Lecture 1: Introduction to discrete mathematics

Rajat Mittal*

IIT Kanpur

1 Course polilcies

This is an introductory course on the mathematics needed in Computer Science. The topics covered here will be useful in the theory, systems and applications; that means, all areas of computer science.

Grading. Tentatively the activities are:

Assignments (10%): 4-5 assignments will be given. They SHOULD be written independently. If you discuss assignment with friends, please mention their name on your assignment.

Quizzes (30%): 4 Quizzes of 50 minutes each. Each will be announced a few days in advance.

Mid-sem exam (25%): 2 hours as scheduled by DoAA.

End-sem exam (35%): 3 hours as scheduled by DoAA.

Most importantly, any immoral behavior like cheating and fraud will be punished with extreme measures and without any exception. `http://www.cse.iitk.ac.in/pages/AntiCheatingPolicy.html`

There will be no attendance. We will use an LMS, probably Moodle to discuss questions and share grades. The course website is `https://www.cse.iitk.ac.in/users/rmittal/course_f18.php`. First course handout can be found on the website.

This note is an introduction, and written to give a feeling about what will be covered in the course. Hence, the terms may be loosely defined. This introduction will make more and more sense as we progress through the course.

2 What is discrete mathematics?

Not surprisingly, the branch of mathematics which deals with *discrete* objects and structures is called discrete mathematics. Here, by discrete set, we mean that the elements are distinct and are not connected in a continuous manner. In other words, we can say that the elements of the set can be counted (set has finite or countably infinite number of elements).

Do not worry if these terms are unfamiliar to you, they will become clearer as the course progresses. At this point, to get the intuition, the set of natural numbers is a discrete set. On the other hand, the set of real numbers is continuous. You have already encountered discrete mathematics while studying permutation/combination, natural numbers and probability theory.

The next question might be, why do we study these discrete objects? On a computer, we can only store discrete objects and hence almost all applications require studying these discrete object. So, it is not an exaggeration to say,

Discrete mathematics plays a fundamental role in Computer Science and is an essential background for almost all of the advanced courses like theory of computation, compilers, databases, operating systems, algorithms and data structures etc. .

To reiterate, one of the main reason for its importance is that the information in a computer is stored and manipulated in a discrete fashion. To say it concisely, computer has a finite precision.

This course will be a collection of various concepts and techniques which will help you in your future endeavors in computer science. These different topics can be broadly divided into five distinct parts related to each other. We will introduce them one by one.

* Thanks to Nitin Saxena for his notes from the previous iteration of the course.

2.1 Proofs

"I have had my results for a long time, but I don't know yet how to arrive at them."
– Karl Friedrich Gauss

Proofs are the way in which we arrive at the result or show that the statement is rigorous mathematically. This will be a short but very important part of the course. Through out the course, we will see many proofs, sometimes multiple proofs of the same result. You should remember that two proofs might give the same result but can give very different intuition. Reproving things your own way is an integral part of research.

These are few of the questions we will worry about in first few lectures.

- What are proofs?
- What are the different techniques used to prove mathematical statements? (Eg. *axioms, induction, implication, contradiction.*)
- Which proofs are mathematically correct?
- Can every statement be proved/ disproved?

These questions are actually part of a logic course. You will be taking a course on formal logic soon. So, we will tackle these questions using examples. There will be lot of examples of proofs as well as lot of different techniques used to prove things in mathematics. The target would be to get a feeling of when is a proof mathematically correct and when does it have an error.

2.2 Combinatorics

"It is difficult to find a definition of combinatorics that is both concise and complete, unless we are satisfied with the statement: Combinatorics is what combinatorialists do."
– W. T. Tutte

Combinatorics can be thought of as *art of counting.* It concerns itself with anything enumerative and mostly asks the questions of type,

how many ways are there to do some well defined operation on a set.

As Peter Cameron explains, most of the other branches in mathematics have a well-defined goal, such as prime number theorem. Unlike them, Combinatorics seems to be a collection of unrelated puzzles chosen at random. Hence this field is very broad, where emphasis is given on techniques rather than results.

