To succeed in this course, you need to know discrete math. I highly recommend that you review at the very least Chapters 1, 5, and 12 of the book "Discrete Mathematics and Its Applications" by Kenneth Rosen.

These notes are a brief review some of the material from that book. However, it is not a substitution for knowing the material from ICS 141/241. If anything in this article does not make sense, I highly recommend that you refer to the Rosen book.

1 Logic (Chapter 1)

1.1 Basics

English language is not very precise and can be quite ambiguous. Therefore, you are less likely to make mistakes if you get used to mathematical notation, which is very precise, but can be difficult to understand if you are not used to it.

Consider the following English sentence. "My computer runs Linux." The negation of this statement can be stated as "It is not the case that my computer runs Linux" or, simply, "My computer does not run Linux". If we can replace the original statement with a variable A, then the second statement (the negation) we can defined as $\neg A$. A is called a *proposition*.

Another example: "My computer has at least 4GB of memory." Let it be defined by B. What is $\neg B$ – the negation of this statement? It is "It is not the case that my computer has at least 4GB of memory." Equivalently, "My computer does not have at least 4GB of memory." And even more simplification leads to "My computer has less than 4GB of memory."

We can combine the above simple propositions to form more complex propositions:

- $A \wedge B$ ("A and B") – Both A and B must be true for the combined statement to be true
- $A \vee B$ ("A or B") – At least one of A or B must be true for the combined statement to be true
- $A \oplus B$ ("A xor B") – Exactly one of A and B must be true (i.e. not both) for the combined statement to be true

For example, $A \wedge B$ means "My computer runs Linux **and** has at least 4GB of memory."

We can use truth tables to define when a statement is true (as a function of the truth values of individual propositions that the statement consists of). For example, for the statements above, here is the truth table:

A	B	$A \wedge B$	$A \vee B$	$A \oplus B$
$true$	$true$	$true$	$true$	$false$
$true$	$false$	$false$	$true$	$true$
$false$	$true$	$false$	$true$	$true$
$false$	$false$	$false$	$false$	$false$

DeMorgan's Law. We can also negate the combined statement $\neg(A \wedge B)$. It says "It is not the case that my computer runs Linux and has at least 4GB of memory." This is where confusion in English language can arise. Does it mean that my computer neither runs Linux, nor has at least 4GB of memory? Or is it possible that my computer runs Linux if it happens to have less than 4GB of memory?

DeMorgan's Law defines what happens when we negate composite propositions:

- $\neg(A \wedge B) = \neg A \vee \neg B$
- $\neg(A \vee B) = \neg A \wedge \neg B$

Thus, the above negation means that "It is not the case that my computer run Linux **or** it is the case that it does not have at least 4GB of memory." Equivalently, it can be rephrased in plain English as "My computer **either** does not run Linux, has less than 4GB of memory, or both." Note, how much simpler it is to write $\neg A \vee \neg B$.

1.2 Implication: $A \implies B$ (pronounced "A implies B")

$A \implies B$ means "If A is true, then B is true". For example,

"If it rained within the past hour, then the pavement is wet."

Here

A = "it rained within the past hour"

B = "the pavement is wet"

So we can interpret the above statement as "If it's true that *it rained within the past hour*, then it's also true that *the pavement is wet*".

Another example:

"If an animal is a lion, then the animal is a mammal."

A = "animal is a lion"

B = "animal is a mammal"

Given a conditional statement $A \implies B$, we want to determine if the whole statement $(A \implies B)$ is true or false. In plain English it means, if we made such a statement as a promise and some parts of it turned out not to be true, would we be breaking our promise?

Example: Suppose we made the statement "If it rained within the past hour, then I promise the pavement will be wet". Would we be lying if the following happened:

- If it did rain within the past hour, but the pavement was dry? Yes, obviously we lied by making that statement.
- If it didn't rain within the past hour, and the pavement was dry? Obviously not, because we didn't make any promises about what happens if it didn't rain within the past hour.
- If it didn't rain within the past hour, and the pavement happened to be wet? This question often causes confusion among students. No, we wouldn't be lying, because maybe it rained 2 hours ago and the pavement hasn't dried yet. Remember, we only make the promise if it rained within the past hour. In other cases all bets are off.

The conditional statement $A \implies B$ is *false* if and only if A is true and B is false, the rest of the time the statement is *true*.

