Assignment 4

Question 1

(a) For GF(32) and GF(2)

$\alpha^5 \rightarrow x^5 + x^4 + x^2 + x + 1$

$\alpha^{15} \rightarrow x^5 + x^3 + 1$

$$g(x) = (x^5 + x^4 + x^2 + x + 1)(x^5 + x^3 + 1)$$

$$= x^{10} + x^8 + x^5 + x^9 + x^7 + x^4 + x^7 + x^6 + x^2 + x^6 + x^4 + x + x^5 + x^3 + 1$$

$$g(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1$$

(b) $h(x) = (x+1)(x^5 + x^2 + 1)(x^5 + x^4 + x^3 + x + 1) \cdot (x^5 + x^3 + x^2 + x + 1)(x^5 + x^3 + x^2 + x + 1)$

alternatively $h(x) = \dfrac{x^{31} + 1}{g(x)}$

$$= x^{21} + x^{20} + x^{18} + x^{16} + x^{14} + x^{10} + x^8 + x^7 + x^6 + x^4 + x + 1$$

(c) $n - k = 10$ from degree of $g(x)$

Therefore $n - k = 10$

$31 - k = 10$

$k = 21$ $\quad r = \dfrac{21}{31}$

(d) $C(x) = m(x)\,g(x)$

$$= (1 + x + x^7)(1 + x^2 + x^3 + x^5 + x^6 + x^8 + x^9 + x^{10})$$

$$= 1 + x^2 + x^3 + x^5 + x^6 + x^8 + x^9 + x^{10}$$
$$+ x + x^3 + x^4 + x^6 + x^7 + x^9 + x^{10} + x^{11}$$
$$+ x^7 + x^9 + x^{10} + x^{12} + x^{13} + x^{15} + x^{16}$$
$$+ x^{17}$$
$$= 1 + x + x^2 + x^4 + x^5 + x^8 + x^9 + x^{10}$$
$$+ x^{11} + x^{12} + x^{13} + x^{15} + x^{16} + x^{17}$$

$= (1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0 \ldots 0)$

(31 bits)

LSB — MSB

(e) $C(x) = x^{n-k}\,m(x) + d(x)$

where $d(x) = \text{remainder}\left(\dfrac{x^{n-k}\,m(x)}{g(x)}\right)$

$$x^{n-k}\,m(x) = x^{10}(x^7 + x + 1)$$
$$= x^{17} + x^{16} + x^{10}$$

$$x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + x^2 + x + 1 \;\overline{)\; x^{17} + x^{16} + x^{10}}$$