In the second part of this course we will look at these different techniques and their application. The kind of puzzles we will be interested in,

- For any positive integer n, prove that there exists a positive integer consisting of digits 1 and 0 only and is divisible by n.
- Calculate the number of ways to distribute n identical balls among m distinct bins.
- Count the permutations of $\{1, 2, \cdots, n\}$ in which each element is mapped to an element different from itself.
- What are the number of valid parenthesis with n '(' and n ')'? (*recurrence, generating function*)
- In how many ways can we partition the number n?
- How many elements less than n are there which are coprime to n?

2.3 Graph theory

"The origins of graph theory are humble, even frivolous."
– N. Biggs, E. K. Lloyd, and R. J. Wilson

Graph theory, as you would guess, is the study of *combinatorial graphs*. We have written *combinatorial graphs*, to make the distinction between graphs (or diagrams) of functions as opposed to the combinatorial graphs we will study. The graphs in graph theory are more like the pictorial representations of networks (communication, transport, social etc.) capturing the properties like connectedness, groups, reachability etc..

Graph theory will be the third part of our course, but it is inherently related to combinatorics. Many people used to consider (still consider) it as a part of combinatorics.

Combinatorial graphs can also be thought of as a graphical representation of combinatorics and related disciplines. They are used to model many different situations involving relations, networks and other mathematical applications. We will be interested in different kind of well-defined structures inside these graphs and counting them.

Again, the questions which will interest us will look like,

- Is there a way to go from Delhi to Mumbai using every city given the connections? (*Hamiltonian path*)
- How many classrooms do we need such that no two friends are in the same room given the friendship network of a class? (*coloring*)
- Does there exist a possible pairing of girls and boys given their preferences? (*matching*)

2.4 Number theory

"Mathematics is the queen of the sciences and number theory is the queen of mathematics. She often condescends to render service to astronomy and other natural sciences, but in all relations she is entitled to the first rank."
– Karl Friedrich Gauss (1777-1855)

We will study some basic properties of numbers (i.e. integers). This is an area where one can ask simple questions but there may not be an easy answer. Number theorey is one of the earliest branches of mathematics, still, it has constantly attracted the attention of most brilliant of mathematicians. We will see some elegant, and basic, techniques in number theory. For example,

- When can a number be factored?
- How many primes are there?
- Test whether two numbers share a factor?
- Is number theory practical? (*cryptography, error-correcting codes*)

2.5 Abstract algebra

"In these days the angel of topology and the devil of abstract algebra fight for the soul of each individual mathematical domain"
– Hermann Weyl

We will look at the devil in this quote. Take a look at the following questions.

- Give a number n which leaves a remainder of 20 when divided by 23 and 62 when divided by 83.

- How many different necklaces can you form with 2 black beads and 8 white beads? How many necklaces can you form with blue, green and black beads?

- What are the last two digits of of a^{40} when a is not divisible by 2 or 5?
- We know that there is an explicit formula for the roots of quadratic equation $ax^2+bx+c=0$, $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. Similarly there are explicit formulas for degree 3 and degree 4 equations. Why don't we have something for degree 5?
- When does the equations of the form $x-y=z$ make sense? If x is a natural number or an integer or a matrix or an apple or a permutation?

When we look at these questions, they seem unrelated and seem to have no common thread. Mathematicians realized long time back that problems in algebra, number theory and even geometry can be solved using very similar techniques. They were interested in finding out the common element among these proofs and were interested in searching for more domains where such techniques are applicable. It turns out that there is a single mathematical theory which can help us understand these questions and give us answers to these seemingly non-related topics.

The mathematical framework which ties these questions together is called *abstract algebra*.

3 How to give a proof?

All of you must have proved a lot of mathematical statements by now and have pretty good intuition about what proofs are. So, we will take an informal approach to proofs. The concept of rigorous and correct mathematical proof will be shown through examples. A more formal approach can be taken through logic, which will be covered in another course.

Theorem 1 (Euclid, c. 300 BC). *Given a natural number n, there exist a prime greater than n.*

Proof. Suppose, for the sake of contradiction, there is no prime greater than n. Define,

$$m = n! + 1.$$

Since $m-1$ is divisible by all the numbers $\{2,\cdots,n\}$, m is not divisible by any of them. This implies that no prime divides m (because all primes are smaller than n). Thus, m itself has to be a prime greater than n. This is a contradiction.

□

Notice that the above proof also proves that there are infinite number of primes.

