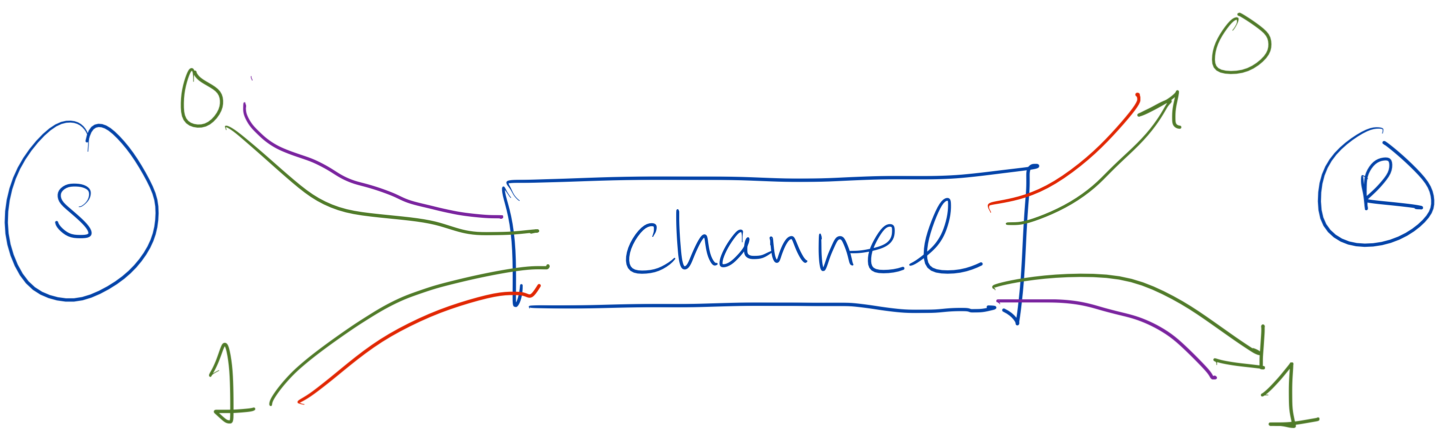
4/17

- Error Correction vs. Detection

Channel Model

- Binary Symmetric Channel



In general

send $D \mid C$ (D: Data, C: $f(D)$)

recv $D' \mid C'$

Accept iff $f(D') = C'$

CRC : Cyclic Redundancy Code

n+1 message bits represented as degree n polynomial.

7	6	5	4	3	2	1	0
1	0	0	1	1	0	1	0

$$\equiv$$

$$\underbrace{x^7 + x^4 + x^3 + x}_{P(x)}$$

$d(P(x)) = \boxed{7}$,

terms = $\boxed{4}$

CRC

Sender & Receiver agree on a divisor poly $G(x)$ of degree k

$d(G) = k$

Data to send : $M(x)$

Transmit $T(x)$

$$T(x) \leftarrow M(x) * x^{k} + R(x)$$

s.t. $G(x) \mid T(x)$

Mapping back

$\downarrow$

$T = M \# C$ $\qquad$ $\sum_{i=0}^{n} \underbrace{\alpha_i}_{GF2} x^i$

$\downarrow$

$R = T + E$

$E = 0$

C say NO error

$\downarrow$

✓

$E \neq 0$

$G \nmid E$

$\downarrow$

C says err

✓

$E \neq 0$

$G \mid E$

$\downarrow$

crc says No err

✗

CRC

All poly coef. are in
GF(2) ← Galois Field

elements of GF(2):
$\{0, 1\}$

Addition ≡ Subtractⁿ ≡ XOR

in GF(2)

