We continue with mathematical/logical objects and their notation, with counting and with proof techniques.

**PROOFS:** (The first part of the notes that follow is repeated from Lecture Notes 4.)

**Implication:** $p \implies q$ (read as “$p$ implies $q$”) is the proposition that is false when $p$ is true and $q$ is false and is true otherwise.

For an implication $p \implies q$ 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:

\[
(p \lor \neg p) \iff T \quad F \implies p \quad \neg q \implies \neg p \quad (p \land q) \implies r \quad p \implies (q \implies r)
\]

\[
p \land \neg p \
\neg p \lor q \quad (p \implies r) \land (q \implies r) \quad (p \lor q) \implies r
\]

---

1Twin 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))
Definition 5.1 Two boolean expressions are logically equivalent (written ≡) 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.)

Example 5.2 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 assignments.

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>p</td>
<td>q</td>
<td>\neg p</td>
<td>\neg q</td>
<td>p \Rightarrow q</td>
<td>p \lor \neg q</td>
<td>\neg q \Rightarrow \neg p</td>
<td>p \land \neg q</td>
<td>\neg(p \land \neg q)</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</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>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The first equivalence in Example 5.2 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 \( p \land \neg q \).

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:

To prove \( p \) we can instead prove that \( \neg p \Rightarrow C \).

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

<table>
<thead>
<tr>
<th>p</th>
<th>\neg p</th>
<th>C</th>
<th>\neg p \Rightarrow C</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>T</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.

To prove \( p \Rightarrow q \) 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!). As we shall see in a future lecture when we examine Boolean Algebra there is a more interesting way of manipulating logical equivalences between boolean expressions.

**Example 5.3** 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 5.4** Prove that \( \sqrt{2} \) is irrational. \(^2\)

\(^2\) \( \sqrt{2} \) 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!
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 there are integers \( a \) and \( b \) (\( b \neq 0 \)) with no common factors such that
\[
\sqrt{2} = \frac{a}{b}
\]
Squaring both sides of the above equation gives
\[
2 = \frac{a^2}{b^2} \quad \quad \quad a^2 = 2b^2 \tag{1}
\]
From (1) we conclude that \( a^2 \) is even.

Lemma \(^3\) 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
\[
a = 2k \tag{2}
\]
Combining (1) and (2) we get
\[
4k^2 = 2b^2 \quad \quad \quad 2k^2 = b^2
\]
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 
\textit{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 5.5 (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
\[
n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k}
\]

\(^3\)A “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!
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.

**Example 5.6** Prove that \( \sqrt{2} \) is irrational using the unique factorization theorem.

**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.  

**Example 5.7** Prove that there exist two irrational numbers, \( x \) and \( y \), such that \( x^y \) is rational.

**Solution:** Consider \( w = \sqrt{2}^{\sqrt{2}} \). It is beyond the scope of this class to determine whether \( w \) is rational or irrational. No matter!

We have two cases:

**Case 1:** \( w \) is rational. Then we take \( x = y = \sqrt{2} \) and we are done.

**Case 2:** \( w \) is irrational. Then we take \( x = w \) and \( y = \sqrt{2} \) and we are done again because

\[
\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2
\]

In both cases we have found irrationals \( x, y \) such that \( x^y \) is rational.

(This is an example of a *non-constructive* proof. It shows that \( x, y \) exist but it doesn’t show what they are! In fact, it can be shown, with difficulty, that \( \sqrt{2}^{\sqrt{2}} \) is irrational. )

---

\(^{4}\)It follows from Gelfond’s Theorem which answered Hilbert’s 7th problem. Google it.
Example 5.8 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. Let \( q \) be any prime number. Because of the way \( n \) is constructed, when \( n \) is divided by \( q \) the remainder is 1. That is, \( n \) is not a multiple of \( q \). This contradicts the Fundamental Theorem of Arithmetic.

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. Hence, the number \( N_2 = n(n + 1) \) must have at least two different prime factors. 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. 

COUNTING We continue studying how to use combinations and what are their properties.

Example 5.9 How many 8-letter strings can be constructed by using the 26 letters of the alphabet if each string contains 3, 4, or 5 vowels? There is no restriction on the number of occurrences of a letter in the string.

