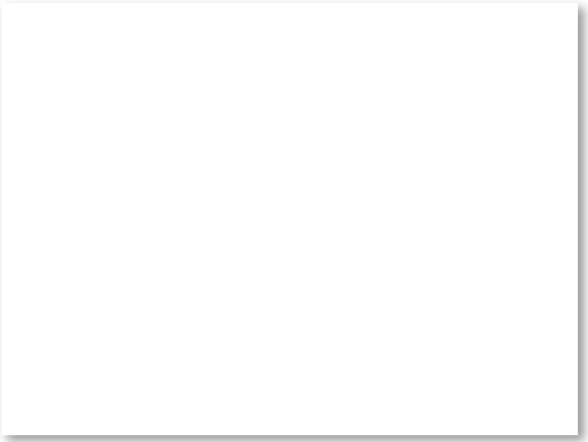
Checksums

- Idea: sum up data in N-bit words

- Stronger protection than parity

Internet Checksum

- Sum is defined in 1s complement arithmetic (must add back carries)
  - And it's the negative sum
- "*The checksum field is the 16 bit one's complement of the one's complement sum of all 16 bit words …*" – RFC 791



Internet Checksum (2)

Sending:

1. Arrange data in 16-bit words
2. Put zero in checksum position, add

3. Add any carryover back to get 16 bits

4. Negate (complement) to get sum

```
0001
f203
f4f5
f6f7
```

Internet Checksum (3)

Sending:

1. Arrange data in 16-bit words
2. Put zero in checksum position, add
3. Add any carryover back to get 16 bits
4. Negate (complement) to get

```
  0001
  f203
  f4f5
  f6f7
+(0000)
------
 2ddf0
   ↓
  ddf0
+    2
------
  ddf2
   ↓
  220d
```

Internet Checksum (4)

Receiving:

1. Arrange data in 16-bit words
2. Checksum will be non-zero, add

```
  0001
  f203
  f4f5
  f6f7
+ 220d
------
```

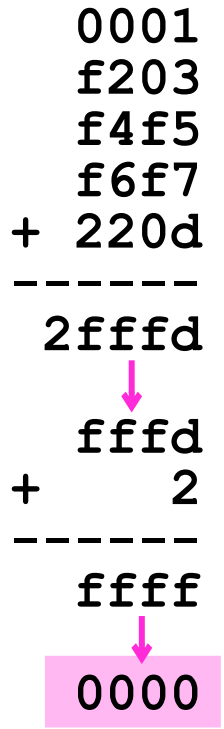
3. Add any carryover back to get 16 bits

4. Negate the result and check it is 0

Internet Checksum (5)

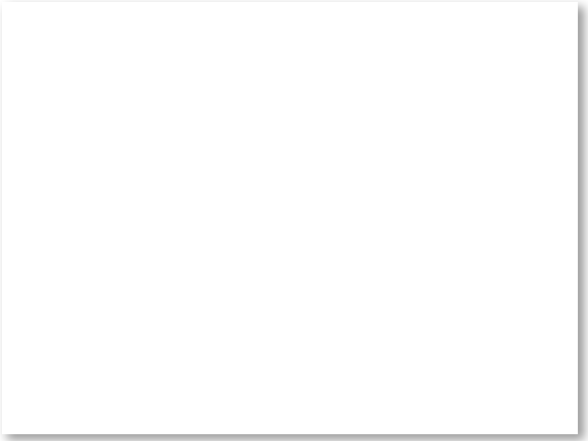
Receiving:

1. Arrange data in 16-bit words
2. Checksum will be non-zero, add
3. Add any carryover back to get 16 bits
4. Negate the result and check it is 0



Internet Checksum (6)

- How well does the checksum work?
  - What is the distance of the code?
  - How many errors will it detect/correct?
- What about larger errors?



- Suppose a 6-bytes packet content is
  - 0xABCC, 0x960B, 0x5A3D

What is the checksum for this packet?

0x is a hexadecimal representation that each symbol (0-9, A-F) represents 4 bits binary within the value of 0-15. For more details see: http://en.wikipedia.org/wiki/Hexadecimal

Normal summation: 0xABCC+0x960B+0x5A3D = 0x19C14

Wrap up carry-out value: 0x9C14 + 0x1 = 0x9C15

So the checksum is: 0xFFFF – 0x9C15 = 0x63EA

Error Detection in Practice

- CRCs are widely used on links
  - Ethernet, 802.11, ADSL, Cable …
- Checksum used in Internet
  - IP, TCP, UDP … but it is weak
- Parity
  - Is little used