1 Chapter 6

6.1. Consider the Galois field $GF(2^4)$ given by table 2.8. The element $\beta = \alpha^7$ is also a primitive element. Let $g_0(X)$ be the lowest-degree polynomial over $GF(2)$ that has

$$\beta, \beta^2, \beta^3, \beta^4$$

as its roots. This polynomial also generates a double-error-correcting primitive BCH code of length 15.

1. Determine $g_0(X)$.
2. Find the parity-check matrix of this code.
3. Show that $g_0(X)$ is the reciprocal of the polynomial $g(X)$ that generates the (15, 7) double-error-correcting BCH given in example 6.1.

Solution.

1. $g_0(X) = LCM(o_1, o_2, o_3, o_4)$ where o_i is equal to thee minimum polynomial of β^i. The minimum polynomial of an element is the polynomial with least degree and the element as its root. The minimum polynomial of an element is irreducible and is a factor of $X^{2^m} + X$ where $m = 4$. The irreducible factors of $X^{2^m} + X$ are

   $$Y * (Y + 1) * (Y^2 + Y + 1) * (Y^4 + Y + 1) * (Y^4 + Y^3 + 1) * (Y^4 + Y^3 + Y^2 + Y + 1)$$

   The minimum polynomials are then found to be

   $$(Y^4 + Y^3 + 1), (Y^4 + Y^3 + 1), (Y^4 + Y^3 + Y^2 + Y + 1), (Y^4 + Y^3 + 1)$$

   for each β respectively. We know that ever power of β has the same minimum polynomial as some proceeding odd power of β. As a result we can reduce our LCM function to $g_0(X) = LCM(o_1, o_3)$. To get the LCM of a set of polynomials you need to multiply the unique factors of each one. Instead because our set of polynomials are minimum and therefor irreducible we only have to multiply the unique polynomials in our set, resulting in

   $$\begin{aligned} g_0(X) &= LCM(o_1, o_3) \\ &= LCM((Y^4 + Y^3 + 1), (Y^4 + Y^3 + Y^2 + Y + 1)) \\ &= (Y^4 + Y^3 + 1) * (Y^4 + Y^3 + Y^2 + Y + 1) \\ &= (Y^8 + Y^4 + Y^2 + Y + 1)) \end{aligned}$$

   Which is a (15,8) code by $(2^m - 1, 2^(m - 1))$.

2. The parity-check matrix of this code is generated by the root of $g_0(X)$ in the following form:

$$\begin{bmatrix} 1 & \beta & \beta^2 & \beta^3 & \dots & \beta^{14} \\ 1 & \beta^3 & (\beta^3)^2 & (\beta^3)^3 & \dots & (\beta^3)^{14} \end{bmatrix}$$

3. The reciprocal of $g(X)$ defined by

$$\begin{aligned} g_0(X) &= (X^7)g(X^{-1}) \\ &= 1 + X + X^2 + X^4 + X^8 \end{aligned}$$

6.2. Determine the generator polynomial of all primitive BCH codes of length 31. Use the Galois field $GF(2^5)$ generated by $p(X) = X^5 + X^2 + 1$.

Solution. First list out all the elements of $GF(2^5)$ and their minimum polynomials:

$$\begin{aligned} Y^5 + Y^2 + 1 &= a^1, a^2, a^4, a^8, a^{16} \\ Y^5 + Y^4 + Y^3 + Y^2 + 1 &= a^3, a^6, a^{12}, a^{17}, a^{24} \\ Y^5 + Y^3 + Y^2 + Y + 1 &= a^7, a^{14}, a^{19}, a^{25}, a^{28} \\ Y^5 + Y^4 + Y^2 + Y + 1 &= a^5, a^9, a^{10}, a^{18}, a^{20} \\ Y^5 + Y^4 + Y^3 + Y + 1 &= a^{11}, a^{13}, a^{21}, a^{22}, a^{26} \\ Y^5 + Y^3 + 1 &= a^{15}, a^{23}, a^{27}, a^{29}, a^{30} \\ Y + 1 &= a^{31} \end{aligned}$$