$A(x)$ can divide $B(x)$
iff $d(A(x)) \le d(B(x))$

Assume $G(x) = \underbrace{x^3 + x^2 + 1}_{1101}$

$M(x) =$

$x^7 + x^4 + x^3 + x$] 10011010

$$
\begin{array}{l}
1101 \;\big)\; \underbrace{10011010}_{M}\,000 \\
\quad 1101 \\
\quad \overline{01001} \\
\quad\;\; 1101 \\
\quad\;\; \overline{1000} \\
\quad\;\; 1101 \\
\quad\;\;\; \overline{1011} \\
\quad\;\;\; 1101 \\
\quad\;\;\;\; \overline{1100} \\
\quad\;\;\;\; 1101 \\
\quad\;\;\;\;\; \overline{1000} \\
\quad\;\;\;\;\; 1101 \\
\quad\;\;\;\;\;\; \overline{101}
\end{array}
$$

1000

$T = M * x^k + R$

↓

$\underbrace{10011010}_{M}\underbrace{101}_{CR}$

K

R → 101

Constructing $T(x)$

$$L = M(x) \ll k$$

Divide L by G, α remainder

$$T(x) = L + \alpha$$

---

what do we receive?

$$R(x) = T(x) + \underbrace{E(x)}_{\text{error}}$$

crc passes iff

$$G(x) \mid R(x)$$

Characterising $E(x)$

Suppose single bit error

$$
\begin{array}{lcccccccccccc}
T(x)= & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
 & B & A & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
\\
R(x)= & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
 & B & A & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0
\end{array}
$$

what is $E(x)$?

$$x^7 + \underbrace{x^3 + x^2 + \cancel{1}}$$

$$R = T(x) + G(x)$$

$$G \mid R \Leftarrow G \mid T \wedge G \mid G$$

odd # of errors

$E(x)$ has odd number of terms

To detect odd # of errors:

make $G(x) = (x+1)\,P(x)$

i.e. $x+1$ is a factor of $G(x)$

Recall: CRC fails iff $G(x) \mid E(x)$

Lemma:

$\nexists$ no poly in $GF(2)$ w/ $x+1$ as a factor w/ an odd # of terms

$E = G\alpha$

$G = (x+1)\beta$

$E = (x+1)\alpha\beta$

if this is true what do we know?

E has odd # of terms

$x+1 \mid G$ CRC will fail

iff $G \mid E \Rightarrow x+1 \mid E$

Lemma:

$\exists$ no poly in GF(2)

w/ x+1 as a factor

ē an odd # of

terms

Proof: Suppose not.

