

Sets

David L. Dill
Department of Computer Science
Stanford University

1 / 37

Announcements

Problem session at 7 PM today.

New room for problem session: Meyer Forum (in the Meyer Library).

New lecture room: Pending.

2 / 37

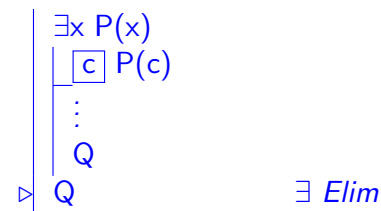
Outline

- Existential Elimination
- Axiomatic method
- First-Order Language of Sets
- Axiom of Extension
- Axiom of Comprehension
- Empty Set, Subset, Superset
- Intersection and Union
- Powerset
- Russell's Paradox

3 / 37

Existential Elimination

Also called Existential Instantiation.



Important: c must not appear in Q .

4 / 37

Example Proof Using Existential Elimination

This is true:

$$\exists x \forall y R(x, y) \Rightarrow \forall y \exists x R(x, y).$$

Intuition: If there is one person who likes everyone, then everyone is liked by someone.

It can be proved in System F :

| | | | |
|----|-------------------------------|----------------------|-----------------------|
| 1. | $\exists x \forall y R(x, y)$ | | |
| 2. | $\boxed{a} \forall y R(a, y)$ | | |
| 3. | \boxed{b} | | |
| 4. | $R(a, b)$ | \forall Elim: 2 | |
| 5. | $\exists x R(x, b)$ | \exists Intro: 4 | |
| 6. | $\forall y \exists x R(x, y)$ | \forall Intro: 3–5 | |
| 7. | $\forall y \exists x R(x, y)$ | | \exists Elim: 2–6,1 |

5 / 37

Informal Proof Using Existential Instantiation

Facts:

By definition, n is rational if there exist integers p and q such that $n = p/q$.

For each pair of integers m and n , there exists a largest common factor k such that $m = ak$ and $n = bk$ for some integers a and b .

Theorem: Every rational number n can be written in the form p/q , where p and q are integers having no common factors.

proof: By definition, every rational number n there exist integers u and v such that $n = u/v$. Let k be the largest integer that evenly divides u and v . Then u/k and v/k are the desired p and q . \square

This proof used Existential Instantiation twice, once for each of the two facts at the top of the slide.

It also uses Existential Generalization, because it constructs the specific p and q to demonstrate their existence.

6 / 37

Existential Instantiation

Corresponds to Existential Elimination in Fitch.

- Observe that there exists something with property P.
- “Call it a,” where a is a new name (or “Let the even prime be a”).
- Prove Q.

Caution: Keep track of whether a depends on a previously instantiated universal variable.

Fallacious proof:

Let n be any number.

Since every number has a larger number, there is a number m such that $m > n$.

But, since n was chosen arbitrarily, every number must be less than m .

Problem: choice of m depended on prior choice of n .

7 / 37

Theories

A *sentence* in predicate logic is a formula with no free variables.

Another word for “sentence” is *closed formula*.

A *signature* is the set of predicate and function (and constant) symbols that are available in what I have been calling a “dialect” of predicate logic.

For example, a signature for integer arithmetic might consist of \leq , 0, 1, and $+$.

8 / 37

Theories, cont.

A *theory* with a given signature is a set of sentences (the true statements in that theory.)

Since the set of sentences is infinite, they are not listed explicitly. In fact, there may not be any way to check whether a sentence is in a theory or not.

Usually, *proofs* are used to show that a sentence is in a theory.

9 / 37

Axioms

The usual approach to defining a theory in logic, so that you can do proofs, is to define a set of axioms.

Axioms are assumptions that define the properties of functions and predicates in a domain of interest.

The process of defining them is called *axiomatizing a theory*.

Axioms are implicit premises for every proof.

For many first-order theories of interest, there are infinitely many axioms. So we can't write them down. The best we can do is give a precisely defined test for what is and is not an axiom.

Mathematicians and logicians like to define systems with the minimum signatures and axioms they can, because it makes mathematics about the system easier to do.

