Date:2019/12/20
Designer:陳麒宇(r07943034)

Dependable Systems and Networks

HW #3

Due Jan. 6, 2020

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?

   The error detection capabilities will not change

   Code distance>=error capability+1

data	Odd parity bit		Code distance	Even parity bit		Code distance
	110101	110111		110101	110111	
1 parity bit	1	0	2	0	1	2
2 parity bits	10	00	2	00	10	2

   經由表格比對後可以發現，對於任何data bit的出錯數量來說，無論是在odd parity與even parity的error detection，我們可以知道使用1 parity bit與使用2 parity bits的error detection capability是相同的

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

   M-of-N code指的是在N-bit的codeword中有M bits為1，本題可以用兩種方式討論code distance：

   A. 第一種是對於single-bit-error來說，error的出現會使得整個codeword中1的總數加1或減1，被偵測到後parity bit也會改變，因此整體的bits改變數量為2
   B. 另一種是在codeword中出現兩個bits的error，他不會被偵測到因此parity bit不會改變，整體的bits的改變數量也是2，從而得知Hamming distance of an M-of-N code is 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) Hamming code	(2) single parity bit per byte
Error correction	Single error correction	None
Error detection	Double error detection	Single error detection
Overhead	higher	Lower
Types of multiple errors	可進行 double error detection，但是對於 3-bit error 可能會有不正確的 error correction	在相同 byte 中的偶數 bits 的錯誤無法偵測，但奇數 bits 的錯誤可正確偵測

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).

假設每個packet的傳輸只要發生錯誤就要重新傳遞，本題中每個packet有240+32 = 272bits，故完全沒錯的機率為(1-10^-3)^272 = 0.762

Data rate = 240/272 = 0.8824

Throughput = 0.762*0.8824*12000 = 8065(bit/sec)

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

假設每個packet的傳輸只要發生錯誤就要重新傳遞，本題中每個packet有240+32+8 = 280bits，故完全沒錯與錯一個的機率為C_0^{280}*(1-10^-3)^280 + C_1^{280}*(1-10^-3)^279*10^-3 = 0.9675

Data rate = 240/280 = 0.8571

Throughput = 0.9675*0.8571*12000 = 9951(bit/sec)

(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?

假設每個packet的傳輸只要發生錯誤就要重新傳遞，本題中每個packet有240+32+16 = 288bits，故完全沒錯與錯一個與錯兩個的機率為C_0^{288}*(1-10^-3)^288 + C_1^{288}*(1-10^-3)^287*10^-3 + C_2^{288}*(1-10^-3)^286*(10^-3)^2 = 0.9968

Data rate = 240/288 = 0.8333

Throughput = 0.9968*0.8333*12000 = 9967(bit/sec)

不建議增加check bits，因為增加8個ECC bits在throughput上僅增加約16(bit/sec)，對於整體的throughput沒有明顯的效益

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.

Data	Separable	Non-separable
0000	00000	00000
0001	00011	00011
0010	00101	00110
0011	00110	00101
0100	01001	01100
0101	01010	01111
0110	01100	01010
0111	01111	01001
1000	10001	11000
1001	10010	11011
1010	10100	11110
1011	10111	11101
1100	11000	10100
1101	11011	10111
1110	11101	10010
1111	11110	10001

Separable code與non-separable code的集合是重疊的，但是彼此對應的data有所不同

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 $g_2(X)$.

$g_2(X) = (X^7 - 1) / (X + 1)(X^3 + X + 1) = X^3 + X^2 + 1$

(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?

總共6種不同的cyclic codes，可以由(X + 1)、$g_1(X)$、$g_2(X)$互相組合而成：

$(X + 1)$ → (7, 6) cyclic codes

$g_1(X)$ → (7, 4) cyclic codes

$g_2(X)$ → (7, 4) cyclic codes

$(X + 1)g_1(X)$ → (7, 3) cyclic codes

$(X + 1) g_2(X)$ → (7, 3) cyclic codes

$g_1(X)g_2(X)$ → (7, 1) cyclic codes

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

In this problem, (7, 4) code with $g(X) = X^3 + X + 1$

Data	Separable	Non-separable
0000	0000000	0000000
0001	0001011	0001011
0010	0010110	0010110
0011	0011101	0011101
0100	0100111	0101100
0101	0101100	0100111
0110	0110001	0111010
0111	0111010	0110001
1000	1000101	1011000
1001	1001110	1010011
1010	1010011	1001110
1011	1011000	1000101
1100	1100010	1110100
1101	1101001	1111111
1110	1110100	1100010
1111	1111111	1101001

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.

若X = 01101且$C(X) = |X|_3 = \{-1, 0, 1\}$

C'(X)		Shifted-out	
		0	1
C(X)	0	0	1
	1	-1	0
	2	1	-1

A. X = 11010 → C(X) = -1

B. X = 10100 → C(X) = -1

C. X = 01000 → C(X) = -1

D. X = 10000 → C(X) = 1

E. X = 00000 → C(X) = 0