PROOFS:

In Lecture 2 we talked (a bit vaguely) about statements. We said that statements that depend on variables are called predicates. By “depend” we meant that their logical truth or falsehood depend on values given to those variables. Then, we dove deeper into the logical structure of mathematical statements and we identified quantifier and logical connectives among their building bricks. This allowed us to state in Lecture 3 proof patterns such as how to disprove an implication and proof by contrapositive. Naturally, you asked what justifies such proof patterns! We shall discuss these justifications here in the context of a brief introduction to Propositional Logic.

An atomic proposition is a statement that is either true or false. For example, “2 + 2 = 4” and “Tannen was born in Philadelphia” are atomic propositions. A proposition is a statement constructed from atomic propositions using the logical connectives that we saw earlier: conjunction, disjunction, negation, implication, biconditional (but no quantification!). For example “2 + 2 = 4 and 4 + 4 = 8” and “Tannen was born in Philadelphia or Tannen was born in Ploiești” are propositions.

The truth value (true or false) of a proposition built with one logical connective is defined by truth tables, see below. In this truth table $P$ and $Q$ are arbitrary (perhaps atomic) propositions, $T$ stands for true and $F$ stands for false:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$\neg P$</th>
<th>$P \land Q$</th>
<th>$P \lor Q$</th>
<th>$P \Rightarrow Q$</th>
<th>$P \Leftrightarrow Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

In particular:

**Implication:** $P \Rightarrow Q$ (read as “$P$ implies $Q$”) is the proposition that is false when $P$ is true and $Q$ is false but is true otherwise.

---

1 What about the quantifiers: for all/there exists? Together with predicates such as “$kn = k^2+1$” or “$x^2 < x+40$”, whose truth depends on values given to variables such as $k, n, x$, and together with the logical connectives mentioned above, they form sentences of first-order logic. This is sometimes called predicate calculus just as proposition logic is sometimes called propositional calculus. We shall not discuss first-order logic in this class but you may want to retain that the statements that we use (such as those in Propositions 3.8 and 3.9 in Lecture 3) are first-order logic sentences.
Recall that for an implication $P \Rightarrow Q$ we call $P$ its **premise** and $Q$ its **conclusion**.

An interesting observation is

An implication whose premise is false is always true, regardless of the conclusion. Or “false implies anything”.

For example, consider “if $2 + 2 = 5$ then there exist infinitely many twin primes”.

Some people say that such an implication “holds vacuously”. This expression is inspired by a particular case when we have an implication under an universal quantifier. Here is an example. The following statement is vacuously true: for any natural number $n$ such that $kn = k^2 + 1$ for some integer $k > 1$, there exist twin primes bigger than $n$! If you have been misled into thinking that the statement says something interesting about the Twin Primes Conjecture notice that there are no natural numbers $n$ such that $kn = k^2 + 1$ for some integer $k > 1$! (Can you prove this?) So inside this statement there is an implication whose premise is false. The use of “vacuous” here refers to the fact that the set of natural numbers $n$ such that $kn = k^2 + 1$ for some integer $k > 1$ is empty.

When are propositions **equivalent**? Suppose we have some atomic propositions whose truth value can be assigned. We shall call these boolean variables and giving each one of them a truth values (T or F) will be called a **truth assignment**.

A proposition built from boolean variables is also called a **boolean expression**. In what follows we use $p, q, r, \ldots$ for boolean variables. In addition to the boolean variables we allow the “trivial” atomic propositions T and F. Here are some examples of boolean expressions:

$$ (p \lor \neg p) \iff T \quad F \Rightarrow p \quad \neg q \Rightarrow \neg p \quad (p \land q) \Rightarrow r \quad p \Rightarrow (q \Rightarrow r) $$

$$ p \land \neg p \quad \neg p \lor q \quad (p \Rightarrow r) \land (q \Rightarrow r) \quad (p \lor q) \Rightarrow r $$

**Definition 4.1** Two boolean expressions are **logically equivalent** (written $\equiv$) if they have the same truth value for every truth assignment to their variables.

For example, it is easy to see that $\neg \neg p \equiv p$ (we call this the **Law of Double Negation**), that $p \land \neg p \equiv F$ (we call this the **Law of Contradiction**), and that $p \lor \neg p \equiv T$ (we call this the **Law of the Excluded Middle**; it is also known as **Tertium Non Datur** (Latin for “a third (possibility) is not given”)). The same with the **De Morgan Laws** $\neg(p \land q) \equiv (\neg p) \lor (\neg q)$ and $\neg(p \lor q) \equiv (\neg p) \land (\neg q)$. (We shall check some of these in class.)

