CS 70 Discrete Mathematics and Probability Theory
Summer 2019 Course Notes **Note 1**

1 Propositional Logic

1.1 Propositions and Propositional Formulae

In order to be fluent in working with mathematical statements, you need to understand the basic framework of the language of mathematics. This first lecture, 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.

Our first building block is the notion of a **proposition**, which is simply 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) Henry VIII was unpopular. (What is "unpopular?")

Propositions may be joined together to form more complex statements, known as propositional formulae. 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.

One can use these connectives (also known as logical operators) to combine propositional formulae instead of just propositions. This allows us to create more complicated formulae, such as $\neg((P \wedge Q) \vee R)$. When doing this, however, it is important to use parentheses to mark what order the operators are to be applied in. If we had written the previous formula as $\neg P \wedge Q \vee R$, that could have been interpreted as $(\neg P) \wedge (Q \vee R)$, which is much different from what we intended.

Sanity check! If we let P stand for the proposition "3 is odd," Q stand for "4 is odd," and R for "4+5=49," what are the values of $P \wedge R$, $P \vee R$ and $\neg Q$?

1.2 Truth Tables

We would like some way of describing formulae so that it is easier to compare them. In particular, we would like a way of determining if two formulae, say $P \wedge Q$ and $Q \wedge P$, are *equivalent*, or in other words that they "mean the same thing". To do this, we will treat formulae as functions, where the inputs are the truth values (either true or false) assigned to each constituent proposition and the output is the truth value of the overall formula. The *truth table* of a formula is then the evaluation table of its corresponding function. For example, here are truth tables for conjunction and negation:

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

P	$\neg P$
F	T
T	F

Sanity check! Write down the truth table for disjunction (OR).

We say that two formulae are equivalent if they have the same truth table. For our example above, we have the following (combined) truth table for $P \wedge Q$ and $Q \wedge P$:

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

Here, we can see that $P \wedge Q$ and $Q \wedge P$ always give the same output given the same input, and so are equivalent.

We now have the tools necessary to show our first interesting result:

Claim 1.1. *Propositional formulae with the logical operators $\wedge$, $\vee$, and $\neg$ are fully expressive. That is, given any truth table, we can create a formula that is true exactly on those inputs where the truth table is.*

We won't give a full proof of this claim (proofs come in the next note!), but we will sketch how to construct such a formula. To this end, we first note that we can create a formula which is satisfied only by some particular input by simply using conjunctions ("and") to say that each input proposition must take on the value we wish it to. For example, if we had three propositions P, Q, and R, $P \wedge (\neg Q) \wedge (\neg R)$ is satisfied exactly when P is true and Q and R are false.

Now suppose we are given a target truth table. For each assignment of truth values to propositions (ie, each input) that have a target output of true, we can use the previous paragraph to create a formula that is true on that input and nowhere else. We can then combine all of those formulae using disjunctions ("or") to create our final formula. Thus, for the following truth table

P	Q	φ
F	F	T
F	T	T
T	F	T
T	T	F

the formula we construct would be $\varphi = ((\neg P) \wedge (\neg Q)) \vee ((\neg P) \wedge Q) \vee (P \wedge (\neg Q))$.

Sanity check! Can you see why this construction will match our target truth table?

1.3 De Morgan's Laws

Now that we have our three main operators, we introduce *De Morgan's Laws*, which show one way in which they interact. De Morgan's Laws are the following two equivalences:[1]

$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$

Intuitively, the first equivalence says that if two things aren't both true, at least one of them must be false; the second says that if neither of two things are true, they must both be false.

Sanity check! Verify both of De Morgan's Laws by writing down the appropriate truth tables.

Note that the first equivalence (along with the fact that $\neg(\neg P) \equiv P$) allows us to eliminate all instances of $\vee$ in a formula by replacing $P \vee Q$ with $\neg((\neg P) \wedge (\neg Q))$. By applying this to the formula constructed by Claim 1.1, we can get a formula matching our target truth table using only $\neg$ and $\wedge$. Thus, we can in fact strengthen Claim 1.1 to say that we only need $\neg$ and $\wedge$ to be fully expressive. Similarly, we can use the second equivalence to remove all instances of $\wedge$ in a formula[2], meaning that we could alternatively strengthen Claim 1.1 to say that $\neg$ and $\vee$ suffice to be fully expressive.

[1] $\equiv$ is shorthand for "is equivalent to"

[2] However, we cannot remove all $\wedge$s and all $\vee$s simultaneously, as removing one creates the other.

1.4 Implications

While it is nice that we can express whatever we want with just the operators we have so far, having more operators makes things easier to express. The most important and subtle operator is **implication**:

> (4) **Implication**: $P \implies Q$ ("P implies Q" or "if P then Q"). True if P is false or Q is true.

Here, P is called the *hypothesis* of the implication, and Q is the *conclusion*; you may also see P called the *antecedent* and Q the *consequent*. We encounter implications frequently in everyday life; here are a couple of examples:

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

Here is the truth table for $P \implies Q$ (along with an extra column that we'll explain in a moment):

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 $1+2=18$." (These are statements that we never make in everyday life, but are perfectly natural in mathematics.)[3] When an implication is true because the hypothesis is false, we say that it is *vacuously true*.