These minimum polynomials form all the irreducible factors of $X^31 + 1$.

$$(Y^5 + Y^4 + Y^2 + Y + 1), (Y^5 + Y^4 + Y^3 + Y + 1), (Y^5 + Y^4 + Y^3 + Y^2 + 1)$$

$$(Y + 1), (Y^5 + Y^2 + 1), (Y^5 + Y^3 + 1), (Y^5 + Y^3 + Y^2 + Y + 1)$$

Now any combination of these factor will produce a binary BCH code but to get a primitive BCH code we must find the generators that have a^1 and any other odd powers in a run as roots. Below are the first four but there is a total of 16.

$$\begin{aligned} a^1 &= Y^5 + Y^2 + 1 \\ a^1 + a^3 &= (Y^5 + Y^2 + 1) * (Y^5 + Y^4 + Y^3 + Y^2 + 1) \\ a^1 + a^3 + a^5 &= (Y^5 + Y^2 + 1) * (Y^5 + Y^4 + Y^3 + Y^2 + 1) * (Y^5 + Y^4 + Y^2 + Y + 1) \\ a^1 + a^3 + a^5 + a^7 &= (Y^5 + Y^2 + 1) * (Y^5 + Y^4 + Y^3 + Y^2 + 1) * (Y^5 + Y^4 + Y^2 + Y + 1) * (Y^5 + Y^3 + Y^2 + Y + 1) \end{aligned}$$

In total the odd numbers between 1 and the length of our code 31 is 16 and so there are 16 primitive BCH codes of length 31.

6.3. Suppose that the-double-error correcting BCH code constructed in Problem 6.2 is used for error correction a BSC. Decode the received polynomials $r_1(X) = X^7 + X^{30}$ and $r_2(X) = 1 + X^{17} + X^{28}$.

Solution.

1. A linear shift register has a defined length
2. A linear shift register that has a greater length will also produce a greater sequence
3. A sequence from a linear shift register is obtained by taking the content of the register and
4. Compute the syndrome
5. Create the minimum LSFR with the coeffs of the syndrome S
6. The resulting connection polynomial of degree d is our sigma polynomial
7. take the coeffs from our new polynomial of degree d sigma and its coeefs are error locations.
8. Get our generator from Problem 6.1 not 6.2 $g_0 = Y^8 + Y^4 + Y^2 + Y + 1$
9. Remember that $\beta = a^7 = a^4 + a^2$
10. Take the received polynomial $r_1(X) = X^7 + X^{30}$ and compute the syndrom

$$S_1 = r_1(\beta) = r_1(a^7) = r_1(a^4 + a^2) = a^4 + a^3 + a^2 + 1$$

$$S_2 = r_1(\beta^2) = a^4 + a^2 + a$$

$$S_3 = r_1(\beta^3) = a^4 + a^3 + a^2 + a$$

$$S_4 = r_1(\beta^4) = a^4 + a^3 + 1$$

11. Then run the Berlcamp algorithm to get the locater polynomial
12. Invert the roots of the locater polynomial to find the error locations.
13. Because we are working with binary BCH codes we are done.
14. For r_1 there was an error at the seventh and first bit.
15. For r_2 there was an error on the sixteenth and fourth bit.

6.4. Consider a t-error-correcting BCH code of length $n = 2^m - 1$. If $2t + 1$ is a factor of n, prove the minimum distance of this code is exactly $2t + 1$. (Hint: Let $n = l(2t + 1)$. Show that $(X^n + 1)/(X^l + 1)$ is a code polynomial of weight $2t + 1$.)

Solution. We know that the minimum distance of a t-error-correcting BCH code is at least $2t + 1$. If we can find a code with weight $2t + 1$ then we are done. The minimum distance of a code is the number of consecutive powers of an element that are roots of the generator polynomial plus one. Code polynomials are multiples of the generator polynomial and therefor share roots. We need to find a polynomial that has an element and up to $2t$ powers of it as its roots. We know from the book it has at least $2t$ so we need only show that there exits a code polynomial without $\beta^(2t + 1)$ as its root.

