^3 + \alpha^2$. So

$$[0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1]^T.$$

(i) The binary Golay code is a *cyclic code*. Describe how it is constructed as a cyclic code.

Consider the polynomial $x^{23} - 1$ in $F_2[x]$. Calculating the cyclotomic coset mod 23 containing 1, we get:

$C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$ with 11 elements. So the multiplicative order of 2 mod 23 is 11, and the 23rd roots of 1 lie in $F_{2^{11}}$ but in no smaller field. The only other cyclotomic coset is C_5, also with 11 elements. Thus in $F_2[x]$, the factorization of $x^{23} - 1$ into irreducibles is

$$x^{23} - 1 = (x-1)m_1(x)m_5(x)$$

where $m_1(x)$ and $m_5(x)$ are irreducible polynomials of degree 11. The cyclic code of lenth 23 with generator polynomial $m_1(x)$ has dimension 12 and minimum distance at least 5 (4 "consecutive roots"). It actually has minimum distance 7 and is the (23,12,7)-binary Golay code.

(j) For BCH(k,t), what is the fundamental equation? What is its significance for BCH(k,t)? Describe how the Euclidean algorithm determines the fundamental equation.

Fundamental equation is $w(z) = u(z)z^{2t} + s(z)l(z)$ where $s(z)$ is the syndrome polynomial, $w(z)$ is the error evaluator polynomial, and $l(z)$ is the error locator polynomial (reciprocal of its roots are error locations). Thus $l(z)$ locates errors when t or fewer are made in using BCH(k, t). By applying the EA to z^{2t} and the syndrome polynomial $s(z)$ until the first remainder $r_j(z)$ with degree less than t, we are able to express $r_j(z)$ as

$$r_j(z) = u_j(z)z^{2t} + v_j(z)s(z).$$

Here $r_j(z), u_j(z), v_j(z)$ are all the same constant multiple of the error evaluator, co-evaluator, and locator polynomials. So we can find the roots of $v_j(z)$ to determine error locations.