Using the system is easier if there are lots of theorems and operators. These are typically defined or proved from a minimal signature and set of axioms.

10 / 37

Set Theory

Informally, a set is a collection of “things.” The “things” are specified (or understood) and can be anything – including other sets.

Primary goal: Teach concepts of set theory.

Secondary goals:

- Use the logic we just learned.
- See how logic is used to build up a big theory.

11 / 37

The First-Order Language of Sets

- Boolean Connectives, quantifiers
- Individual constants and variables.
- Binary relations: = and \in .

There are two “sorts” of variables: variables that can be anything, and variables that must be sets.

We'll generally use lower-case for “anything” variables and upper case for variables that have to be sets.

$x \in A$ is pronounced “ x is a member of A .” (People also say “included” or “contained”, but those words are also used for subset, which is confusing).

That's it. Everything else (e.g., \emptyset , \subseteq , \supseteq , \cap , \cup) is defined in terms of these.

Note: $x \notin A$ is an abbreviation for $\neg(x \in A)$.

12 / 37

Frequently Occurring Sets

The *natural numbers*, $\mathbf{N} = \{0, 1, 2, \dots\}$.

The *integers*, $\mathbf{Z} = \{\dots - 2, -1, 0, 1, 2, \dots\}$.

The *rational numbers*, $\mathbf{Q} = \{p/q \mid p \in \mathbf{Z} \wedge q \in \mathbf{N} \wedge q \neq 0\}$

The *reals*, \mathbf{R} (rationals, plus π , e , $\sqrt{2}$, etc.)

Notation: $\forall i \in \mathbf{N} (\text{even}(i) \leftrightarrow \neg \text{odd}(i))$ is an abbreviation for
 $\forall i [i \in \mathbf{N} \rightarrow (\text{even}(i) \leftrightarrow \neg \text{odd}(i))]$

13 / 37

Axiom of Extension

Set theory can be described by a set of simple axioms from which all theorems can be derived.

The *axiom of extension* says that two sets are equal if they have exactly the same members (there is nothing to a set other than its members).

$$\forall A \forall B [\forall x (x \in A \leftrightarrow x \in B) \rightarrow A = B]$$

Consequences:

Order doesn't matter: $\{1, 2\} = \{2, 1\}$

Duplicates don't matter: $\{1, 2, 1\} = \{1, 2\}$

In each case, the axiom of extension says they have to be equal.

14 / 37

Comprehension Axiom

Informally, this says: "Every property defines a set."

"Property" means a first-order formula.

The comprehension axiom says that any set we can define using *set builder notation* actually exists.

$$\{n \mid n \in \mathbf{N} \wedge \exists k (k \in \mathbf{N} \wedge n = 2k)\}$$

We sometimes abbreviate this:

$$\{n \in \mathbf{N} \mid \exists k \in \mathbf{N} (n = 2k)\}$$

If $P(x)$ is some first-order formula, $\exists A \forall x (x \in A \leftrightarrow P(x))$ holds.

Detail: Due to the limitations of first order logic, the "axiom" of comprehension is actually an *infinite collection* of first-order axioms, one for each property P .

The comprehension axiom is actually a "pattern" of axioms. An infinite collection of axioms like this is called an *axiom scheme*.

15 / 37

List Notation for a Set

To describe a finite set, you can list the elements explicitly.

This is sometimes called the *extensional representation* of the set.

E.g., $\{1, 2, 3\}$.

This is also an abbreviation for the use of the comprehension axiom.

We can define a set A which is $\{1, 2, 3\}$ in FOL as follows:

$$\forall x (x \in A \leftrightarrow (x = 1 \vee x = 2 \vee x = 3)),$$

then use A whenever we need the set.

16 / 37

The empty set

The axioms of comprehension and extension can be used to show that there exists a unique *empty set*

The comprehension axiom says this set exists: $\{x \mid x \neq x\}$.

The extension axiom can be used to prove that there is only one empty set.

The empty set could be written $\{\}$, but is usually written \emptyset .

17 / 37

Subset

Subset is usually written \subseteq (sometimes older books use \subset).