We can represent this via the truth table (note that the only time $A \implies B$ is false is when A is true, but B is false):

A	B	$A \implies B$
$true$	$true$	$true$
$true$	$false$	$false$
$false$	$true$	$true$
$false$	$false$	$true$

Now, if we know that $A \implies B$ is true, can we say anything about the truth of its *converse*, i.e., $B \implies A$? The simplest way is to look at the truth table:

A	B	$A \implies B$	$B \implies A$
$true$	$true$	$true$	$true$
$true$	$false$	$false$	$true$
$false$	$true$	$true$	$false$
$false$	$false$	$true$	$true$

If we look at the lines when $A \implies B$ is true, $B \implies A$ is sometimes true, and sometimes false. In plain English, consider the above example: "If an animal is a lion, then the animal is a mammal", A is "animal is a lion" and B is "animal is a mammal". Then $B \implies A$ would mean "If an animal is a mammal, then the animal is a lion". Of course, this statement is not a true statement – there are mammals that aren't lions.

How about the *inverse* of $A \implies B$, which is denoted as $\neg A \implies \neg B$. Before we look at the truth table, consider the above example again. $\neg A \implies \neg B$ would stand for "If an animal is not a lion, then it is not a mammal". Obviously, this is not true – tigers, for example, aren't lions and yet they are mammals. And it is confirmed by the truth table (remember, $\neg A \implies \neg B$ is *true* only if $\neg A$ is *true*, but $\neg B$ is $false$):

A	B	$\neg A$	$\neg B$	$A \implies B$	$\neg A \implies \neg B$
$true$	$true$	$false$	$false$	$true$	$true$
$true$	$false$	$false$	$true$	$false$	$true$
$false$	$true$	$true$	$false$	$true$	$false$
$false$	$false$	$true$	$true$	$true$	$true$

How about the contrapositive of $A \implies B$, which is denoted by $\neg B \implies \neg A$? Again consider the above example first. $\neg B \implies \neg A$ stands for "If an animal is not a mammal, then it is not a lion". Obviously this is a true statement. Let's look at the truth table.

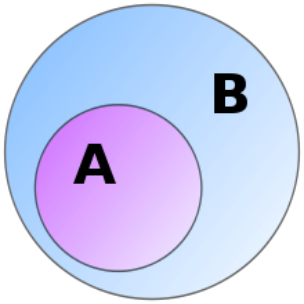
A	B	$\neg A$	$\neg B$	$A \implies B$	$\neg B \implies \neg A$
$true$	$true$	$false$	$false$	$true$	$true$
$true$	$false$	$false$	$true$	$false$	$false$
$false$	$true$	$true$	$false$	$true$	$true$
$false$	$false$	$true$	$true$	$true$	$true$

Note, that if $A \implies B$ is true, so is $\neg B \implies \neg A$. Thus, we can say $(A \implies B) \implies (\neg B \implies \neg A)$.

Moreover, whenever $\neg B \implies \neg A$ is true, so is $A \implies B$, thus we can say $(\neg B \implies \neg A) \implies (A \implies B)$. Whenever, $X \implies Y$ **and** $Y \implies X$, we say that X and Y are equivalent (denoted by $X \iff Y$). Thus, any statement and its contrapositive are equivalent (also can be verified by checking that their truth tables are the same). We will use this fact to prove by contraposition in Section 2.2.

Finally, note that $\neg A \implies \neg B$ is the contrapositive of $B \implies A$. You can verify their equivalence, by comparing their corresponding truth table entries above.

Sometimes it helps to think of implications in terms of Venn diagrams. For example, the Venn diagram to the right represents "everything in A is also in B". It can be interpreted as $A \implies B$. Then the contrapositive, which states "Anything that is not in B is also not in A" is obviously true.



1.3 Quantifiers

If the mathematical/logical expressions are confusing, simply rewrite them in plain English and they will make sense. That's the difference between understanding and memorization.

There are two important quantifiers that you should know about.

- *Universal* quantifier $\forall$ (pronounced "for all", "for any", "for every")
- *Existential* quantifier $\exists$ (pronounced "exists")

E.g.

- $\forall x \in A : x \in B$. In plain English: "For all x in A, x is in B". In other words, "Every x that is in A is also in B".
- $\exists x \in A : x \in B$. In plain English: "Exists x in A, such that x is in B". In other words, "There is at least one x in A, that is also in B.
- $\forall x \in \Re, \exists y \in \Re : xy = 20$. Meaning: "For every x among real numbers, there exists y among real numbers, such that $xy = 20$".