Solution: Let \( E \) be the set of 8-letter strings that contain at least 3 vowels. Let \( E_i \) be the set of 8-letter strings containing exactly \( i > 0 \) vowels (so \( i \in \{1, 2, 3, 4, 5\} \))

An element of \( E_i \), i.e., a 8-letter string with exactly \( i \) vowels, can be constructed using the following steps.

Step 1. Choose \( i \) locations out of the available 8 locations for vowels.

Step 2. Choose the vowels for each of the \( i \) locations.

Step 3. Choose the consonants for each of the remaining \( 8 - i \) locations.
Step 1 can be performed in \( \binom{8}{i} \) ways. Step 2 can be performed in \( 5^i \) ways. Step 3 can be performed in \( 21^{8-i} \) ways. By the multiplication rule, the number of 8-letter strings with exactly \( i \) vowels is given by

\[
|E_i| = \binom{8}{i} \cdot 5^i \cdot 21^{8-i}
\]

Since the sets \( E_3, E_4, \) and \( E_5 \) partition (divide in pairwise disjoint subsets) the set \( E \), by the sum rule we get

\[
|E| = \sum_{i=3}^{5} |E_i| = \sum_{i=3}^{5} \binom{8}{i} \cdot 5^i \cdot 21^{8-i}
\]

Addendum. The following question was raised in class in one of the previous offerings of this course. What if we want to count all 8-letter strings with distinct letters that have 3, 4, or 5 vowels? In this case, the above procedure still applies. However, the number of ways of doing each step changes. Step 1 can be performed in \( \binom{8}{i} \) ways. Step 2 can be performed in \( (5)^i \) ways. Step 3 can be performed in \( (21)^{8-i} \) ways. By the multiplication rule, the number of 8-letter strings with distinct letters that have exactly \( i \) vowels is given by

\[
\binom{8}{i} \cdot (5)^i \cdot (21)^{8-i}
\]

The total number of 8-letter strings with distinct letters that have 3, 4, or 5 vowels is

\[
\sum_{i=3}^{5} \binom{8}{i} \cdot (5)^i \cdot (21)^{8-i}
\]

Mathematicians often say **binomial coefficients** instead of “combinations”. We are about to see why. A binomial is a sum of two terms, such as \( a + b \). The **binomial theorem** gives an expression for \( (a + b)^n \) where \( a \) and \( b \) are real numbers and \( n \) is a natural number.

**Theorem 5.10** For any real numbers \( a \) and \( b \) and natural number \( n \)

\[
(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k
\]

**Proof:** The formula is easily checked for \( n = 0 \). For \( n \geq 1 \), observe that each term (monomial) in the expansion of \( (a + b)^n \) is of the form \( a^{n-k} b^k \), \( k = 0, 1, 2, \ldots, n \). How many times does \( a^{n-k} b^k \) occur in the expansion? This is the same number of times as there are orderings of \( n-k \) \( a \)'s and \( k \) \( b \)'s. This is equal to \( \binom{n}{k} \). Thus the coefficient of like terms of the form \( a^{n-k} b^k \) is \( \binom{n}{k} \). This proves the theorem.

\[
\square
\]
Pascal’s Triangle  We know that $(a + b)^0 = 1$, $(a + b)^1 = a + b$, $(a + b)^2 = a^2 + 2ab + b^2$, $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, etc.

Blaise Pascal observed some interesting relationships between the binomial coefficients when arranged in rows as follows:

Specifically, observe that each binomial coefficient is the sum of the two just above it. Formally:

**Theorem 5.11 (Pascal’s Identity)**  If $n$ and $k$ are positive integers with $n \geq k$ then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

**Proof:** This can be easily verified using the factorial formula for combinations. However, the following proof is more insightful.