$$x^7 + x^5 + x^4 + x^3 + x^2 + x$$

$$x^{17} + x^{16} + x^{15} + x^{13} + x^{12} + x^{10} + x^9 + x^8 + x^7$$

$$x^{15} + x^{13} + x^{12} + x^9 + x^8 + x^7$$

$$x^{15} + x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^6 + x^5$$

$$x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^5$$

$$x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4$$

$$x^{13} + x^{11} + x^7 + x^4$$

$$x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3$$

$$x^{12} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3$$

$$x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^3 + x^2$$

$$x^{11} + x^{10} + x^7 + x^6 + x^4 + x^2$$

$$x^{11} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x^2 + x$$

$d(x) \Rightarrow x^7 + x^3 + x$

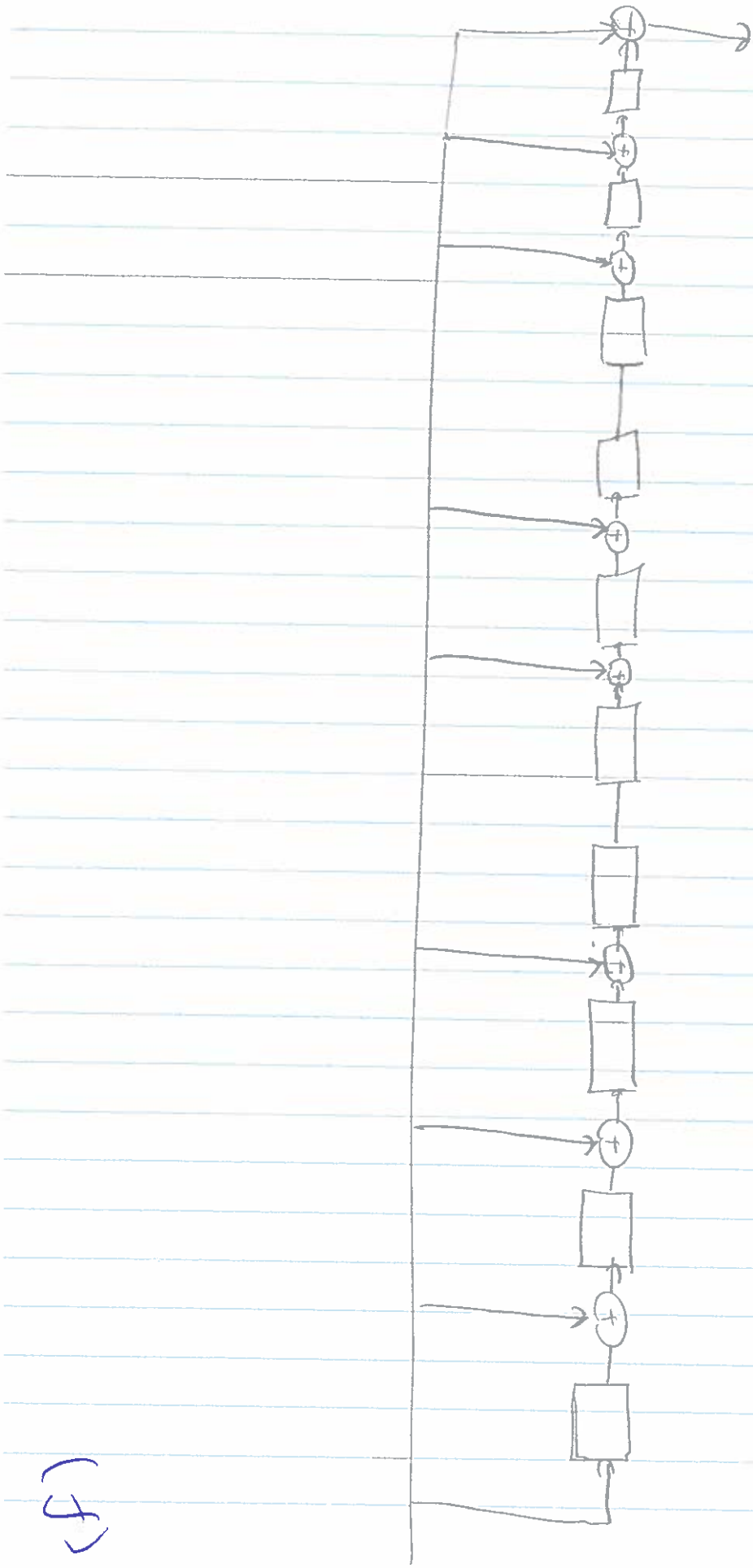
$$c(x) = x + x^3 + x^7 + x^{10} + x^{16} + x^{17}$$

MSB

1

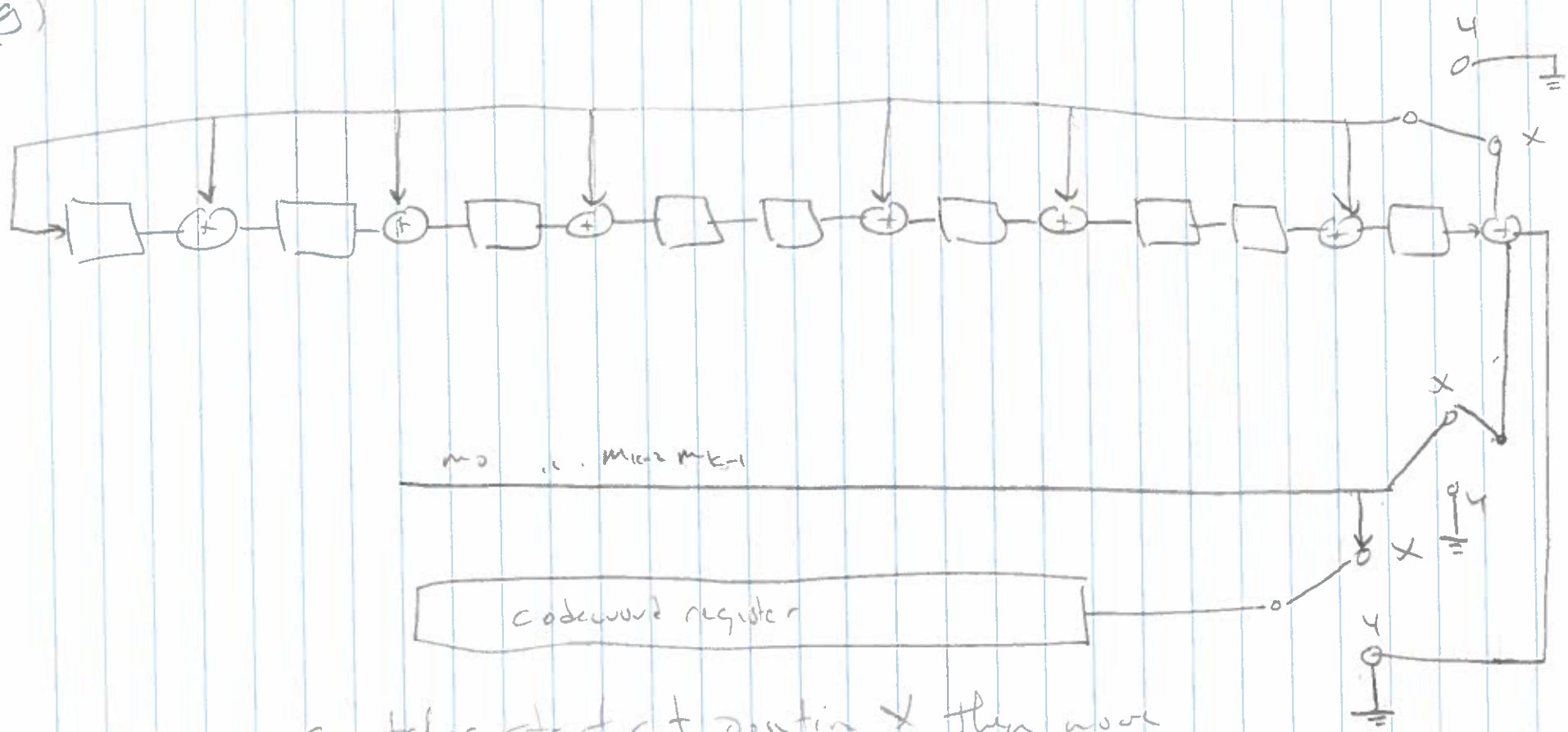
$$c = (0\,1\,0\,1\,0\,0\,0\,|\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,0\,0\,0 \ldots . 0)$$

