CS 70 Discrete Mathematics and Probability Theory
Summer 2014 James Cook
Note 1

Course Outline

CS70 is a course on "Discrete Mathematics and Probability for Computer Scientists." The purpose of the course is to teach you about:

- **Fundamental ideas in computer science:**
  - Boolean logic
  - Modular arithmetic, public-key cryptography, error-correcting codes, secret sharing protocols
  - Graphs: paths, cuts, hypercubes
  - The power of randomization ("flipping coins") in computation: load balancing, hashing, inference, overcoming noise in communication channels
  - Uncomputability and the halting problem

  Many of these concepts underlie the more advanced courses in computer science.

- **Precise, reliable, powerful thinking:**
  - Proofs of correctness. These are essential to analyzing algorithms and programs
  - Induction and recursion
  - Probability theory

- **Problem solving skills:**
  - These are emphasized in the discussion sections and homeworks.

Course outline (abbreviated)

- Propositions, propositional logic and proofs
- Mathematical induction, recursion
- The stable marriage problem
- Modular arithmetic, the RSA cryptosystem
- Polynomials over finite fields and their applications: error-correcting codes, secret sharing
- Graphs: Eulerian paths, hypercubes.
- Probability and probabilistic algorithms: load balancing, hashing, expectation, variance, concentration, conditional probability, Bayesian inference, law of large numbers.
- Diagonalization, self-reference, and uncomputability

Getting Started

In order to be fluent in mathematical statements, you need to understand the basic framework of the language of mathematics. This first week, we will start by learning about what logical forms mathematical theorems may take, and how to manipulate those forms to make them easier to prove. In the next few lectures, we will learn several different methods of proving things.

Propositions

A **proposition** is a statement which is either true or false.

These statements are all propositions:

(1) $\sqrt{3}$ is irrational.
(2) $1+1=5$.
(3) Julius Caesar had 2 eggs for breakfast on his 10^{th} birthday.

These statements are clearly not propositions:

(4) $2+2$.
(5) $x^2+3x=5$.

These statements aren't propositions either (although some books say they are). Propositions should not include fuzzy terms.

(6) Arnold Schwarzenegger often eats broccoli. (What is "often?")
(7) Barack Obama is popular. (What is "popular?")

Propositions may be joined together to form more complex statements. Let P, Q, and R be variables representing propositions (for example, P could stand for "3 is odd"). The simplest way of joining these propositions together is to use the connectives "and", "or" and "not."

(1) **Conjunction**: $P \wedge Q$ ("P and Q"). True only when both P and Q are true.

(2) **Disjunction**: $P \vee Q$ ("P or Q"). True when at least one of P and Q is true.

(3) **Negation**: $\neg P$ ("not P"). True when P is false.

Statements like these, with variables, are called *propositional forms.* If we let P stand for the proposition "3 is odd," Q stand for "4 is odd," and R for "5 is even," then the propositional forms $P \wedge R$, $P \vee R$ and $\neg Q$ are false, true, and true, respectively. Note that $P \vee \neg P$ is always true, regardless of the truth value of P. A propositional form that is always true regardless of the truth values of its variables is called a *tautology*. A statement such as $P \wedge \neg P$, which is always false, is called a *contradiction*.

A useful tool for describing the possible values of a propositional form is a **truth table**. Truth tables are the same as function tables. You list all possible input values for the variables, and then list the outputs given those inputs. (The order does not matter.)

Here are truth tables for conjunction, disjunction and negation:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	$\neg P$
T	F
F	T

The most important and subtle propositional form is an **implication**:

(4) **Implication**: $P \implies Q$ ("P implies Q"). This is the same as "If P, then Q."

Here, P is called the *hypothesis* of the implication, and Q is the *conclusion*. [1]

Examples of implications:

If you stand in the rain, then you'll get wet.
If you passed the class, you received a certificate.

An implication $P \implies Q$ is false only when P is true and Q is false. For example, the first statement would be false only if you stood in the rain but didn't get wet. The second statement above would be false only if you passed the class yet you didn't receive a certificate.

Here is the truth table for $P \implies Q$:

P	Q	$P \implies Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Note that $P \implies Q$ is always true when P is false. This means that many statements that sound nonsensical in English are true, mathematically speaking. Examples are statements like: "If pigs can fly, then horses can read" or "If 14 is odd then $1+2=18$." When an implication is stupidly true because the hypothesis is false, we say that it is *vacuously true*. Note also that $P \implies Q$ is logically equivalent to $\neg P \vee Q$, as can be seen from the above truth table.