---

$^2$Twin primes are primes that are 2 apart: 3 and 5, 17 and 19, 41 and 43, etc. The Twin Prime Conjecture says that there are infinitely many twin primes. As of 1/23/2017, 11AM, it is not known whether this conjecture is true or false. (See [http://www.slate.com/articles/health_and_science/do_the_math/2013/05/yitang_zhang_twin_primes_conjecture_a_huge_discovery_about_prime_numbers.html](http://www.slate.com/articles/health_and_science/do_the_math/2013/05/yitang_zhang_twin_primes_conjecture_a_huge_discovery_about_prime_numbers.html))
Example 4.2  Show that \( p \Rightarrow q \equiv \neg q \Rightarrow \neg p \equiv \neg p \lor q \equiv \neg(p \land \neg q) \).

Solution: By the truth table below. The first two columns are the truth assignment.

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

The first equivalence in Example 4.2 justifies the **proof by contrapositive** pattern, i.e., to prove an implication we can instead prove its contrapositive. The last equivalence justifies how to disprove an implication \( p \Rightarrow q \); you prove \( p \lor \neg q \).

The **proof by contradiction** pattern uses propositions of the form \( r \land \neg r \) which called above *contradictions*. Their truth value is always F. We say that \( \neg r \) *contradicts* \( r \) and vice versa. In what follows \( C \) stands for a proposition that is a contradiction. Although \( C \) typically contains boolean variables, we don’t show them for simplicity and we just consider \( C \) as a proposition that is always false.

Suppose \( p \) is some proposition whose truth we want to deduce. In a proof by contradiction, we suppose that \( p \) is false and show that this assumption leads logically to a contradiction, \( C \). In other words, we prove the implication \( \neg p \Rightarrow C \). So we have the following proof by contradiction pattern:

\[
\text{To prove } p \text{ we can instead prove that } \neg p \Rightarrow C.
\]

This is because \( \neg p \Rightarrow C \equiv p \), as the following truth table shows:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Most often we use a variant of this pattern because usually we have to prove an implication \( p \Rightarrow q \). In this pattern we first assume \( p \). Next, we prove \( q \) by contradiction using \( p \) as needed.

\[
\text{To prove } p \Rightarrow q \text{ we can instead prove that } p \land \neg q \Rightarrow C.
\]

To justify this, we could simply show by truth table that \( p \Rightarrow q \equiv p \land \neg q \Rightarrow C \) (check it!).

Example 4.3  If \( 3n + 2 \) is odd then \( n \) is odd.
Solution: Proof by contradiction (using the second pattern above). Assume that $3n + 2$ is odd. Now assume (toward a contradiction) that $n$ is even. Since $n$ is even, there exists an integer $k$ such that $n = 2k$. Thus $3n + 2$ can be written as

$$3(2k) + 2 = 2(3k + 1)$$

Since $k$ is an integer, clearly $3k + 1$ is an integer. Thus $3n + 2$ is even. This contradicts the premise above, that $3n + 2$ is odd. ■

If you are thinking that the proof above is essentially a proof by contrapositive you are not wrong! In fact, any proof by contrapositive can be immediately transformed into a proof by contradiction that follows the second pattern:

Assume $p$.
Assume toward a contradiction that $\neg q$.

Put here your proof of the contrapositive $\neg q \Rightarrow \neg p$.
This derives $\neg p$.
Now you have reached a contradiction between $\neg p$ and $p$.

Recall the definition of rational numbers (in class).

Example 4.4 Prove that $\sqrt{2}$ is irrational. [3]

Solution: Proof by contradiction.

Assume, toward a contradiction (some people say “for a contradiction”; or they don’t say anything if they just announced that the proof is by contradiction; either is OK), that $\sqrt{2}$ is a rational number. Then $\sqrt{2}$ can be expressed as a fraction with integer numerator and denominator. In fact w.l.o.g. [4] we can assume the rational number is ”in lowest terms”, i.e. that there exist integers $a$ and $b$ ($b \neq 0$) with no common divisors (factors) other than 1 such that

$$\sqrt{2} = \frac{a}{b}$$

Why w.l.o.g.? Because having $a$ and $b$ be with just 1 as a common divisor is stronger, but still equivalent to the original assumption. Indeed, we can keep dividing $a$ and $b$ by their common divisors $\neq 1$ until no more such division is possible.

---

[3] $\sqrt{2}$ is the length of the diagonal of the square of side 1. When, around 500 BC, one of Pythagoras’s disciples discovered this fact and its proof it caused great existential anxiety among the philosophers of the Pythagorean School who believed that all mathematical quantities must relate to each other as natural numbers do. Legend has it that said disciple was drowned at sea by other philosophers to keep his discovery secret. As you can see, Math has its martyrs too!

