English Proofs and Sets

CSE 311 Autumn 23
Lecture 10

Announcements

Dates/Times/Locations of the midterm and final are confirmed!

Thank you for your patience!

Midterm: Wed. Nov 15, 6-7:30 PM BAG 131,154
Final: Mon. Dec. 11, 4:30-6:20 PM, KNE 130

Some of you will have conflicts!

- E.g., due to work schedules, exams for other courses, etc.
- More information on alternate exam times as we get closer (we'll schedule as we find out more specifically who needs one).
- No need to email me; we'll send out a form before each exam to let us know what you need.

We’ve got A LOT of definitions today

You don’t need me to read things aloud to you.

We’ll cover the subtle/tricky things in lecture.

Other things are left for you to read on your own. The section is marked in the slide deck.

Today’s concept check should be very useful to get the definitions down! You might find tomorrow’s section more helpful if you’ve done today’s concept check already (but deadline is Friday morning like usual)

Returning to English Proofs

Breakdown the statement

“if x is even then x^2 is even.”

In symbols, that’s: $\forall x\left(\mathrm{Even}(x) \to \mathrm{Even}\left(x^2\right)\right)$

Let’s break down the statement to understand what the proof needs to look like:

$\forall x$ comes first. We need to introduce an arbitrary variable

$\mathrm{Even}(x) \to \mathrm{Even}(x^2)$ is left. We prove implications by assuming the hypothesis and setting the conclusion as our goal

$\mathrm{Even}(x)$ is our starting assumption, $\mathrm{Even}(x^2)$ is our goal

If x is even, then x^2 is even.

1.	Let a be arbitrary	
2.1	$\texttt{Even}(a)$	Assumption
2.2	$?$	?
2.3	$?$	?
2.4	$?$	?
2.5	$?$	?
2.6	$?$	?
2.7	$\texttt{Even}(a^2)$	?
3.	$\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)
4.	$\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro ∀ (3)

If x is even, then x^2 is even.

1. Let a be arbitrary	
2.1 $\texttt{Even}(a)$	Assumption
2.2 $\exists y\ (2y = a)$	Definition of Even (2.1)
2.3 $2z = a$	Elim ∃(2.2)
2.4 $a^2 = 4z^2$	Algebra (2.3)
2.5 $a^2 = 2 \cdot 2z^2$	Alegbra (2.4)
2.6 $\exists w(2w = a^2)$	Intro ∃ (2.5)
2.7 $\texttt{Even}(a^2)$	Definition of Even
3. $\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)
4. $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro ∀ (3)

If x is even, then x^2 is even.

1. Let a be arbitrary	
2.1 $\mathtt{Even}(a)$	Assumption
2.2 $\exists y\ (2y = a)$	Definition of Even (2.1)
2.3 $2z = a$	Elim ∃(2.2)
2.4 $a^2 = 4z^2$	Algebra (2.3)
2.5 $a^2 = 2 \cdot 2z^2$	Alegbra (2.4)
2.6 $\exists w(2w = a^2)$	Intro ∃ (2.5)
2.7 $\mathtt{Even}(a^2)$	Definition of Even
3. $\mathtt{Even}(a) \rightarrow \mathtt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)
4. $\forall x(\mathtt{Even}(x) \rightarrow \mathtt{Even}(x^2))$	Intro ∀ (3)

Let x be an arbitrary even integer.
By definition, there is an integer y such that $2y = x$.

Squaring both sides, we see that $x^2 = 4y^2 = 2 \cdot 2y^2$.

Because y is an integer, $2y^2$ is also an integer, and x^2 is two times an integer.
Thus x^2 is even by the definition of even.
Since x was an arbitrary even integer, we can conclude that for every even x, x^2 is also even.

Converting to English

Start by introducing your assumptions.

Introduce variables with “let.” Introduce assumptions with “suppose.”

Always state what type your variable is. English proofs don’t have an established domain of discourse.

Don’t just use “algebra” explain what’s going on if you can explain better.

We don’t explicitly intro/elim $\exists/\forall$ so we end up with fewer “dummy variables”

Let x be an arbitrary even integer.
By definition, there is an integer y such that $2y = x$.

Squaring both sides, we see that $x^2 = 4y^2 = 2 \cdot 2y^2$.

Because y is an integer, $2y^2$ is also an integer, and x^2 is two times an integer.
Thus x^2 is even by the definition of even.
Since x was an arbitrary even integer, we can conclude that for every even x, x^2 is also even.

Let’s do another!

First a definition

Rational

A real number x is rational if (and only if) there exist integers p and q, with $q \neq 0$ such that $x = p/q$.

$$\texttt{Rational}(x) \coloneqq \exists p \exists q(\texttt{Integer}(p) \land \texttt{Integer}(q) \land (x = p/q) \land q \neq 0)$$

Let’s do another!