6.5. Is there a binary t-error-correcting BCH code of length 2^m+1 for $m > 3$ and $t < 2^{m-1}$. If there is such a code, Determine its generator polynomial.

Solution. The length of the code is the LCM of the orders of the powers of β that make up our generator polynomial. First find an element that has our desired length as it order. For example $a^6 + a^4 + a^3 + 1$ has order $17 = 2^4 + 1$ so our m is now 4. Next check to see if the powers of that element also have order 17, We have chosen 4 consecutive powers of β so our minimum distance will be at least $4 = 2t$ and this dictates that $t = 2$. Next find the minimum polynomial of our chosen betas. Then get the LCM of the minimum polynomials, this is our generator polynomial

$$X^{16}+X^{15}+X^{14}+X^{13}+X^{12}+X^{11}+X^{10}+X^9+X^8+X^7+X^6+X^5+X^4+X^3+X^2+X+1$$

We have now found a code that has length $2^m + 1$ for $m > 3$ (This could also have worked with $m = 2$) and has $t < 2^(m - 1)$.

6.10. Consider the Galois field $GF(2^6)$ given by Table 6.2. Let $\beta = \alpha^3, l_0 = 2$, and $d = 5$. Determine the generator polynomial of the BCH code that has

$$\beta^2, \beta^3, \beta^4, \beta^5$$

as its roots (the general form presented at the end of section 6.1). What is the length of this code?

Solution. This generator polynomial generates a (64, 21) code.

6.11. Let $l_0 = -t$ and $d = 2^t + 2$. Then we obtain a BCH code of designed distance $2^t + 2$ whose generator polynomial has

$$\beta^{-t}, \dots, \beta^{-1}, \beta^0, \beta^1, \dots, \beta^t$$

and their conjugates as all its roots.

1. Show that this code is a reversible cyclic code.
2. Show that if t is odd, the minimum distance of this code is at least $2^t + 4$. (Hint: show that $\beta^{-(t+1)}$ and β^{t+1} are also roots of the generator polynomial.)

Solution.

1. The first is obvious as the very definition of the polynomial is symmetrical and therefore reversible.
2. We are given a hint that if $\beta^{-(t+1)}$ and β^{t+1} are also roots then the minimum distance of the code is at least $2^t + 4$. In other words show that $\beta^{-(t+1)}$ and β^{t+1} are conjugates of our starting roots. Again in other words show that for $i \in (-t, -(t-1), \dots, -1, 0, 1, \dots, t-1, t)$ show that $(t+1) = i^(2^x)$ where x is some integer greater than 0. This is trivially true.

7.1. Consider the triple-error-correcting RS code given in Example 7.2. Find the code polynomial for the message

$$a(X) = 1 + a^5X + aX^4 + a^7X^8$$

Solution. First generate the block code, to do so our parameters are:

1. Our field is $GF(2^4)$
2. $n = q - 1 = 2^4 - 1 = 15$
3. Our generator polynomial is

$$X^6 + X^5a^{10} + X^4a^{14} + X^3a^4 + X^2a^6 + Xa^9 + a^6$$

and has degree $n - k = 2t = 6$

Now to encode our message we can use the three steps from Section 5.3

1. We know our generator polynomial has degree $n - k$ so the first step is to multiply $1 + a^5X + aX^4 + a^7X^8 * X^6 = u(X) = a^7X^{14} + aX^4 + a^5X + 1$
2. Next we divide our new polynomial $u(X)$ by the generator polynomial and get the remainder $b(X)$

$$g(X)/X^{14}a^7 + X^{10}a + X^7a^5 + X^6 = b(X) = aX^5 + a^6X^4 + X^3 + a^5X^2 + a^{13}X + a^5$$

3. Lastly add the polynomial $u(x)$ to the remainder to generate the code polynomial.

$$b(X) + u(x) = a^7X^{14} + aX^5 + a^11 * X^4 + X^3 + a^5 * X^2 + a^7 * X + a^10$$

7.2. Using the Galois field $GF(2^5)$ given in Appendix A, find the generator polynomials of the double and triple error correcting RS codes of length 31.

