Notes 1

1 Introduction

1.1 Administrivia

Introductions.

Books in the COOP are under 18.062

Recitation is a must, since new material will be covered.

HW policies:

- Homework due Tuesday at *start* of class.
- Late work penalized till Thursday. Then a zero.
- Collaboration is encouraged, but you must
  - understand and write up the solution yourself in your own words
  - cite *all* your collaborators.

HW1 due next Tuesday. More and easier questions than usual.

1.2 Class Content

- proofs
- abstraction
- tools that ease proofs and abstraction

We will spend the whole semester introducing various abstractions and tools. To begin, we concentrate on proofs, studying them in relation to abstractions we already know.

1.3 Propositions

Knowledge consists of *propositions*, such as

- 2+3=5
- if $a = b$ and $b = c$ then $a = c$
- The sum of the interior angles of a triangle is 180°
- Every even integer greater than 2 is the sum of two prime numbers (Goldbach's conjecture).
- For all $n \geq 1$, $1 + 2 + \cdots + n = n(n+1)/2$
- For all $n \geq 0$, $n^2 + n + 41$ is a prime number.
- With perfect play, chess is a win for white.
- The Pentium chip divides properly.
- Every map can be colored with four colors, so that no two adjacent regions have the same color (Four Color Theorem).
- With a fair coin, the probability of getting 50 heads in 100 tosses is 1/2.

Each of these propositions is either *true* or *false.* We (and Intel) would like to know which.

Notes:

- Not all sentences are propositions:
  - $+2 ** = 3$
  - What time is it?
  - this proposition is false
- Propositions involve previously *defined* terms:
  - prime, map, triangle, chess, fair coin, probability
  - $+$, $=$, 1, $\geq$

Many ways to decide what's true:

- evidence (eg, general relativity, big bang),

- reputable authority (eg, Professor),
- inner conviction (eg, religion),

But these methods can go wrong:

- evidence: $n^2 + n + 41$. Program works fine on all test cases, but...,
- authority: Intel says Pentium is fine
- conviction: there aren't any bugs in *my* programs...

so mathematics focuses on a particularly convincing kind of argument: a *proof.*

- begin with true propositions
- combine using specific inference rules
- derive more true propositions

Goal: know and admit *all* unproven assumptions.

Theorem 1 $\frac{d}{dx}\ln(3x+1) = \frac{3}{3x+1}$

Proof.

$$\begin{aligned} \frac{d}{dx}1 &= 0 \\ \frac{d}{dx}3x &= 3 \\ \frac{d}{dx}(u+v) &= \frac{d}{dx}u + \frac{d}{dx}v \end{aligned}$$

Combine, with $u = 3x$, $v = 1$:

$$\begin{aligned} \frac{d}{dx}(3x+1) &= 3 \\ \frac{d}{dx}\ln u &= \frac{1}{u}\frac{du}{dx} \end{aligned}$$

Combine, with $u = 3x + 1$. ■

This was a *direct proof:* start with knowns, plug together till you get desired result.

1.4 Why Proofs?

Proofs convince others.

A proof assures you haven't made mistakes.

A proof can often be reused, like a well written program.

A proof pins down *why* something is true, so you can know whether it will stay true when things change.

A failure to prove something often reveals the reason it is false.

Program verification: proof that a program does the right thing.

- Pentium
- Airbus A300
- Therac 25

2 Nuts and Bolts

2.1 Logical Proof Systems

A logical proof system consists of:

- A **language** for stating propositions
- **Axioms:** statments accepted as true
- **Rules of inference:** acceptable ways of combining propositions
- **Theorems:** propositions that can be derived by applying the inference rules to the axioms.

Note: we must always have some axioms: there are no "self evident" propositions.

A system is

- **consistent** if a statement and its complement cannot both be derived.
- **complete** if can prove or disprove every proposition

Russell and Whitehead, *Principia Mathematica*, tried to completely axiomatize mathematics but failed.

Gödel's Theorems:

- no axiomatization of arithmetic is complete and consistent.
- "arithmetic is consistent" is a proposition that cannot be proved in arithmetic.
- Gensen: "arithmetic is consistent" can be proved by adding some reasonable-sounding axioms, but these axioms can't be proved consistent.

There are true facts in math that cannot be proven!