A is a *subset* of B if [FOL formula?]

A is a *proper subset* of B ($A \subset B$ or $A \subsetneq B$) if it is a subset but $A \neq B$.

If $A \subseteq B$ then $B \supseteq A$ (B is a *superset* of A), etc.

We can prove these properties using only the definitions so far:

Reflexivity $A \subseteq A$

Transitivity If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Anti-symmetry If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

18 / 37

Subset

Subset is usually written \subseteq (sometimes older books use \subset).

A is a *subset* of B if [FOL formula?] $\forall x (x \in A \rightarrow x \in B)$

A is a *proper subset* of B ($A \subset B$ or $A \subsetneq B$) if it is a subset but $A \neq B$.

If $A \subseteq B$ then $B \supseteq A$ (B is a *superset* of A), etc.

We can prove these properties using only the definitions so far:

Reflexivity $A \subseteq A$

Transitivity If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Anti-symmetry If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

19 / 37

Informal Proofs of Set Equality

The preceding gives two common proof strategies for showing that two sets are equal:

- Prove they have the same members: Show that $x \in A$ iff $x \in B$ for each x .
We have already talked about strategies for proving \leftrightarrow .
- Prove $A \subseteq B$ and $B \subseteq A$. Each of these proofs is likely to be of the form "Let x be any member of A ... so, $x \in B$, also."
(But there are often other ways to show $B \subseteq A$).

These are closely related, since you can do the first kind of proof by proving implication in each direction.

As usual, explain what you are doing:

"First, we prove that $A \subseteq B$..."

"Now, we prove that $B \subseteq A$..."

"Therefore, $A = B$."

20 / 37

Singleton Sets

Given an object y , there exists a set with y as its only member: $\{y\}$.

Using the property $x = y$, the Comprehension axiom says so:
 $\exists A \forall x (x \in A \leftrightarrow x = y)$

That's not quite correct: The only problem with the above is that the logical formula is not a sentence. There is a *free variables* in our property: y .

There is more to the comprehension axiom than I said. Here's the full story: If P is some first-order formula with free variables x, z_1, z_2, \dots, z_n , there is a set:

$$\forall z_1 \forall z_2 \dots \forall z_n \exists A \forall x (x \in A \leftrightarrow P(x, z_1, \dots, z_n))$$

Here is the *correct* sentence defining the singleton A

$$\forall y \exists A \forall x (x \in A \leftrightarrow x = y)$$

21 / 37

Singleton Sets are not Individuals

x and $\{x\}$ are totally different things.

x could be a set of many things, or a number or other non-set.

$\{x\}$ is a set of exactly one thing.

Example:

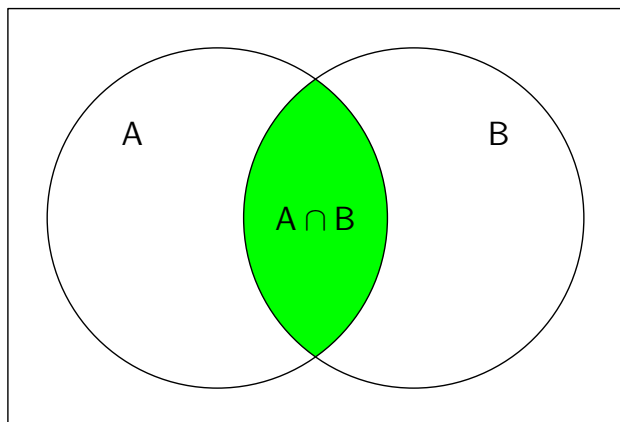
\emptyset is a set of zero things.

$\{\emptyset\}$ is a set of one thing.