$$E(x) = \underbrace{(x+1) * Q(x)}_{2n+1 = \text{odd \# of terms}}$$

$$E(1) = 2n\underset{x^a + x^b}{(1+1)} + 1 = 1$$

Also

$$E(1) = (1+1) * Q(x) = 0$$

#

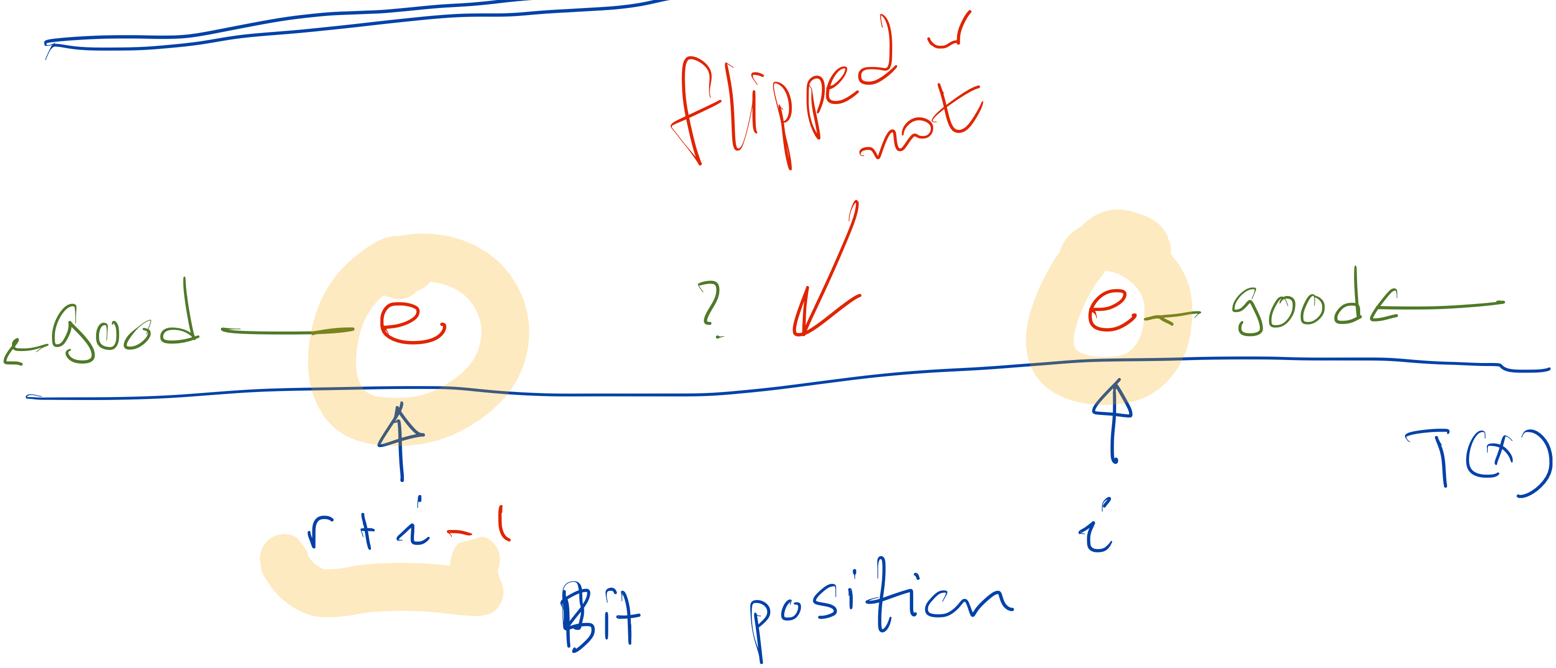
odd # of terms

$\downarrow$

$$\underbrace{x^a + x^b + \ldots x^\alpha}_{\text{odd number of } x^i}$$

$$\underbrace{(x^a + x^b)}_{\substack{n \text{ of these} \\ \| \\ 0}} + \underbrace{x^\alpha}_{1}$$

Burst Errors



r-bit burst starting @ position i

$$E(x) = \underbrace{x^{i}}_{\text{Starting position}} * \underbrace{\left(B(x) \right)}_{\text{Burst poly}}$$

$$d(B) = r-1$$

Suppose

length of burst   degree of $G(x)$

$$r \le k$$

then

$$\underset{= k}{G(x)} \nmid \underset{< k}{B(x)}$$

$\therefore$

$$G(x) \nmid x^i$$

$$\wedge \quad G(x) \nmid B(x)$$

$$\Rightarrow \quad G(x) \nmid E$$

Caveat

Assumption of co-primality

True iff $G(x)$ is prime or co-prime w/ $B(x)$ or x^i

$$\left[\begin{array}{l} G \nmid A \wedge G \nmid B \\ \Rightarrow G \nmid AB \end{array}\right.$$

$6 \nmid 9$, $6 \nmid 4$, but

$6 \mid 36$!

k+1 bit burst error

error iff

$G(x) = B(x)$

Prob. of error ?

$$\overbrace{1 \quad k-1 \quad 1}^{k+1 \text{ bits}}$$

$G(x) \wedge B(x)$

B eob

G : d1(0)