Look at the following exercise,

Exercise 1. Recall the formula for the infinite geometric sum. Using that, one can deduce the following:

$$\begin{aligned}
&\cdots + x^{-2} + x^{-1} + 1 + x + x^2 + \cdots \\
&= \frac{x^{-1}}{1-x^{-1}} + \frac{1}{1-x} \\
&= \frac{1}{x-1} + \frac{1}{1-x} \\
&= 0\,.
\end{aligned}$$

What could be the problem?

One of the applications of the formula is incorrect! The series needs to converge

3.1 What is a Proof?

A *proof* of a statement is a correct mathematical argument which ultimately shows that the statement is true. A proof, in general, consists of a series of mathematical steps, where any step is derived (implied) from the previous step or is part of the axioms, definitions, hypotheses or premises. *Hypothesis* (or *premise*) is the mathematical statement given to us.

Axioms are the things we assume to be true in a mathematical system. The oldest known axioms are the axioms of geometry mentioned in Euclid's book.

Example 1 (Euclid's axioms). – There is a unique line from any point to any point.
– There is a unique circle with any center and radius.

Let us take an example of a simple proof. Suppose we want to prove, *If n is odd, then n^2 is odd.*

Proof. n is odd (hypothesis)
$\Leftrightarrow$ $n = 2k+1$ (definition of odd)
$\Leftrightarrow$ $n^2 = 4k^2 + 4k + 1$
$\Leftrightarrow$ $n^2 = 2(2k^2 + 2k) + 1$
$\Rightarrow$ n^2 is odd (definition of odd) □

Exercise 2. Why do we have one-directional arrow in a step and bidirectional ones in the others?

To assert that some statements may not be equivalent.

The implications from one step to another is the critical part and most of the mistakes happen there. We need to make sure that every implication either follows from a hypothesis/axiom/definition or is *straightforward* enough.

The *conclusion* part of an implication is usually asserted by the words: hence, thus, therefore, consequently, whence, etc.

Most of the theorems can be seen as one mathematical statement implying another. Let us represent the mathematical statements as p, q. Then, we will write $p \Rightarrow q$ for the fact that statement p implies statement q. Another important concept is *equivalence*, $p \Leftrightarrow q$, which is the same as saying that $p \Rightarrow q$ and $q \Rightarrow p$. The latter is called the *converse* of the former, and vice-versa.

For example, in the statement *If n is odd, then n^2 is odd*, we can represent *n is odd* as p and *n^2 is odd* as q. Then the statement is $p \Rightarrow q$.

Exercise 3. Is the converse true?

ue but requires a slightly different proof.

The English statements of "if-then" are implications and "iff/if and only if" are equivalences. Consider the following theorems.

- If n is odd then n^2 is of the form $4k+1$.
- For all primes, a^p leaves a remainder a when divided by p.
- Every prime greater than 2 is odd.
- $\sqrt{2}$ is irrational.
- n^2 is even if n is even.

Exercise 4. Represent each of these theorems in the form $p \Rightarrow q$ or $p \Leftrightarrow q$.

Now we will look at various techniques by which theorems can be proved. These include direct proofs, contrapositive, proof by contradiction and proof by induction.

3.2 Direct proofs

This is the most obvious way of proving truth. If we need to prove $p \Rightarrow q$, we start with p, derive different mathematical statements which end at q. The initial example given above for showing that n^2 is odd if n is odd was proven using direct proof.

Let us take another example. Suppose we want to show: All perfect squares are of the form $4k$ or $4k+1$.

Proof. n is either even or odd.
$\Rightarrow$ n is of the form $2k$ or $2k+1$.
$\Rightarrow$ Squaring, $n^2 = 4k^2$ or $n^2 = 4k^2 + 4k + 1$.
$\Rightarrow$ Hence, n^2 is of the form $4k$ or $4k+1$. □

This is an *indirect* proof of: $4k+2, 4k+3$ are never perfect squares!

3.3 Contrapositive proofs

A slightly more involved way of proving $p \Rightarrow q$ is to prove that if q is false then p is false too. Denote *not* (negation) of a statement p by $\neg p$. A proof by contrapositivity involves showing $\neg q \Rightarrow \neg p$ instead of showing $p \Rightarrow q$.

What does this mean in natural language. Consider the statement, if Ravan goes to the forest then Sita will not come out of the hut. Clearly, if Sita is outside the hut then it means that Ravan did not go the forest.