LSB — parity bits — message



5

(9)



switches start at position X then move to position Y once the message word is fully loaded into the encoder.

(b) let $\beta = \alpha^5$ $g(x)$ has $\beta, \beta^2, \beta^3, \beta^4$ as roots $\rightarrow \delta = 4$ $d_{min} \geq \delta + 1$

$d_{min} \geq 5$

Question 2

$g(x)$ has to divide X^4+1

$X^4+1 = (X+1)^4$ therefore

$g_1(x) = X+1$

$g_2(x) = X^2+1$

$g_3(x) = X^3+X^2+X+1$

are all possible generator polynomials of of cyclic codes of length 4

$$X^6+1 = (X^3+1)(X^3+1) \text{ or } (X^3+1) = (X^2+X+1)(X+1)$$

$\therefore$ $g_1(x) = X+1$

$g_2(x) = X^2+1$

$g_3(x) = X^2+X+1$

$g_4(x) = X^3+1$

$g_5(x) = X^4+X^2+1$

$\Rightarrow$ $g_6(x) = X^4+X^3+X+1$

$g_7(x) = X^5+X^4+X^3+X^2+X+1$

it is possible to have cyclic codes of any length but it is not possible to have BCH codes of even length since $ord(\beta) = n$ and all $GF(2^m)$ elements must divide 2^m-1 which is odd, therefore all β in any $GF(2^m)$ field has odd order.

~~Yes, it is possible to have an even length cyclic code as long as n divides $2^m - 1$.~~

Question 3

$d_{min} \geq 4 \rightarrow \delta = 3$

need $\alpha^7, \alpha^{14} : \alpha^{21} = \alpha^6$ as roots

$\rightarrow GF(16) \rightarrow \quad \alpha^7, \alpha^{14} \rightarrow x^4+x^3+1$

$\alpha^6 \rightarrow x^4+x^3+x^2+x+1$

$$g(x) = (x^4+x^3+1)(x^4+x^3+x^2+x+1)$$

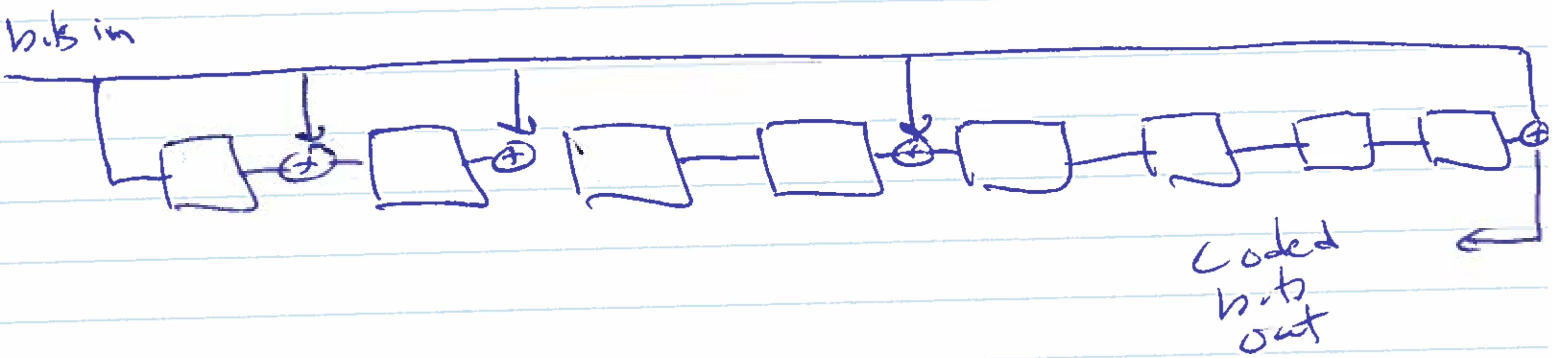
$$= x^8+x^7+x^6+x^5+x^4+x^7+x^6+x^5+x^4$$
$$+x^3+x^4+x^3+x^2+x+1$$

