# Class Notes for Lecture 1

## 1 Introduction

### 1.1 6.042 Topics

- The most important discrete mathematical *structures* for modelling computer systems.

  Numbers, sets, graphs, state machines, probability distributions, ...

- The most useful mathematical *techniques* for reasoning about these mathematical structures.

  Propositional and predicate logic, induction, recurrences, generating functions, ...

- The notion of *mathematical proof* as a discipline for reasoning carefully about such structures.

  Careful proofs associated with virtually everything covered in the course, proofs in class, proofs in homework, lots of examples of pitfalls in writing proofs ...

This class is divided into 3 parts, each covering a third of the term:

- Introduction to basic notions of proofs, using simple, familiar structures like sets and natural numbers.
- Methods for analysis and counting.
- Probability.

Proofs appear throughout the term.

This course moves rapidly from topic to topic.

- Disadvantage: none last long enough for thorough coverage.
- Advantage: boredom/confusion is temporary.

# 2 Basic Proof Notions

## 2.1 Proofs – What and Why

**What is a proof?**

Layman's definition of proof: "A method of ascertaining the truth."

There are many ways to decide what's true in society and even in science:

- Law: judge and jury.
- Religion: inner conviction.
- Education: reputable authority (e.g., the professor).
- Science: evidence of experiment/observation (e.g., General Relativity, The Big Bang).
- Statistics: sampling (testing examples).

But these methods can go wrong:

- Conviction: There aren't any bugs in *my* programs....
- Authority: Intel says the Pentium is fine. Stalin said evolution was wrong.
- Religion: whose?

General problem: these methods don't convince everyone.

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

Idea: specify everything so precisely that everyone is convinced.

## 2.2 Propositions

The first thing to specify: what kind of things do we prove?

A *proposition* is a statement that is either true or false, but not both.

Knowledge consists of *propositions*, such as

- 2+3=5.
- For every $a$, $b$ and $c$, if $a = b$ and $b = c$ then $a = c$.
- The sum of the interior angles of every triangle is 180°.
- 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.
  - Evidence: 41, 43, 47, 53, 61, 71, ....
  - Works up to 40.
  - Fails at 41.
  - Proving by example is classical methodology in many fields.
  - Some examples in number theory have their first counter-example in the **billions**.
- With perfect play, chess is a win for white.
- The Pentium chip does what it claims.
- Every even integer greater than 2 is the sum of two prime numbers (Goldbach's conjecture, 1742).
  - Raised in *The Boston Globe* as "one of great unsolved mysteries."
  - Globe gave example: $20 = 9 + 11$ (oops).
- Every map can be colored with four colors, so that no two adjacent regions have the same color (Four Color Theorem).
  - First "proved" in 1879.
  - The "proof" stood for 10 years before a flaw was found.
  - Recently proved with computer aid.
  - Still debated whether this is a valid proof (need to prove the computer is working correctly).
- $a^4 + b^4 + c^4 = d^4$ has no positive integer solutions.
  - Conjectured by Euler (1769).
  - Counterexample by Elkies, 218 years later.
  - Smallest counterexample: $95800^4 + 217519^4 + 414560^4 = 422481^4$.
- With a fair coin, the probability of getting 50 heads in 100 tosses is 1/2.
- O.J. did it.
- My algorithm gives the right answer on any input.

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

Notes:

- Not all sentences are propositions:

  - $+x**z = f$.
  - What time is it?
  - This sentence is false.

- Propositions involve previously *defined* terms:
  - prime, map, triangle, chess, fair coin, probability.
  - $+$, $=$, 1, $\geq$.

## 2.3 Mathematical proofs

Now we know what we want to prove. How do we do it?

In mathematics, a proof is a verification of a proposition by a chain of logical deductions from a base set of axioms. An axiom is a proposition that is assumed to be true.

- Begin with true propositions.
- Combine using specific inference rules.
- Derive more true propositions.

One should know and admit *all* unproven assumptions (axioms).

Example:

**Theorem 2.1** $\frac{d}{dx}\ln(3x+1) = \frac{3}{3x+1}$

*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:* it started with knowns and plugged them together until it produced the desired result.

- Language: numbers, functions, derivative operator.
- Axioms: chain rule, sum rule.
- Inference Rule: substitution for equivalents.

## 2.4 Basic Concepts/Notation

Our language uses propositional logic as a substrate.

### 2.4.1 Boolean Operators

Boolean Operators can be thought of as functions with some number of inputs (each chosen from true and false) whose value for any particular inputs must also be either true or false. Boolean operators combine Boolean symbols to produce Boolean expressions. If Boolean symbols are used to represent propositions, this allows propositions to be combined to produce new propositions. Boolean expressions are useful for brevity and precision, just like arithmetic expressions. It is important to remember that Boolean operators are concerned only with whether a proposition is true or false and not with what the proposition actually might **mean**. If

- $p$ denotes "I like chocolate" and
- $q$ denotes "I like ice cream,"

then

- $\neg p$ means "not $p$" (I don't like chocolate). This expression is true iff (if and only if) $p$ is false.
- $p \wedge q$ means "$p$ and $q$" (I like chocolate and I like ice cream). This expression is true iff $p$ and $q$ are both true.
- $p \vee q$ means "$p$ or $q$." This expression is true iff *one or both* of $p$ and $q$ is true. This is *not* an exclusive or. How could you formulate an exclusive or?
- $p \implies q$ means "$p$ implies $q$" or "if $p$ then $q$" (If I like chocolate, then I like ice cream). This expression is true iff the truth values of $p$ and $q$ are *consistent* with $p$ representing something that implies whatever $q$ represents. (That is, the expression is true unless $p$ is true but $q$ is still false.) **Note:** $p \implies q$ is true when $p$ is false (by definition)!