2.2 Our Language

2.2.1 Boolean Operators

Boolean symbols are useful for brevity and precision, just like arithmetic symbols. If

- p denotes "I like chocolate"
- q denotes "I like ice cream"

then

- $p \wedge q$ means "p and q" (I like chocolate and I like ice cream). True iff p and q are both true.
- $p \vee q$ means "p or q." True iff *one or both* of p and q is true. *Not* an exclusive or. (How could I formulate exclusive or?)
- $p \Rightarrow q$ means "p implies q" or "if p then q" (If I like chocolate, then I like ice cream). True iff p being true makes q true.
- **note:** $p \Rightarrow q$ is certainly true when p is false!

2.2.2 Sets

A *set* is a collection of objects:

- $x \in S$ means "x is in the set S"

- $\emptyset$ is the empty set (contains no elements).
- $A \cap B$ means "the intersection of A and B" (the set of elements in both sets).
- $A \cup B$ means "the union of A and B" (elements in either set).

We won't be axiomatic about sets ("naive set theory").

2.2.3 Predicates

Predicates are "propositions" that depend on variables. $P(x, y, z)$ denotes a predicate on variables x, y, z. For example, define:

- $R(x)$: x is an odd number
- $Q(x)$: $x > 2$
- $P(x)$: x is a prime number

These predicates are *not* propositions, because they can be true or false depending on x. They are like functions from variables to truth values.

- $P(2)$ is true
- $R(2)$ is false
- $P(4) \vee R(3)$ is true
- $Q(3) \wedge R(4)$ is false
- $Q(1) \Rightarrow R(2)$ is true.

2.3 Quantifiers

Many propositions assert that something is true for all or some elements of a given domain (e.g., all numbers). Let's agree in advance on a *universe of discourse.*

- "$\forall$" means "for all." $\forall x P(x)$ is a statement that is true if $P(x)$ is true for *every* x in the universe of discourse.
- "$\exists$" means "there exists." $\exists x P(x)$ is true if $P(x)$ is true for *at least one* x in the universe of discourse.

- "$\exists!$" means "there exists *exactly* one."
- "$\forall x \in S$" means "for every x in the set S." $(\forall x \in S)P(x)$ is equivalent to $(\forall x)(x \in S \Rightarrow P(x))$.

Quantifies can turn predicates into propositions, e.g.

$$\forall x, P(x) \wedge Q(x) \Rightarrow R(x)$$

This expression is a (true) proposition, because the variable in the predicates is *bound*.

$\forall x \exists y$ is *different* from $\exists y \forall x$:

- $S(x, y)$: student x falls asleep in class y.
- $\forall y \exists x P(x, y)$: "In every class, some student will fall asleep"
- $\exists x \forall y P(x, y)$: "There exists a student who will fall asleep in every class."
- what is my universe of discourse above?

2.4 Axioms

Axioms are propositions that are *assumed* to be true ("axiom" comes from a greek "to think worthy," not "to be true"). It is not wrong to make assumptions (in fact, it is unavoidable), but to be rigorous you have to state your assumptions explicitly.

$a = b$ and $b = c$ implies $a = c$.

Euclidean geometry has an axiom: Given a line l and a point p not on l, there is exactly one line through p parallel to l.

Spherical geometry has an axiom contradicting Euclid's: Given a line l and a point p not on l, there is *no* line through p parallel to l.

So does hyperbolic geometry: Given a line l and a point p not on l, there are *infinitely many* lines through p parallel to l.

None of these axioms is "better" than any other: in fact, all yield equally consistent logical proof systems.

Modern mathematicians still argue about which axioms are "right," e.g., the Axiom of Choice (whose affirmation and negation are equally consistent).

Of course, different axioms lead to very different theorems. But anyone who agrees with your axioms and inference rules has to accept your theorems.

2.5 Inference Rules for Propositions

When does one proposition follow from another?