[1] P is also called the *antecedent* and Q the *consequent*.

$P \implies Q$ is the most common form mathematical theorems take. Here are some of the different ways of saying it:

(1) if P, then Q;
(2) Q if P;
(3) P only if Q;
(4) P is sufficient for Q;
(5) Q is necessary for P;
(6) Q unless not P.

If both $P \implies Q$ and $Q \implies P$ are true, then we say “P if and only if Q" (abbreviated P iff Q). Formally, we write $P \iff Q$. P if and only if Q is true only when P and Q have the same truth values.

For example, if we let P be “3 is odd," Q be “4 is odd," and R be “6 is even," then $P \implies R$, $Q \implies P$ (vacuously), and $R \implies P$. Because $P \implies R$ and $R \implies P$, P if and only if R.

Given an implication $P \implies Q$, we can also define its

(a) **Contrapositive**: $\neg Q \implies \neg P$
(b) **Converse**: $Q \implies P$

The contrapositive of “If you passed the class, you received a certificate" is “If you did not get a certificate, you did not pass the class." The converse is “If you got a certificate, you passed the class." Does the contrapositive say the same thing as the original statement? Does the converse?

Let’s look at the truth tables:

P	Q	$\neg P$	$\neg Q$	$P \implies Q$	$Q \implies P$	$\neg Q \implies \neg P$	$P \iff Q$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	F
F	T	T	F	T	F	T	F
F	F	T	T	T	T	T	T

Note that $P \implies Q$ and its contrapositive have the *same* truth values everywhere in their truth tables; propositional forms having the same truth values are said to be **logically equivalent**, written “$\equiv$". Thus we may write $(P \implies Q) \equiv (\neg Q \implies \neg P)$. Many students confuse the contrapositive with the converse: note that $P \implies Q$ and $\neg Q \implies \neg P$ are logically equivalent, but $P \implies Q$ and $Q \implies P$ are not!

When two propositional forms are logically equivalent, we can think of them as “meaning the same thing." We will see next time how useful this can be for proving theorems.

Quantifiers

The mathematical statements you’ll see in practice will not be made up of simple propositions like “3 is odd." Instead you’ll see statements like:

(1) For all natural numbers n, $n^2 + n + 41$ is prime.
(2) If n is an odd integer, so is n^3.
(3) There is an integer k that is both even and odd.

In essence, these statements assert something about lots of simple propositions all at once. For instance, the first statement is asserting that 0^2+0+41 is prime, 1^2+1+41 is prime, and so on. The last statement is saying that as k ranges over every possible integer, we will find at least one value for which the statement is satisfied.

Why are the above three examples considered to be propositions, while earlier we claimed that "$x^2+3x=5$" was not? The reason is that in these three examples, there is an underlying "universe" that we are working in. The statements are then *quantified* over that universe. To express these statements mathematically we need two **quantifiers**: The *universal quantifier* $\forall$ ("for all") and the *existential quantifer* $\exists$ ("there exists"). Note that in a *finite* universe, we can express existentially and universally quantified propositions without quantifiers, using disjunctions and conjunctions respectively. For example, if our universe U is $\{1, 2, 3, 4\}$, then $(\exists x \in U)P(x)$ is logically equivalent to $P(1) \vee P(2) \vee P(3) \vee P(4)$, and $(\forall x \in U)P(x)$ is logically equivalent to $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$. However, in an infinite universe, such as the natural numbers, this is not possible.

Examples:

(1) "Some mammals lay eggs." Mathematically, "some" means "at least one," so the statement is saying "There exists a mammal x such that x lays eggs." If we let our universe U be the set of mammals, then we can write: $(\exists x \in U)(x \text{ lays eggs})$. (Sometimes, when the universe is clear, we omit U and simply write $\exists x(x \text{ lays eggs})$.)

(2) "For all natural numbers n, n^2+n+41 is prime," can be expressed by taking our universe to be the set of natural numbers, often denoted as $\mathbf{N}$: $(\forall n \in \mathbf{N})(n^2+n+41 \text{ is prime})$.

Some statements can have multiple quantifiers. As we will see, however, quantifiers do not commute. You can see this just by thinking about English statements. Consider the following (rather gory) example:

Example:

> "Every time I ride the subway in New York, somebody gets stabbed."
> "There is someone, such that every time I ride the subway in New York, that someone gets stabbed."