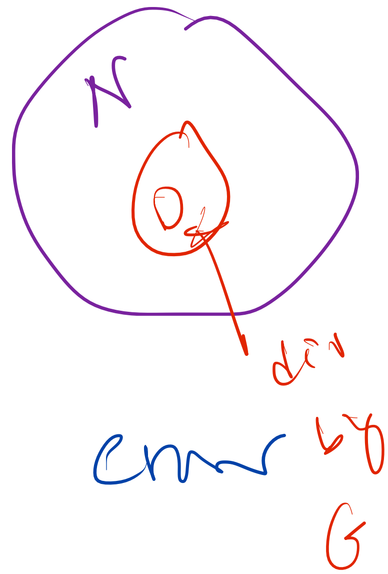
B sob

G by assumptn

$P = 2^{-(k-1)}$

Longer Bursts:

$$d(B) > d(G)$$



Prob. of $\neg$ detecting error

$$e^{-k}$$

Let $N = \{ \text{poly of } d(k+i) \}$
$i > 1$

$$P(\text{error}) = \frac{|D|}{|N|}$$

$$D = \{ p \in N \text{ s.t. } G \mid p \}$$

2 isolated single bit errors:

$$E(x) = x^i + x^j$$

$$= x^j \cancel{*} \underbrace{(x^{i-j} + 1)}$$

Assume $x \nmid G \Rightarrow G(x) = \sum_{\alpha} x^{\alpha} + \underline{1}$,

"sufficient" condition to detect 2 bit errors is

$$G(x) \nmid (x^{\alpha} + 1),$$

$$\alpha < \text{frame length}$$

magic

$\exists$ "simple" poly in $GF(2)$ that do not divide $x^\alpha + 1$

$\forall\ \alpha < 2^{15}$!

whatever.

ECC

Parity → Even
Parity → Odd

1D

1 1 0 1 $\underbrace{1}_{p}$

even parity

2D

1	0	1	1		1
1	1	0	1		1
1	0	0	0		1
0	0	0	0		0
1	1	1	0		?

Hamming Codes

- All bit positions that are 2^x are parity

$D = 1001\ 1010\ 10$

$T(x) =$

p	p	1	p	0	0	1	p	1	0	1	0
1	2	3	4	5	6	7	8	9	A	B	C

Parity Computat^n^

Bit Position 1

check 1

skip 1

assume 0 to start

Ø	P	1	P	0	0	1	P	1	0	1	0
1	2	3	4	5	6	7	8	9	A	B	C

Bit position 2

Assume Ø at 2

Check 2

Skip 2

Ø	1	1	P	0	0	1	P	1	0	1	0
1	2	3	4	5	6	7	8	9	A	B	C

Bit pos. 4

check 4

skip 4

0	1	1	1	0	0	1	P	1	0	1	0
1	2	3	4	5	6	7	8	9	A	B	C

Bit position 8

0 1 1 1 0 0 1 ~~0~~ 1 0 1 0

1 2 3 4 5 6 7 8 9 A B C

Transmit

0 1 1 1 0 0 1 0 1 0 1 0

0

Suppose bit 7 is flipped

$d(G) = K$

$d(B) < K$

$E = x^i * B$

Show $G \nmid B$

$\S\ \bar{Q}(\cdot) = d(\text{highest term}) - d(\text{lowest term})$

$\bar{Q}(x^3 + x + 1) = 3 - 0 = 3$

$\bar{Q}(x^{18} + x^{17}) = 18 - 17 = 1$

$\bar{Q}$ is invariant upon multiplicat^n by x^i $\forall i$

G, $B * x^i$

$$\bar{Q}(P) = \bar{Q}(P * x^i)$$

$\forall i$

Suppose

$$G \mid E, \quad E = x^i * \underbrace{B}_{\text{Burst}}$$

$\exists\, Q$ s.t.

$$\underbrace{G \cdot Q}_{} = \underbrace{E}_{}$$

$$Q(E) \downarrow < x$$

$$(x^k + \dots + 1) * (x^a + \dots x^b)$$

$$\downarrow \bar{Q}$$

$$\underbrace{k + a - b \geq k}_{\bar{Q}(GQ)}$$

if $a \mid b$

then $\exists\, c$

s.t. $ac = b$