Let p and q be propositions. Then if p is true, and $p \Rightarrow q$ (read p *implies* q) is true, we can conclude that q is true. This is a rule called *modus ponens.*

Modus Ponens: $\begin{array}{l} p \\ p \Rightarrow q \\ \hline q \end{array}$

Syllogism: $\begin{array}{l} p \Rightarrow q \\ q \Rightarrow r \\ \hline p \Rightarrow r \end{array}$

Modus Tolens: $\begin{array}{l} p \Rightarrow q \\ \neg q \\ \hline \neg p \end{array}$

Boolean Algebra is a useful aid in reasoning and inferring. For example,

$$[(p \vee q) \wedge \neg p] \Rightarrow q$$

so we can derive an inference rule:

Disjunctive Syllogism: $\begin{array}{l} p \vee q \\ \neg p \\ \hline q \end{array}$

2.6 Inference Rules for Predicates

Negation:

- $(\forall x)S(x)$ is equivalent to $\neg(\exists x)\neg S(x)$
  - $(\forall x)S(x)$: For all primes $x \geq 2$, x is odd.
  - $\neg(\exists x)S(x)$: There is no prime $x \geq 2$ such that x is not odd.
- $(\exists x)S(x)$ is equivalent to $\neg(\forall x)\neg S(x)$.

Universal generalization is a way to prove $\forall x P(x)$:

- "Let $x \geq 2$. Then x is prime or composite."
- Conclude: $\forall x \geq 2$, x is prime or composite (explain $\forall x \geq 2$).

We often leave out universal quantifiers if they are implicit.

Like axioms, inference rules are an *agreement* to believe certain inferences. For example, the intuitionists (e.g. Brouwer) *reject* the claim that $\neg\forall x \neg P(x)$ implies $\exists x P(x)$. They claim that to prove something exists, you actually have to construct it.

2.7 Peano's Axioms and Addition

Briefly, we will carefully follow a logical proof system (generally, we won't be so careful).

Peano's Axioms define the natural numbers $\mathbb{N}$. We add two primitive symbols: 0 and $'$ (successor).

1. $0 \in \mathbb{N}$
2. $\forall x \in \mathbb{N},\ x' \in \mathbb{N}$
3. $\forall x, y \in \mathbb{N},\ x' = y' \Rightarrow x = y$ (no two numbers have same successor)
4. $\neg\exists x \in \mathbb{N}$ such that $0 = x'$ (equivalently, $\forall x \in \mathbb{N}, x' \neq 0$)
5. (Induction) $\forall S \subseteq N$, if $0 \in S$ and $(x \in S \Rightarrow x' \in S)$, then $S = \mathbb{N}$.

Notation: $1 = 0'$, $2 = 1'$, etc.

We now *define* addition:

- $n + 0 = n$ (implicit universal quantification)
- $n + k' = (n + k)'$

This is a *recursive* definition: it lets us compute $n + k$ for any n, k. For example,

$$\begin{aligned} 3 + 2 &= 3 + 1' \\ &= (3 + 1)' \\ &= (3 + 0')' \\ &= ((3 + 0)')' \\ &= (3')' \\ &= 4' \\ &= 5. \end{aligned}$$

Addition is *commutative:* $m + n = n + m$. How can we prove this?

Lemma 2 $0 + n = n$

Proof. Let $S = \{n \in \mathbb{N} \mid 0 + n = n\}$ ("The set of all $n \in \mathbb{N}$ such that $0 + n = n$"). We prove $S = \mathbb{N}$.

- $0 \in S$ since $0 + 0 = 0$ by definition of $+$.
- if $x \in S$, so that $0 + x = x$, then

$$\begin{aligned} 0 + x' &= (0 + x)' \quad \text{(definition of } +) \\ &= x', \quad (\text{since } x \in S) \end{aligned}$$

  so $x' \in S$. In other words, $\forall x, (x \in S) \Rightarrow (x' \in S)$.

Therefore, by the induction axiom, $S = \mathbb{N}$. ∎

Lemma 3 $m' + n = m + n'$

Proof. Fix m. Let $S = \{n \mid m' + n = m + n'\}$. We prove $S = \mathbb{N}$.

- $0 \in S$, since $m' + 0 = m' = (m + 0)' = m + 0'$
- if $n \in S$, so that $m' + n = m + n'$, then

$$\begin{aligned} m' + n' &= (m' + n)' \quad \text{(definition of } +) \\ &= (m + n')' \quad (\text{true for } n) \\ &= (m + (n')' \quad \text{(definition of } +) \end{aligned}$$

Since $0 \in S$, and $n \in S \Rightarrow n' \in S$, the induction axiom proves $S = \mathbb{N}$. We proved $P(m)$, therefore by universal generalization, we know that $(\forall m)P(m)$. ∎

Lemma 4 $m + n = n + m$

Proof. Let $S = \{n \mid (\forall m) m + n = n + m\}$. We prove $S = \mathbb{N}$.

