Introduction to Coding

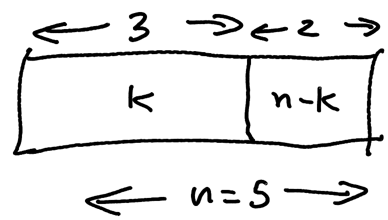
Exercise 1: What is a modulo-2 sum? What is the modulo-2 sum of 1, 0 and 1? What is the modulo-2 sum if the number of 1's is an even number?

mod(sum of bits , 2)

$1+0+1=2 \quad \mathrm{mod}(2,2)=0$

if # 1's is even then modulo-2 sum is 0.

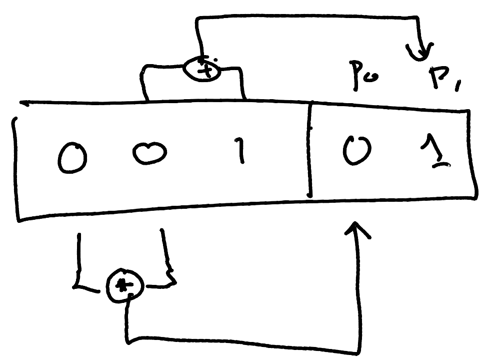
$n=5,\ k=3$



Exercise 2: 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?

$d_0 \ d_1 \ d_2 \ p_0 \ p_1$

$p_0 = d_0 \oplus d_1 = 0$
$p_1 = d_1 \oplus d_2 = 1$



there are $2^k = 2^3 = 8$ possible (correct) codewords.

data			parity	
0	0	0	0	0
0	0	1	0	1
0	1	0	1	1
0	1	1	1	0

There are 2^k valid codewords for an (n,k) code.

Exercise 3: 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?

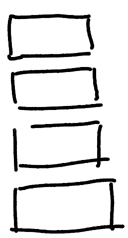
$$\begin{array}{r} 11100 \\ \oplus\ 11011 \\ \hline \end{array}$$

$0+0+1+1+1 = 3 = d$

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

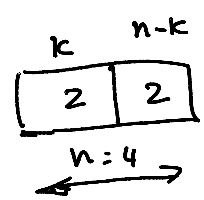
$d_{min} = 2$

Exercise 4: 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*?*.



$2^k = 4 \qquad k = 2$

$n = 4$



Exercise 5: The data rate over the channel is 50 Mb/s; a rate 1/2 code is used. What is the throughput?

↳ average data bits received per unit time.

50 Mb/s < $\frac{1}{2}$ of bits are data 25 Mb/s → throughput.

$\frac{1}{2}$ of bits are parity 25 Mb/s

Exercise 6: Write the addition and multiplication tables for $GF(2)$. What logic function can be used to implement modulo-2 addition? Modulo-2 multiplication?

for $GF(2)$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Exercise 7: What is the polynomial representation of the codeword 01101?

$$\rightarrow \quad 0 \quad 1 \quad 1 \quad 0 \quad 1$$

$$\rightarrow 0x^4 + 1x^3 + 1 \cdot x^2 + 0x^1 + 1x^0 = x^3 + x^2 + 1 \leftarrow$$

Exercise 8: 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?

$$\begin{array}{rrrrrr}
 & & & 1x^2 & + 0x^1 & + 1x^0 \\
 & & 1x^3 & + 0x^2 & + 1x^1 & + 0x^0 \\
\hline
 & & & 0x^2 & 0x^1 & + 0x^0 \\
 & & 1x^3 & + 0x^2 & + 1x^1 & \\
0 & 0 & 0 & & & \\
1x^5 & 0x^4 & 1x^3 & & & \\
\hline
1x^5 & + 0x^4 & + 2x^3 & + 0x^2 & + 1x & + 0x^0
\end{array}$$

if used modulo-2 addition:

1 0 0 0 1 0

which can be a bit sequence.

Exercise 9: 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 any one to three bits of the message and compute the remainder again. Add the generator polynomial, or a shift of it, to the message and compute the CRC again.

$G(x) = x^3 + 0x^2 + x + 1$ (4 terms).

$\hookrightarrow n-k = 3$

$M(x) = (1x^3 + 0x^2 + 0x + 1)\, x^3$

$= x^6 + x^3 \Rightarrow 1001000$

$\frac{M(x)}{G(x)} =$

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

$x^3 + 0x^2 + x + 1 \,\big)\, x^6 + 0x^5 + 0x^4 + 1x^3 + 0x^2 + 0x + 0$

$x^6 + 0x^5 + 1x^4 + 1x^3$

0 0 1 0 0

0 0 0 0

1 0 0 0

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

0 1 1 0

1 1 0

CRC = R(x) $\longrightarrow$ 1 1 0

message = 1001110

1011) 1001110

1011

0101

1011

1011

0000 ✓

CRC check passes.

01

1011) 0111110

1111

1011

1001

1011

0100

100 ← not zero check fails

message = 1001110

1011

1000101

1011) 1000101

1011

0111

1110

1011

1011

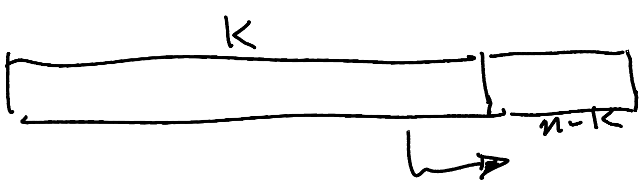
1011

000 → CRC passes!

Exercise 10: Is a 32-bit CRC guaranteed to detect 30 consecutive errors? How about 30 errors evenly distributed within the message?

- Yes because a 30-bit error polynomial cannot be a multiple of $G(x)$.
- Possible, if these 30 errors are a multiple of $G(x)$.

Exercise 11: 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?



for any given k bits only one correct CRC.

probability that n-k random bits are this (correct) CRC are $\frac{1}{2^{n-k}}$.

if $n-k = 16$ probability of random message passing CRC check $\frac{1}{2^{16}} \approx 1$ in 65K.

$n-k = 32$ prob. $\frac{1}{2^{32}} \approx$ 1 in 4×10^9