Solutions for Homework 2

1. (*Weights of codewords in a cyclic code*)

   Let $g(X)$ be the generator polynomial of a binary cyclic code of length n.

   (a) Show that if $g(X)$ has $X+1$ as a factor then the code contains no codewords of odd weight.

   Solution :

   $v(X) \in GF(2)[X]$ is a code polynomial iff it is of degree at most $n-1$ and can be written as $v(X) = u(X)g(X)$ for some polynomial $u(X) \in GF(2)[X]$. Since $X+1$ divides $g(X)$, it follows that $X+1$ divides $v(X)$. Hence $v(1) = 0$. This means precisely that the weight of the corresponding codeword $(v_0, \ldots, v_{n-1})$ is even.

   (b) Show that if n is odd and $X+1$ is not a factor of $g(X)$ then the code contains the codeword consisting of all 1's.

   Solution :

   The claim of this part of the problem is true whether n is odd or even.

   $$X^n + 1 = (X+1)(1 + X + X^2 + \ldots + X^{n-1}) \ .$$

   Since $g(X)$ divides $X^n + 1$ and does not have $X+1$ as a factor, it must divide $1 + X + X^2 + \ldots + X^{n-1}$. In other words, the length n word consisting of all 1's is a codeword.

   (c) Show that if n is the smallest integer such that $g(X)$ divides $X^n + 1$ then the code has minimum weight at least 3.

   Solution :

   If there is a codeword of weight 1, the associated code polynomial is X^m, for some $0 \le m \le n-1$. Since the code is cyclic, it follows that 1 is also a code polynomial. But then the code is trivial (every word is a codeword), and $g(X) = 1$, contradicting the hypothesis.

   If there is a codeword of weight 2, the associated code polynomial is $X^m + X^l$ for some $0 \le m < l \le n-1$. Since the code is cyclic, it follows that $1 + X^{l-m}$ is also a code polynomial. Hence $g(X)$ divides $1 + X^{l-m}$, which contradicts the hypothesis. since $l - m < n$.

   Thus under the hypothesis the smallest weight of a nonzero codeword must be at least 3.

   (d) Suppose $g(X)$ is such that the code contains both even-weight and odd-weight codewords. Let $A(z)$ denote the weight enumerator polynomial of the code. Show that the polynomial $(X+1)g(X)$ also generates a binary cyclic code of length n, and that this has weight enumerator polynomial

   $$A_1(z) = \frac{1}{2}\left[A(z) + A(-z)\right] \ .$$

Solution :

Let $\mathcal{C}$ denote the binary cyclic code (n, k) with generator polynomial $g(X)$. We know that $g(X)$ divides $X^n + 1$. Since $\mathcal{C}$ contains both even and odd weight codewords, $X + 1$ does not divide $g(X)$. Thus $(X + 1)g(X)$ divides $X^n + 1$. Hence it is the generator polynomial of a binary cyclic $(n, k - 1)$ code. Let $\mathcal{C}_1$ denote this code.

We claim that $\mathcal{C}_1$ is comprised of the even weight codewords of $\mathcal{C}$.

Consider a codeword of $\mathcal{C}$. The corresponding code polynomial can be uniquely written in the form $a(X)g(X)$, where $a(X) \in GF(2)[X]$ is of degree at most $k - 1$. The codeword has even weight iff its code polynomial is divisible by $X + 1$. Since $X + 1$ does not divide $g(X)$, it follows that the codeword has even weight iff $X + 1$ divides $a(X)$, i.e. $a(X) = b(X)(X + 1)$ for some $b(X) \in GF(2)[X]$. But this means the code polynomial has the form $b(X)((X+1)g(X))$, so the corresponding codeword is in $\mathcal{C}_1$.

For the converse, consider a codeword in $\mathcal{C}_1$. Its code polynomial is of the form $b(X)(X + 1)g(X)$ for a unique $b(X) \in GF(2)[X]$ of degree at most $k - 2$. Writing this as $(b(X)(X + 1))g(X)$ we see that the codeword is in $\mathcal{C}$ and has even weight.

