Lecture 4: Proofs

Notes:

- Have your clickers ready
- Grab a handout
- HW 1 out yesterday, due Friday 2/7 at 5PM; office hours start today

Previously:

Defn: $A = B$ if $A \subseteq B$ and $B \subseteq A$

Defn: $A \subseteq B$ if every $x \in A$ is also in B

Defn: $A \cup B := \{x \mid x \in A \text{ or } x \in B\}$

Defn: $A \cap B := \{x \mid x \in A \text{ and } x \in B\}$

Claim: $\underbrace{A \cup (B \cap C)}_{LHS} = \underbrace{(A \cup B) \cap (A \cup C)}_{RHS}$

Proof: . . . today

Proofs

Each sentence in a proof should be:

- Clear
- True
- Justified

At each point in a proof, there is

- a **goal** proposition
  - what you're trying to prove
- and some propositions that you **know**
  - assumptions, definitions, or things already proven

The proof is done when you "know" the goal (i.e. when you've proved it)

(handout)

Discrete Structures CS2800	Table of proof techniques Everything you need to know for 2800 (almost)

Proofs are written using a small set of basic building blocks. **All** proofs should be completed using the following proof techniques[1]. This is the **most** important material to understand in CS 2800: it is necessary for everything else we will do. Luckily, you'll get lots of practice this semester.

Each sentence in a proof should be:

- Clear (all terms have definitions)
- True
- Justified (using proof techniques listed below)

At each point in a proof, there is

- a **goal** proposition (what you're trying to prove)
- and some propositions that you **know** (assumptions, definitions, or things already proven)

Never confuse them! If you make a statement, you are telling the reader that it is something you have proved, so you better have already proved it! Say "we want to show..." to reiterate the goal without claiming you've proven it.

Valid proof steps:

- **Use** something you know.
- **Reduce** your goal to a simpler goal (the "to prove it" column below)

The following table shows how to do this for each kind of proposition:

Proposition	To prove it	To use it	To disprove it, prove
P and Q	Prove both P and Q	Use either P or Q	P is false or Q is false
P or Q	Prove P. Alternatively, prove Q	To prove R, prove R in the P and Q cases (case analysis)	P is false and Q is false
for all $x \in A$, $P(x)$	Prove $P(y)$ for an arbitrary $y \in A$	Conclude P for any specific $y \in A$	There is some $x \in A$ for which P is false (counterexample)
if P then Q	Assume P and prove Q	If you know P, you can conclude Q	P is true but Q is false
there exists an $x \in A$ such that P	Give a specific $y \in A$ and prove $P(y)$	Use an arbitrary $y \in A$ that satisfies $P(y)$	for any $x \in A$, P is false
P is false	Prove the logical negation of P (also, you always know P is either true or false)	If you can also prove P, you can conclude R (contradiction)	P

[1]Mostly: we'll add a few more techniques during the semester.

Proof exercise

Previously:

for all $x \in A$, $x \in B$

Defn: $A = B$ if $A \subseteq B$ and $B \subseteq A$

Defn: $A \subseteq B$ if every $x \in A$ is also in B

Defn: $A \cup B := \{x \mid x \in A \text{ or } x \in B\}$

Defn: $A \cap B := \{x \mid x \in A \text{ and } x \in B\}$

→ implicitly: for all A, B, C

Claim: $\underbrace{A \cup (B \cap C)}_{LHS} = \underbrace{(A \cup B) \cap (A \cup C)}_{RHS}$

Proof: by iClicker! What's the next step?

iClicker key:

- A. Use an "and" stmt
- B. Prove an "and" stmt
- C. Use an "or" stmt
- D. Prove an "or" stmt
- E. Prove a "for all" stmt

– I WTS LHS ⊆ RHS and RHS ⊆ LHS.
what are A, B, C?

– WTS for all A, B, C, LHS = RHS.

(implicit) → (E): choose arbitrary sets A, B, C.
now we WTS LHS ⊆ RHS and RHS ⊆ LHS.

(B) (LHS ⊆ RHS)

(E) ⇒ choose arb. x ∈ LHS,
WTS x ∈ RHS. Since x ∈ LHS,
either x ∈ A or x ∈ B ∩ C.

(C) if x ∈ A, ...
WTS x ∈ RHS.
(D) → well, since x ∈ A, x ∈ A ∪ B.
similarly, x ∈ A ∪ C.
(B) So x ∈ (A ∪ B) ∩ (A ∪ C) so x ∈ RHS ✓

on the other hand, if x ∈ B ∩ C ...
WTS x ∈ RHS. ...

know	goal
A, B, C arb. sets	~~for all A,B,C LHS = RHS.~~
~~x ∈ LHS~~	~~LHS = RHS~~
~~x ∈ A ∪ (B ∩ C)~~	LHS ⊆ ~~RHS~~ and ~~RHS ⊆ LHS~~
~~x ∈ A or x ∈ B ∩ C~~	~~x ∈ RHS~~ ~~x ∈ (A ∪ B) ∩ (A ∪ C)~~
x ∈ A.	x ∈ A ∪ B and x ∈ A ∪ C
x ∈ A ∪ B	
x ∈ A ∪ C	x ∈ A or x ∈ B.

(RHS ⊆ LHS)

...

Completed proof (as I would likely submit it for homework)

Claim: $\underbrace{A \cup (B \cap C)}_{LHS} = \underbrace{(A \cup B) \cap (A \cup C)}_{RHS}$

Proof: Choose arbitrary sets A, B, and C; we want to show that $RHS \subseteq LHS$ and $LHS \subseteq RHS$.

To see that $LHS \subseteq RHS$, choose an arbitrary $x \in LHS$. We will show that $x \in RHS$. Since $x \in LHS$, we know either $x \in A$ or $x \in B \cap C$. In the former case, $x \in A \cup B$ and $x \in A \cup C$, so $x \in (A \cup B) \cap (A \cup C) = RHS$. In the latter case, we have $x \in B$ and $x \in C$ (by definition). Since $x \in B$, we have $x \in A \cup B$, and similarly $x \in A \cup C$; thus $x \in RHS$, as required.

To see that $RHS \subseteq LHS$, choose an arbitrary $x \in RHS$. We will show that $x \in LHS$. We know that either $x \in A$ or $x \notin A$. If $x \in A$, then $x \in LHS$ and we are done, so we only need consider the $x \notin A$ case. Since $x \in RHS$, we know that $x \in (A \cup B)$ and $x \in (A \cup C)$. Since $x \notin A$, we have $x \in B$ (otherwise $x \notin A \cup B$); similarly we have $x \in C$. Thus $x \in B \cap C$, so $x \in A \cup (B \cap C) = LHS$ as required.