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?

$3+1+2=6$, $C = 6 \bmod 4 = 2$

would transmit 3, 1, 2, 2.

sum is $3+1+2+2 = 8$

$3+1+1+2 \bmod 4 = 3$ ← error

$3+1+2+0+2 \bmod 4 = 0$ ← does not detect extra 0

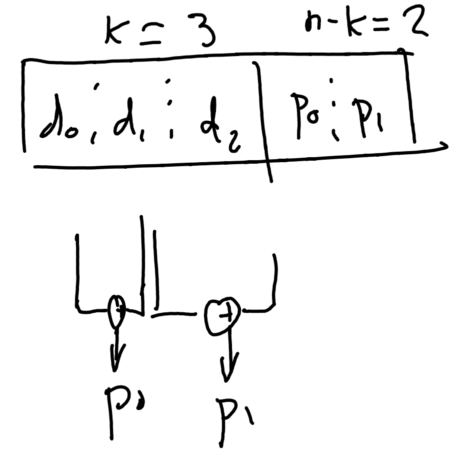
$1+2+3+2 \bmod 4 = 0$ ← does not detect change in order

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?

- remainder after divide by 2.
- $1+0+1 \bmod 2 = 2 \bmod 2 = \underline{\underline{0}}$
- zero

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?

$n = 5$



$p_0 = d_0 \oplus d_1$

$p_1 = d_1 \oplus d_2$

$2^k = 8$ valid codewords.

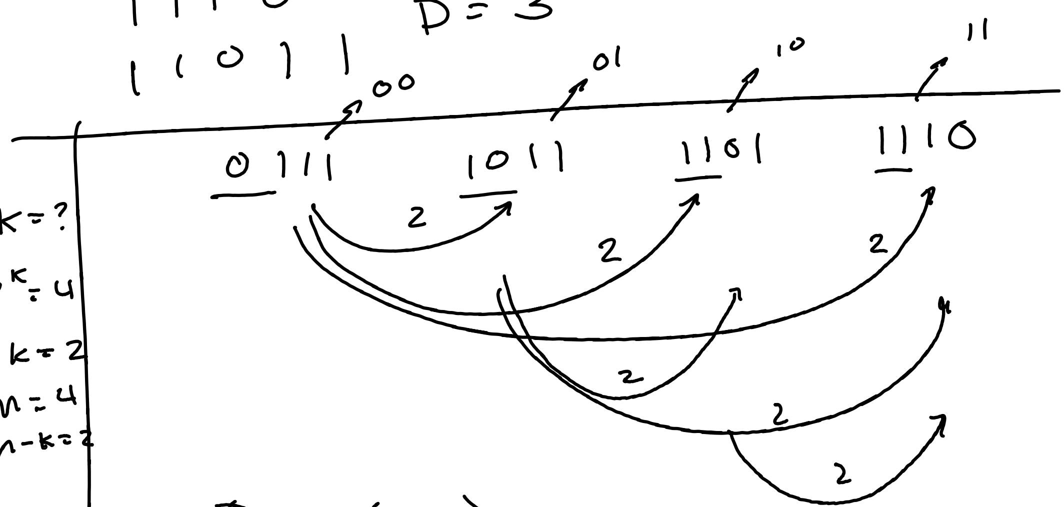
d_0	d_1	d_2	p_0	p_1
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	1	1	1	0
1	0	0	1	0
1	0	1	1	1
1	1	0	0	1
1	1	1	0	0

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?

11100
11011

$D = 3$

$k = ?$
$2^k = 4$
$k = 2$
$n = 4$
$n-k = 2$



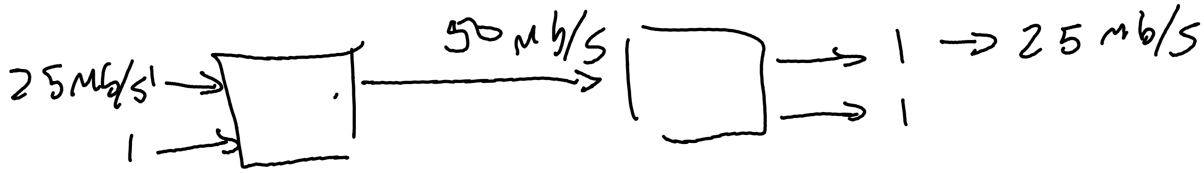
$D_{min}\ (d_{min}) = 2$

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?*.

if $2^k = 4$ $\quad k = \log_2 4 = 2$

$n = 4$, 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?



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

XOR

×	0	1
0	0	0
1	0	1

AND

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

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

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

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?

$(x^2+1)(x^3+x)$

$x^5 + x^3 + x^3 + x$

if normal arithmetic:

$x^5 + 2x^3 + x$

if GF(2) coefficients:

only this one is a bit sequence. $\rightarrow x^5 + x$

$$
\begin{array}{r}
1x^2 + 0x + 1x^0 \\
1x^3 + 0x^2 + 1x + 0x^0 \\
\hline
1
\end{array}
$$

1, 0, 1

$$
\begin{array}{r}
101 \\
1010 \\
\hline
1010 \\
101000 \\
\hline
110010
\end{array}
$$

$x^5 + x^4 + x$

no carries

100010

$x^5 + x$

GF( ) { element 0, 1; operation

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.

$n-k=3$ (# of bits in remainder = order of $G(x)$)

$k = 4$

$n-k=3$

$M(x) = (x^3 + 1) \cdot x^3$

$= x^6 + x^3$

$= 1x^6 + 0x^5 + 0x^4 + 1x^3 + \underline{0x^2 + 0x + 0}$

Calculate Remainder

$$
\begin{array}{r}
1x^3 \quad 0x^2 \quad 1x \\
1x^3 + 0x^2 + 1x + 1x^0 \,\big)\, 1x^6 + 0x^5 + 0x^4 + 1x^3 + 0 \quad 0 \quad 0 \\
1x^6 + 0 \quad 1x^4 + 1x^3 \\
\hline
0 \quad 0 + 1 + 0 \quad 0 \quad 0 \\
1x^3 + 0 \quad 1 \quad 1x^0 \\
\hline
0 \quad 0 \quad 1 \quad 1 \quad 0
\end{array}
$$

$\underbrace{1\,1\,0}_{\text{remainder}}$ = CRC

we transmit $M(x)$ + remainder

$= \underbrace{\overbrace{1001}^{k=4}\ \overbrace{110}^{n-k=3}}_{n=7}$

$$
\begin{array}{r}
100 \\
1011 \,\big)\, 1001110 \\
1011 \\
\hline
01011 \\
1011 \\
\hline
0000
\end{array}
$$

$$
\begin{array}{r}
0001 \\
1011 \,\big)\, 0001010 \\
0010 \\
\hline
0101 \\
\hline
1010 \\
1011 \\
\hline
1
\end{array}
$$

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

- Yes.
- No, may not be detected.

e.g.:

```
101
  101
    101
-------
1000001 ←
```

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?

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

$$\frac{1}{2^{16}} \approx 10^{-5}$$

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