Poll: from the reading

The reading for today talked about Hamming codes, which are used to encode messages before being transmitted from sender to receiver. What is the point of Hamming codes?

A) They compress the message, so fewer bits need to be transmitted.
B) They encrypt the message, so an eavesdropper cannot read transmitted message.
C) They augment the message, so that if bits are corrupted during transmission, they can be fixed.
D) More than one of the above.
E) None of the above.

COSC 290 Discrete Structures

Lecture 11: Error correcting codes

Prof. Michael Hay

Friday, Feb. 16, 2018

Colgate University

Plan for today

1. Error-correcting codes
2. Error-correcting codes: an abstract view
3. Minimum distance

Error-correcting codes

Basic setup

- Sender wants to transmit k-bit message $m \in \{0,1\}^k$
- Message m encoded as a n-bit codeword $c \in \mathcal{C} \subseteq \{0,1\}^n$
- Codeword c is transmitted over a noisy channel which may corrupt message.
- Receiver receives c', a (possibly corrupted) n-bit string.
- Receiver decodes c' into message m'

(drawn on board)

Error detection and correction

Instead of sending k-bit message directly, a *larger* n-bit codeword is sent.

The goal: design an encoding scheme with these properties...

- Error Correction if a “small” number of bits are corrupted, the receiver can correct those bits and recover message m.
- Error Detection if a “medium” number of bits are corrupted, the receiver can at least detect corruption (and perhaps request re-transmission).
- Efficiency Size of codewords should close to size of messages (i.e., avoid making them too large).

Applications

- Digital storage (Reed-Solomon codes and CDs/DVDs)
- Internet
- Deep-space telecommunications
- Related ideas are used to verify transactions in Bitcoin (blockchain)
- ... many others...

Performance measures

To judge the quality of a coding scheme, we need two measures:

- Something that measures efficiency:
  We will use rate, the ratio between message length and codeword length, k/n.
- Something that measures ability to correct/detect errors:
  We will use something called minimum distance for reasons that will be clear soon.

Example: repetition code

A size ℓ repetition code takes message m, and sends ℓ copies of m.

Example:

- Suppose $m \in \{0,1\}^2$ and $\ell = 3$.
- If message $m = 10$ then $c = 10\ 10\ 10$.
- If message $m = 11$ then $c = 11\ 11\ 11$.
- Suppose the receiver gets $c' = 10\ 10\ 11$,
    - Can the receiver detect an error? how?
    - Can the receiver correct an error? how?

Poll: repetition code

A size ℓ repetition code takes a k-bit message m, and sends ℓ copies of m. Suppose that ℓ is odd, so $\exists t \in \mathbb{Z} : \ell = 2t + 1$.

We will say the code can tolerate x errors if any set of x bits can be corrupted in the codeword and the receiver can correct all x errors, thereby recovering the original message.

Which of the following statements is true about the ℓ repetition code?

A) It can tolerate 1 error, and its rate is $1/\ell$.
B) It can tolerate t errors, and its rate is $1/\ell$.
C) It can tolerate $\ell - 1$ errors, and its rate is $1/\ell$.
D) It can tolerate 1 error, and its rate is k/ℓ.
E) It can tolerate t errors, and its rate is k/ℓ.
F) It can tolerate $\ell - 1$ errors, and its rate is k/ℓ.

Error-correcting codes: an abstract view

Error correcting codes: an abstract view

A code is a set $\mathcal{C} \subseteq \{0,1\}^n$ where $|\mathcal{C}| = 2^k$.

- Encoding: a bijective function *encode* : $\{0,1\}^k \to \mathcal{C}$ maps k-bit messages to codewords in $\mathcal{C}$.
  Both the sender and receiver know this function.
- Sender sends c; receiver receives c'.
- Error detection: the receiver will conclude an error has occurred if and only if $c' \notin \mathcal{C}$.
- Error correction: receiver chooses $c'' \in \mathcal{C}$ that is *closest* to c'.
- After correction, receiver decodes c'' by applying inverse of *encode*.

Distance measure for bit strings

Let $x, y \in \{0, 1\}^n$ be two n-bit strings. The Hamming distance between x and y, denoted $\Delta(x, y)$, is the number of positions in which x and y differ.

$$\Delta(x, y) := |\{ i \in \{1, 2, \ldots, n\} : x_i \neq y_i \}|$$

Example:

- $x = 1000011$
- $y = 1\underline{1}000\underline{0}1$
- $\Delta(x, y) = 2$

Example

Example code where $\mathcal{C} := \{100111, 101010, 010110, 010111\}$. Since $|\mathcal{C}| = 2^2$, we can use code to send 2-bit messages.

m	$c \in \mathcal{C}$
00	10 01 11
01	10 10 10
10	01 01 10
11	01 01 11

Note: the rows of this table define one particular *encode* function.

Poll: decoding a message

Suppose the receiver gets $c' = 10\ 10\ 11$, can the receiver detect an error? If so, can receiver correct the error?

A) The receiver can never be 100% certain there was an error.
B) The receiver knows there's an error, but cannot correct it.
C) The receiver knows there's an error, and would correct it to be 10 01 11.
D) The receiver knows there's an error, and would correct it to be 10 10 10.
E) None of the above / more than one of the above.

m	$c \in \mathcal{C}$
00	10 01 11
01	10 10 10
10	01 01 10
11	01 01 11

Poll: are all errors detectable?

Recall the following

- A code is a set $\mathcal{C} \subseteq \{0, 1\}^n$ where $|\mathcal{C}| = 2^k$.
- Receiver receives a n-bit string, c'.
- The receiver will conclude an error has occurred if and only if $c' \notin \mathcal{C}$.

Two part question:

1. If the receiver concludes that an error has occurred, can we be sure that an error has, in fact, occurred?
2. If the receiver concludes that no error has occurred, can we be sure that no errors have, in fact, occurred?

A) 1) Yes, 2) Yes
B) 1) Yes, 2) No
C) 1) No, 2) Yes
D) 1) No, 2) No

Minimum distance

Minimum Distance

The minimum distance of code $\mathcal{C}$ is the smallest Hamming distance between two distinct codewords in $\mathcal{C}$.

$$\min \{ \Delta(x, y) : x, y \in \mathcal{C} \text{ and } x \neq y \}$$

m	$c \in \mathcal{C}$
00	10 01 11
01	10 10 10
10	01 01 10
11	01 01 11

Poll: minimum distance

Consider this code $\mathcal{C}$?

m	$c \in \mathcal{C}$
00	10 01 11
01	10 10 10
10	01 01 10
11	01 01 11

What is its minimum distance?

A) 0

B) 1

C) 2

D) 3

The minimum distance of code $\mathcal{C}$ is the smallest Hamming distance between two distinct codewords in $\mathcal{C}$.

$$\min \{ \Delta(x, y) : x, y \in \mathcal{C} \text{ and } x \neq y \}$$

Theorem: minimum distance and detecting/correcting errors

If the minimum distance of a code $\mathcal{C}$ is $2t + 1$, then $\mathcal{C}$ can detect $2t$ errors and correct t errors.

Proofs on board