$$g(x) = x^8+x^4+x^2+x+1$$

$n-k = 8 \qquad n = 15$

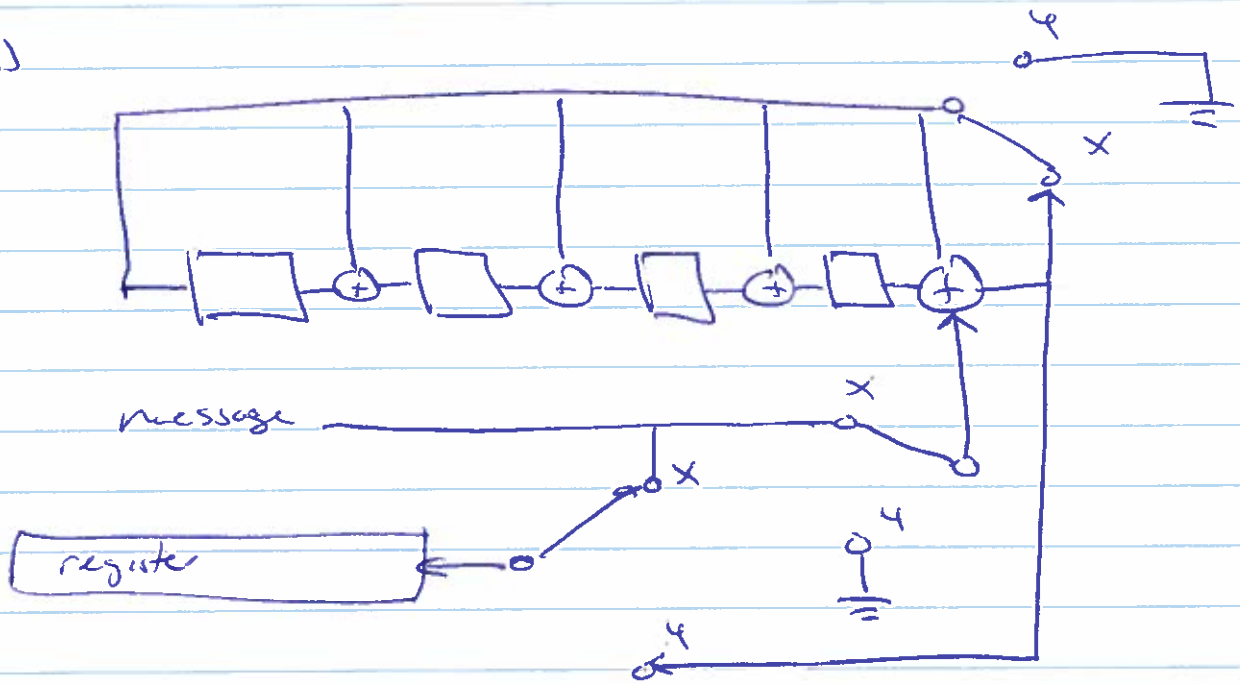
$k = 15-8 = 7$

$r = \frac{7}{15}$



Question 4

(a)



(b) BCH bound does not apply here because α^3 is a root of $s(x)$: α^3 only has order 5, BCH bound applies to codes of length $2^m - 1$ only if β is a primitive in $GF(2^m)$

$$m(x) = 1 + x$$
$$c(x) = (1+x)(1+x+x^2+x^3+x^4)$$
$$= 1 + x + x^2 + x^3 + x^4 + x + x^2 + x^3 + x^4 + x^5$$
$$= 1 + x^5 \rightarrow \text{weight } 2$$

if we find all codewords, we will find $d_{min} = 2$

(c) it can't even correct all single bit error patterns. $t = 0$

(d) it is clearly not a codeword since $r(x)$ is not divisible by $g(x)$. But since the code cannot even correct all error patterns of weight 1, we can't decode it. However the error has been detected.