C&O 331: Assignment #4 solutions

---

1. (a) $s_2 = [B|I_{12}]r_1^T = (1001\ 0001\ 0000)^T$. Since $w(s_2) \leq 3$, the error vector is $e_1 = (0, s_2^T)$. r_1 is corrected to $c_1 = (0000\ 0000\ 0011\ 0110\ 1100\ 1001)$.

   (b) $s_2 = [B|I_{12}]r_2^T = (1101\ 1001\ 0110)^T$, which has weight > 3. Since s_2 differs in positions 3 and 5 from column 5 of B, the error vector is $e_2 = (0000\ 1000\ 0000\ 0010\ 1000\ 0000)$. r_2 is corrected to $c_2 = (0011\ 0000\ 0000\ 0110\ 0100\ 1110)$.

   (c) $s_1 = [I_{12}|B]r_3^T = (0110\ 0001\ 0110)^T$, which has weight > 3. Since s_1 differs in positions 1 and 4 from column 5 of B, the error vector is $e_3 = (1001\ 0000\ 0000\ 0000\ 1000\ 0000)$. r_3 is corrected to $c_3 = (0110\ 0000\ 0000\ 0011\ 0010\ 0111)$.

2. The factorization of $x^{17} - 1$ over $\mathbb{Z}_2$ is $x^{17} - 1 = g_1(x)g_2(x)g_3(x)$, where

$$\begin{aligned} g_1(x) &= 1 + x \\ g_2(x) &= 1 + x + x^2 + x^4 + x^6 + x^7 + x^8 \\ g_3(x) &= 1 + x^3 + x^4 + x^5 + x^8. \end{aligned}$$

   (a) $2^3 = 8$.

   (b) The possible generator polynomials of cyclic subspaces of $V_{17}(\mathbb{Z}_2)$ are $g_1g_2g_3$, g_1g_2, g_2g_3, g_1g_3, g_3, g_2, g_1, and 1. They generate cyclic subspaces of dimensions 0, 8, 1, 8, 9, 9, 16, and 17, respectively. Thus the values of k, $1 \leq k \leq 17$, for which a cyclic subspace of dimension k exists are 1, 8, 9, 16, and 17.

   (c) There is no subspace of dimension 12.

   (d) g_1g_2 (or g_1g_3) is the generator polynomial for a cyclic subspace of dimension 8.

3. (a) We have to prove that $C_1 \bigcap C_2$ is a vector subspace of $V_n(F)$.
   First note that $0 \in C_1 \bigcap C_2$, so $C_1 \bigcap C_2$ is non-empty.
   Let $c_1, c_2 \in C_1 \bigcap C_2$. Then, since C_1 and C_2 are closed under vector addition, we have $c_1 + c_2 \in C_1$ and $c_1 + c_2 \in C_2$. Hence $c_1 + c_2 \in C_1 \bigcap C_2$.
   Let $c \in C_1 \bigcap C_2$ and $\lambda \in F$. Then, since C_1 and C_2 are closed under scalar multiplication, we have $\lambda c \in C_1$ and $\lambda c \in C_2$. Hence $\lambda c \in C_1 \bigcap C_2$.
   We conclude that $C_1 \bigcap C_2$ is a linear code.

   (b) Let $c \in C_1 \bigcap C_2$. Since C_1 and C_2 are cyclic, $\pi(c)$ (the right cyclic shift of c) is in C_1 and in C_2. Hence $\pi(c) \in C_1 \bigcap C_2$, whence $C_1 \bigcap C_2$ is a cyclic code.

