MATH 4383-001/5383-001
Exam II
April 23, 2010

INSTRUCTIONS

Show your work on all problems.

ANSWERS

Throughout, F denotes the finite field $\mathbb{Z}_2[x]/f$ where $f = x^4 + x + 1$ and α denotes the element $x^3 + 1$ of F

F as powers of α

$$\alpha = x^3+1; \alpha^2 = x^3+x^2+1; \alpha^3 = x^3+x^2+x+1; \alpha^4 = x^3+x^2+x; \alpha^5 = x^2+x+1$$

$$\alpha^6 = x^3 + x; \alpha^7 = x^2 + 1; \alpha^8 = x^3 + x + 1; \alpha^9 = x^3 + x^2; \alpha^{10} = x^2 + x$$

$$\alpha^{11} = x + 1; \alpha^{12} = x^3; \alpha^{13} = x^2; \alpha^{14} = x; \alpha^{15} = 1$$

1. Let $a, b \in \mathbb{Z}_2[x]$ be $a = x^5 + x^2 + x$ and let $b = x^2 + x + 1$. Use the Euclidean algorithm to find the highest common factor r of a and b and express it in the form $r = ua + vb$ for some $u, v \in \mathbb{Z}_2[x]$. noindent ANSWER

k	Q	R	U	V
-1		$x^5 + x^2 + x$	1	0
0		$x^2 + x + 1$	0	1
1	$x^3 + x^2$	x	1	$x^3 + x^2$
2	$x + 1$	1	$x + 1$	$x^4 + x^2 + 1$

Then $r_3 = 0$ so $r_2 = 1$ is the HCF r of a and b, and

$$1 = (x + 1)(x^5 + x^2 + x) + (x^4 + x^2 + 1)(x^2 + x + 1)$$

2. Let $\beta = x^2 + x + 1 \in F$. Determine ord($\beta$).

ANSWER From the F table, $\beta = \alpha^5$. Then $\beta^2 = (\alpha^5)^2 = \alpha^10 = x^2 + x$ and $\beta^3 = (\alpha^5)^3 = \alpha^{15} = 1$ so ord(β) $= 3$

The next questions refer to the BCH code BCH$(4, 2)$ using the field F and the element α.

3. Find the generating polynomial g of BCH$(4, 2)$.

ANSWER g is the product of the distinct polynomials among m_{α^i} for $1 \leq i \leq 4$. Since $m_\alpha = m_{\alpha^2} = m_{\alpha^4}$, all we need to look at is m_α and m_{α^3}.

From the table, $\alpha^4 + \alpha^3 + 1 = x^3 + x^2 + x + x^3 + x^2 + x + 1 + 1 = 0$, so α is a root of $X^4 + X^3 + 1$. This is irreducible, so $m_\alpha = X^4 + X^3 + 1$. From the table, $(\alpha^3)^4 + (\alpha^3)^3 + (\alpha^3)^2 + (\alpha^3) + 1 = x^3 + x^3 + x^2 + x^3 + x + x^3 + x^2 + x + 1 = 0$, so α^3 is a root of $X^4 + X^3 + X^2 + X + 1$. This is irreducible, so $m_{\alpha^3} = X^4 + X^3 + X^2 + X + 1$. Both irreducibles are distinct, so

$$g(X) = (X^4 + X^3 + 1)(X^4 + X^3 + X^2 + X + 1)$$

4. How many codewords are there in BCH$(4, 2)$?

ANSWER BCH$(4, 2)$ has block size $2^4 - 1 = 15$ and consists of polynomials of degree at most $15 - 1 = 14$ which are multiples of g. Since g has degree 8, this means that BCH$(4, 2)$ consists of the multiples of g by all polynomials of degree 6 or less. There are $2^7 = 128$ binary polynomials of degree 6 or less, so BCH$(4, 2)$ has 128 elements.