

CS103A

9/26/08

When submitting assignments electronically, use the following as the Instructor's Email Address:

cs103a.submit@gmail.com

and **Robert Plummer** as the instructor's name.

Also, be sure to download the Hints and Solutions from:

lpl.stanford.edu

What is a proof?

Science: "prove" a hypothesis using inductive reasoning, i.e., the scientific method.

We gather bits of specific information together and use our own knowledge and experience in order to make an observation about what must be true.

Does not produce mathematical certainty.

Everyday example:

Observation: John came to class late this morning.

Observation: John's hair was uncombed.

Prior experience: John is very fussy about his hair.

Conclusion: John overslept

Do we ever use inductive reasoning in mathematics?

Yes, we use it to form hypotheses.

$$\begin{aligned} 1 &= 1^2 \\ 1 + 3 &= 2^2 \\ 1 + 3 + 5 &= 3^2 \\ 1 + 3 + 5 + 7 &= 4^2 \end{aligned}$$

What is a proof?

Law: convince one set of 12 people, or a judge, none of whom may be experts in the subject matter, that your explanation is valid. Can use deductive and inductive reasoning, precedent, psychological tricks, etc.

What is a proof?

Math: we do proofs with deductive reasoning and the rules of logic.

A proof is a step-by-step demonstration that a conclusion follows from some premises.

Each step is a logical consequence of the ones that come before it.

All proofs must be **rigorous**. That is, each step in a proof must provide definitive evidence that the intermediate conclusion follows from things already established.

- (a) If my glasses are on the kitchen table, then I saw them at breakfast.
- (b) I was reading the newspaper in the living room or I was reading the newspaper in the kitchen.
- (c) If I was reading the newspaper in the living room, then my glasses are on the coffee table.
- (d) I did not see my glasses at breakfast.
- (e) If I was reading my book in bed, then my glasses are on my bed table.
- (f) If I was reading the newspaper in the kitchen, then my glasses are on the kitchen table.

Intermediate conclusions:

Conclusion: My glasses are on the coffee table.

Formal vs. Informal Proofs

Formal proof

- Uses a fixed set of rules that specify what kinds of steps are acceptable
- Usually presented in a highly stylized way
- No steps are left out

Informal proof

- Uses a less formal version of rules
- Usually stated in English
- Obvious steps are omitted

Formal and informal proofs are both **rigorous**. They differ in style.

Fitch-Style Formal Proofs

Fitch, Frederic (1908-1987)

US philosopher who, in his classic textbook *Symbolic Logic* (1952) gave a particularly elegant formulation of natural deduction, which is the basis of the system used in LPL.

In LPL, the system is called **F**.

Fitch wanted a system with a standardized way of laying out a proof that makes clear:

- What the premises are
- How each step in the proof is obtained from previous steps

He also wanted a small but complete set of inference rules, so that things could be proved about the system itself.

Fitch-Style Formal Proofs

We lay out proofs in **F** like this:

| | |
|----------------|------|
| P ₁ | |
| P ₂ | |
| ... | |
| P _n | |
| S ₁ | Rule |
| S ₂ | Rule |
| ... | |
| S _m | Rule |
| S | Rule |

Fitch-Style Formal Proofs

We lay out proofs in **F** like this:

| | | |
|----------------|------|---|
| P ₁ | | Premises |
| P ₂ | | |
| ... | | |
| P _n | | |
| S ₁ | Rule | A rule must be given to justify each step |
| S ₂ | Rule | |
| ... | | |
| S _m | Rule | |
| S | Rule | The conclusion is the last line |

The "Fitch bar" separates the premises from the rest of the proof

Sentences derived from premises and preceding derived sentences

We normally number the steps, so we can refer to them in rules.