- $p \iff q$ means "$p$ if and only if $q$" (I like chocolate if and only if I like ice cream). This expression is true iff the truth values of $p$ and $q$ are *consistent* with $p$ and $q$ representing logically equivalent things. That is, this expression is true iff $p$ and $q$ have the same truth value (either both true or both false).

A *tautology* is a Boolean expression, such as $p \vee \neg p$, that is true regardless of the truth values of its Boolean variables. Two Boolean formulas are *equivalent* iff they have the same truth value regardless of the truth values of their variables (where common variables have the same value in both expressions).

The *contrapositive* of an implication $p \implies q$ is the expression $\neg q \implies \neg p$. An implication and its contrapositive are equivalent.

**Note:** neither the converse nor the inverse of an implication are equivalent to the implication (but the converse is equivalent to the inverse).

### 2.4.2 Predicates

Predicates are similar to propositions but they 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 propositions.

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

## 2.5 Quantifiers

Many propositions assert that something is true for all or some elements of a given domain (e.g., all numbers). The following quantifiers presume a particular *universe of discourse* has been agreed upon in advance.

- "$\forall$" means "for all." $\forall x P(x)$ is a statement that is true iff $P(x)$ is true for *every* $x$ in the universe of discourse.
- "$\exists$" means "there exists." $\exists x P(x)$ is true iff $P(x)$ is true for *at least one* $x$ in the universe of discourse.
- "$\nexists$" mean "there does not exist" ("there is no").
- "$\exists!$" 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 $(\forall x)(x \in S \implies P(x))$.

Quantifiers can turn predicates into propositions, e.g.

$$\forall x, P(x) \wedge Q(x) \implies R(x).$$

Note that each appearance of $x$ is associated with the $\forall$ quantifier. A variable associated with a quantifier in this way is said to be *bound*. Since every variable in the above expression is bound, it is a proposition. If $P$, $Q$, and $R$ are the predicates defined above, this proposition is true.

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

- $S(x, y)$ : student $x$ will fall 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 the universe of discourse above?

## 2.6 Axioms

Axioms are propositions that are *assumed* to be true. One does not prove axioms. They are simply accepted as reasonable assumptions. ("Axiom" comes from 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.

The rule is **not** "don't make assumptions", but rather **"state them."**

Some typical examples of axioms from various parts of mathematics:

- If $a = b$ and $b = c$ then $a = c$.
- 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 $l$. (parallel postulate)

- Sometimes an axiom from one domain contradicts an axiom from another. 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 three axioms is "better" than any other: all yield equally consistent logical proof systems.
- Modern mathematicians still argue about which axioms are "right," e.g., the Axiom of Choice (whose assertion and denial are equally consistent with other commonly agreed upon axioms).

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

What axioms to accept will generally be no problem in this class:

- You can assume that everything you've learned so far (e.g., in high school) is true.
- This may change when we cover probability because faulty assumptions are easy to make. Testing on O.J.'s blood was an example of how probabilistic reasoning can be "assumption dependent."

## 2.7 Inference Rules for Propositions

Once you have axioms and some propositions that are believed to be true, all you need is a system of rules for combining true proposition to form new true propositions. Such rules are called *inference rules.* The most famous rule is modus ponens:

- Let $p$ and $q$ be propositions.
- If $p$ is true and $p \implies q$ is true then q is true.

This rule and some others are written below in a format where the truth of all expressions above the line permits the expression below the line to be inferred to be true.

Modus Ponens: $$\frac{\begin{array}{c} p \\ p \implies q \end{array}}{q}$$

Syllogism: $$\frac{\begin{array}{c} p \implies q \\ q \implies r \end{array}}{p \implies r}$$

Modus Tolens (proof by contradiction): $\dfrac{\begin{array}{l} p \implies q \\ \neg q \end{array}}{\neg p}$

Proof by cases: $\dfrac{\begin{array}{l} a \vee b \\ a \implies q \\ b \implies q \end{array}}{q}$

You don't have to remember the names of these rules: just use them correctly.

Boolean Algebra is a useful aid in reasoning and inferring. Mathematics accepts as inference rules all propositional tautologies. That is, if $A \to B$ is a tautology, then $\dfrac{\mathrm{A}}{\mathrm{B}}$ is a valid inference rule. For example,

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

so we can derive an inference rule:

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

In fact, you can get the same power with just three inference rules, but it makes life harder.

## 2.8 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 $x > 2$, $x$ is odd.
  - $\neg(\exists x)\neg S(x)$ : There is no prime $x > 2$ 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.

We often leave out universal quantifiers if they are implicit.

Like axioms, inference rules are an *agreement* to believe certain inferences. For example, the constructivists (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. Brouwer retracted his most famous theorem after he became a constructivist, since the proof was nonconstructive.