Note that the order of $\forall$ and $\exists$ matters. For example, compare the following statement with the last one above:

> $\exists x \in \Re, \forall y \in \Re : xy = 20$. Meaning: "Exists x among real numbers, such that for all y among real numbers $xy = 20$.

The last statement isn't true: there is no real number such that if you multiply it with any other real number, you get 20.

Negating quantifiers. To negate an existential quantifier, simply put a slash through $\exists$:

$$\neg(\exists x : P(x)) \iff \nexists x : P(x)$$

In plain English: Negation of "Exists x such that $P(x)$ is $true$", is equivalent to saying "There does not exist x such that $P(x)$ is $true$". The second statement can be rephrased as, "For every x, $P(x)$ is $false$". Thus, we can also rewrite the negation of an existential quantifier in terms of universal quantifier.

$$\neg(\exists x : P(x)) \iff \forall x : \neg P(x)$$

To negate a universal quantifier, first rewrite it in terms of the existential quantifier:

$$\forall x : P(x) \iff \nexists x : \neg P(x)$$

It says: "For every x, $P(x)$ is true" is equivalent to saying "There does not exist x, such that '$P(x)$ is $true$' is negated", which, in turn, is equivalent to saying "There does not exist x, such that $P(x)$ is $false$".

Example: "All lions are mammals" is equivalent to saying "There does not exist a lion that is not a mammal".

Then, to negate a universal quantifier:

$$\neg(\forall x : P(x)) \iff \neg(\nexists x : \neg P(x)) \iff \exists x : \neg P(x)$$

In plain English: Negation of "For every x, $P(x)$ is $true$" is equivalent to saying "Exists x, such that $P(x)$ is $false$".

Example: Negation of "All mammals are lions" is equivalent to saying "There exists a mammal that is not a lion".

2 Proof techniques

2.1 Direct proof

Suppose we want to prove the statement: "If n is an odd integer, then n^2 is odd". It is of the form $A \implies B$, where A is "n is an odd integer" and B is "n^2 is odd". This is a common form of things we are trying to prove.

Direct proof of a statement $A \implies B$, starts by assuming A is true and uses logical steps to come to the conclusion that B is true too.

For example, in the above statement, assume A is true, i.e., n is an odd integer. Then we can rewrite it as $n = 2k + 1$ for some integer k (definition of being odd). Then

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \tag{1}$$

Let $m = 2k^2 + 2k$. Since k is an integer, so is m. Then we can rewrite (1) as $n^2 = 2m + 1$, where m is some integer, i.e., n^2 is odd. □

The square at the end of the line above stands for Q.E.D., which are initials of the Latin phrase *quod erat demonstrandum*, which means "which had to be proven". It's customary to indicate the end of a proof by writing Q.E.D. or putting the above square symbol.

2.2 Proof by contraposition

When we have to prove a statement $A \implies B$, sometimes it is easier to prove the contrapositive $\neg B \implies \neg A$ (i.e. If not B, then not A). Since a statement and its contrapositive are equivalent, proving one to be true, implies the other to be true too.

Thus, a *proof by contraposition* starts by assuming $\neg B$ is true and uses logical steps to come to the conclusions that $\neg A$ is true.

Example: Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof. It's not obvious how to prove that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ from the equation $n = ab$. Instead, we will prove by contraposition. The contrapositive of the above statement is:

"If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n \neq ab$".

Proving this statement is easy: simply multiply a and b. You will get $ab > \sqrt{n} \cdot \sqrt{n} = n$. But if $ab > n$, then it cannot be that $ab = n$. And we are done!

If it is clear for you why the contrapositive is the statement above, you can skip the rest of the proof. However, if it's not clear how we got to the statement above, here is the explanation.

We have a conditional statement:

If A then B (or, equivalently, $A \implies B$)

where

A : "$n = ab$ (where a and b are positive integers)"
B : "$a \leq \sqrt{n}$ or $b \leq \sqrt{n}$"

Since we want to prove $\neg B \implies \neg A$, we need to determine what $\neg B$ and $\neg A$ are.

