S-72.341 CODING METHODS

Tutorial 5, Solutions

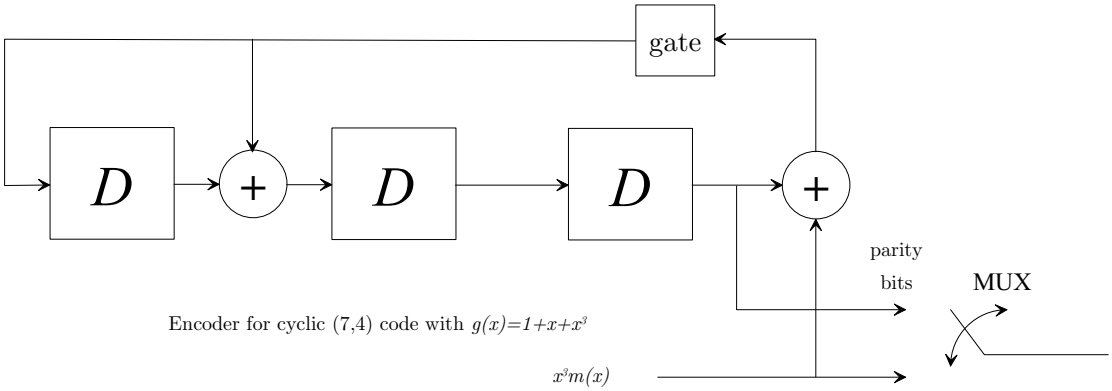
1. The systematic encoding procedure is explained on page 107 of the course book.

   a) Message word can be represented as a polynomial $m(x) = 1 + x^2 + x^3$. Then following the systematic encoding procedure we get the code polynomial as

   $$c(x) = \underbrace{x^3 m(x) \bmod g(x)}_{\text{parity check part}} + \underbrace{x^3 m(x)}_{\text{message part}} = 1 + x^3 + x^5 + x^6$$

   corresponding to code word 1001011.

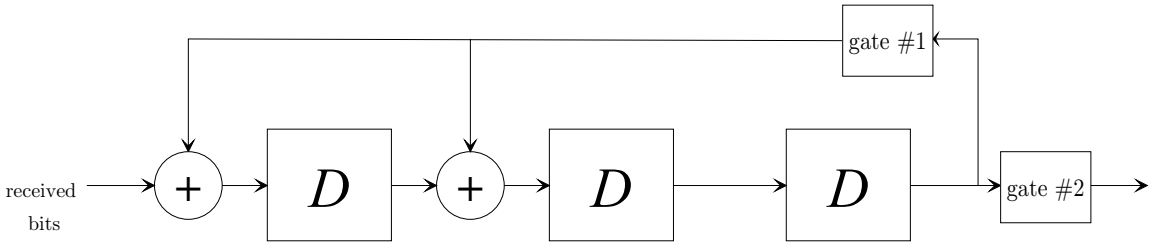
   b) Systematic encoding circuit is shown in the figure below. Compare to Figure 5-12 of the book.



   Shift register values are given in the following table. In the final stage the registers have value 100, which is the parity-check part of the given message word.

Input	SR values
1	0 0 0
1	1 1 0
0	1 0 1
1	1 0 0
-	1 0 0

2. Syndrome computation circuit is shown in the figure below.



Syndrome computation circuit for cyclic (7,4) code with $g(x)=1+x+x^3$

Syndrome computation procedure is shown in the table below.

Input	SR values
1	0 0 0
1	1 0 0
0	1 1 0
1	0 1 1
0	0 1 1
0	1 1 1
1	1 0 1
-	0 0 0

In the final stage of syndrome computation shift registers have values 000, i.e. zero syndrome.

3. Every root of $x^{31}-1$ has order 1 or 31, because 31 is prime. There are 30 elements of order 31 and one element of order 1 in GF(32)=GF(2^5). There are 6 conjugacy classes with respect to GF(2), each having cardinality 5. Thus, the binary cyclic codes of block length 31 have dimensions of the form $5i+j$, where $i = 0,1,...,6$ and $j = 0,1$.

4. To factor $x^{63}-1$ we notice that there are $\phi(63)=36$ primitive elements in GF(64), $\phi(21)=12$ of order 21, $\phi(9)=6$ of order 9, $\phi(7)=6$ of order 7, $\phi(3)=2$ of order 3, and one element of order 1. By Theorem 3-3 conjugacy classes will have 6,3,2, or 1 element. It is easy to verify that conjugacy classes for primitive elements have 6 elements, totalling 6 such conjugacy classes. Similarly, elements of order 21 and 9 have 6 elements in each conjugacy class. Thus, there

are a total of 9 conjugacy classes with cardinality of 6. Elements of order 7 are in two conjugacy classes of cardinality 3, and elements of order 3 are all in one conjugacy class. Summing up, the dimension of the cyclic codes of length 63 have dimension of the form $6i + 3j + 2k + m$, where $i = 0,1,...,9$; $j = 0,1,2$; $k = 0,1$; and $m = 0,1$. There are binary cyclic codes of every dimension from 0 to 63.

5. Since $x^{19} + 1$ is not of the form $x^{q^m - 1} - 1$, we have to find the smallest m such that $19 \mid 2^m - 1$. After a stupid and painful trial and error procedure we finally discover that $m = 18$. Thus, an element of order 19 can be found in $\mathrm{GF}(2^{18})$ and $x^{19} + 1$ can be factored as $x^{19} + 1 = (x + 1)\left(x^{18} + x^{17} + ... + 1\right)$. Binary cyclic codes of length 19 can have dimension 0,1,18, or 19.

6. We must find the smallest m satisfying $33 \mid 8^m - 1$. Again, by trial and error $m = 10$. There are $\phi(33) = 20$ elements of order 33, so these elements are divided to two conjugacy classes of cardinality 10. Conjugacy classes must have cardinality 1,2,5, or 10. Since $\phi(11) = 10$, and 11 does not divide $8^2 - 1$ or $8^5 - 1$, then $11 \mid 8^{10} - 1$, and elements of order 11 form a conjugacy class with 10 elements in it. Of course there is one element of unit order. Thus, there must also be one conjugacy class of cardinality 2 so that everything sums to 33. Check: Cardinalities of conjugacy classes sum to $3 \cdot 10 + 2 + 1 = 33$. An 8-ary cyclic code of length 33 can have dimension 0, 1, 2, 3, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, or 33.