Lecture 4: Proofs

Today:

- Finish our first proof
- Quantifiers (for all and there exists)
- Some function properties: injectivity and surjectivity (next time!)
- Logical negation (next time!)

Announcements:

- None today

for any (sets) A, B, C,

(review) Not good proofs

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

Not a proof: Draw Venn diagrams for both sides, note they are the same (only works for the examples you draw, not for all A, B, and C)

examples good, but are not proofs!

Poor style:

$x \in LHS$ means $x \in A$ or ($x \in B$ and $x \in C$)
equivalently ($x \in A$ or $x \in B$) and ($x \in A$ or $x \in C$)
equivalently ($x \in A \cup B$) and ($x \in A \cup C$)
i.e. $x \in (A \cup B) \cap (A \cup C)$

- Relies on logical manipulation
  - Logically sound, but we haven't explained why
- Logic doesn't really show what's going on
- Hard to read
- Doesn't scale beyond very simple proofs

A good proof

for all A, B, C

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

Proof: Reminders:

- **Defn:** $A \cup B := \{x \mid x \in A$ **or** $x \in B\}$
- **Defn:** $A \cap B := \{x \mid x \in A$ **and** $x \in B\}$
- **Defn:** $A \subseteq B$ if for all $x \in A$, x is in B
- **Defn:** $A = B$ if $A \subseteq B$ and $B \subseteq A$

if $X \subseteq Y$
and $Z \subseteq Y$
then $X \cup Z \subseteq Y$. ?

in the context of a def^n, I mean "if and only if", "means"

WTS P and Q, show both.

WTS ∀x, P: choose arb x

Choose arbitrary sets A, B, C. We WTS (want to show) LHS = RHS, in other words, WTS LHS ⊆ RHS and RHS ⊆ LHS.

need to fill in to complete proof! (good exercise!)

Step 1: WTS LHS ⊆ RHS, i.e.
WTS for all x ∈ LHS, x ∈ RHS.
Choose arb. value x ∈ LHS.

def^n

Then x ∈ A ∪ (B ∩ C), so
either x ∈ A or x ∈ B ∩ C.

Know P or Q, consider both

In Case 1, if x ∈ A then
x ∈ A ∪ B (by def^n of ∪), also
x ∈ A ∪ C. so x ∈ (A ∪ B) ∩ (A ∪ C)
= RHS ✓

step 2: RHS ⊆ LHS

⋮

in the second case, where x ∈ B ∩ C,
we again WTS that x ∈ (A ∪ B) ∩ (A ∪ C).
i.e. we WTS the x ∈ A ∪ B and
that x ∈ A ∪ C. But x ∈ A ∪ B since
x ∈ B (because x ∈ B ∩ C). Similarly
x ∈ C, so x ∈ A ∪ C, as desired. ✓
in Both cases, x ∈ RHS. ✓

WTS P or Q, show P

So LHS ⊆ RHS and RHS ⊆ LHS ✓
so LHS = RHS.

copied from above
RHS = (A ∪ B) ∩ (A ∪ C)

WTS P and Q, have shown both

Proof techniques

Whenever it would be useful: gather and plug in **definitions**

If you want to **prove** "**for all** $x \in A, P$"

- You want to give a proof that works for any $x \in A$
- Instruct the reader to choose an *arbitrary* x
- Make no assumptions about x (other than $x \in A$)
- Give a proof of P for that arbtirary x

If you know "P **or** Q" and want to **use** it in a proof:

- Consider both cases separately
- Prove your goal in both cases

If you know "P **and** Q" and want to **use** it in a proof:

- You may use P
- You may use Q

If you want to **prove** "P **and** Q":

- Prove P and separately prove Q

To prove "P or Q":
→ may prove either one.