It now follows that

$$A_1(z) = \frac{1}{2}\left[A(z) + A(-z)\right] \ ,$$

where $A_1(z)$ denotes the weight enumerator polynomial of $\mathcal{C}_1$ and $A(z)$ denotes the weight enumerator polynomial of $\mathcal{C}$. Indeed, the polynomial on the right hand side of the equation above just enumerates the even weight codewords in $\mathcal{C}$.

2. (*Cyclic codes*)

(a) i. Show that $g(X) = 1 + X^2 + X^4 + X^6 + X^7 + X^{10}$ generates a (21,11) cyclic code.
Solution :
We need to show that $g(X)$ divides $X^{21} + 1$. Note that

$$g(X) = (X + 1)(X^3 + X^2 + 1)(X^6 + X^4 + X^2 + X + 1) \ .$$

As can be seen from any table enumerating the minimal polynomials of the elements of $GF(2^m)$ for small values of m, each of the factors is the minimal polynomial of some elements in $GF(64)$. It follows that $g(X)$ divides $X^{63} + 1$. Let α denote a primitive element in $GF(64)$. The tables also show that $X^3 + X^2 + 1$ is the minimal polynomial of the conjugates $\{\alpha^{27}, \alpha^{54}, \alpha^{45}\}$ in $GF(64)$ and $X^6 + X^4 + X^2 + X + 1$ is the minimal polynomial of the conjugates $\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}\}$ in $GF(64)$. Each of the roots of these polynomials satisfies the equation $X^{21} + 1 = 0$. It follows that $g(X)$ divides $X^{21} + 1$.

ii. Let $r(X) = 1 + X^5 + X^{17}$ be a received polynomial. Compute the syndrome of $r(X)$.
Solution :
The syndrome polynomial $s(X)$ when the received polynomial is $r(X)$ is the remainder of $r(X)$ when divided by the generator polynomial $g(X)$. Direct

computation gives :

$$s(X) = X^8 + X^6 + X^4 + X^3 + 1 \ .$$

(b) Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two cyclic codes of length n generated by $g_1(x)$ and $g_2(x)$ respectively. What is the generator polynomial for the smallest cyclic code that contains the set $\mathcal{C}_1 \cup \mathcal{C}_2$?

Solution :

Let $g(x) = gcd(g_1(x)g_2(x))$. The cyclic code $\mathcal{C}$ generated by $g(x)$ contains $\mathcal{C}_1 \cup \mathcal{C}_2$. Also, there are polynomials $a(x)$ and $b(x)$ (with coefficients from the field in which the symbols lie) such that

$$a(x)g_1(x) + b(x)g_2(x) = g(x) \ ,$$

as can be seen by applying Euclid's algorithm. This equation then also holds modulo x^n+1. Since $a(x)g_1(x)mod(x^n+1)$ is a code polynomial for $\mathcal{C}_1$ and $b(x)g_2(x)mod(x^n+1)$ is a code polynomial for $\mathcal{C}_2$, and since any code containing $\mathcal{C}_1 \cup \mathcal{C}_2$ is closed under sums, it follows that $g(x)$ is a code polynomial in any code that contains $\mathcal{C}_1 \cup \mathcal{C}_2$. It then follows that any cyclic code containing $\mathcal{C}_1 \cup \mathcal{C}_2$ must contain $\mathcal{C}$. Thus $g(x)$ is the generator polynomial of the smallest cyclic code containing $\mathcal{C}_1 \cup \mathcal{C}_2$.

(c) Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two cyclic codes of length n generated by $g_1(x)$ and $g_2(x)$ respectively. Show that the code polynomials common to both $\mathcal{C}_1$ and $\mathcal{C}_2$ also form a cyclic code $\mathcal{C}_3$. Determine the generator polynomial of $\mathcal{C}_3$. If d_1 and d_2 are the minimum distances of $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively, what can you say about the minimum distance of $\mathcal{C}_3$?