Let us look at some mathematical examples. Show that if there is a prime $n > 3$ then $n+1$ is not a perfect square. Here p is "$n \geq 3$ is a prime number" and q is "$n+1$ is not a perfect square".

Proof. We will start with $\neg q$, i.e., $n+1$ is a perfect square.
$\Rightarrow$ there exist x, s.t., $x^2 = n+1$.
$\Rightarrow$ $x^2 - 1 = n$.
$\Rightarrow$ n can be factored as $(x+1)(x-1)$, where $(x-1) \neq 1$.
$\Rightarrow$ n is not a prime. □

Note 1. The previous theorem can be equivalently stated as, there is no prime number $n > 3$ for which $n+1$ is a perfect square.

Exercise 5. Convince yourself that direct proof of the previous theorem will be difficult.

Warning: There is a common fallacy, where instead of proving $\neg q \Rightarrow \neg p$ some people prove $\neg p \Rightarrow \neg q$. You should be very careful, $\neg p \Rightarrow \neg q$ is NOT equivalent to $p \Rightarrow q$.

Example 2. Consider the statement: If n is not of the form $6k+3$ then n^2 is not divisible by 3. You can check that this statement is not true. On the other hand, we can prove $\neg p \Rightarrow \neg q$ in this case.

$\neg p$ means that n is of the form $6k+3$. On squaring, $n^2 = 36k^2 + 36k + 9 = 3(12k^2 + 12k + 3)$. So, $\neg q$ is true (3 divides n^2).

3.4 Contradiction

Another technique, related to contrapositivity, is the method of contradiction. In this case, if we want to prove that p is true, then we assume $\neg p$ and arrive at something false (like 2 is an odd number, etc.) or something contrary to the hypothesis.

The first example of a proof by contradiction will be the fact that $\sqrt{2}$ is not rational.

Proof. Suppose $\sqrt{2}$ is rational. This implies that there exist $a, b \in \mathbb{N}$ with no common factor s.t. $\sqrt{2} = \frac{a}{b}$. Squaring, $2 = \frac{a^2}{b^2}$. This implies that there is a common factor (namely, 2) between a and b.

Exercise 6. Prove that if $2 = \frac{a^2}{b^2}$ then a and b have 2 as a common factor.

From $a^2 = 2b^2$ one can deduce that 2 divides a. Say, $a = 2a'$.
Then we get $2a'^2 = b^2$, which implies that 2 divides b.

But this violates the hypothesis that a and b have no factor in common. This is a contradiction. □

Our last example will require some definitions in set theory. It is easy to define *cardinality* of a set (size of a set) when the set is finite. It is the number of elements in the set. How about the *cardinality* when the set is infinite. Would you say that the cardinality of the set of odd integers O is the same as the cardinality of the set of even integers E?

The intuition seems to suggest that they should be the same ($|O| = |E|$?). The reason being that you can establish a one to one relation between the two sets, e.g., $x \to x - 1$, which covers the two sets entirely.

Note 2. We denote the cardinality of a set S by $|S|$.

The *cardinality* for any two sets are defined to be equal if there is a bijection between the two sets. Remember that *bijection* means that the relation is one to one and onto.

Similarly, we can say that $|S| \leq |T|$ if there is an injection (one to one mapping) from S to T. There is a theorem (Schröder-Bernstein) which states that if there are injections from S to T and T to S then there is a bijection between S and T.

Exercise 7. Show that the cardinality of natural numbers is same as cardinality of integers.

The same can be shown for integers and rationals. Though, the number of rationals and number of reals are not the same. Things can get weird at infinity !!

Let us see another beautiful proof by contradiction about the cardinality of set and its power set. It will use an argument called *diagonalization*, you can extend it to prove that the set of integers have strictly smaller cardinality than the set of real numbers.

Theorem 2. *The cardinality of a set S is not equal to the cardinality of its powerset 2^S (set of all subsets).*

Note 3. This statement sounds trivial if the set is finite. But we will prove this even for infinite sets.

Proof. Suppose the cardinality of the set and its powerset are equal. By definition, there exists a bijection between the set and its powerset. Let $\phi : S \to 2^S$ be a bijection. Define a new subset of S,

$$T := \{x : \ x \in S, \ x \notin \phi(x)\} .$$

In words, T is the set of elements of S which are not in their image (under ϕ).

