CSN08704

Telecommunications

5: Error Coding

Data, Audio, Video and Images

http://asecuritysite.com/comms

Prof Bill Buchanan

CSN08704

Telecommunications

5: Error Coding: Modulo-2

Data, Audio, Video and Images

http://asecuritysite.com/comms

Prof Bill Buchanan

Modulo-2

Digital coding uses modulo-2 arithmetic where addition becomes the following operations:

- 0+0=0 1+1=0
- 0+1=1 1+0=1

It performs the equivalent operation to an exclusive-OR (XOR) function. For modulo-2 arithmetic, subtraction is the same operation as addition:

- 0–0=0 1–1=0
- 0–1=1 1–0=1

Multiplication is performed with the following:

- $0\times0=0$ $0\times1=0$
- $1\times0=0$ $1\times1=1$

which is an equivalent operation to a logical AND operation.

Binary Manipulation

- Link.

10111	x^4+x^2+x+1
1000 0001	x^7+1
1111 1111 1111 1111	$x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1$
10101010	$x^6+x^4+x^2+x$

For example:	101×110
is represented as:	$(x^2+1)\times(x^2+x)$
which equates to:	$x^4+x^3+x^2+x$
which is thus:	11110

Binary Manipulation

- $x^4+x^4+x^2+1+1$ becomes x^2

as $x^4+x^4=0$

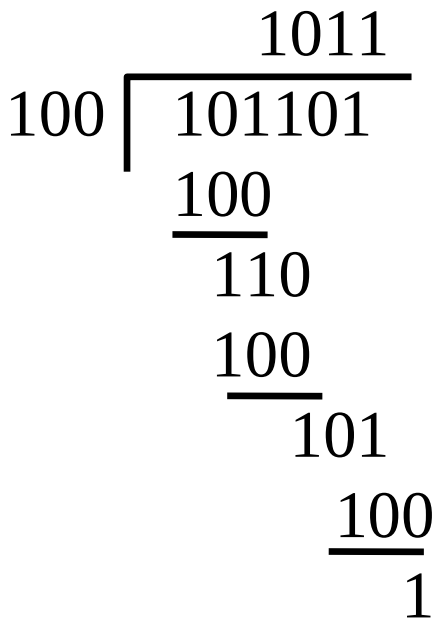
Binary Manipulation

- Link.

Thus:	10101×01110
is represented as:	$(x^4+x^2+1)\times(x^3+x^2+x)$
which equates to:	$x^7+x^6+x^5+x^5+x^4+x^3+x^3+x^2+x$
which equates to:	$x^7+x^6+x^4+x^2+x$
which is thus:	11010110

Modulo-2 Division

- Link.



Hamming distance

- Hamming difference between 101101010 and 011101100? Link.
- The Hamming distance can be used to determine how well the code will cope with errors. The minimum Hamming distance $\min\{d(C_1,C_2)\}$ defines by how many bits the code must change so that one code can become another code.
- A code C can **detect** up to N errors for any code word if $d(C)$ is greater than or equal to $N+1$ (that is, $d(C) \geq N+1$).
- A code C can **correct** up to M errors in any code word if $d(C)$ is greater than or equal to $2M+1$ (that is, $d(C) \geq 2M+1$).

Error detection

- For example: {00000, 01101, 10110, 11011} has a Hamming distance of 3. Link.

- $d(C) \geq N+1$

- d(C) is 3, thus N must be 2. So we can detect one or two bits in error in the code.

- Eg 00000 could become 01010 ... and this will be detected as an error, as the code does not exist.

Error correction

- For example: {00000, 01101, 10110, 11011} has a Hamming distance of 3. Link.

- $d(C) \geq 2M+1$

- d(C) is 3, thus M must be 1. So we can correct one bit in error in the code.

- Eg 00000 could become 00010 ... and as the nearest code will be “00000”.

Examples

- What is the Hamming distance of {00000000, 11111111, 11110000, 01010101} Link? How many errors can be detected? How many errors can be corrected?
- What is the Hamming distance of {10111101011, 10011111011, 11110101011, 10100101011, 10111101000} Link?

CSN08704

Telecommunications

5: Error Coding: Error Correction

Data, Audio, Video and Images

http://asecuritysite.com/comms

Prof Bill Buchanan

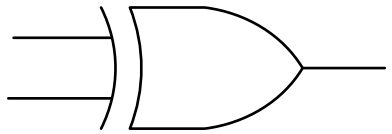
Linear and cyclic codes

- **Linear Code:** sum of any two codes equals another code - {00, 01, 10, 11} and {00000, 01101, 10110, 11011}.
- **Cyclic Codes:** Linear Code + When a cyclic shift also gives a code word - {0000, 0110, 0011, 1001, 1100, 0001, 0010, 0100, 1000}
- Is {000, 010, 011, 100, 001} cyclic?

