SOLUTIONS/HINTS TO PROBLEM SET 8

Problem 1.
4.1.11:
(a) $q(x) = x^3$, $r(x) = x^4 + x^2$.
(b) $q(x) = x^5 + 1$, $r(x) = 0$.
(c) $q(x) = x^4 + x^2 + x + 1$, $r(x) = 0$.
(d) $q(x) = x^7 + x^6 + x^4 + 1$, $r(x) = 0$.

Problem 2.
4.1.19:
(a) $1 + x^4$.
(b) $1 + x^2$.
(c) $x + x^4$.

4.1.20: We must compute the remainder when $f(x)$ is divided by $h(x) = x^7+1$ (i.e., $f(x)$ mod $h(x)$), and the remainder when $p(x)$ is divided by $h(x)$ (i.e., $p(x)$ mod $h(x)$). Using the long division algorithm, we get:
(a) $f(x)$ mod $h(x) = x^3 + x + 1$ and $p(x)$ mod $h(x) = x^3 + x + 1$.
Hence, $f(x) \equiv h(x) \pmod{h(x)}$.
(b) $f(x)$ mod $h(x) = x^5 + x^2 + x$ and $p(x)$ mod $h(x) = x^5 + x$.
Hence, $f(x) \not\equiv h(x) \pmod{h(x)}$.
(c) $f(x)$ mod $h(x) = x + 1$ and $p(x)$ mod $h(x) = x + 1$.
Hence, $f(x) \equiv h(x) \pmod{h(x)}$.

4.1.21:
$(f(x) + g(x))$ mod $h(x)$ and $(f(x)g(x))$ mod $h(x)$
(a) $x^6,\ x^2 + x^6$.
(b) $x + x^5,\ x + x^3 + x^4 + x^5 + x^6$.
(c) $x + x^2 + x^4 + x^5,\ x + x^2 + x^4$.

Problem 3. If $v = (v_0, v_1, v_2, \ldots, v_{n-2}, v_{n-1})$ and $\pi(v) = (v_{n-1}, v_0, v_1, \ldots, v_{n-3}, v_{n-2})$ are the equal then

$$v_0 = v_{n-1}, v_1 = v_0, v_2 = v_1, \ldots, v_{n-2} = v_{n-3}, v_{n-1} = v_{n-2}.$$

This can only happen if v is either the all-zero or the all-one word.

Problem 4.
(a) From Corollary 4.2.18, the generator polynomial of the smallest cyclic code containing $x^5 + x^3 + x$ (the given word of length 6) is

$$g(x) = \gcd(x^5 + x^3 + x, x^6 + 1) = x^4 + x^2 + 1.$$

This can be computed in a similar way to computing the greatest common divisor between two integers (Euclidean algorithm).

(c) The generator polynomial of the smallest cyclic code containing the given word of length 8, namely, $x^6 + x^5 + x^2 + x$, is

$$g(x) = \gcd(x^6 + x^5 + x^2 + x, x^8 + 1) = x^5 + x^4 + x + 1.$$

Problem 5.

(c) The three words of length 4 in S are linearly independent. So the code C generated by them is a $(4,3)$-linear cyclic code. The generator polynomial has degree $t = n - k = 1$ and it is the unique polynomial of degree 1 in C. The third word in S corresponds to a polynomial of degree 1, namely, $x+1$. Hence, $g(x) = x+1$.

(e) The four words of length 5 in S are linearly independent. So the code C generated by them is a $(5,4)$-linear cyclic code. The generator polynomial has degree $t = n - k = 1$ and it is the unique polynomial of degree 1 in C. The first word in S corresponds to a polynomial of degree 1, namely, $x+1$. Hence, $g(x) = x+1$.

Problem 6.

4.3.4:

(a) The codeword corresponding to the message $1 + x^3$ is
$$v(x) = g(x) \cdot (1 + x^3) = 1 + x^2 + x^5 + x^6.$$
The codeword corresponding to the message x is
$$v(x) = g(x) \cdot x = x + x^3 + x^4.$$
The codeword corresponding to the message $x + x^2 + x^3$ is
$$v(x) = g(x) \cdot (x + x^2 + x^3) = x + x^2 + x^6.$$

(b) The message polynomial corresponding to $c(x) = x^2 + x^4 + x^5$ is
$$c(x)/g(x) = x^2.$$
The message polynomial corresponding to $c(x) = 1 + x + x^2 + x^4$ is
$$c(x)/g(x) = 1 + x.$$
The message polynomial corresponding to $c(x) = x^2 + x^3 + x^4 + x^6$ is
$$c(x)/g(x) = x^2 + x^3.$$

Problem 7.

4.3.9: H is produced as follows. First compute $x^i \bmod g(x)$, for $i = 0, \ldots, n-1$. Each result corresponds to a row of H.

(c)
$$\begin{aligned} 1 \bmod g(x) &= 1 \\ x \bmod g(x) &= x \\ x^2 \bmod g(x) &= 1 \\ x^3 \bmod g(x) &= x \\ x^4 \bmod g(x) &= 1 \\ x^5 \bmod g(x) &= x \\ x^6 \bmod g(x) &= 1 \\ x^7 \bmod g(x) &= x \end{aligned}$$

Thus,
$$H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(d) As in the previous part, first compute $x^i \bmod g(x)$, for $i = 0, \ldots, 8$. In this case, $g(x) = 1 + x^3 + x^6$. Each result corresponds to a row of H.

$$\begin{aligned}
&1 \bmod g(x) = 1 \\
&x \bmod g(x) = x \\
&x^2 \bmod g(x) = x^2 \\
&x^3 \bmod g(x) = x^3 \\
&x^4 \bmod g(x) = x^4 \\
&x^5 \bmod g(x) = x^5 \\
&x^6 \bmod g(x) = 1 + x^3 \\
&x^7 \bmod g(x) = x + x^4 \\
&x^8 \bmod g(x) = x^2 + x^5
\end{aligned}$$

Thus,

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

Problem 8.

4.4.6:

(a) Notice that $x^4 + 1 = (x+1)^4$. With the notation of Corollary 4.4.4, $n = 2^2$. Thus the number of proper cyclic codes of length 4 is equal to $(2^2+1)^1 - 2 = 3$.

(b) The factorization of $x^5 + 1$ into irreducible factors is:
$$x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1).$$
Again, by Corollary 4.4.4, the number of proper cyclic codes of length 5 is equal to $(2^0+1)^2 - 2 = 2$.

(c) The factorization of $x^7 + 1$ into irreducible factors is:
$$x^7 + 1 = (x+1)(x^3 + x^2 + 1)(x^3 + x + 1).$$
Again, by Corollary 4.4.4, the number of proper cyclic codes of length 7 is equal to $(2^0+1)^3 - 2 = 6$.

(d) Notice that $x^{14} + 1 = (x^7+1)^2$. With the notation of Corollary 4.4.4, $n = 2 \cdot 7$. Thus the number of proper cyclic codes of length 14 is equal to $(2^1+1)^3 - 2 = 25$.

4.4.7:

The generator polynomials of proper cyclic codes of length $n = 4$ are the divisors of $(x+1)^4$ which are different from 1 and $(x+1)^4$. They are: $x+1, (x+1)^2$, and $(x+1)^3$.

The generator polynomials of proper cyclic codes of length $n = 5$ are the divisors of $x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1)$ which are different from 1 and $x^5 + 1$. They are: $x + 1$ and $x^4 + x^3 + x^2 + x + 1$.

4.4.8:

From $x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$, one generator of degree 4 for a cyclic code of length 7 equals $(x+1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$ and another equals $(x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$.