Solution.

1. First our field is $GF(2^5)$ generated by $p(X) = X^5 + X^2 + 1$.
2. Constructing our field in sage gives us:

   $$g_2(X) = (X - a)(X - a^2)(X - a^3)(X - a^4) \quad = X^4 + a^{24}X^3 + a^{19}X^2 + a^{29} * X + a^{10}$$

   and

   $$g_3(X) = (X - a)(X - a^2)(X - a^3)(X - a^4)(X - a^5)(X - a^6) \quad = X^6 + a^{10}X^5 + a^9X^4 + a^{24}X^3 + a^{16}X^2 + a^{24}$$

7.4. Consider the triple-error-correcting RS code of length 15 given in Example 7.2. Decode the received polynomial

$$r(X) = X^{13}a^3 + X^8a^9 + X^3a^4$$

using the Berlekamp algorithm.

Solution. See the sage files for how its done, $v(x) = 0$.

7.5. Continue problem 7.4. Decode the received polynomial with the Euclidean algorithm.

Solution. See the sage files for how its done, $v(x) = 0$.

7.6. Consider the triple-error-correcting RS code of length 31 constructed in Problem 7.2. Decode the received polynomial

$$r(X) = a^2 + a^{21}X^{12} + a^6X^{20}$$

using the Euclidean algorithm.

Solution. See the sage files for how its done, $v(x) = 0$.

7.7. Continue problem 7.6. Decode the received polynomial in the frequency domain using transform decoding.

Solution. See the sage files for how its done, $v(x) = 0$.

7.8. For the same RS code of problem 7.6, decode the following received polynomial with two erasures:

$$r(X) = (*)X^3 + a^5X^7 + (*)X^{18} + a^3X^21$$

with the Euclidean algorithm.

Solution. See the sage files for how its done, $v(x) = 0$.

7.9. Prove the dual code of an RS code is also an RS code.

Solution. To get a dual code from a RS code there are 3 steps:

1. First we need to find the parity-check matrix generator polynomial. Remember that $X^n + 1 = g(X)h(X)$ so by dividing $X^n + 1/g(X) = h(X)$.
2. Notice that $h(X)$ contains all the roots of $X^n + 1$ minus the roots of $g(X)$. Since $g(X)$ contained the first $n - k$ roots, $h(X)$ has k roots starting from $n - k$.
3. Now grab the reciprocal of the parity-check polynomial $X^k h(X^{-1})$. Now it has k roots starting from one.
4. This polynomial has degree k, is a factor of $X^n + 1$, and has k consecutive powers of a as roots starting from one.

7.10. Prove that the $(2^m - 1, k)$ RS code with minimum distance d contains the primitive binary BCH code of length $(2^m - 1)$ with designed distance d as a subcode. This code is called a subfield subcode.

Solution. The primitive binary BCH codes and the RS codes are constructed in the exact same way except the RS codes have coeffs in a non binary field. Because the non binary fields contains all elements of the binary field, and g is constructed the exact same way you need only filter out non binary field elements to get the binary BCH code of length $2^m - 1$.

7.13.

Solution. We can wright the coefficents of $v(X)$ as a list of equasions:

$$\begin{aligned}
v_0 &= (a_0(\alpha^0)^0) + (a_1(\alpha^0)^1) + (a_2(\alpha^0)^2) + \ldots + (a_{k-1}(\alpha^0)^{k-1}) \\
v_1 &= (a_0(\alpha^1)^0) + (a_1(\alpha^1)^1) + (a_2(\alpha^1)^2) + \ldots + (a_{k-1}(\alpha^1)^{k-1}) \\
v_2 &= (a_0(\alpha^2)^0) + (a_1(\alpha^2)^1) + (a_2(\alpha^2)^2) + \ldots + (a_{k-1}(\alpha^2)^{k-1}) \\
&\vdots \\
v_{2^m-2} &= (a_0(\alpha^{2^m-2})^0) + (a_1(\alpha^{2^m-2})^1) + (a_2(\alpha^{2^m-2})^2) + \ldots + (a_{k-1}(\alpha^{2^m-2})^{k-1})
\end{aligned}$$