22 / 37

Intersection

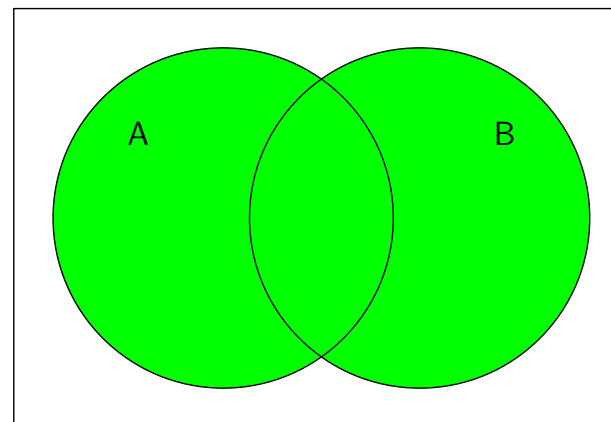
$A \cap B$ (set intersection) can be defined as $\{x \mid x \in A \wedge x \in B\}$.



23 / 37

Union

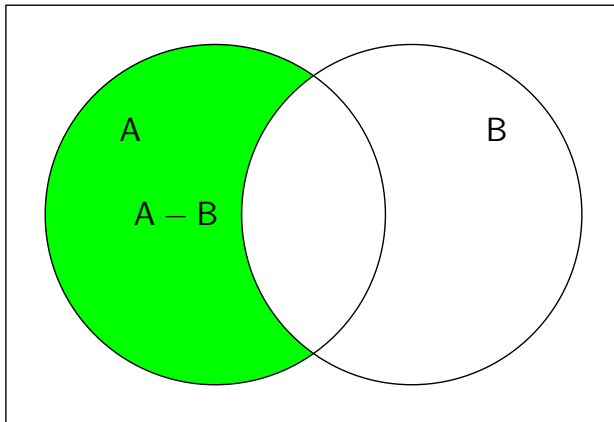
$A \cup B$ (set union) can be defined as $\{x \mid x \in A \vee x \in B\}$.



24 / 37

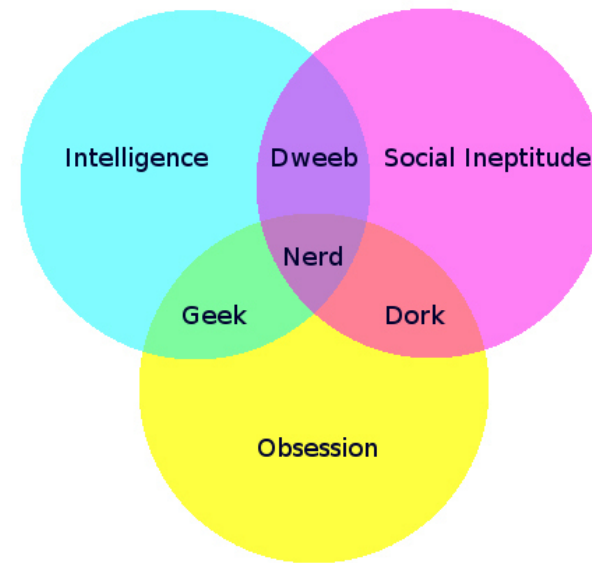
Set Difference

$$A - B = \{x \in A \mid x \in A \wedge x \notin B\}$$



25 / 37

Nerd Theory



26 / 37

Union or Intersection of a Set of Sets

It's also possible to define unions and intersections over sets of sets (even infinite sets of sets). Let \mathcal{C} be a *set of sets*. Then,

$$\bigcup \mathcal{C} = \{x \mid \exists A \in \mathcal{C} (x \in A)\}$$

$$\bigcap \mathcal{C} = \{x \mid \forall A \in \mathcal{C} (x \in A)\}$$

Examples:

$$\bigcup \{\{1, 2, 5\}, \{1, 3, 5\}, \{1, 2\}, \{1, 4\}\} = \{1, 2, 3, 4, 5\}$$

$$\bigcap \{\{1, 2, 5\}, \{1, 3, 5\}, \{1, 2\}, \{1, 4\}\} = \{1\}$$

27 / 37

Useful Properties of Set Operations

Let A , B , and C be any sets (*i.e.*, these are all universally quantified).

$$\emptyset \subseteq A$$

$$A \cap B = B \cap A$$

$$A \cup B = B \cup A$$

$$A \cap B = B \equiv B \subseteq A$$

$$A \cup B = B \equiv A \subseteq B$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

There is an obvious resemblance to the laws of Boolean algebra.