To determine $\neg B$, note that B can be written as "$X \vee Y$", where X stands for "$a \leq \sqrt{n}$" and Y stands for "$b \leq \sqrt{n}$". Thus, we want "$\neg(X \vee Y)$". By DeMorgan's rule, "$\neg(X \vee Y)$" = "$(\neg X \wedge \neg Y)$". X says "a is less or equal to $\sqrt{n}$". Negation of this statement is "a is not less or equal to $\sqrt{n}$". In other words, "a is greater than $\sqrt{n}$". Thus, $\neg X \iff$ "$a > \sqrt{n}$". Similarly, for $\neg Y \iff$ "$b > \sqrt{n}$". Thus, $\neg B \iff$ "$a > \sqrt{n}$ and $b > \sqrt{n}$".

A states "n equals ab". $\neg A$ simply means "n does not equal ab" or, mathematically, "$n \neq ab$".

Thus, putting it all together gives us $\neg B \implies \neg A$ is equivalent to:

If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $n \neq ab$.

□

2.3 Proof by contradiction

Suppose we want to prove that some statement A is *true*. *Proof by contradiction* assumes that A is $false$, i.e. assumes $\neg A$ is *true* and then uses logical steps to show that our assumption would lead to two contradictory statements being true. Since two contradictory statements cannot be true, it implies that our assumption that A is $false$ was wrong, i.e. A is *true*.

Example: Prove that $\sqrt{2}$ is an irrational number.

Proof. For the sake of contradiction, assume the opposite. That is, assume $\sqrt{2}$ is a rational number, i.e. $\sqrt{2} = \frac{a}{b}$, where a and b are integers with no common divisors larger than 1. If we square both sides of the equation, we get $2 = \frac{a^2}{b^2}$ or, equivalently, $2b^2 = a^2$. Thus, a^2 is an even number and can be written as $a = 2k$ for some integer k. Then $2b^2 = (2k)^2 = 4k^2$. That means that $b^2 = 2k^2$, i.e. is also an even number. Thus,

both a and b are even numbers. In that case 2 is a divisor of both a and b. But we also said that a and b don't have common divisors larger than 1. The two statements are contradictory, therefore, our assumption that $\sqrt{2}$ is rational must be wrong. Therefore, $\sqrt{2}$ is irrational. □

Example: Prove by contradiction the following: "If $3n + 2$ is odd, then n is odd".

Proof. We are trying to prove the statement A of the form $X \implies Y$, where X is "$3n + 2$ is odd" and Y is "n is odd". Assume $\neg A$ is *true*, i.e. A is $false$. By the definition of implication (e.g. see the truth table), the only time $X \implies Y$ is false is when X is *true* and Y is $false$. Thus, we assume that "$3n + 2$ is odd" and "n is not odd", i.e., "n is even".

If n is even, then we can rewrite it as $n = 2k$ for some integer k. Then $3n+2 = 3 \cdot 2k+2 = 2(3k+1) = 2m$, where $m = (3k + 1)$, i.e. is some integer. Then, by definition of even numbers, $3n + 2$ is also even. But remember one of our assumptions was that "$3n + 2$ is odd", i.e. we have two contradictory statements that are both *true*, which is impossible. Thus, at least one of our assumptions that "$3n + 2$ is odd" (i.e. X is *true*) and "n is even" (Y is $false$) where wrong. But if we change the truth value of any of them, $negA$ (our original assumption) will not be true anymore, i.e. A must be true. But A is exactly the conditional the statement we are trying to prove. □

The above example gives a simple strategy for proving conditional statements (implications): Assume the premise (the *if* part) is true, but the conclusion (the *then* part) is false (this is equivalent to assuming that the conditional statement we are trying to prove is false). Then use logical steps to show that the negation of the premise is also true. Both the premise and its negation cannot be true at the same time, therefore, our assumption that the statement we are trying to prove is $false$ was wrong, i.e. the statement must be *true*.

Question: How is it similar to and how is it different from the proof by contraposition?

2.4 Proof by induction

Another powerful proof technique is *proof by induction*. When proving a statement that $P(n)$ is true for any positive n using proof by induction, we have to show two things:

Basis step: Prove that $P(1)$ is true, i.e. $P(n)$ is true for $n = 1$.

Inductive step: Prove that $P(k) \implies P(k + 1)$ for every positive integer k. In other words, if $P(k)$ is true for some positive integer k, then $P(k + 1)$ is also true. Assumption "$P(k)$ is true" is known as the *inductive hypothesis*.

Example: Using induction prove that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for any positive integer n.

Proof. Let $P(n)$ be the proposition that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, i.e., the sum of first n positive integers is $\frac{n(n+1)}{2}$.