Which can then be simlfiyed to:

$$\begin{aligned}
v_0 &= a_0 + a_1 + a_2 + \ldots + a_{k-1} \\
v_1 &= a_0 + (a_1\alpha) + (a_2\alpha^2) + \ldots + (a_{k-1}\alpha^{k-1}) \\
v_2 &= a_0 + (a_1\alpha^3) + (a_2\alpha^4) + \ldots + (a_{k-1}\alpha^{2(k-1)}) \\
&\vdots \\
v_{2^m-2} &= a_0 + (a_1\alpha^{2^m-2}) + (a_2\alpha^{2(2^m-2)}) + \ldots + (a_{k-1}\alpha^{(k-1)(2^m-2)})
\end{aligned}$$

9.1. Consider the (6, 3) linear code generated by the following matrix:

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

1. Put this generator into Trellis-oriented form.
2. Determine the active time spans of the rows in the trellis oriented generator matrix.
3. Determine the space state dimension profile of the bit-level 6-section trellis for the code.
4. Determine the state defining information set at each time instant.
5. Determine the input information bit at each time instant.
6. Determine the output function in each bit interval.

Solution.

1. $$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$
2. $t(g_0) = [0, 4], t(g_1) = [1, 3], t(g_2) = [3, 5]$
3. $p = [0, 1, 1, 2, 2, 2, 1, 0]$ for $0 \leq i \leq n$
4. $A_i^s =$
   (a) $\{\}$
   (b) $\{a_0\}$
   (c) $\{a_1\}$
   (d) $\{a_0, a_1\}$
   (e) $\{a_1, a_2\}$

(f) $\{a_0, a_2\}$

(g) $\{a_2\}$

(h) $\{\}$

5. $a^* =$

(a) $\{a_0\}$

(b) $\{a_1\}$

(c) $\{a_0\}$

(d) $\{a_2\}$

(e) $\{a_0\}$

(f) $\{\}$

(g) $\{\}$

(h) $\{\}$

6. $a^0 =$

(a) $\{\}$

(b) $\{a_0\}$

(c) $\{\}$

(d) $\{a_0\}$

(e) $\{a_1\}$

(f) $\{a_0\}$

(g) $\{a_2\}$

(h) $\{\}$

9.2. Construct the trellis oriented generator matrix for the first-order RM code, (1, 5), of length 32.

Solution. First get the 6 generating tuples of the RM code:

$$v_0 = 11111111111111111111111111111111$$

$$v_5 = 00000000000000001111111111111111$$

$$v_4 = 00000000111111110000000011111111$$

$$v_3 = 00001111000011110000111100001111$$

$$v_2 = 00110011001100110011001100110011$$

$$v_1 = 01010101010101010101010101010101$$

Since this is a first-order code we arange these tuples as the rows of our matrix and were done. Next to put this matrix in TOF arange the rows such that the trailling one is in desending order, Then add the bottom row to every row above to get:

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}$$

Now construct the table:

