COSC 290 Discrete Structures

Lecture 12: Proof by contrapositive

Prof. Michael Hay
Monday, Sep. 25, 2017
Colgate University

Plan for today

1. Direct Proofs
2. Proof by contrapositive

Direct Proofs

Direct Proof Template

- **Claim**: *Write the theorem/claim to be proved, "If p, then q"*
- **Proof**:
  - **Given**: *Assume that p is true*
  - **Want to show**: *q is true*
  - *Write main body of proof... show how q logically follows from p*
  - *End the body with... "[restate q], which is what was to be shown." This identifies for the reader that you reached what you set out to reach.*
  - **Conclusion**: "Therefore, [restate theorem]."

Applying Template to Problem 4.12

- **Claim 4.12(a)**: "For any $t \geq 0$, if the minimum distance of code $\mathcal{C}$ is $2t+1$, then $\mathcal{C}$ cannot detect $2t+1$ errors."
- **Proof**:
  - **Given**:
    - Let t be any integer such that $t \geq 0$.
    - Assume that $\mathcal{C} \subseteq \{0,1\}^n$ has minimum distance of $2t+1$.
    - (Implicit assumption) $n \geq 2t+1$
  - **Want to show**: $\mathcal{C}$ cannot detect $2t+1$ errors.
  - *What follows must apply to any t and $\mathcal{C}$ matching the given conditions!*

Recall from previous class

Last time, we showed that "$\mathcal{C}$ cannot detect $2t+1$ errors" 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 (i.e., error detection concludes that no error has occurred).

This observation is the key to our proof strategy.

Example of "proof by construction" (p. 433): We find a pair c and c' and then show the pair satisfies above condition.

Rest of proof shown on board

Minimum Distance

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

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

Example: this $\mathcal{C}$ has minimum distance 1:

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

Common mistakes

- Showing error detection fails for a specific t.
- Showing error detection fails for a specific coding scheme (and a specific t).

Applying Template to Problem 4.12

- **Claim 4.12(b)**: "For any $t \geq 0$, if the minimum distance of code $\mathcal{C}$ is $2t+1$, then $\mathcal{C}$ cannot correct $t+1$ errors."
- **Proof**:
  - **Given**:
    - Let t be any integer such that $t \geq 0$.
    - Assume that $\mathcal{C} \subseteq \{0,1\}^n$ has minimum distance of $2t+1$.
    - (Implicit assumption) $n \geq 2t+1$
  - **Want to show**: $\mathcal{C}$ cannot correct $t+1$ errors.
  - *What follows must apply to any t and $\mathcal{C}$ matching the given conditions!*

Our strategy for 4.12(b)

By the same reasoning, "$\mathcal{C}$ cannot correct $t+1$ errors" is logically equivalent to the claim that there exists $c \in \mathcal{C}$ and $c' \in \{0,1\}^n$ such that $0 < \Delta(c, c') \leq t+1$ and error correction will fail (it will "correct" c' to some codeword other than c).

Again "proof by construction" (p. 433): find a pair c and c' and then show the pair satisfies above condition. Specifically, we'll show that received codeword $c' \notin \mathcal{C}$ will be mistakenly "corrected" to some *other* codeword $c'' \in \mathcal{C}$.

Rest of proof shown on board

Proof by contrapositive

Proof by contrapositive

To prove a proposition of the form

$$\forall x : P(x) \implies Q(x)$$

you can equivalently prove its contrapositive form

$$\forall x : \neg Q(x) \implies \neg P(x)$$

Procedure for proof by contrapositive

1. Derive contrapositive form $\neg q \implies \neg p$.
2. Assume q is false (take it as “given”).
3. Show that $\neg p$ logically follows.

Truth table for implication

p	q	$\neg q$	$\neg p$	$\neg q \implies \neg p$	
T	T	F	F	T	
T	F	T	F	F	*Rule this row out!*
F	T	F	T	T	
F	F	T	T	T	

Proof by Contrapositive Template

- **Claim**: *Write the theorem/claim to be proved, “If p, then q”*
- **Proof**: *“We will prove the contrapositive: [state claim in contrapositive form]”* It’s important to say this! Why?
  - **Given**: *Assume that $\neg q$ is true*
  - **Want to show**: *$\neg p$ is true*
  - *Write main body of proof...*
  - *End the body with... “[restate $\neg p$], which is what was to be shown.”*
  - **Conclusion**: “Therefore *by proving its contrapositive*, we have shown [restate theorem].”

Example

- **Claim**: “Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.
- **Proof**: “We will prove the contrapositive”
  - **Given**: Assume that ...
  - **Want to show**: ...
  - *[Proof details]*
  - **Conclusion**: “Therefore *by proving its contrapositive*, we have shown ...”

Poll: What is given?

- **Claim**: "Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.
- **Proof**: "We will prove the contrapositive"
  - **Given**: Assume that ... what goes here?

A) $x + y \neq 0$ or $x - y \neq 0$
B) $x + y = 0$ or $x - y = 0$
C) $x + y = 0$ and $x - y = 0$
D) $x = 0$
E) None of above / More than one

Poll: What do we want to show?

- **Claim**: "Let x, y be numbers such that $x \neq 0$. Then either $x + y \neq 0$ or $x - y \neq 0$.
- **Proof**: "We will prove the contrapositive"
  - **Given**: Assume that $x + y = 0$ and $x - y = 0$.
  - **Want to show**: ... what goes here?

A) $x \neq 0$
B) $x = 0$
C) $x = 0$ and $y = 0$
D) $x + y \neq 0$ or $x - y \neq 0$
E) None of above / More than one

When to use proof by contrapositive?

Since $p \implies q$ is logically equivalent to $\neg q \implies \neg p$, it shouldn't matter whether you use direct proof or proof by contrapositive.

In practice, can try both and see which one gives you a better starting place (e.g., more information).

Common use case: proving $p \iff q$

- $p \iff q \equiv (p \implies q) \wedge (q \implies p)$
- $q \implies p \equiv \neg p \implies \neg q$
- So prove $p \iff q$ by proving $p \implies q$ and then $\neg p \implies \neg q$. In both cases you get to start with p and work towards q.