Solution :

Since the intersection of any two binary linear codes is a binary linear code, we know that $\mathcal{C}_3$ is a binary linear code. Let $v(X)$ be the polynomial associated to a binary string that is in $\mathcal{C}_1 \cap \mathcal{C}_2$. Then $v(X)$ is divisible by both $g_1(X)$ and $g_2(X)$. It follows that it is divisible by

$$g_3(X) = \text{l.c.m.}(g_1(X), g_2(X)) \ ,$$

where "l.c.m." stands for "least common multiple". Conversely, if the polynomial associated to a binary string is divisible by $g_3(X)$ it follows that it is divisible by both $g_1(X)$ and $g_2(X)$ and so the corresponding binary string is in $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathcal{C}_3$. It follows that $\mathcal{C}_3$ is a cyclic code, with generator polynomial $g_3(X)$.

$\mathcal{C}_3$ may be the trivial code comprised of the zero codeword. If it has at least one nonzero codeword, its minimum distance can be no smaller than the maximum of the minimum distances of $\mathcal{C}_1$ and $\mathcal{C}_2$, because every nonzero codeword in $\mathcal{C}_3$ lies in both $\mathcal{C}_1$ and $\mathcal{C}_2$.

3. (*Polynomials*)

(a) Show that $X^5 + X^3 + 1$ is irreducible over GF(2).

Solution :

Neither 0 nor 1 is a root of the polynomial X^5+X^3+1, so it has no factors of degree 1 in $GF(2)[X]$. Also, for the same reason, if it had a factor of degree 2 in $GF(2)[X]$ this factor would have to be irreducible. The only irreducible polynomial of degree 2 in $GF(2)[X]$ is X^2+X+1. If this were a factor of X^5+X^3+1 in $GF(2)[X]$, it would also be a factor of X^5+X^3+1 in $GF(4)[X]$, which would mean that α, any primitive element of $GF(4)[X]$ with minimal polynomial X^2+X+1, would be a root of X^5+X^3+1 in $GF(4)[X]$. However, $\alpha^5+\alpha^3+1=\alpha^2\neq 0$ in $GF(4)$. Thus X^5+X^3+1 does not have any factors of degree 2 in $GF(2)[X]$. It now follows that this polynomial is irreducible in $GF(2)[X]$, since if it were reducible it would have to have a factor of degree 1 or a factor of degree 2.

(b) Let $f(X)$ be a polynomial of degree n over GF(2) with nonzero constant term. Let $f^*(X)$ denote its reciprocal polynomial, i.e.

$$f^*(X)=X^n f(X^{-1})\ .$$

i. Prove that $f(X)$ is irreducible over GF(2) if and only if $f^*(X)$ is irreducible over GF(2).
Solution :
Since the reciprocal of $f^*(X)$ is $f(X)$ it is enough to show that if $f(X)$ is reducible over GF(2) then $f^*(X)$ is reducible over GF(2).

Suppose we had a nontrivial factorization $f(X)=a(X)b(X)$, with $deg(a(X))=k$, where $1\leq k\leq n-1$. Note that both $a(X)$ and $b(X)$ have nonzero constant term. The reciprocal polynomials of $a(X)$ and $b(X)$ are $a^*(X)=X^k a(X^{-1})$ and $b^*(X)=X^{n-k}b(X^{-1})$ respectively, and we have $f^*(X)=a^*(X)b^*(X)$, so $f^*(X)$ is also reducible over GF(2).

ii. Prove that $f(X)$ is primitive over GF(2) if and only if $f^*(X)$ is primitive over GF(2).
Solution :
Since the reciprocal of $f^*(X)$ is $f(X)$ it is enough to show that if $f(X)$ is not primitive over GF(2) then $f^*(X)$ is not primitive over GF(2).