i	G_i^s	a^*	a^0	A_i^s	State lable
0	$\{\}$	a_0	0	$\{\}$	()
1	$\{g_0\}$	a_1	0	$\{a_0\}$	()
2	$\{g_0, g_1\}$	a_2	a_1	$\{a_0, a_1\}$	()
3	$\{g_0, g_2\}$	a_1	0	$\{a_0, a_2\}$	()
4	$\{g_0, g_1, g_2\}$	a_3	$\{a_1, a_2\}$	$\{a_0, a_1, a_2\}$	()
5	$\{g_0, g_3\}$	a_1	0	$\{a_0, a_3\}$	()
6	$\{g_0, g_1, g_3\}$	a_2	a_1	$\{a_0, a_1, a_3\}$	()
7	$\{g_0, g_2, g_3\}$	a_1	0	$\{a_0, a_2, a_3\}$	()
8	$\{g_0, g_1, g_2, g_3\}$	a_4	$\{a_1, a_2, a_3\}$	$\{a_0, a_1, a_2, a_3\}$	()
9	$\{g_0, g_4\}$	a_1	0	$\{a_0, a_4\}$	()
10	$\{g_0, g_1, g_4\}$	a_2	a_1	$\{a_0, a_1, a_4\}$	()
11	$\{g_0, g_2, g_4\}$	a_1	0	$\{a_0, a_2, a_4\}$	()
12	$\{g_0, g_1, g_2, g_4\}$	a_3	$\{a_1, a_2\}$	$\{a_0, a_1, a_2, a_4\}$	()
13	$\{g_0, g_3, g_4\}$	a_1	0	$\{a_0, a_3, a_4\}$	()
14	$\{g_0, g_1, g_3, g_4\}$	a_2	a_1	$\{a_0, a_1, a_3, a_4\}$	()
15	$\{g_0, g_2, g_3, g_4\}$	a_1	0	$\{a_0, a_2, a_3, a_4\}$	()
16	$\{g_0, g_1, g_2, g_3, g_4\}$	a_0	a_5	$\{a_0, a_1, a_2, a_3, a_4\}$	()
17	$\{g_1, g_2, g_3, g_4, g_5\}$	0	a_1	$\{a_1, a_2, a_3, a_4, a_5\}$	()
18	$\{g_2, g_3, g_4, g_5\}$	a_1	a_2	$\{a_2, a_3, a_4, a_5\}$	()
19	$\{g_1, g_3, g_4, g_5\}$	0	a_1	$\{a_1, a_3, a_4, a_5\}$	()
20	$\{g_3, g_4, g_5\}$	$\{a_1, a_2\}$	a_3	$\{a_3, a_4, a_5\}$	()
21	$\{g_1, g_2, g_4, g_5\}$	0	a_1	$\{a_1, a_2, a_4, a_5\}$	()
22	$\{g_2, g_4, g_5\}$	a_2	a_1	$\{a_2, a_4, a_5\}$	()
23	$\{g_1, g_4, g_5\}$	a_2	a_1	$\{a_1, a_4, a_5\}$	()
24	$\{g_4, g_5\}$	$\{a_1, a_2, a_3\}$	a_4	$\{a_4, a_5\}$	()
25	$\{g_1, g_2, g_3, g_5\}$	0	a_1	$\{a_1, a_2, a_3, a_5\}$	()
26	$\{g_2, g_3, g_5\}$	a_1	a_2	$\{a_2, a_3, a_5\}$	()
27	$\{g_1, g_3, g_5\}$	0	a_1	$\{a_1, a_3, a_5\}$	()
28	$\{g_3, g_5\}$	$\{a_1, a_2\}$	a_3	$\{a_3, a_5\}$	()
29	$\{g_1, g_2, g_5\}$	0	a_1	$\{a_1, a_2, a_5\}$	()
30	$\{g_2, g_5\}$	0	a_2	$\{a_2, a_5\}$	()
31	$\{g_5\}$	0	a_5	$\{a_5\}$	()
32	$\{\}$	0	0	$\{\}$	()

9.3. Construct the bit level Trellis for the (6, 3) code given in Problem 9.1. Lable its states based on the state defininig information set using $Pmax(C)$ bits.

Solution.

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

i	G_i^s	a^*	a^0	A_i^s	State lable
0	$\{\}$	$\{a_0, a_1, a_2\}$	0	$\{\}$	(000)
1	$\{g_0, g_1, g_2\}$	0	$\{a_0, a_2\}$	$\{a_0, a_1, a_2\}$	$(a_1a_2a_3)$
2	$\{g_1\}$	$\{a_0, a_2\}$	a_1	$\{a_1\}$	$(0a_10)$
3	$\{g_0, g_2\}$	0	a_2	$\{a_0, a_2\}$	(a_10a_2)
4	$\{g_0\}$	a_2	a_0	$\{a_0\}$	(a_000)
5	$\{g_2\}$	a_0	a_2	$\{a_2\}$	$(00a_2)$
6	$\{g_0, g_1\}$	0	$\{a_0, a_1\}$	$\{a_0, a_1\}$	(a_0a_10)
7	$\{\}$	0	0	$\{\}$	(000)

$$Pmax(C) = 3$$

9.4. Find the parity-check matrixs for the (6, 3) code given in problem 9.1. Lable the states of its bit level trellis base on the parity-check matrix.