By definition, T is an element of 2^S. Since ϕ is a bijection, T will have a pre-image $t \in S$. Consider the two cases,

Case 1: Suppose $t \in T$. Since t is in its image, it should not be in the special set T (by definition). So $t \notin T$, a contradiction.

Case 2: Suppose $t \notin T$. Since t is not in its image, it should be in the special set T. So $t \in T$, again a contradiction.

Since the two cases cover all possibilities, we proved that a bijection cannot exist. Hence, the cardinality of S and 2^S are different.

Note 4. There is an injection from S to 2^S, but not vice-versa!

Another way to look at the same proof is the following. Look at the schematic matrix below. The i-th column corresponds to the i-th element of set S, say x_i. The i-th row represents the image of x_i, i.e., $\phi(x_i)$. The (i, j)-th entry of the 0/1 matrix denotes whether x_j is an element of $\phi(x_i)$ (entry 0 means $x_j \notin \phi(x_i)$).

$$\begin{array}{c|c|c|c|c} & x_1 & x_2 & x_3 & \cdots \\ \hline \phi(x_1) & 0 & 1 & 0 & \cdots \\ \hline \phi(x_2) & 1 & 0 & 0 & \cdots \\ \hline \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Look at the diagonal elements of the 0/1 matrix and flip them. The subset corresponding to the diagonal string (T in the previous proof) is not same as any element of 2^S. Because it is different from every subset in at least one position (namely, the diagonal one). Hence it has no pre-image in S. □

This interpretation of the proof is known as the *diagonalization argument.* It is used to prove that integers and reals cannot have a bijection (Cantor 1891). Can you show it using diagonalization? Hint: show that there is no bijection between natural numbers and real numbers between 0 and 1.

The sets which have cardinality less than or equal to integers/ natural numbers /rationals are known as *countable sets.* The sets having cardinality greater than integers (like reals) are called *uncountable sets.*

3.5 Quantification

Many a times the theorems given in mathematics require *quantification* over a large domain. That means the statements look like,

1. Existential: *There exist* an element of the universe (i.e. a mathematical object) which satisfies certain condition.
2. Universal: *For all* elements of the universe certain condition is satisfied.

Note 5. Mathematical universe is the set of elements we are interested in. For example, integers ($\mathbb{Z}$), reals $\mathbb{R}$, set of matrices or set of triangles.

A direct proof of an existential kind of a theorem can be given by an *example.*

Prove that there is an n, such that there is a prime number between n and $2n$.

Proof. Consider the number $n = 5$. There is a prime 7 between 5 and 10, proving the existence. Hence, there is an n such that there is a prime number between n and $2n$. □

Though a direct refutation of an existential statment is harder to prove and requires a more sophisticated mathematical argument.

For example, there exists an n such that there is no prime number between n and $2n$. This statement was refuted by a clever argument of Chebyshev. For more details, look at *Bertrand's postulate.*

Similarly, a direct refutation of a universal kind of a theorem can be given by a *counterexample.* Prove that all primes are of the form $4k + 1$.

Proof. Consider the number 3. It is not of the form $4k + 1$ and we know that 3 is a prime. Hence all primes need not be of the form $4k + 1$. □

It is convenient to use the notation $\exists x \in U$ (resp. $\forall x \in U$) to mean *there exists an element x in the universe U* (for all elements x in the universe U).

Though, proving a universal statement might be hard.

Exercise 8. What is the relation between proving an existential kind of theorem and refuting a universal kind of theorem?

Negation of an existential statement is a universal one.

3.6 Induction

Mathematical induction is one of the strongest tools to prove universal statements about natural numbers (statements like *for all natural numbers n, $n \leq 2^n$*). For the use of induction, the range of the universal statement should be countable.

Note 6. Induction can be generalized to uncountables with some effort. Then, it is called *transfinite induction.* We will not go into its details.

Say, we want to prove $\forall x P(x)$ where $x \in \mathbb{N}$ and $P(x)$ is a property of x. Then, mathematical induction proceeds by showing two things.

1. *Base case:* $P(0)$ is true.
2. *Induction step:* If $P(m)$ is true then $P(m+1)$ is true.
   $P(m)$ *is true* is called the *induction hypothesis.*

This seemingly simple technique has lot of variations and can prove very complicated theorems. Let us start with a simple example.