- $0 \in S$, since $m + 0 = m = 0 + m$ by Lemma 2.

- Suppose $n \in S$, so that $(\forall m) m + n = n + m$. Then

$$\begin{aligned} m + n' &= (m+n)' \quad \text{(definition)} \\ &= (n+m)' \quad \text{(true for } n\text{)} \\ &= n + m' \quad \text{(definition)} \\ &= n' + m \quad \text{(previous lemma)} \end{aligned}$$

Therefore, $S = \mathbb{N}$ by induction axiom. ∎

Have we been rigorous? No: naive set theory. Set theory axioms are harder than you might think.

Real numbers can be defined by about 10 axioms.

3 How To Prove Things

3.1 The Real World

Rigorous logical proof systems are nice, but no one really has the time or energy to be so careful. We prove things in a less formal way. The objective is to convince everyone that a truly rigorous proof could be built if someone took the time to do it. As a result, even great mathematicians can goof proofs.

- Andrew Wiles and Fermat's Last Theorem
- Kempe's invalid "proof" of the Four Color Theorem stood for 10 years (1879–1890)
- Gauss's 1799 Ph.D. thesis is usually referred to as being the first rigorous proof of the Fundamental Theorem of Algebra (every polynomial has a zero over the complex numbers). But it contains quotes like

  > "If a branch of an algebraic curve enters a bounded region, it must necessarily leave it again. ... Nobody, to my knowledge, has ever doubted [this fact]. But if anybody desires it, then on another occasion I intend to give a demonstration which will leave no doubt."

  Fields Medalist Steve Smale writes about this, calling it an "immense gap" in the proof that was not filled in until 1920, more than a hundred years later.

- In 1900 Poincare carelessly claimed a certain very simple topological characterization of the 3-dimensional sphere. Later realizing it was not so obvious, he demoted the claim to the status of a "conjecture" in 1904. The Poincare Conjecture is now one of the biggest open questions in mathematics (two Fields Medals have been given out for partial progress on it).

- In the 1940's Paul Erdos conjectured a certain combinatorial fact about arithmetic progressions (every set of natural numbers of positive density contains arbitrarily long arithmetic progressions), and offered \$1000 for a proof or disproof. Endre Szemeredi proved the conjecture in 1972, but the proof was so long and badly written that Erdos was not sure whether to believe it. Finally, Andras Hajnal stepped in and wrote a much clearer version of the same proof, which was eventually published under Szemeredi's name. At some point during the write-up, Hajnal informed Erdos that he was now confident enough of the proof that he was willing to buy it from Szemeredi for \$500.

- There's also the story of Newton waiting 20 years to publish the Principia because he didn't see how to prove one could assume all the mass of a sphere to be concentrated at its center when calculating gravitational attraction. The proof ultimately required the invention of calculus ...

3.2 What we Expect

Basic objective: like a scientific experiment, it has to be possible for someone else to "replicate" (ie, understand) your proof.

In the real world, anything that can be cited can be used without proof. But in homework, where everything we ask you to prove is already known, this defeats the purpose (namely, learning how to prove something that isn't already known).

We don't expect you to reprove arithmetic. Anything from high school math can be used without proof.

Once something has been proved, you can use it again without proof, citing the theorem. Once it has been used so often as to become commonplace, you can even stop citing the theorem.

No new axioms!

When in doubt about whether something can be stated without proof, prove it!

Elements of a proof:

- correctness
- clarity
- brevity
- elegance

"The book proof" (Paul Erdos).

There are lots of ways to prove things, we now give some examples.

3.3 Direct Proof

Direct proofs are the most straightforward: we mix together previous axioms and theorems until the desired claim is inferred.

We say a *divides* b if there exists an integer t such that $a = bt$. We write $a \mid b$.

- $3 \mid 6$
- $3 \nmid 7$

Theorem 5 *If $a \mid b$ and $a \mid c$, then $a \mid b + c$.*

Proof. By definition of divisibility, $(\exists t) b = at$ and $(\exists s) c = as$.
Therefore, $b + c = at + as = a(t + s)$.
Therefore, by definition, $a \mid b + c$. ∎

Note: distributivity was assumed without mention.

3.4 Proof by Contradiction

$$\frac{p \Rightarrow FALSE}{\neg p}$$

Proofs can go "backwards":

- Begin by assuming the desired theorem is false.
- Using inference rules, conclude something known false.
- Conclude that the assumption is wrong.

