Dependable Systems and Networks

HW #3

R07943098 劉治硯

Due Dec. 24, 2018

1. (20 points) To an n-bit word with a single parity bit (for a total of (n + 1) bits), a second parity bit for the (n+1)-bit word has been added. How would the error detection capabilities change?

It's same as before.
Adding a parity bit doesn't make difference on d(Min distance) on data or parity bits.

2. (20 points) Show that the Hamming distance of an M-of-N code is 2.

M-of-N: There are M bits of 1 in N bits code.
That means when a single bit error(having total (M+1) or (M-1) 1 in code) exist, it can be detected.
According to Distance property, at least (# of error detection) + 1 is needed.
So answer is 1+1=2

3. (20 points) Compare two parity codes for data words consisting of 64 data bits: (1) a (72; 8) Hamming code and (2) a single parity bit per byte. Both codes require eight check bits. Indicate the error correction and detection capabilities, the expected overhead, and list the types of multiple errors that are detectable by these two codes.

	(1)	(2)
correction	1 bit	0
detection	2 bits	1 bit
overhead	high	small
situation	detect 2 bit error but correct wrong for some 3 bit error	can detect odd bit error in same byte

4. (20 points) A communication channel has a probability of 10^{-3} that a bit transmitted on it is erroneous. The data rate is 12000 bps. Data packets contain 240 information bits, a 32-bit CRC for error detection, and 0, 8, or 16 bits for error correction coding (ECC). Assume that if eight ECC bits are added, all single-bit errors can be corrected, and if sixteen ECC bits are added all double-bit errors can be corrected.

(a) Find the throughput in information bits per second of a scheme consisting of error detection with retransmission of bad packets (i.e., no error correction).

(b) Find the throughput if eight ECC check bits are used, so that single-bit errors can be corrected. Uncorrectable packets must be retransmitted.

(c) Finally find the throughput if sixteen ECC check bits are appended, so that two-bit errors can be corrected. As in (b), uncorrectable packets must be retransmitted. Would you recommend increasing the number of ECC check bits from 8 to 16?

(a) $(1-10^{-3})^{(240+32)}$ *(240/272)*12000 = 8065bps

(b) $[(1-10^{-3})^{(240+32+8)}$ +280*$(1-10^{-3})^{(240+32+8-1)}]$*(240/280)*12000 = 9955bps

(c) $[(1-10^{-3})^{(240+32+16)}$+288$(1-10^{-3})^{(240+32+16-1)}$ +C(288, 2)*$(1-10^{-3})^{(240+32+16-2)}]$*(240/288)*12000 = 9966bps

From (b)'s and (c)'s answer above, adding ECC code increase throughput. we should do so

5. (20 points) Derive all codewords for the separable 5-bit cyclic code based on the generating polynomial X +1 and compare the resulting codewords to those for the nonseparable code.

	code word			code word	
Digit	nonseparable	separable	Digit	nonseparable	separable
0	00000	00000	8	11000	10001
1	00011	00011	9	11011	10010
2	00110	00101	10	11110	10100
3	00101	00110	11	11101	10111
4	01100	01001	12	10100	11000
5	01111	01010	13	10111	11011
6	01010	01100	14	10010	11101
7	01001	01111	15	10001	11110

6. (20 points) Given that $X^7 - 1 = (X + 1)g_1(X)g_2(X)$, where $g_1(X) = X^3 + X + 1$

(a) Calculate $g_2(X)$.

(b) Identify all the (7, k) cyclic codes that can be generated based on the factors of $X^7 - 1$. How many different such cyclic codes exist?

(c) Show all the codewords generated by $g_1(X)$ and their corresponding data words.

(a)X^3+X^2+1

(b)Combination of X^7-1 factors can make a cyclic code

$(X+1) \rightarrow$ (7,6) cyclic code

$g_1(X) \rightarrow$ (7,4) cyclic code

$g_2(X) \rightarrow$ (7,4) cyclic code

$(X+1)g_1(X) \rightarrow$ (7,3) cyclic code

$(X+1)g_2(X) \rightarrow$ (7,3) cyclic code

$g_1(X)g_2(X) \rightarrow$ (7,1) cyclic code

(c)

	code word			code word	
Data word	nonseparable	separable	Data word	nonseparable	separable
0	0000000	0000000	8	1011000	1000101
1	0001011	0001011	9	1010011	1001110
2	0010110	0010110	10	1001110	1010011
3	0011101	0011101	11	1000101	1011000
4	0101100	0100111	12	1110100	1100010
5	0100111	0101100	13	1111111	1101001
6	0111010	0110001	14	1100010	1110100
7	0110001	0111010	15	1101001	1111111

7. (20 points) Given a number X and its residue modulo-3, $C(X) = |X|_3$; how will the residue change when X is shifted by one bit position to the left if the shifted-out bit is 0? Repeat this for the case where the shifted-out bit is 1. Verify your rule for X = 01101 shifted five times to the left.

$C(X) = |X|_3$ means only (0,1,-1) will show up.

When msb of x = 0 $\rightarrow$ C(X) * (-1)

When msb of x = 1 $\rightarrow$ $(C(X)+(-1)^{\text{floor}(\log 2\ x)}) * (-1)$

initial: x = 01101, C(x)=1 => $C_{next}(x)$= -1

1. x = 11010, C(x)=-1 => $C_{next}(x)$= -1
2. x = 10100, C(x)=-1 => $C_{next}(x)$= -1
3. x = 01000, C(x)=-1 => $C_{next}(x)$= -1
4. x = 10000, C(x)=-1 => $C_{next}(x)$= 1
5. x = 00000, C(x)=1 => $C_{next}(x)$= 0