Solution. Here is our generator matrix:

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

By adding the fifth and second row the first, and by adding the fourth to the third we get the generator in standard form:

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

Next transpose P and add a new identity matrix:

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

Then to put the parity check matrix in TOF, move the top row to the bottom:

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

Then contstruct the table for the state labbleing.

i	State lable
0	(000)
1	(a_000)
2	$(0a_10)$
3	$(0a_1a_2)$
4	$(00a_2)$
5	(a_000)
6	$(0a_10)$
7	(000)

9.5. Construct the bit-level minimal trellis for the (8, 7) even parity-check code.

Solution. First get the generator matrix for the code:

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

Then construct the table for it:

i	G_i^s	a^*	a^0	A_i^s	Stat
0	$\{\}$	$\{a_0, a_1, a_2, a_3, a_4, a_5, a_6\}$	0	$\{\}$	(000
1	$\{g_0, g_1, g_2, g_3, g_4, g_5, g_6\}$	0	$\{a_1, a_2, a_3, a_4, a_5, a_6\}$	$\{a_0, a_1, a_2, a_3, a_4, a_5, a_6\}$	$(a_0a_1a_2$
2	$\{g_0\}$	g_1	g_0	$\{g_0\}$	$(a_00$
3	$\{g_1\}$	g_2	g_1	$\{g_1\}$	$(0a_1$
4	$\{g_2\}$	g_3	g_2	$\{g_2\}$	(00
5	$\{g_3\}$	g_4	g_3	$\{g_3\}$	(000
6	$\{g_4\}$	g_5	g_4	$\{g_4\}$	(000
7	$\{g_5\}$	g_6	g_5	$\{g_5\}$	(000
8	$\{g_6\}$	0	g_6	$\{g_6\}$	(000
9	$\{\}$	0	0	$\{\}$	(000

9.6. construct the bit-level trellis for the first order RM code, RM(1,5), of length 32. Lable its states based on the state defining information set using Pmax(C) bits.

Solution. Check out Problem 9.2 for same solution.

11.1. Consider the (3,1,2) nonsystimatic feedforward encoder with

$$g^{(0)} = (110)$$

,

$$g^{(1)} = (101)$$

,

$$g^{(2)} = (111)$$

1. Draw an encoder block diagram.
2. Find time-domain generator matrix G.
3. Find the codeword v corasponding to the message $u = (110, 011, 101)$

Solution.

1. Draw an encoder block diagram.
2. $$G = \begin{bmatrix} 111 & 101 & 011 & 0 & 0 & 0 & 0 & 0 \\ 0 & 111 & 101 & 011 & 0 & 0 & 0 & 0 \\ 0 & 0 & 111 & 101 & 011 & 0 & 0 & 0 \\ 0 & 0 & 0 & 111 & 101 & 011 & 0 & 0 \end{bmatrix}$$
3. Find the codeword v corasponding to the message $u = (110, 011, 101)$

11.2.

Solution.

1. $$g_1 = (100, 100, 100, 100)$$
$$g_2 = (000, 110, 010, 100)$$
$$g_3 = (000, 010, 101, 101)$$

2.

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

3. First get the generator matrix above and truncate it to three rows, then multply the message as a vertical matrix:

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & & & & & & & & \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & & & & & & & & \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} =$$

$$1010000011101110011$$

11.4.

Solution.

1.

$$g_1 = 11 * 01X * 11X^2$$

$$g_2 = 01 * 10X * 10X^2$$