Fitch-Style Formal Proofs

We lay out proofs in **F** like this:

| | |
|------------|-------------|
| 1. Cube(c) | |
| 2. c = b | |
| 3. Cube(b) | =Elim: 1, 2 |

Fitch-Style Formal Proofs

Proofs in **F** will involve:

Atomic sentences

The identity relation =

Boolean Connectives (truth-functional connectives)

| | symbol | meaning | example |
|-------------|--------|---------|---------|
| disjunction | ∨ | or | P ∨ Q |
| conjunction | ∧ | and | P ∧ Q |
| negation | ¬ | not | ¬P |

We use the connectives to build larger sentences from smaller ones

Boolean Connectives (truth-functional connectives)

| | symbol | meaning | example |
|-------------|----------|---------|--------------|
| disjunction | \vee | or | $P \vee Q$ |
| conjunction | \wedge | and | $P \wedge Q$ |
| negation | \neg | not | $\neg P$ |

For each connective (and the identity relation) we will have:

- An introduction rule
A way to produce a sentence using the connective from sentences that don't
- An elimination rule
A way to produce a sentence that doesn't use the connective from sentences that do

Identity Elimination: = Elim

Substitution of equals

If $b = c$, then whatever holds for b for c .

From
 $\dots b \dots$ (i.e. a sentence involving b)
 and
 $b = c$

we can conclude

$\dots c \dots$ (the same sentence with c substituted for b)

| | |
|------------|--------------|
| 1. Cube(d) | |
| 2. $d = e$ | |
| 3. Cube(e) | = Elim: 1, 2 |

Identity Elimination: = Elim

| | |
|-------|-------------------------|
| . | |
| . | |
| P(n) | P is a sentence using n |
| . | |
| . | |
| n = m | |
| . | |
| . | |
| P(m) | =Elim |

Identity Elimination: = Elim

| | |
|---------|-------------------------|
| . | |
| . | |
| 4 P(n) | P is a sentence using n |
| . | |
| . | |
| 8 n = m | |
| . | |
| . | |
| P(m) | =Elim: 4, 8 |

Identity Introduction: = Intro

Reflexivity of =

At any point in a proof, we can introduce $a = a$, where a is any name or complex term.

No other steps need be cited in the justification.

| | |
|------------|--------------|
| 1. $a = b$ | |
| 2. $a = a$ | = Intro |
| 3. $b = a$ | = Elim: 2, 1 |

Symmetry of Identity

Identity Introduction: = Intro

| | |
|-------|---------|
| . | |
| . | |
| . | |
| a = a | = Intro |
| . | |
| . | |
| . | |

| | | |
|----|---------|-------------|
| 1. | $a = b$ | |
| 2. | $b = c$ | |
| | | |
| 3. | $a = c$ | = Elim 1, 2 |

Transitivity of Identity

Reiteration: Reit

Any step in a proof can be repeated.

| | | |
|--|---|------|
| | P | |
| | . | |
| | . | |
| | . | |
| | P | Reit |

This is never necessary, but sometimes it can make a proof easier to understand.

Demonstration of Nonconsequence

To show that a conclusion does not follow from a set of premises:

find a possible circumstance where the premises are true and the conclusion is false.

| | | |
|--|-------|---|
| | P_1 | Instead of trying the proof, we might try to find a <u>counterexample</u> . |
| | P_2 | |
| | ... | |
| | P_n | |
| | | |
| | Q | |

Demonstration of Nonconsequence

To show that a conclusion does not follow from a set of premises:

find a possible circumstance where the premises are true and the conclusion is false.

| | |
|--|---------------|
| | SameRow(b, c) |
| | SameRow(a, d) |
| | SameCol(d, f) |
| | FrontOf(a,b) |
| | |
| | FrontOf(f, c) |

Demonstration of Nonconsequence

To show that a conclusion does not follow from a set of premises:

find a possible circumstance where the premises are true and the conclusion is false.

| | |
|--|---------------|
| | SameRow(b, c) |
| | SameRow(a, d) |
| | SameCol(d, f) |
| | FrontOf(a,b) |
| | |
| | FrontOf(f, c) |