[4] This stands for **without loss of generality**.
By the way, the elegant terminology here is to say that $a$ and $b$ are relatively prime or coprime. Squaring both sides of the above equation gives

$$
2 = \frac{a^2}{b^2} \quad \text{(1)}
$$

From (1) we conclude that $a^2$ is even.

**Lemma**  Let $z$ be an integer. If $z^2$ is even then $z$ is even.

**Proof of Lemma** We prove the contrapositive: if $z$ is odd then $z^2$ is odd. Indeed if $z = 2y + 1$ for some integer $y$ then $z^2 = 4y^2 + 4y + 1 = 2x + 1$ where $x = 2y^2 + 2y$ is also integer. Therefore $z^2$ is odd.

Back to the main proof. The Lemma implies that $a$ is even. Then, for some integer $k$, let

$$a = 2k \quad \text{(2)}$$

Combining (1) and (2) we get

$$
4k^2 = 2b^2 \\
2k^2 = b^2
$$

The above equation implies that $b^2$ is even and hence, by the Lemma, $b$ is even. Since we know $a$ is even this means that $a$ and $b$ have 2 as a common factor which contradicts the assumption that $a$ and $b$ have no common factors.

We will now give a very elegant proof for the fact that “$\sqrt{2}$ is irrational” using the unique factorization theorem, a.k.a. the prime factorization theorem, which is also called the Fundamental Theorem of Arithmetic. This theorem states that every positive integer $> 1$ can be uniquely represented as a product of powers of primes. More formally, it can be stated as follows.

**Theorem 4.5 (The Fundamental Theorem of Arithmetic)** Given any integer $n > 1$, there exist a positive integer $k$, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$
n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}
$$

and any other expression of $n$ as a product of powers of primes is identical to this except, perhaps, for the order in which the factors are written.

We omit the proof of this important theorem but you can find in many elementary textbooks. Here is an easy consequence:

---

5A “lemma” is a statement that you prove on your way to proving a more important statement, like a “theorem”. The irrationality of $\sqrt{2}$ was certainly a Theorem with capital “T” for the ancients!
Corollary 4.6  An integer \( n > 1 \) is composite iff it is divisible by some prime \( p < n \).

Proof in class.

Example 4.7  Prove that \( \sqrt{2} \) is irrational using the Fundamental Theorem of Arithmetic (actually, Corollary [4.6]).

Solution: Assume for the purpose of contradiction that \( \sqrt{2} \) is rational. Then there are integers \( a \) and \( b \) (\( b \neq 0 \)) such that

\[
\sqrt{2} = \frac{a}{b}
\]

Squaring both sides of the above equation gives

\[
2 = \frac{a^2}{b^2}
\]

\[
a^2 = 2b^2
\]

Let \( S(m) \) be the sum of the number of times each prime factor occurs in the unique factorization of \( m \). Note that \( S(a^2) \) and \( S(b^2) \) are even. Why? Because the number of times that each prime factor appears in the prime factorization of \( a^2 \) and \( b^2 \) is exactly twice the number of times that it appears in the prime factorization of \( a \) and \( b \). Then, \( S(2b^2) = 1 + S(b^2) \) must be odd. This is a contradiction as \( S(a^2) \) is even and the prime factorization of a positive integer is unique. \( \blacksquare \)

Example 4.8  Prove that there are infinitely many prime numbers.

Solution: Assume, for the sake of contradiction, that there are only finitely many primes. Let \( p \) be the largest prime number. Then all the prime numbers can be listed as

\[
2, 3, 5, 7, 11, 13, \ldots, p
\]

Consider an integer \( n \) that is formed by multiplying all the prime numbers and then adding 1. That is,

\[
n = (2 \times 3 \times 5 \times 7 \times \cdots p) + 1
\]

Clearly, \( n > p \). Since \( p \) is the largest prime number, \( n \) cannot be a prime number. In other words, \( n \) is composite. By Corollary [4.6] \( n \) is divisible by some prime \( q < n \). Therefore \( q \) must be among \( 2, 3, \ldots, p \). Because of the way \( n \) is constructed, when \( n \) is divided by \( q \) the remainder is 1. That is, \( n \) is not divisible by \( q \). Contradiction.

Alternate Proof by Filip Saidak. Let \( n \) be an arbitrary positive integer greater than 1. Since \( n \) and \( n + 1 \) are consecutive integers, they must be relatively prime\(^6\) (prove this!). Hence, the number

\( ^6 \)Two distinct positive integers are said to be relatively prime if their only common divisor is 1.
$N_2 = n(n + 1)$ must have at least two different prime divisors. Similarly, since the integers $n(n + 1)$ and $n(n + 1) + 1$ are consecutive, and therefore relatively prime, the number

$$N_3 = n(n + 1)[n(n + 1) + 1]$$

must have at least three different prime factors. This process can be continued indefinitely, so the number of primes must be infinite. ■