Block parity

- Odd parity (make number of 1s odd) or Even parity (make number of 1s even).
- Detects single bit errors.
- Cannot detect when two bits in error in the same position.
- Example (binary). Link.
- Example (int). Link.

1	0000 0001
4	0000 0100
12	0000 1100
–1	1111 1111
–6	1111 1010
17	0001 0001
0	0000 0000
–10	1111 0110
	1110 1011



CSN08704

Telecommunications

Cyclic Redundancy Check

Data, Audio, Video and Images

Cyclic redundancy checking (CRC)

Example: We have 32, and make it divisible by 9, we add a ‘0’ to make ‘320’, and now divide by 9, to give 35 remainder 4. So lets add ‘4’ to make 324. Now when it is received we divide by 9, and if the answer is zero, there are no errors, and we can ignore the last digit.

CRC-CCITT: $x^{16}+x^{12}+x^5+1$

$x^{16}+x^{12}+x^5+1$ G(x)

- The error correction code is 16 bits long and is the remainder of the data message polynomial G(x) divided by the generator polynomial P(x) ($x^{16}+x^{12}+x^5+1$, i.e. 1000100000100001).
- The quotient is discarded and the remainder is truncated to 16 bits. This is then appended to the message as the coded word.

CRC Example

- Example. Link.

For a 7-bit data code 1001100 determine the encoded bit pattern using a CRC generating polynomial of $P(x) = x^3 + x^2 + x^0$. Show that the receiver will not detect an error if there are no bits in error.

$P(x) = x^3 + x^2 + x^0$ (1101)
$G(x) = x^6 + x^3 + x^2$ (1001100)

Multiply by the number of bits in the CRC polynomial.

$x^3(x^6 + x^3 + x^2)$
$x^9 + x^6 + x^5$ (1001100000)

Figure 5.3 shows the operations at the transmitter. The transmitted message is thus:

1001100001

```
          1111101
      ┌─────────
1101  │1001100000
       1101
       ----
        1001
        1101
        ----
        1000
        1101
        ----
        1010
        1101
        ----
        1110
        1101
        ----
        1100
        1101
        ----
         001
```

Figure 5.3

CRC (Receiving)

- Example. Link.

For a 7-bit data code 1001100 determine the encoded bit pattern using a CRC generating polynomial of $P(x) = x^3 + x^2 + x^0$. Show that the receiver will not detect an error if there are no bits in error.

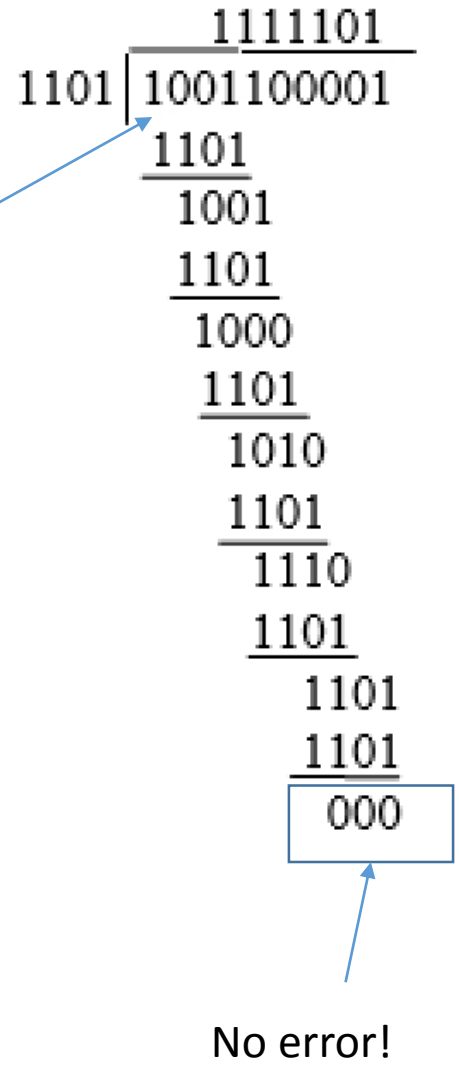
$P(x) = x^3 + x^2 + x^0$ (1101)
$G(x) = x^6 + x^3 + x^2$ (1001100)

Multiply by the number of bits in the CRC polynomial.

$x^3(x^6 + x^3 + x^2)$
$x^9 + x^6 + x^5$ (1001100000)

Figure 5.3 shows the operations at the transmitter. The transmitted message is thus:

1001100001



LRC/VRC

- Link.

	F	r	e	d	d	y	LRC
b0	0	0	1	0	0	1	**0**
b1	1	1	0	0	0	0	**0**
b2	1	0	1	1	1	0	**0**
b3	0	0	0	0	0	1	**1**
b4	0	1	0	0	0	1	**0**
b5	0	1	1	1	1	1	**1**
b6	1	1	1	1	1	1	**0**
VRC	0	1	1	0	0	0	**1**

CSN08704

Telecommunications

Hamming Code

Data, Audio, Video and Images

http://asecuritysite.com/comms

Prof Bill Buchanan

Hamming Codes

Error correction: *m* is number of bits in the data symbol

n is number of Hamming bits

$$2^n \geq m + n + 1$$

Eg if we have 4 bits (*m*=4). Then to correct we need *n*=3 (as 8 is greater than or equal to 4+3+1).

