Introduction to Coding

Exercise 1: Compute the modulo-4 checksum, C, of a frame with byte values 3, 1, and 2. What values would be transmitted in the packet? What would be the value of the sum at the receiver if there were no errors? Determine the sum if the received frame was: 3, 1, 1, C? 3, 1, 2, 0, C? 1, 2, 3, C?

$6 + c = 0$

what is c?

$c = 4 - (\text{sum} \bmod 4)$

$= 4 - (6 \bmod 4)$

$= 4 - 2 = 2$

3	1	2	c=2

no errors: $(3+1+2+2) \bmod 4 = 0$

$(3+1+1+2) \bmod 4 = 3$

error detected.

$(3+1+2+0+2) = 0$

added zero not detected.

$(1, 2, 3, 2) = 0$

permutation not detected.

Exercise 2: What is a modulo-2 sum? What is the modulo-2 sum of 1, 0 and 1? What is the modulo-2 sum if the number of 1's is an even number?

modulo-2 sum = remainder after divide by 2

= l.s. bit of binary number

= 1 if odd, 0 if even.

$1+0+1 \bmod 2 = 2 \bmod 2 = 0$

0 ("even parity").

Exercise 3: A (5,3) code computes the two parity bits as: $p_0 = d_0 \oplus d_1$ and $p_1 = d_1 \oplus d_2$ where d_i is the i'th data bit. What codeword is transmitted when the data bits are $(d_0, d_1, d_2) = (0, 0, 1)$? How many different codewords are there in the code? What are the first four codewords? In general, how many codewords are there for an (n, k) code?

$d_0 \; d_1 \; d_2$

$$\underbrace{\underbrace{0\;\;0\;\;1}_{d,\;k=3}\;\;\underbrace{\underset{p_0}{0}\;\;\underset{p_1}{1}}_{n-k=2}}_{n=5}$$

$p_0 = d_0 \oplus d_1$

$p_1 = d_1 \oplus d_2$

$8 = 2^3 = 2^k$ valid codewords

general case

Exercise 4: What is the Hamming distance between the codewords 11100 and 11011? What is the minimum distance of a code with the four codewords 0111, 1011, 1101, 1110?

$$\begin{array}{r} 1\,1\,1\,0\,0 \\ \oplus\; 1\,1\,0\,1\,1 \\ \hline 0\,0\,\underbrace{1\,1\,1} \end{array}$$

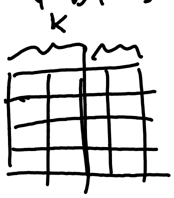
3 bits differ $\Rightarrow d = 3$

	0111	1011	1101	1110
0111	0	2	2	2
1011		0	2	2
1101			0	2
1110				0

$d_{min} = 2$

Exercise 5: What is the code rate of a code with 4 codewords each of which is 4 bits long? *Hint: If a code has* 2^k *codewords, what is* k*?*.

4 bits in each c/w $\rightarrow n = 4$



$$k = \log_2(\#\text{of c/w}) = \log_2 4 = 2$$

$$\text{rate} = \frac{k}{n} = \frac{2}{4} = \frac{1}{2}$$

Exercise 6: The data rate over the channel is 50 Mb/s; a rate 1/2 code is used. What is the throughput?

50 Mb/s $\rightarrow$ $\frac{1}{2} = \frac{k}{n}$ 25 Mb/s is useful data & throughput.

Exercise 7: Write the addition and multiplication tables for $GF(2)$. What logic function can be used to implement modulo-2 addition? Modulo-2 multiplication?

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

Exercise 8: What is the polynomial representation of the codeword 01101?

$$0x^4 + 1x^3 + 1x^2 + 0x + 1x^0$$

$$= x^3 + x^2 + 1$$

Exercise 9: What is the result of multiplying $x^2 + 1$ by $x^3 + x$ ~~if the coefficients are regular integers?~~ If the coefficients are values in $GF(2)$? Which result can be represented as a bit sequence?

$$
\begin{array}{r}
x^2 + 1 \\
x^3 + x \\
\hline
x^3 + x \\
x^5 + x^3 + \\
\hline
x^5 + 0x^3 + x \\
= x^5 + x
\end{array}
\qquad \longleftrightarrow \qquad
\begin{array}{cccccccc}
x^5 & x^4 & x^3 & x^2 & x^1 & x^0 & & \\
\hline
 & & & 1 & 0 & 1 & & \\
 & & 1 & 0 & 1 & 0 & & \\
\hline
 & & & 0 & 0 & 0 & \leftarrow & 0 \\
 & & 1 & 0 & 1 & & \leftarrow & 1 \\
 & 0 & 0 & 0 & & & \leftarrow & 0 \\
1 & 0 & 1 & & & & \leftarrow & 1 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & & \\
\end{array}
$$

$$= x^5 + x$$

$x^3 \quad x^2 \quad x \quad x^0$

Exercise 10: If the generator polynomial is $G(x) = x^3 + x + 1$ and the data to be protected is 1001, what are $n - k$, $M(x)$ and the CRC? Check your result. Invert the last bit of the CRC and compute the remainder again.

$n - k = 3 =$ order of $G(x)$

$$M(x) = \underbrace{\overbrace{1001}^{k}\ \overbrace{\_\ \_\ \_}^{n-k}}_{n}$$

$G(x) = 1011$

$$\frac{M(x)}{G(x)} = 1011 \overline{)1001000}$$

```
         1010
     _________
1011 ) 1001000
       1011
       ----
        0100
        0000
        ----
         1000
         1011
         ----
          0110
          0000
          ----
           110
```

transmit

```
1011 ) 1001110
       1011
       ----
         1011
         1011
         ----
          000   remainder = 0
```

msg → 1001110

error → 11101

```
1011 ) 1110100
       1011
       ----
        1011
        1011
        ----
           0
```

Exercise 11: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors ~~evenly~~ randomly distributed within the message? 1024 bits

$0 - 0 \; \underbrace{e \; e \; e \quad\quad}_{31} \; 0 \; 0 \; 0$

yes. any error burst length ≤ 31 bits will be detected.

No. it could be a multiple of $G(x)$ (although unlikely).

$$
\begin{array}{rl}
\overbrace{101100}\;\, & G(x) \cdot x^2 \\
10110\;\, & G(x) \cdot x \\
\hline
111010\;\, &
\end{array}
$$

$G(x) \cdot (x^2 + x)$

Exercise 12: What is the probability that a CRC of length $n-k$ bits will be the correct CRC for a randomly-chosen codeword? Assuming random data, what is the undetected error probability for a 16-bit CRC? For a 32-bit CRC?

$\dfrac{1}{2^{n-k}}$

for $n-k = 16$ U.E.P. $= \dfrac{1}{2^{16}} \approx 10^{-5}$

32 $\dfrac{1}{2^{32}} \approx 10^{-9}$