The first statement is saying that every time I ride the subway someone gets stabbed, but it could be a different person each time. The second statement is saying something truly horrible: that there is some poor guy Joe with the misfortune that every time I get on the New York subway, there is Joe, getting stabbed again. (Poor Joe will run for his life the second he sees me.)

Mathematically, we are quantifying over two universes: $T = \{\text{times when I ride on the subway}\}$ and $P = \{\text{people}\}$. The first statement can be written: $(\forall t \in T)(\exists p \in P)(p \text{ gets stabbed at time } t)$. The second statement says: $(\exists p \in P)(\forall t \in T)(p \text{ gets stabbed at time } t)$.

Let's look at a more mathematical example:

Consider

1. $(\forall x \in \mathbf{Z})(\exists y \in \mathbf{Z})(x < y)$
2. $(\exists y \in \mathbf{Z})(\forall x \in \mathbf{Z})(x < y)$

The first statement says that, given an integer, I can find a larger one. The second statement says something very different: that there is a largest integer! The first statement is true, the second is not.

Quantifiers and Negation

What does it mean for a proposition P to be false? It means that its negation $\neg P$ is true. Often, we will need to negate a quantified proposition (the motivation for this will become more obvious next lecture when we look at proofs). For now, let's look at an example of how to go about this.

Example:

Assume that the universe is $\{1,2,3,4\}$ and let $P(x)$ denote the propositional formula "$x^2 > 10$." Check that $\exists x P(x)$ is true but $\forall x P(x)$ is false. Observe that both $\neg(\forall x P(x))$ and $\exists x \neg P(x)$ are true because $P(1)$ is false. Also note that both $\forall x \neg P(x)$ and $\neg(\exists x P(x))$ are false, since $P(4)$ is true. The fact that each pair of statements had the same truth value is no accident, as the formulae

$$\neg(\forall x P(x)) \equiv \exists x \neg P(x)$$

$$\neg(\exists x P(x)) \equiv \forall x \neg P(x)$$

are laws that hold for any proposition P quantified over any universe. (Recall that "$\equiv$" means logically equivalent.) It is helpful to think of English sentences to convince yourself (informally) that these laws are true. For example, assume that we are working within the universe $\mathbf{Z}$ (the set of all integers), and that $P(x)$ is the proposition "x is odd." We know that the statement $(\forall x P(x))$ is false, since not every integer is odd. Therefore, we expect its negation, $\neg(\forall x P(x))$, to be true. But how would you say the negation in English? Well, if it is not true that every integer is odd, then that must mean there is some integer which is not odd (i.e. even). How would this be written in propositional form? That's easy, it's just: $(\exists x \neg P(x))$.

To see a more complex example, fix some universe and propositional formula $P(x,y)$. Assume we have the proposition $\neg(\forall x \exists y P(x,y))$ and we want to push the negation operator inside the quantifiers. By the above laws, we can do it as follows:

$$\neg(\forall x \exists y P(x,y)) \equiv \exists x \neg(\exists y P(x,y)) \equiv \exists x \forall y \neg P(x,y).$$

Notice that we broke the complex negation into a smaller, easier problem as the negation propagated itself through the quantifiers. Note also that the quantifiers "flip" as we go.

Let's look at a trickier example:

Write the sentence "there are at least three distinct integers x that satisfy $P(x)$" as a proposition using quantifiers! One way to do it is

$$\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge z \neq x \wedge P(x) \wedge P(y) \wedge P(z)).$$

(Here all quantifiers are over the universe $\mathbf{Z}$ of integers.) Now write the sentence "there are **at most** three distinct integers x that satisfy $P(x)$" as a proposition using quantifiers. One way to do it is

$$\exists x \exists y \exists z \forall d (P(d) \Longrightarrow d = x \vee d = y \vee d = z).$$

Here is an equivalent way to do it:

$$\forall x \forall y \forall v \forall z ((x \neq y \wedge y \neq v \wedge v \neq x \wedge x \neq z \wedge y \neq z \wedge v \neq z) \Longrightarrow \neg(P(x) \wedge P(y) \wedge P(v) \wedge P(z))).$$

[Check that you understand both of the above alternatives.] Finally, what if we want to express the sentence "there are **exactly** three distinct integers x that satisfy $P(x)$"? This is now easy: we can just use the *conjunction* of the two propositions above.