Theorem 3. *Prove that* $0+1+4+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof. Let $P(n)$ be the hypothesis that $0+1+4+9+\cdots+n^2 = n(n+1)(2n+1)/6$.

Base: $P(0)$ means that $0 = \frac{0\times1\times1}{6}$.

Induction: For the inductive step we need to show,

$$0+1+\cdots+(n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

By induction hypothesis, $0+1+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$. Adding $(n+1)^2$ to both the sides,

$$\begin{aligned} 0+1+\cdots+(n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)(n+2)(2n+3)}{6}\,. \end{aligned}$$

Hence, we complete the induction and prove the theorem.

□

Exercise 9. Prove that $2^n \geq n$ by induction.

Hint: Notice that this problem is well suited for induction. Once 2^n becomes bigger than n. After that, we multiply the bigger quantity by 2 and only add 1 in the smaller quantity. So the inequality remains true for $n+1$.

Let us try another example.

Theorem 4. *Show that every number $n > 0$ can be written in a binary representation,*

$$n = b_r 2^r + \cdots + 2b_1 + b_0\,.$$

Where, r is some integer and $b_0, b_1, \cdots, b_r$ are bits $(0/1)$.

Proof. Let $P(n)$ be the hypothesis that n can be written in a binary representation.

Base: $P(1)$– clearly $1 = b_0$ gives the binary representation.

Exercise 10. Does it matter that the base case is $P(1)$ instead of $P(0)$?

Induction: We will assume a slightly different hypothesis, "$P(k)$ is true for all $k < m$", and show that $P(m)$ is true.

Exercise 11. Show that this version of induction step reduces to the old one.

Let $Q(k)$ be the induction hypothesis that $P(0), P(1), \cdots, P(k)$ is true.

Now to prove $P(m)$, consider two cases:

Case 1: If m is even, then $m' = \frac{m}{2}$ is an integer and is less than m. Let m' have a binary representation,

$$m' = b_r 2^r + \cdots + 2b_1 + b_0.$$

Then, m will have the binary representation,

$$m = 2m' = b_r 2^{r+1} + \cdots + 2b_0 + 0 = c_{r+1} 2^{r+1} + \cdots + 2c_1 + c_0.$$

Case 2: If m is odd, then $m' = \frac{m-1}{2}$ is an integer and is less than m. Let m' have a binary representation,

$$m' = b_r 2^r + \cdots + 2b_1 + b_0.$$

Then, m will have the binary representation,

$$m = 2m' + 1 = b_r 2^{r+1} + \cdots + 2b_0 + 1 = c_{r+1} 2^{r+1} + \cdots + 2c_1 + c_0.$$

Since these two cases exhaust all the possibilities, we are done. □

Exercise 12. How can you prove that the binary representation of a number is unique?

Use the fact that $2^n > 2^{n-1} + 2^{n-2} + \cdots + 2 + 1$.

The induction technique can be modified in various ways. We will take an example of *multi-dimensional* induction. You can convince yourself that, in spirit, this is the same as the original version.

Theorem 5. *Suppose there is a function $f(m,n)$ satisfying the following equalities,*

$$f(m+1,n) = f(m,n) + 2(m+n) + 1 \text{ and } f(m,n+1) = f(m,n) + 2(m+n) + 1.$$

If $f(0,0) = 0$, show that $f(m,n) = (m+n)^2$ satisfies these constraints.

Proof. The hypothesis $P(m,n)$ represents the fact that $f(m,n) = (m+n)^2$.

Base: $f(0,0) = (0+0)^2 = 0$ is true.

Induction: We need to be careful here and need to "move one step in each direction".

1. $P(m,n)$ is true implies $P(m+1,n)$.

$$f(m+1,n) = f(m,n) + 2(m+n) + 1 = (m+n)^2 + 2(m+n) + 1 = (m+n+1)^2 = ((m+1)+n)^2$$

2. $P(m,n)$ is true implies $P(m,n+1)$.

$$f(m,n+1) = f(m,n) + 2(m+n) + 1 = (m+n)^2 + 2(m+n) + 1 = (m+(n+1))^2$$

□

We have given an informal introduction to proofs using examples. Students interested in more formal notions of proof should read the section below and references mentioned there. There is a separate course on logic where you will study these in much more detail.