Note also from the truth table that $P \implies Q$ is equivalent to $(\neg P) \vee Q$. When working with implications, it can sometimes be useful to convert them to this form — especially when you are negating an implication, as converting it to this form will allow you to apply De Morgan's Laws.

$P \implies Q$ 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 $P \iff Q$. Note that $P \iff Q$ is true only when P and Q have the same truth values (both true or both false).

For example, if we let P be "3 is odd," Q be "4 is odd," and R be "6 is even," then the following are all true: $P \implies R$, $Q \implies P$ (vacuously), and $R \implies P$. Because $P \implies R$ and $R \implies P$, we also see that $P \iff R$ is true.

[3] If this seems strange to you, consider our previous example "if you stand in the rain, they you'll get wet". This is a reasonable statement even if you didn't stand in the rain and didn't get wet.

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, so they are logically equivalent: $(P \implies Q) \equiv (\neg Q \implies \neg P)$. 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.

2 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 (even infinitely many!) 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 $\exists x P(x)$ is logically equivalent to $P(1) \vee P(2) \vee P(3) \vee P(4)$, and $\forall x P(x)$ 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, denoted as $\mathbb{N}$: $(\forall n \in \mathbb{N})(n^2+n+41 \text{ is prime})$.

Sanity check! Use quantifiers to express the following two statements: "For all integers x, $2x+1$ is odd", and "There exists an integer between 2 and 4".

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 example:

> "All students at Berkeley have a favorite class."
> "There is a class that all Berkeley students consider their favorite."

The first statement is saying that every student has a favorite class, but it could be a different class for each person. The second statement is saying something much stronger: that there is some class so good every student loves it more than any other.

Mathematically, we are quantifying over two universes: the set S of students and the set C of classes. The first statement can be written: $(\forall s \in S)(\exists c \in C)(c \text{ is } s\text{'s favorite class})$. The second statement says: $(\exists c \in C)(\forall s \in S)(c \text{ is } s\text{'s favorite class})$.

Let's look at a more mathematical example:

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

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.

2.1 De Morgan's Laws Again

There are equivalents to De Morgan's Laws for quantifiers:

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

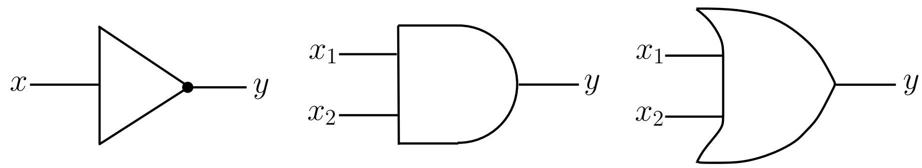
These are quite intuitive when phrased in English. The first says that if not all xs satisfy P, there must be some x which doesn't satisfy it; the second says that if there doesn't exist an x satisfying P, all xs must not satisfy it.

Sanity check! Use these equivalences to write $\neg(\forall x\ \exists y\ P(x,y))$ in terms of quantifiers and $\neg P(x,y)$. What general rule does this suggest when "pushing" negations through multiple quantifiers?

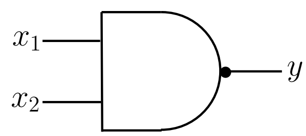
---

3 Exercises

1. Although primitive at first glance, logic is key to fundamental areas of computer science such as digital circuit design. For example, below we depict logic gates used in circuits corresponding respectively to NOT, AND, and OR:

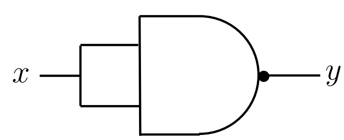


Here, the wires coming in from the left are the *input* wires, and the wires exiting from the right are the *output* wires. For example, the AND gate takes in input bits x_1 and x_2, and outputs $y = x_1 \wedge x_2$. A remarkable fact regarding circuits is that the NAND gate,



which computes $y = \neg(x_1 \wedge x_2)$ (note the black dot on the output wire, which indicates negation), is *universal*. In other words, each of the other three gates NOT, AND, and OR, can be *simulated* using just the NAND gate! How could this be? Let's work it out for ourselves to find out!

   (a) Convince yourself (for example, via truth table), that the following circuit simulates the NOT gate, i.e. that $y = \neg x$:



   (b) How would you simulate the AND gate? (Hint: Note that NAND is just AND composed with NOT, and the exercise above just demonstrated how to simulate NOT.)

   (c) How would you simulate the OR gate?

   (d) Using the previous three parts, argue that propositional formulae using NAND as the only operator are fully expressive as in Claim 1.1.

2. The rules of logic can also help us reason about *games*. For example, consider a two-player game with the following properties: There are two players, Toby and Fritz, and the game consists of two turns. First, Toby takes a turn, and then Fritz, and then one of them is declared the winner (i.e. there are no ties).

   (a) Show that either Toby or Fritz must have a winning strategy in the following sense: The person with the winning strategy *always* wins the game. (Hint: Consider the case where Toby has a winning strategy. Then, we can model this via the proposition "there exists a move by Toby such that for all moves by Fritz, Toby wins." Use the law of the excluded middle to argue that if this statement is false, then its negation must be true — what is the negation of this statement?)

   (b) Which property of the game allowed us to apply the law of the excluded middle in part (a) above?