Let $S = \{x_1, x_2, \ldots, x_n\}$ be the set of $n$ elements. We count the number of subsets of size $k$ in two ways. One way gives the combinations of $k$ our of $n$, i.e., the LHS of Pascal’s Identity. In the second way, we observe that $k$-element subsets of $S$ can be partitioned into those that contain $x_n$ and those that don’t. For the former type of subset the other $k-1$ elements come from $S \setminus \{x_n\}$. There are $\binom{n-1}{k-1}$ ways of choosing these subsets. For the latter type of subset all of the $k$ elements must be chosen from $S \setminus \{x_n\}$. There are $\binom{n-1}{k}$ ways of doing this. Thus, by the sum rule the number of $k$-element subsets of $S$ is given by the RHS of Pascal’s Identity.  

**Combinatorial proof.** We now prove a couple of identities using the following technique. To prove an identity we will pose a counting question. We will then answer the question in two ways, one answer will correspond to LHS and the other would correspond to the RHS of the identity. We have seen an example of this technique in the proof of Pascal’s Identity. This technique is often called a *combinatorial proof.*
Example 5.12  Prove that

\[
\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} = 0
\]

Solution: One way to solve this problem is by substituting \( a = 1 \) and \( b = -1 \) in the Binomial Theorem, yielding

\[
0^n = 0 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k.
\]

However, a combinatorial proof will give us more insight into what the expression means. We want to prove that

\[
\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots
\]

Consider a set \( X = \{x_1, x_2, x_3, \ldots, x_n\} \). We want to show that the total number of subsets of \( X \) that have even size equals the total number of subsets of \( X \) that have odd size. We will now show that both these quantities equal \( 2^{n-1} \) from which the claim follows.

An even-sized subset of \( X \) can be constructed as follows.

1. Step 1. Decide whether \( x_1 \) belongs to the subset or not.
2. Step 2. Decide whether \( x_2 \) belongs to the subset or not.
   
   :.
3. Step \( n \). Decide whether \( x_n \) belongs to the subset or not.

Note that there are 2 choices for each of the first \( n - 1 \) steps but exactly one choice for performing step \( n \). This is because if we have choose an even number of elements from \( X \setminus \{x_n\} \) then we must leave out \( x_n \) otherwise we must include \( x_n \) in the subset. Hence using the multiplication rule the total number of even-sized subsets of \( X \) equals \( 2^{n-1} \).

To compute the number of odd-sized subsets we could proceed similarly. Or, we could count complementarily: since we know that the total number of subsets of \( X \) is \( 2^n \), the total number of odd-sized subsets of \( X \) is \( 2^n - 2^{n-1} = 2^{n-1}(2 - 1) = 2^{n-1} \).

Example 5.13  Prove that \( \sum_{k=0}^{n} \binom{n}{k} = 2^n \).

Solution: We pose the following counting question.

Given a set \( S \) of \( n \) distinct elements how many subsets are there of the set \( S \)?

From earlier lectures, we know that the answer is \( 2^n \). This gives us the RHS.
Another way to compute the answer to the question is as follows. The powerset $2^S$ containing all possible subsets can be partitioned into $S_0, S_1, \ldots, S_n$, where $S_i$, $0 \leq i \leq n$, is the set of all subsets of $S$ that have cardinality $i$. Thus

$$|2^S| = |S_0| + |S_1| + \ldots + |S_n|$$

$$= \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$$

$$= \sum_{k=0}^{n} \binom{n}{k} = \text{LHS}$$

This proves the claim.

(How do you derive the same identity from the Binomial Theorem?)

Example 5.14 Give a combinatorial proof to show that

$$\sum_{k=0}^{r} \binom{n}{k} \binom{m}{r-k} = \binom{n+m}{r}$$

Solution: We pose the following counting question.

There are $n$ men and $m$ women. How many ways are there to form a committee of $r$ people from this group of people?

By definition, there are $\binom{n+m}{r}$ distinct committees of $r$ people. This gives us the RHS.

The set $S$ of all possible committees of $r$ people can be partitioned into subsets $S_0, S_1, S_2, \ldots, S_r$, where $S_k$ is the set of committees in which there are exactly $k$ men and the rest $r-k$ are women. Note that $|S_k| = \binom{n}{k} \binom{m}{r-k}$. Thus we have

$$|S| = \sum_{k=0}^{r} \binom{n}{k} \binom{m}{r-k}$$

which gives us the left hand side of the expression.