4 Logic (Advanced)

We will call mathematical statements as *propositions*. For example, "n is odd" is a proposition and so is "n^2 is odd". Other examples are,

- $x + y = 3$
- $n + 1$ is prime
- $y^2 = z$
- $\frac{1}{2}$ is irrational

These propositions can be combined or operated upon by operators like AND ($\wedge$), OR ($\vee$) and NOT ($\neg$). Suppose p and q are two propositions, the operators can be specified by the truth tables. We use T to denote that proposition is true and F for false.

NOT: ¬ p

p	$\neg p$
T	F
F	T

AND: $p \wedge q$

p	q	$p \wedge q$
T	T	T
F	T	F
T	F	F
F	F	F

OR: $p \vee q$

p	q	$p \vee q$
T	T	T
F	T	T
T	F	T
F	F	F

Such operators are also used in common language and they have similar meaning. The important distinction to remember is that "OR" is true if both the propositions are true (i.e. it is not *exclusive*).

Another operator of importance in this context is implication, which can be defined in terms of previous operators.

Implication: $p \Rightarrow q \cong \neg p \vee q$

p	q	$p \Rightarrow q$
T	T	T
F	T	T
T	F	F
F	F	T

For the implication $p \Rightarrow q$, p is called the hypothesis and q is called the conclusion. So an implication is *only* false if hypothesis is T but conclusion is F. For example, the statement "n is odd and $n = 2$ implies $n^2 = 6$" is in fact true!

Exercise 13. What are the propositions and operators in the above statement?

The equivalence $p \Leftrightarrow q$ means $p \Rightarrow q$ and $q \Rightarrow p$.

Exercise 14. Make the truth table of $\Leftrightarrow$.

4.1 Quantified statements

Many theorems in mathematics involve quantification. To make sense of quantification, we need to introduce predicates. A *predicate* can be thought of as a function which outputs a proposition. For example, $P(x) = x \geq 3$ is a predicate which depends upon x, i.e., the truth value depends upon x. A predicate can be a function of multiple variables. Eg. "n is odd" can be considered as a predicate with n as a variable.

There are two kinds of *quantifiers* which can be applied on a predicate.

– *Existential quantification ($\exists x : P(x)$)*: Says that there exists an element x in the *universe* which makes the predicate $P(x)$ true.
– *Universal quantification ($\forall x : P(x)$)*: Says that $P(x)$ is true for all the possible values of x in the *universe*.

The *universe* is generally clear from the context. Otherwise it is specifically stated. Let us look at some more examples.

1. There exist a natural number smaller than 0.
2. All natural numbers are real numbers.
3. Every x is equal to zero.
4. There is a y which is the square root of x.
5. For all natural x there exists a y, s.t., $y > x$.

Exercise 15. Find out the quantifiers, predicate and universe in the examples given above.

4.2 Rules of inference

The mathematical steps or statements in a proof are propositions (quantified predicates) or combination of propositions (quantified predicates). To prove a mathematical statement means to show that the value of the corresponding proposition (quantified predicate) is T (true). Many a times the statement/ theorem which needs to be proven will look like $p \Rightarrow q$.

Exercise 16. For the statement "If n is odd, then n^2 is odd", what are the propositions and what are the operators. Can you write it as an implication in terms of quantified predicate.

For a proof, we go from one step to another using *rules of inference.* Below you will find some examples of rules of inference.

– $p \vee q$ can be inferred from p.
– q can be inferred from p and $p \Rightarrow q$.
– $\neg p$ can be inferred from $\neg q$ and $p \Rightarrow q$.
– $p \Rightarrow r$ can be inferred from $p \Rightarrow q$ and $q \Rightarrow r$.
– $\exists x : P(x)$ can be inferred from $P(c)$ where c belongs to the universe.
– $P(c)$ for some element c in universe can be inferred from $\exists x : P(x)$.
– $\forall x : P(x)$ can be inferred from the fact that $P(c)$ is true for arbitrary c in universe.
– $P(c)$ for c in universe can be inferred from $\forall x : P(x)$.

Hence, a proof is a series of mathematical steps where one step can be derived from the previous one using rules of inference. For more details about logic and formal notions of proof, please read the first and third chapter of Rosen's book [**?**].

References

1. K. H. Rosen. Discrete Mathematics and Its Applications. *McGraw-Hill*, 1999.
2. N. L. Biggs. Discrete Mathematics. *Oxford University Press*, 2003.