MAT 3343, APPLIED ALGEBRA, FALL 2003

Answers to Problem Set 6

Peter Selinger

Problem 1. Let $p(x) = x^3 + x + 1$ be the generator polynomial.

(a) The sixteen codewords are shown here with their corresponding plaintext words:

0000000	0000	0100111	0100	1000101	1000	1100010	1100
0001011	0001	0101100	0101	1001110	1001	1101001	1101
0010110	0010	0110001	0110	1010011	1010	1110100	1110
0011101	0011	0111010	0111	1011000	1011	1111111	1111

(b) 0011101 1011000 1110100

(c) The Hamming distance is 3; thus this code detects 2 errors and corrects 1.

(d) The syndrome is the remainder of the division by $p(x)$. We have

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

so therefore:

codeword	syndrome
0110110	111
1110000	100
0110100	101

We can decode using the "nearest neighbor" method. We find 0010110 1110100 1110100 for the corrected codewords, and 0010 1110 1110 for the decoded message. Alternatively, we can do part (f) first and use the parity check matrix to find the error positions corresponding to each syndrome.

(e) The rows of the generator matrix are the codewords for 1000, 0100, 0010, 0001:

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

(f) The columns of the parity check matrix form a basis for the null space of G.

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

Problem 2. A primitive element is an element of order 15. From Handout 5, we already know that α is a primitive element. More generally, if $\beta = \alpha^k$, then we have $\beta^m = 1$ iff $\alpha^{km} = 1$ iff $15|km$. So the order of β is the smallest m such that $15|km$. We can use this to calculate the order of each element:

Element	Order
α^0	1
α	15
α^2	15
α^3	5
α^4	15
α^5	3
α^6	5
α^7	15

Element	Order
α^8	15
α^9	5
α^{10}	3
α^{11}	15
α^{12}	5
α^{13}	15
α^{14}	15

So the primitive elements are: α, α^2, α^4, α^7, α^8, α^{11}, α^{13}, α^{14}. Indeed, these are precisely the element α^m such that $\gcd(m, 15) = 1$.

Problem 3. For calculations in $GF(32)$, we refer to the representation shown in Table 1 (on page 4).

(a) We first calculate $p_3(x)$.

Method 1: We are looking for an irreducible polynomial $p(x)$ such that $p(\alpha^3) = 0$. Letting $x = \alpha^3$, we first calculate x^n for various n:

$$\begin{aligned} x^0 &= \alpha^0 = 1 && (00001) \\ x^1 &= \alpha^3 && (01000) \\ x^2 &= \alpha^6 = \alpha^3 + \alpha && (01010) \\ x^3 &= \alpha^9 = \alpha^4 + \alpha^3 + \alpha && (11010) \\ x^4 &= \alpha^{12} = \alpha^3 + \alpha^2 + \alpha && (01110) \\ x^5 &= \alpha^{15} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 && (11111) \end{aligned}$$

These six expressions correspond to six vectors in a 5-dimensional vector space (shown in vector notation in the right column). Thus, they must be linearly dependent. Using linear algebra, we find the linear dependency: $x^5+x^4+x^3+x^2+x^0 = 0$. Thus the polynomial $p(x) = x^5+x^4+x^3+x^2+1$ has α^3 as a root. Since $x^0, \ldots, x^4$ are linearly independent, no smaller-degree polynomial has α^3 as a root, and thus $p(x)$ is irreducible.

Method 2: There is a second, more complicated method for calculating $p_3(x)$. It is not very practical, but interesting. Since α^3 is a root of $p_3(x)$, and using the fact that $p_3(x^2) = p_3(x)^2$, it follows that α^6, α^{12}, α^{24}, $\alpha^{48} = \alpha^{17}$, and $\alpha^{34} = \alpha^3$ are also roots of $p_3(x)$. Moreover, since $p_3(x)$ is a polynomial of degree at most 5 (as we know from method 1!), these are the only roots of $p_3(x)$, and we calculate:

$$\begin{aligned}
p_3(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^{24})(x-\alpha^{17}) \\
&= (x^2+\alpha x+\alpha^9)(x^2+\alpha^4 x+\alpha^5)(x-\alpha^{17}) \\
&= (x^2+\alpha x+\alpha^9)(x^3+\alpha^{18}x^2+\alpha^{14}x+\alpha^{22}) \\
&= x^5+(\alpha^{18}+\alpha)x^4+(\alpha^{14}+\alpha^{19}+\alpha^9)x^3 \\
&\quad +(\alpha^{22}+\alpha^{15}+\alpha^{27})x^2+(\alpha^{23}+\alpha^{23})x+(\alpha^{31}) \\
&= x^5+x^4+x^3+x^2+1
\end{aligned}$$

(b) Next, we calculate $p_5(x)$. We only use Method 1. Let $x = a^5$, then

$$\begin{array}{ll}
x^0 = \alpha^0 = 1 & (00001) \\
x^1 = \alpha^5 = \alpha^2+1 & (00101) \\
x^2 = \alpha^{10} = \alpha^4+1 & (10001) \\
x^3 = \alpha^{15} = \alpha^4+\alpha^3+\alpha^2+\alpha+1 & (11111) \\
x^4 = \alpha^{20} = \alpha^3+\alpha^2 & (01100) \\
x^5 = \alpha^{25} = \alpha^4+\alpha^3+1 & (11001)
\end{array}$$

We find the linear dependency: $x^5+x^4+x^2+x+1 = 0$. So $p_5(x) = x^5+x^4+x^2+x+1$.

Problem 4. For calculations in $GF(16)$ relative to β where $\beta^4 = 1+\beta^3$, we refer to the representation shown in Table 2 (on page 4).