“The product of two rational numbers is rational.”

What is this statement in predicate logic?

$\forall x \forall y([\texttt{rational}(x) \wedge \texttt{rational}(y)] \rightarrow \texttt{rational}(xy))$

Remember unquantified variables in English are implicitly universally quantified.

Doing a Proof

$\forall x \forall y([\texttt{rational}(x) \land \texttt{rational}(y)] \rightarrow \texttt{rational}(xy))$

"The product of two rational numbers is rational."

DON'T just jump right in!

Look at the statement, make sure you know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Rational

A real number x is rational if (and only if) there exist integers p and q, with $q \neq 0$ such that $x = p/q$.

Let’s do another!

“The product of two rational numbers is rational.”

Let x, y be arbitrary rational numbers.

Therefore, xy is rational.

Since x and y were arbitrary, we can conclude the product of two rational numbers is rational.

Let’s do another!

“The product of two rational numbers is rational.”

Let x, y be arbitrary rational numbers.

By the definition of rational, $x = a/b$, $y = c/d$ for integers a, b, c, d where $b \neq 0$ and $d \neq 0$.

Multiplying, $xy = \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Since integers are closed under multiplication, ac and bd are integers.

Moreover, $bd \neq 0$ because neither b nor d is 0. Thus xy is rational.

Since x and y were arbitrary, we can conclude the product of two rational numbers is rational.

What about an inference proof?
(Skipping a bunch of elim ∧ type steps)

1. Let x be arbitrary ---

2. Let y be arbitrary ---

    3.1 $\texttt{Rational}(x) \land \texttt{Rational}(y)$ Assumption

    3.? $\exists p, q(\texttt{Integer}(p) \land \texttt{Integer}(q) \land q \neq 0 \land x = p/q)$ Defn of Rational

    3.? $x = a/b$ Elim exists (a, b fresh)

    3.? $y = c/d$ Elim exists (c, d fresh)

    3.? $xy = ac/bd$ Algebra

    3.? $bd \neq 0$ Algebra (we'd probably need a new rule here, combining not-equals)

    3.? $\texttt{Integer}(ac)$ (we'd probably need a new rule here)

We don't want to have to write down a formal rule every time we explain something new. Like "an integer times an integer is an integer" but a computer would need us to.

What about an inference proof?
(Skipping a bunch of elim ∧ type steps)

3.? $\texttt{Integer}(ac) \wedge \texttt{Integer}(bd) \wedge bd \neq 0 \wedge xy = ac/bd$

3.? $\exists r, s(\texttt{Integer}(r) \wedge \texttt{Integer}(s) \wedge xy = r/s)$ Intro exists

3.? $\texttt{Rational}(xy)$ Definition of Rational

4. $[\texttt{Rational}(x) \wedge \texttt{Rational}(y)] \to \texttt{Rational}(xy)$

5. $\forall v([\texttt{Rational}(x) \wedge \texttt{Rational}\ (v)] \to \texttt{Rational}(x\mathrm{v}))$ Intro ∀

6. $\forall u \forall v([\texttt{Rational}(u) \wedge \texttt{Rational}(\mathrm{v})] \to \texttt{Rational}(uv))$ Intro ∀

Why English Proofs?

Those symbolic proofs seemed pretty nice. Computers understand them, and can check them.

So what’s up with these English proofs?

They’re far easier for **people** to understand.

But instead of a computer checking them, now a human is checking them.

Sets

Sets

A set is an **unordered** group of **distinct** elements.

We'll always write a set as a list of its elements inside {curly, brackets}.

Variable names are capital letters, with lower-case letters for elements.

$|A| = 2$. "The size of A is 2." or "A has cardinality 2."

$A = \{\text{curly, brackets}\}$

$B = \{0,5,8,10\} = \{5,0,8,10\} = \{0,0,5,8,10\}$

$C = \{0,1,2,3,4,\ldots\}$

Sets

Some more symbols:

$a \in A$ ("a is in A" or "a is an element of A") means a is one of the members of the set.

For $B = \{0,5,8,10\}, \;\; 0 \in B$.

$A \subseteq B$ (A is a subset of B) means every element of A is also in B.

For $A = \{1,2\}$, $B = \{1,2,3\}$ $A \subseteq B$

Sets

Be careful about these two operations:

If $A = \{1,2,3,4,5\}$

$\{1\} \subseteq A$, but $\{1\} \notin A$

$\in$ asks: is this item in that box?

$\subseteq$ asks: is everything in this box also in that box?

Try it!

Let $A = \{1,2,3,4,5\}$

$B = \{1,2,5\}$

Is $A \subseteq A$?

Is $B \subseteq A$?

Is $A \subseteq B$?

Is $\{1\} \in A$?

Is $1 \in A$?

Try it!