Theorem 6 *$\sqrt{2}$ is an irrational number.*

Proof. (Indirect). Assume $\sqrt{2}$ is rational.

Conclude $\sqrt{2}$ can be written as a fraction a/b in lowest terms.
Then $2b^2 = a^2$.

In other words, a^2 is even (since $2b^2$ is even).
Therefore, a is even (the square of an odd number is odd).
Therefore, a^2 is divisible by 4.
But b is odd (since a/b is in lowest terms and a is even).
Thus $2b^2$ is not divisible by 4.
Thus 4 divides a^2, but not $2b^2 = a^2$, contradiction.

Since our assumption leads to a false conclusion, it must be false. Thus, $\sqrt{2}$ is not rational. ■

Note: this process is based on the assumption that math is consistent, since otherwise it would be possible to prove something false.

We freely used lots of basic facts about divisibility, lowest terms for fractions, definitions of square, all without reference or proof.

Pythagoras and his followers knew this proof, but suppressed it because they axiomatically denied the existence of irrational numbers (so their system was not consistent, because they also had an axiom that every line had a numeric length).

3.5 A Nonconstructive Existence Proof

Theorem 7 *For any number n, there is a prime number greater than n.*

Proof. Fix n, and consider $n! + 1 = (1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n) + 1$. If $n! + 1$ is prime, we are done. Otherwise, $n! + 1$ has a prime factor x (relies on the prime number theorem). By definition, $n! + 1$ is divisible by x (without leaving a remainder). But if $n! + 1$ is divided by a number less than n, the remainder is 1. Therefore, $x > n$. ■

(Note: $n! + 1$ need not be prime. $5! + 1 = 11^2$.)

We don't know what x is, only that it exists.

Intuitionists would deny this is a proof.

3.6 Proof by Cases

Proof by cases:

- show $p \Rightarrow (a \vee b)$
- show $a \Rightarrow q$ and $b \Rightarrow q$
- deduce $p \Rightarrow q$

Theorem 8 $(\forall x P(x)) \vee A$ *implies* $\forall x (P(x) \vee A)$

Proof. To prove the theorem, we need to show that if the hypothesis is true, then the consequent is true. So suppose the hypothesis is true. There are two cases: either A is true or A is false.

Case 1: A if true. If A is true, then $P(x) \vee A$ is true regardless of the truth of $P(x)$. Thus, $\forall x (P(x) \vee A)$ is true.

Case 2: A is false. If A is false, then the only way for the hypothesis to be true is for the other disjunct, namely $(\forall x P(x))$, to be true. But if $P(x)$ is always true then certainly $P(x) \vee A$ is always true, in other words $\forall x (P(x) \vee A)$. ■

3.7 Other Proof Methods

- Indirect proof: from $\neg q \Rightarrow \neg p$, deduce $p \Rightarrow q$ (similar to proof by contradiction).
- Vacuous proof: if p is false, then $p \Rightarrow q$ is true.
  - if x is an even prime greater than 2, then x is a perfect square.

3.8 Fallacies

There are several ways to generate in incorrect proof.

$$
\begin{aligned}
\sqrt{-1} &= \sqrt{-1} \\
\sqrt{\frac{1}{-1}} &= \sqrt{\frac{-1}{1}} \\
\frac{\sqrt{1}}{\sqrt{-1}} &= \frac{\sqrt{-1}}{\sqrt{1}} \\
\sqrt{1} \cdot \sqrt{1} &= \sqrt{-1} \cdot \sqrt{-1} \\
1 &= -1
\end{aligned}
$$

Where's the bug?

There are several common fallacies:

Affirming the conclusion:

- If you are tired, you will fall asleep

- You fall asleep
- therefore, you are tired

The fact that the conclusion is true does not make the hypothesis true. Maybe you are just bored.

Denying the hypothesis:
- If you work hard, you will pass the course
- You don't work hard
- therefore, you will fail the course.

Even if the hypothesis is false, the conclusion can be true. Maybe you are smart enough to pass without working.

Circular reasoning: proposition: If n^2 is not divisible by 3, then n is not divisible by 3.

- If n^2 is not divisible by 3, then n^2 is not equal to $3k$ for any integer k.
- therefore, n does not equal $3l$ for any integer l.
- therefore, n is not divisible by 3.

If you assume (or prove) something FALSE, you can prove anything!