How many error correcting bits would be need for 5 bits?

Hamming Codes

The character is `011001`

The Hamming bits are `HHHH`

The message format will be `01H100H1HH`

Position	Code
9	1001
7	0111
3	0011
XOR	1101

10	9	8	7	6	5	4	3	2	1
0	1	1	1	0	0	1	1	0	1

Hamming Codes

10	9	8	7	6	5	4	3	2	1
0	1	1	1	0	0	1	1	0	1

Position	*Code*
Hamming	1101
9	1001
7	0111
3	0011
XOR	0000

No error

Error in bit 5

Position	*Code*
Hamming	1101
9	1001
7	0111
5	0101
3	0011
XOR	0101

Hamming Code

Sending:

$$P_1 = D_1 \oplus D_2 \oplus D_4$$
$$P_2 = D_1 \oplus D_3 \oplus D_4$$
$$P_3 = D_2 \oplus D_3 \oplus D_4$$

111 110 101 **1**00 011 0**1**0 00**1**

D_4 D_3 D_2 P_3 D_1 P_2 P_1

Receiving:

$$S_1 = P_1 \oplus D_1 \oplus D_2 \oplus D_4$$
$$S_2 = P_2 \oplus D_1 \oplus D_3 \oplus D_4$$
$$S_3 = P_3 \oplus D_2 \oplus D_3 \oplus D_4$$

Hamming Code

$$\mathrm{T} = \begin{bmatrix} P_1 & P_2 & D_1 & P_3 & D_2 & D_3 & D_4 \end{bmatrix}$$

$$\mathrm{T}^{\mathrm{T}} = \begin{bmatrix} P_1 \\ P_2 \\ D_1 \\ P_3 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix}$$

$$\mathrm{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$\longleftarrow$ Check of P_1

$\longleftarrow$ Check of P_2

$\longleftarrow$ Check of P_3

$$\mathrm{HT}^{\mathrm{T}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ D_1 \\ P_3 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix}$$

Hamming Code (receiving)

- At the receiver we calculate the Syndrome matrix **S** ... if all zeros ... no error!

$$\mathbf{S} = \mathbf{H}\mathbf{R}^{\mathrm{T}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ D_1 \\ P_3 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \end{bmatrix}$$

Hamming Code (Example)

- Link.

$$\mathbf{T} = [P_1 \quad P_2 \quad D_1 \quad P_3 \quad D_2 \quad D_3 \quad D_4]$$

and $D_1=1, D_2=0, D_3=1, D_4=0$

for even parity:

P_1 checks the 1st, 3rd, 5th and 7th, so $P_1 \oplus D_1 \oplus D_2 \oplus D_4 = 0$; thus $P_1 = 1$
P_2 checks the 2nd, 3rd, 6th and 7th, so $P_2 \oplus D_1 \oplus D_3 \oplus D_4 = 0$; thus $P_2 = 0$
P_3 checks the 4th, 5th, 6th and 7th, so $P_3 \oplus D_2 \oplus D_3 \oplus D_4 = 0$; thus $P_3 = 1$

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{T}^T = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{matrix} \\ \\ \leftarrow D_1 \\ \\ \leftarrow D_2 \\ \leftarrow D_3 \\ \leftarrow D_4 \end{matrix}$$

Hamming Code

- Let's check the Syndrome matrix:

$$\mathbf{HT}^{\mathrm{T}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1.1 \oplus 0.0 \oplus 1.1 \oplus 0.1 \oplus 1.0 \oplus 0.1 \oplus 1.0 \\ 0.1 \oplus 1.0 \oplus 1.1 \oplus 0.1 \oplus 0.0 \oplus 1.1 \oplus 1.0 \\ 0.1 \oplus 0.0 \oplus 0.1 \oplus 1.1 \oplus 1.0 \oplus 1.1 \oplus 1.0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

No error!

Hamming Code

Error:

Error in bit 5

$$\mathbf{R} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\mathbf{HR}^{\mathrm{T}} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1.1 \oplus 0.0 \oplus 1.1 \oplus 0.1 \oplus 1.1 \oplus 0.1 \oplus 1.0 \\ 0.1 \oplus 1.0 \oplus 1.1 \oplus 0.1 \oplus 0.1 \oplus 1.1 \oplus 1.0 \\ 0.1 \oplus 0.0 \oplus 0.1 \oplus 1.1 \oplus 1.1 \oplus 1.1 \oplus 1.0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

CSN08704

Telecommunications

5: Error Coding

Data, Audio, Video and Images

http://asecuritysite.com/comms

Prof Bill Buchanan