Let $A = \{1,2,3,4,5\}$

$B = \{1,2,5\}$

Is $A \subseteq A$?	Yes!
Is $B \subseteq A$?	Yes
Is $A \subseteq B$?	No
Is $\{1\} \in A$?	No
Is $1 \in A$?	Yes

Definitions

$A \subseteq B$ ("A is a subset of B") iff every element of A is also in B.

$$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$$

$A = B$ ("A equals B") iff A and B have identical elements.

$$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \land B \subseteq A$$

Proof Skeleton

How would we show $A \subseteq B$?

$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$

Let x be an arbitrary element of A

…

So x is also in B.

Since x was an arbitrary element of A, we have that $A \subseteq B$.

Proof Skeleton

That wasn't a "new" skeleton! It's exactly what we did last week when we wanted to prove $\forall x(P(x) \rightarrow Q(x))$!

What about $A = B$?

$$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$$

Just do two subset proofs!

i.e. $\forall x(x \in A \rightarrow x \in B)$ and $\forall x(x \in B \rightarrow x \in A)$

What do we do with sets?

We combined propositions with $\vee, \wedge, \neg$.

We combine sets with $\cap$ [intersection],$\cup$, [union] $\bar{}$[complement]

$$A \cup B = \{x : x \in A \vee x \in B\}$$

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

$$\bar{A} = \{x : x \notin A\}$$

That's a lot of elements...if we take the complement, we'll have some "universe" $\mathcal{U}$, and $\bar{A} = \{x : x \in U \wedge x \notin A\}$
It's a lot like the domain of discourse.

Proofs with sets

A proof!

What's the analogue of DeMorgan's Laws…

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

A proof!

What's the analogue of DeMorgan's Laws…

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$
Let x be an arbitrary element of $\bar{A} \cap \bar{B}$.
…
That is, x is in the complement of $A \cup B$, as required.
Since x was arbitrary $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$
Let x be an arbitrary element of $\overline{A \cup B}$.
…
we get $x \in \bar{A} \cap \bar{B}$
Since x was arbitrary $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Since the subset relation holds in both directions, we have $\bar{A} \cap \bar{B} = \overline{A \cup B}$

A proof!

What's the analogue of DeMorgan's Laws…

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \land B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$
Let x be an arbitrary element of $\bar{A} \cap \bar{B}$.
By definition of $\cap$ $x \in \bar{A}$ and $x \in \bar{B}$. By definition of complement, $x \notin A \land x \notin B$.
Applying DeMorgan's Law, we get that it is not the case that $x \in A \lor x \in B$.
That is, x is in the complement of $A \cup B$, as required.
Since x was arbitrary $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$
Let x be an arbitrary element of $\overline{A \cup B}$.
By definition of complement, x is not an element of $A \cup B$. Applying the definition of union, we get, $\neg(x \in A \lor x \in B)$
Applying DeMorgan's Law, we get: $x \notin A \land x \notin B$
By definition of $\cap$ and complement, we get $x \in \bar{A} \cap \bar{B}$
Since x was arbitrary $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Since the subset relation holds in both directions, we have $\bar{A} \cap \bar{B} = \overline{A \cup B}$

Proof-writing advice

When you're writing a set equality proof, often the two directions are nearly identical, just reversed.

It's very tempting to use that $x \in A \leftrightarrow x \in B$ definition.

Be VERY VERY careful. It's easy to mess that up, at every step you need to be saying "if and only if."

Summary: How to show an if and only if

To show $p \leftrightarrow q$ you have two options:

Option A (STRONGLY recommended)

(1) $p \rightarrow q$

(2) $q \rightarrow p$

Option B (discouraged)

p if-and-only-if p' if-and-only-if p'' if-and-only-if … if-and-only-if q

EVERY step must be an if-and-only if (in your justification AND explicitly written).

Two More Set Operations

Set-Builder Notation

Build your own set!

$\{x : \texttt{Conditions}(x)\}$

"The set of all x such that $\texttt{Conditions}(x)$"

In general

$\{\, variable : conditions \,\}$

Will also see | instead of :

Everything that meets the conditions (causes the expression after the : to be true) is in the set. Nothing else is.

$\{x{:}\texttt{Even}(x)\} = \{\dots, -4, -2, 0, 2, 4, \dots\}$

$\{y{:}\texttt{Prime}(y) \wedge \texttt{Even}(y)\} = \{2\}$

Two More Set Operations

Given a set, let's talk about it's powerset.

$\mathcal{P}(A) = \{\mathrm{X}: \mathrm{X} \text{ is a subset of } A\}$

The powerset of A is the **set** of all subsets of A.

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

More Proof Techniques

Proving an exists statement

How do I convince you $\exists x(P(x))$?

Show me the x! And convince me that $P(x)$ is true for that x.