We need to calculate $p_1(x)$, $p_3(x)$ and $p_5(x)$, where $p_n(x)$ is the irreducible polynomial with root β^n. We already know that $p_1(x) = x^4+x^3+1$. To calculate

$\alpha^0 = 1$	00001	$\alpha^{16} = \alpha^4+\alpha^3+\alpha+1$	11011
$\alpha^1 = \alpha$	00010	$\alpha^{17} = \alpha^4+\alpha+1$	10011
$\alpha^2 = \alpha^2$	00100	$\alpha^{18} = \alpha+1$	00011
$\alpha^3 = \alpha^3$	01000	$\alpha^{19} = \alpha^2+\alpha$	00110
$\alpha^4 = \alpha^4$	10000	$\alpha^{20} = \alpha^3+\alpha^2$	01100
$\alpha^5 = \alpha^2+1$	00101	$\alpha^{21} = \alpha^4+\alpha^3$	11000
$\alpha^6 = \alpha^3+\alpha$	01010	$\alpha^{22} = \alpha^4+\alpha^2+1$	10101
$\alpha^7 = \alpha^4+\alpha^2$	10100	$\alpha^{23} = \alpha^3+\alpha^2+\alpha+1$	01111
$\alpha^8 = \alpha^3+\alpha^2+1$	01101	$\alpha^{24} = \alpha^4+\alpha^3+\alpha^2+\alpha$	11110
$\alpha^9 = \alpha^4+\alpha^3+\alpha$	11010	$\alpha^{25} = \alpha^4+\alpha^3+1$	11001
$\alpha^{10} = \alpha^4+1$	10001	$\alpha^{26} = \alpha^4+\alpha^2+\alpha+1$	10111
$\alpha^{11} = \alpha^2+\alpha+1$	00111	$\alpha^{27} = \alpha^3+\alpha+1$	01011
$\alpha^{12} = \alpha^3+\alpha^2+\alpha$	01110	$\alpha^{28} = \alpha^4+\alpha^2+\alpha$	10110
$\alpha^{13} = \alpha^4+\alpha^3+\alpha^2$	11100	$\alpha^{29} = \alpha^3+1$	01001
$\alpha^{14} = \alpha^4+\alpha^3+\alpha^2+1$	11101	$\alpha^{30} = \alpha^4+\alpha$	10010
$\alpha^{15} = \alpha^4+\alpha^3+\alpha^2+\alpha+1$	11111	$\alpha^{31} = 1$	00001

Table 1: Representation of $GF(32)$ with $\alpha^5 = \alpha^2+1$

$\beta^0 = 1$	0001	$\beta^8 = \beta^3+\beta^2+\beta$	1110
$\beta^1 = \beta$	0010	$\beta^9 = \beta^2+1$	0101
$\beta^2 = \beta^2$	0100	$\beta^{10} = \beta^3+\beta$	1010
$\beta^3 = \beta^3$	1000	$\beta^{11} = \beta^3+\beta^2+1$	1101
$\beta^4 = \beta^3+1$	1001	$\beta^{12} = \beta+1$	0011
$\beta^5 = \beta^3+\beta+1$	1011	$\beta^{13} = \beta^2+\beta$	0110
$\beta^6 = \beta^3+\beta^2+\beta+1$	1111	$\beta^{14} = \beta^3+\beta^2$	1100
$\beta^7 = \beta^2+\beta+1$	0111	$\beta^{15} = 1$	0001

Table 2: Representation of $GF(16)$ with $\beta^4 = \beta^3+1$

$p_3(x)$, let $x = \beta^3$. We have

$$\begin{array}{ll} x^0 = \beta^0 = 1 & (0001) \\ x^1 = \beta^3 = \beta^3 & (1000) \\ x^2 = \beta^6 = \beta^3 + \beta^2 + \beta + 1 & (1111) \\ x^3 = \beta^9 = \beta^2 + 1 & (0101) \\ x^4 = \beta^{12} = \beta + 1 & (0011) \end{array}$$

so we get the linear dependency $x^4 + x^3 + x^2 + x + 1 = 0$, so $p_3(x) = x^4 + x^3 + x^2 + x + 1$. To calculate $p_5(x)$, let $x = \beta^5$. We have

$$\begin{array}{ll} x^0 = \beta^0 = 1 & (0001) \\ x^1 = \beta^5 = \beta^3 + \beta + 1 & (1011) \\ x^2 = \beta^{10} = \beta^3 + \beta & (1010) \end{array}$$

We get the linear dependency $x^2 + x + 1 = 0$, so $p_5(x) = x^2 + x + 1$.

It follows that the generator polynomial for the 2-error correcting code is

$$\begin{array}{rcl} \operatorname{lcm}(p_1(x), p_3(x)) & = & (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1) \\ & = & x^8 + x^4 + x^2 + x + 1 \end{array}$$

This code is therefore a $(15, 7)$-code.

The generator polynomial for the 3-error correcting code is

$$\begin{array}{rcl} \operatorname{lcm}(p_1(x), p_3(x), p_5(x)) & = & (x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) \\ & = & (x^8 + x^4 + x^2 + x + 1)(x^2 + x + 1) \\ & = & x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1 \end{array}$$

This code is therefore a $(15, 5)$-code.

Problem 5. We use the representation of $GF(32)$ from Table 1. This problem is easy because we already found $p_3(x) = x^5 + x^4 + x^3 + x^2 + 1$ in Problem 3. We have $p_1(x) = x^5 + x^2 + 1$. Thus, the generator polynomial for the 2-error correcting BCH code is:

$$\begin{array}{rcl} \operatorname{lcm}(p_1(x), p_3(x)) & = & (x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x^2 + 1) \\ & = & x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1 \end{array}$$

The resulting code is a $(31, 21)$-code.