Basis step: $P(1)$: $\sum_{i=1}^{1} i = 1 = \frac{1 \cdot (1+1)}{2}$ ✓

Inductive step: Show that $P(k) \implies P(k+1)$. I.e. we show that if $P(k)$ is true, then $P(k+1)$ is also true. Our inductive hypothesis "$P(k)$ is true" is that $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$. Using this we want to prove that $P(k + 1)$ is true, i.e. $\sum_{i=1}^{k+1} i = \frac{(k+1)([k+1]+1)}{2} = \frac{(k+1)(k+2)}{2}$.

We can write $\sum_{i=1}^{k+1} i$ as $\left(\sum_{i=1}^{k} i\right) + (k+1)$. By the inductive hypothesis $\left(\sum_{i=1}^{k} i\right) = \frac{k(k+1)}{2}$. Thus, we have:

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} \qquad \checkmark
\end{aligned}$$

□

This is another way of proving the summation of the first n positive integers. As you can see, with mathematical induction you don't need to come up with new proof techniques, but simply apply known method (basis step, inductive step). The hardest part is coming up with the inductive hypothesis, but usually it's clear from the problem at hand.

Strong Induction: Proof by strong induction is very similar to proof by induction. We still have to prove the **Basis step**. However, sometimes for the basis step we have to prove several propositions, e.g. that $P(1)$ and $P(2)$ is true. Another difference is in the **Inductive step**, we assume that $P(k)$ is true for *all* positive integers up to k, instead of just for k. Then we use this assumption to prove that $P(k+1)$ is also true.

Example: Prove that every integer n greater than 1 can be written as a product of primes.

Proof. Let $P(n)$ be the proposition that n can be written as the product of primes.

Basis step: $P(2)$ is true, because 2 can be written as a product of one prime, itself. (Note, we don't need to prove $P(1)$, because the statement we are proving holds for integers $n > 1$.) ✓

Inductive step: Assume $P(j)$ is true for all integers j, such that $2 \leq j \leq k$. I.e., any positive integer j that is greater than 2 and not larger than k can be written as a product of primes. Using this we want to prove $P(k+1)$ to be true, i.e. integer $k+1$ can be written as a product of primes.

There are two cases to consider.

1. $k+1$ is a prime itself. Then $P(k+1)$ is true, because $k+1$ can be written as a product of a single prime (itself).

2. $k+1$ is a composite number. I.e., $k+1$ can be written as $a \cdot b$, where $a < k+1$ and $b < k+1$. By inductive hypothesis, since both a and b are at most k, we know that they can be written as products of primes. Therefore, $k+1$ can be written as a product of primes. ✓

□

Note that it is not sufficient to use regular induction, because a and b will not necessarily equal k, thus, we require an assumption that all numbers smaller than $k+1$ can be written as a product of primes.

Induction is perfect for proving correctness of a recursive algorithm.

Example: *Fibonacci number* $F(n)$ is defined recursively as follows: $F(1) = F(2) = 1$, and $F(i) = F(i-1) + F(i-2)$ for any $i > 2$. The first few Fibonacci numbers are the following: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ Consider the following procedure that returns n-th Fibonacci number:

```
1:  fib(n)
2:    if 0 < n < 3
3:      return 1
4:    else
5:      return fib(n-1) + fib(n-2)
```

Prove that the procedure call `fib(n)` returns n-th Fibonacci number.

Proof. We will use strong induction. Let $P(n)$ be the proposition "The procedure returns the correct n-th Fibonacci number".

Basis step: Invocations `fib(1)` and `fib(2)` will return 1 in line 3, which equals $F(1)$ and $F(2)$, respectively. Note, we proved $P(1)$ is true and $P(2)$ is true as the basis step. ✓

Inductive step: Let $P(j)$ be true for $1 \leq j \leq k$, i.e., the algorithm returns the correct Fibonacci number up to k. We prove that then $P(k+1)$ is true, i.e. when invoked as `fib(k+1)` the procedure will return $F(k+1)$. Invocation `fib(k+1)` returns `fib((k+1)-1) + fib((k+1)-2) = fib(k) + fib(k-1)` in line 5. By inductive hypothesis we know that `fib(k)` returns $F(k)$ and `fib(k-1)` returns $F(k-1)$, i.e. the procedure `fib(k+1)` returns $F(k) + F(k-1)$. Since $F(k+1)$ is defined as $F(k) + F(k-1)$, the invocation of `fib(k+1)` returns $F(k+1)$, the $(k+1)$-th Fibonacci number. ✓ □