Why?

28 / 37

Powerset

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

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Also written 2^A . (Note: if A is a finite set with n members, the powerset has 2^n members.)

Example: If $A = \{1, 2, 3\}$, what is the powerset?

Example: What is $\mathcal{P}(\emptyset)$?

Powerset

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

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Also written 2^A . (Note: if A is a finite set with n members, the powerset has 2^n members.)

Example: If $A = \{1, 2, 3\}$, what is the powerset?

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Note that this has $2^3 = 8$ members.

Example: What is $\mathcal{P}(\emptyset)$?

Powerset

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

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}$$

Also written 2^A . (Note: if A is a finite set with n members, the powerset has 2^n members.)

Example: If $A = \{1, 2, 3\}$, what is the powerset?

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Note that this has $2^3 = 8$ members.

Example: What is $\mathcal{P}(\emptyset)$?

$\mathcal{P}(\emptyset) = \{\emptyset\}$ Note that it has $2^0 = 1$ member.

Hints for Informal Proofs

Often, when you want to prove something about a set $\{x \mid P(x)\}$ the first step should be:

Restate the premise or goal using $P(x)$.

For example: Suppose $A = \{x \mid P(x)\}$ and $B = \{x \mid Q(x)\}$, and you want to prove $A \subseteq B$. All you really have to do is prove $\forall x (P(x) \rightarrow Q(x))$.

- Start with “Let x be any object such that $P(x)$ ”
- Prove $Q(x)$ somehow.
- Conclude $A \subseteq B$.

This is a special case of the general heuristic: “First, try expanding the definitions.”

Russell's Paradox

"A theory should be as simple as possible, but no simpler." —
Albert Einstein

There is a minor problem with the theory we've presented:

IT'S WRONG.

It is "inconsistent" – meaning that it is possible to prove a contradiction.

Why is this a bad thing?

33 / 37

Russell's Paradox

"A theory should be as simple as possible, but no simpler." —
Albert Einstein

There is a minor problem with the theory we've presented:

IT'S WRONG.

It is "inconsistent" – meaning that it is possible to prove a contradiction.

Why is this a bad thing? It makes proofs too easy — prove \perp , then use \perp Elim.

34 / 37

Russell's Paradox

We can use the axiom of comprehension to prove that there exists a set of all sets that do not contain themselves. Let's call it Z .

In set builder notation:

$$Z = \{X \mid X \notin X\}$$

Or, writing it all out:

$$\exists Z \forall X (X \in Z \leftrightarrow X \notin X).$$

There are two cases $Z \in Z$ or $Z \notin Z$.

Suppose $Z \in Z$. Then, $Z \notin Z$, by the definition of Z (a contradiction).

Suppose $Z \notin Z$. Then, $Z \in Z$, by the definition of Z (also, a contradiction).

So, in either case, there is a contradiction.

35 / 37

No need for panic

To stay out of trouble, when you use the Comprehension Axiom, make sure a set exists that you are then restricting with a property.

Don't imagine that you have a "universal set" that has all sets.

All the properties I've claimed in this lecture except the axiom of comprehension and Russell's paradox are still true in the "fixed-up" theory.

36 / 37

Fixing Set Theory

Set theory has been patched up in several ways.

One theory of *Zermelo-Frankel set theory (ZF)*.

It replaces the Comprehension axiom with a weaker axiom, the *Axiom of Separation*, which basically says you have to have a set before you can build a set with a property.

If P is a property and A is a set (which must exist, of course), the set $\{x \mid x \in A \wedge P(x)\}$ also exists.

(Alternative notation: $\{x \in A \mid P(x)\}$ also exists.)

Formally: $\forall A \exists B \forall x (x \in B \leftrightarrow x \in A \wedge P(x))$

(actually, need to have the $\forall z_1 \dots$ in front for other free variables).

This change then breaks other things: We can't prove that unions, powersets, etc. exist using only the axiom of separation, so there are additional axioms to say various sets exist, plus some other subtle ones.