Problem set 8

Please turn in the problem set. You can place it on the desk.

COSC 290 Discrete Structures

Lecture 11: Proofs and codes, continued...

Prof. Michael Hay
Friday, Sep. 22, 2017
Colgate University

Plan for today

1. Hamming codes
2. Problem Set Questions

Hamming codes

Hamming code

Claim: Hamming code has a minimum distance of 3.

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

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

Poll: What to show?

We want to support claim that the Hamming code $\mathcal{C}$ has a minimum distance of at least 3. Which of the following statements provides sufficient support for our claim? Note: we use *encode* to mean the function that generates a Hamming codeword c for message m.

A) There exists two codewords $c \in \mathcal{C}$ and $c' \in \mathcal{C}$ such that $c \neq c'$ and $\Delta(c, c') \geq 3$.
B) There exists two messages $m \in \{0,1\}^k$ and $m' \in \{0,1\}^k$, such that $m \neq m'$ and $\Delta(encode(m), encode(m')) \geq 3$.
C) For any two codewords $c \in \mathcal{C}$ and $c' \in \mathcal{C}$, if $c \neq c'$, then $\Delta(c, c') \geq 3$.
D) For any two messages $m \in \{0,1\}^k$ and $m' \in \{0,1\}^k$, if $m \neq m'$, then then $\Delta(encode(m), encode(m')) \geq 3$.
E) None of above / More than one

Claim

The claim we want to prove is

$$\forall m \in \{0,1\}^k : \forall m' \in \{0,1\}^k :$$
$$\Delta(m, m') > 0 \implies \Delta(encode(m), encode(m')) \geq 3$$

(where *encode* is the function that generates a Hamming codeword c for message m).

Claim, with slight notation change

The claim we want to prove is

$$\forall m \in \{0,1\}^k : \forall m' \in \{0,1\}^k :$$
$$\Delta(m, m') > 0 \implies \Delta(c, c') \geq 3$$

(where c denotes the Hamming codeword for m and c' denotes Hamming code word for m').

Proof by cases

$\forall \langle m, m' \rangle \in \left(\{0,1\}^k \times \{0,1\}^k \right) : \Delta(m, m') > 0 \implies \Delta(c, c') \geq 3$

Cases:

- $\langle m, m' \rangle$ pairs such that $\Delta(m, m') \geq 3$
- $\langle m, m' \rangle$ pairs such that $\Delta(m, m') = 2$
- $\langle m, m' \rangle$ pairs such that $\Delta(m, m') = 1$
- $\langle m, m' \rangle$ pairs such that $\Delta(m, m') = 0$ (trivial case)

Important: when proving by cases, make sure your cases cover all possibilities!

For each case, we need to show $\Delta(m, m') > 0 \implies \Delta(c, c') \geq 3$.

Shown on board

Poll: What to show for second case?

We are considering the case where $\Delta(m, m') = 2$. Recall that we are using $c := encode(m)$ and $c' := encode(m')$. What do we want to show?

A) $\Delta(c, c') = 3$

B) $\Delta(c, c') \geq 3$

C) That c and c' differ in at least one parity bit.

D) That c and c' differ in at least two parity bits.

E) None / More than one

Problem Set Questions

Problem 4.13

Claim: If the minimum distance of a code $\mathcal{C}$ is $2t$, then $\mathcal{C}$ can detect ?? errors (and correct ?? errors).

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

Proof:

- Error detection: essentially identical to proof on Wednesday (or in book on p. 408). Why?
  Because proof does not depend in any way on minimum distance being odd.
- Error correction: proof depends on number of errors being strictly less than half minimum distance.

Problem 4.12

Claim: If the minimum distance of a code $\mathcal{C}$ is $2t+1$, then $\mathcal{C}$ cannot *detect* $2t+1$ errors and cannot *correct* $t+1$ errors.

Let's break this into two smaller claims:

- Claim (a): If the minimum distance of a code $\mathcal{C}$ is $2t+1$, then $\mathcal{C}$ cannot *detect* $2t+1$ errors.
- Claim (b): If the minimum distance of a code $\mathcal{C}$ is $2t+1$, then $\mathcal{C}$ cannot *correct* $t+1$ errors.

Problem 4.12, part (a)

Claim (a): If the minimum distance of a code $\mathcal{C}$ is $2t+1$, then $\mathcal{C}$ cannot *detect* $2t+1$ errors.

Let p be "the minimum distance of code $\mathcal{C}$ is $2t+1$."

Let q be "$\mathcal{C}$ cannot detect $2t+1$ errors."

Claim (a) expressed logically: $p \implies q$.

Proof approach: direct proof, "assume the antecedent" (p. 246): assume p is true, show q must be true. But what exactly does q mean?

$\mathcal{C}$ cannot detect errors

Let q be "$\mathcal{C}$ cannot detect $2t+1$ errors."

Exercise (and slight digression): formalize q as a proposition in predicate logic...

- Your proposition should define c as any codeword.
- Your proposition should define c' as any (possibly corrupted) codeword.
- You can use predicate $\mathit{hasError}(c')$ which is True if error detection believes c' contains an error, and False otherwise.
- First, express "$\mathcal{C}$ *can* detect $2t+1$ errors" and then just negate the whole expression.

Expressing q in logic

Let q be "$\mathcal{C}$ cannot detect $2t+1$ errors."

q can be expressed logically as

$$\neg\left(\forall c \in \mathcal{C} : \forall c' \in \{0,1\}^n : (0 < \Delta(c,c') \leq 2t+1) \implies \mathit{hasError}(c')\right)$$
$$\equiv \exists c \in \mathcal{C} : \exists c' \in \{0,1\}^n : (0 < \Delta(c,c') \leq 2t+1) \wedge \neg \mathit{hasError}(c')$$

Side note

Your proofs do not necessarily need to express everything in formal logic. The point of this exercise is show that a sound proof argument should follow the rules of logic (even though you may express your proof in a natural language).

Proof by construction

Recap:

- $p =$ "$\mathcal{C}$ has minimum distance $2t + 1$."
- $q =$ "$\mathcal{C}$ cannot detect $2t + 1$ errors"
- Claim: $p \implies q$
- Proof: direct proof (by assuming the antecedent)
  - Given: p is true
  - Want to show: q must be true.
- Approach:
  - We just showed that q is logically equivalent to the claim that there exists $c \in \mathcal{C}$ and $c' \in \{0, 1\}^n$ such that $0 < \Delta(c, c') \leq 2t + 1$ and *hasError*(c') returns False.
  - Now, we proceed with a "proof by construction" (p. 433). We find a pair c and c' and then show the pair satisfies above condition.

Shown on board

Proof of (b)

For (b), similar set up except q is "$\mathcal{C}$ cannot correct $t + 1$ errors."

By the same reasoning we used with (a), ...

- Given: $\mathcal{C}$ has minimum distance $2t + 1$
- Want to show: there exists $c \in \mathcal{C}$ and $c' \in \{0, 1\}^n$ such that $0 < \Delta(c, c') \leq t + 1$ and error correction will fail (it will "correct" c' to some codeword other than c).

Shown on board