Suppose $f(X)$ is not primitive over GF(2). Then $f(X)$ divides X^t+1 for some $t<2^n-1$, which then means $X^t+1=g(X)f(X)$ for some $g(X)$ with nonzero constant term. The polynomial X^t+1 is its own reciprocal and the reciprocal polynomial of $g(X)$ is $g^*(X)=X^{t-n}g(X^{-}1)$. We then have $X^t+1=g^*(X)f^*(X)$, which means that $f^*(X)$ divides X^t+1, and since $t<2^n$ and $deg(f^*(X))=n$, it follows that $f^*(X)$ is not primitive.

4. (*Calculations in finite fields*)

Let α be a primitive element in GF(2^4) satisfying $\alpha=\alpha^4+1$. In the following problems you will find it useful to refer to Table 2.8 on pg. 47 of the text.

(a) Find the roots of $X^3+\alpha^6X^2+\alpha^9X+\alpha^9$ in GF(2^4).
Solution :
$X^3+\alpha^6X^2+\alpha^9X+\alpha^9=(X+\alpha)(X+\alpha^3)(X+\alpha^5)$.

(b) Solve the following system of equations in GF(2^4) :

$$\begin{aligned} X + \alpha^5 Y + Z &= \alpha^7 \\ X + \alpha Y + \alpha^7 Z &= \alpha^9 \\ \alpha^2 X + Y + \alpha^6 Z &= \alpha \end{aligned}$$

Solution :
$(X, Y, Z) = (\alpha^{12}, \alpha^{14}, \alpha^{10})$.

5. (*Determining all binary cyclic codes*)

Determine all the binary cyclic codes of length 21.

Hint : What is the factorization of $X^{21} + 1$ into irreducible factors over GF(2) ? The decomposition of the nonzero elements of GF(64) into cyclotomic cosets may be useful in answering this question.

Solution :

Consider the field $GF(64)$ generated by the primitive polynomial $X^6 + X + 1$. The polynomial $X^{63} + 1$ splits into factors of degree 1 over this field, and since

$$X^{63} + 1 = (X^{21} + 1)(X^{42} + X^{21} + 1) \ ,$$

the polynomial $X^{21} + 1$ splits into factors of degree 1 over this field. In fact, the roots of $X^{21} + 1$ are precisely :

$$1, \alpha^3, \alpha^6, \alpha^9, \alpha^{12}, \alpha^{15}, \alpha^{18}, \alpha^{21}, \alpha^{24}, \alpha^{27}, \alpha^{30}, \alpha^{33}, \alpha^{36}, \alpha^{39}, \alpha^{42}, \alpha^{45}, \alpha^{48}, \alpha^{51}, \alpha^{54}, \alpha^{57}, \alpha^{60} \ .$$

The minimal polynomials of these elements are :

$X^6 + X^4 + X^2 + X + 1$	whose roots are $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48},$ and α^{33}
$X^3 + X^2 + 1$	whose roots are $\alpha^9, \alpha^{18},$ and α^{36}
$X^6 + X^5 + X^4 + X^2 + 1$	whose roots are $\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51},$ and α^{39}
$X^2 + X + 1$	whose roots are α^{21} and α^{42}
$X^3 + X + 1$	whose roots are $\alpha^{27}, \alpha^{54},$ and α^{45} .

Thus, the factorization of $X^{21} + 1$ into irreducible factors in $GF(2)[X]$ is $X^{21} + 1 = (X+1)(X^6+X^4+X^2+X+1)(X^3+X^2+1)(X^6+X^5+X^4+X^2+1)(X^2+X+1)(X^3+X+1)$.

There are six distinct irreducible factors of $X^{21} + 1$, each with multiplicity 1. A binary cyclic code of length 21 is determined by its generator polynomial, which is a polynomial that divides $X^{21} + 1$. Thus there are $2^6 = 64$ binary cyclic codes of length 21, given respectively by the 2^6 distinct polynomials that divide $X^{21} + 1$ in $GF(2)[X]$.