Domain: Integers

Claim $\exists x\ \mathrm{Even}(x)$

Proof: Consider $x = 2$. We see that $2 = 2 \cdot 1$. Since 1 is an integer $2 = 2k$ for an integer k, which means 2 is even by definition, as required.

Two claims, two proof techniques

Suppose I claim that for all sets A, B, C: $A \cap B \subseteq C$

That…doesn’t look right.

How do you prove me wrong?

What am I trying to prove? First write symbols for “¬(for all sets A, B, C …)”

Then ‘distribute’ the negation sign.

Two claims, two proof techniques

Suppose I claim that for all sets A, B, C: $A \cap B \subseteq C$

That…doesn’t look right.

How do you prove me wrong?

Want to show: $\exists A, B, C: A \cap B \nsubseteq C$

Consider $A = \{1,2,3\}$, $B = \{1,2\}$, $C = \{2,3\}$, then $A \cap B = \{1,2\}$, which is not a subset of C.

Proof By [Counter]Example

To prove an existential statement (or disprove a universal statement), provide an example, and demonstrate that it is the needed example.

You don’t have to explain where it came from! (In fact, you **shouldn’t)**

Computer scientists and mathematicians like to keep an air of mystery around our proofs.

(or more charitably, we want to focus on just enough to believe the claim)

Skeleton of an Exists Proof

To show $\exists x(P(x))$

Consider $x =$[the value that will work]

[Show that x does cause $P(x)$ to be true.]

So [value] is the desired x.

You’ll probably need some “scratch work” to determine what to set x to.
That might not end up in the final proof!

Proof By Cases

Let $A = \{x : \texttt{Prime}(x)\}$, $B = \{x: \texttt{Odd}(x) \vee \texttt{PowerOfTwo}(x)\}$

Where $\texttt{PowerOfTwo}(x) \coloneqq \exists c(\texttt{Integer}(c) \wedge x = 2\hat{}c)$

Prove $A \subseteq B$

We need two different arguments – one for 2 and one for all the other primes…

Proof By Cases

Let x be an arbitrary element of A.

We divide into two cases.

Case 1: x is even

If x is even and an element of A (i.e. both even and prime) it must be 2.

So it equals 2^c for $c = 1$, and thus is in B by definition of B.

Case 2: x is odd

Then $x \in B$ by satisfying the first requirement in the definition of B.

In either case, $x \in B$. Since an arbitrary element of A is also in B, we have $A \subseteq B$.

Proof By Cases

Make it clear how you decide which case your in.

It should be obvious your cases are “exhaustive”

Reach the same conclusion in each of the cases, and you can say you’ve got that conclusion no matter what (outside the cases).

Advanced version: sometimes you end up arguing a certain case “can’t happen”

Read on Your Own

Some old friends (and some new ones)

$\mathbb{N}$ is the set of **Natural Numbers; $\mathbb{N}$** = {0, 1, 2, …}
$\mathbb{Z}$ is the set of **Integers**; $\mathbb{Z}$ = {…, -2, -1, 0, 1, 2, …}
$\mathbb{Q}$ is the set of **Rational Numbers**; e.g. ½, -17, 32/48
$\mathbb{R}$ is the set of **Real Numbers**; e.g. 1, -17, 32/48, π,$\sqrt{2}$
[n] is the set **{1, 2, ..., n}** when **n** is a positive integer
{} = ∅ is the **empty set**; the *only* set with no elements

Some old friends (and some new ones)

Our natural numbers start at 0.
Common in CS, other resources start at 1.

$\mathbb{N}$ is the set of **Natural Numbers;** $\mathbb{N}$ = {0, 1, 2, …}

$\mathbb{Z}$ is the set of **Integers**; $\mathbb{Z}$ = {…, -2, -1, 0, 1, 2, …}

$\mathbb{Q}$ is the set of **Rational Numbers**; e.g. ½, -17, 32/48

$\mathbb{R}$ is the set of **Real Numbers**; e.g. 1, -17, 32/48, π,$\sqrt{2}$

[n] is the set **{1, 2, …, n}** when **n** is a positive integer

{} = $\varnothing$ is the **empty set**; the *only* set with no elements

In LaTeX \mathbb{R}
In Office \doubleR

Use this symbol not {}.
In LaTex \varnothing In Office \emptyset.

More Connectors!

$A \setminus B$ "A minus B"

$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

$A \bigoplus B$ "XOR" (also called "symmetric difference")

$$A \bigoplus B = \{x : x \in A \bigoplus x \in B\}$$

More Connectors!

$A \times B = \{(a, b): a \in A \land b \in B\}$

Called “the Cartesian product” of A and B.

$\mathbb{R} \times \mathbb{R}$ is the “real plane” ordered pairs of real numbers.

$\{1,2\} \times \{1,2,3\} = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}$