   (c) Let $g(x) = \text{lcm}(g_1(x), g_2(x))$. Note that $g(x)$ is monic and divides $x^n - 1$.
   Let $c(x) \in C_1 \bigcap C_2$. Since $c(x) \in C_1$ and $c(x) \in C_2$, it follows that $g_1(x)|c(x)$ and $g_2(x)|c(x)$. Hence $g(x)|c(x)$.
   Conversely, if $c(x) = a(x)g(x)$, where $a(x) \in F[x]$, then $c(x) \in C_1$ since $g_1(x)|g(x)$, and $c(x) \in C_2$ since $g_2(x)|g(x)$. Hence $c(x) \in C_1 \bigcap C_2$.
   It follows that $C_1 \bigcap C_2 = \{a(x)g(x) \ : \ a(x) \in F[x]\}$. Since $g(x)$ is a monic divisor of $x^n - 1$, it follows from a Theorem proven in class that $g(x)$ is *the* generator polynomial of $C_1 \bigcap C_2$.

4. (a) We prove the result by computing the syndromes of all cyclic burst errors of length 2 or less.

error	syndrome	integer	error	syndrome	integer
0	00000	0	$x^0 + x^1$	11000	24
x^0	10000	16	$x^1 + x^2$	01100	12
x^1	01000	8	$x^2 + x^3$	00110	6
x^2	00100	4	$x^3 + x^4$	00011	3
x^3	00010	2	$x^4 + x^5$	10100	20
x^4	00001	1	$x^5 + x^6$	01010	10
x^5	10101	21	$x^6 + x^7$	00101	5
x^6	11111	31	$x^7 + x^8$	10111	23
x^7	11010	26	$x^8 + x^9$	11110	30
x^8	01101	13	$x^9 + x^{10}$	01111	15
x^9	10011	19	$x^{10} + x^{11}$	10010	18
x^{10}	11100	28	$x^{11} + x^{12}$	01001	9
x^{11}	01110	14	$x^{12} + x^{13}$	10001	17
x^{12}	00111	7	$x^{13} + x^{14}$	11101	29
x^{13}	10110	22	$x^{14} + x^0$	11011	27
x^{14}	01011	11			

Since all syndromes are distinct, we conclude that C is a 2-cyclic burst error correcting code.

i. The received word is decoded to (01011 00000 00001).

ii. The received word is decoded to (10001 00110 10111).

5. (a) First, we must check that $g(x)$ divides $x^7 - 1$ over $\mathbb{Z}_2$. But,

$$x^7 - 1 = (x^3 + x^2 + 1)g(x)$$

so $g(x)$ does generate a binary cyclic $(7, 3)$ code.

To check that it is 2-cyclic burst error correcting, we merely check that all cyclic bursts of length 2 have different syndromes. The following table lists cyclic bursts of length at most 2 and their syndromes (in vector form) where we use the parity-check matrix H such that the syndrome polynomial of $r(x)$ is $r(x)$ mod $g(x)$.

Cyclic burst	Syndrome
0000000	0000
1000000	1000
0100000	0100
0010000	0010
0001000	0001
0000100	1011
0000010	1110
0000001	0111

Cyclic burst	Syndrome
1100000	1100
0110000	0110
0011000	0011
0001100	1010
0000110	0101
0000011	1001
1000001	1111

Since all syndromes are different, C is 2-cyclic burst error correcting.

(b) C^* is just the code obtained by interleaving C to a depth of 2. Since C can correct cyclic bursts of length 2, C^* can correct cyclic bursts of length $2 \cdot 2 = 4$.

(c) Let us de-interleave r into $r_{odd} = (1100011)$ and $r_{even} = (0000110)$ in C. Now use the error-trapping algorithm to determine the error vector e_{odd} and e_{even} for these two vectors in C.

The following table lists the syndromes for cyclic shifts of r_{odd} (in vector form).

i	$x^i r_{odd}(x) \bmod g(x)$
0	0101
1	1001
2	1111
3	1100

When $i = 3$, we get a burst of length 2 which means that e_{odd} satisfies $x^3 e_{odd}(x) = (1100000)$. Hence, $e_{odd} = (0000110)$.

We could do the same for r_{even}. However, noticing that r_{even} is itself a burst of length 2, we must have $r_{even} = e_{even} = (0000110)$. Interleaving e_{odd} and e_{even}, we get the original error vector $e = (0000000\ 0111100)$ for r.