Mathematics for Computer Scientists

Tutorial

Dr S. S. Chandra

Mathematical theorems and their associated proofs are important for formally defining results in computer science. Graphs are an important tool for solving problems that involve relationships efficiently in computer science. In this tutorial, we will be looking at problems that will demonstrate how to write proofs and solve a simple graph problem.

In a proof by contradiction, if we want to show that a concept A is true by assuming the opposite and showing that we arrive at a contradiction. This means our initial assumption must be incorrect and that the opposite, our original concept A, must be true instead.

Problem 1

We shall attempt to prove that $\sqrt{2}$ is an irrational number by proof of contradiction step-by-step.

a) What are rational and irrational numbers? Define each type of number with words and equations.
b) What must then be our initial assumption for our proof in order to prove by contradiction?
c) Write the equation for $\sqrt{2}$ via our initial assumption above and cancel out the square root.
d) What does this say about the numbers either side of the equation?
e) What contradiction is arrived at and what does it prove?

Use the answers of the above points to write your proof as a series of logical statements in several sentences.

Problem 2

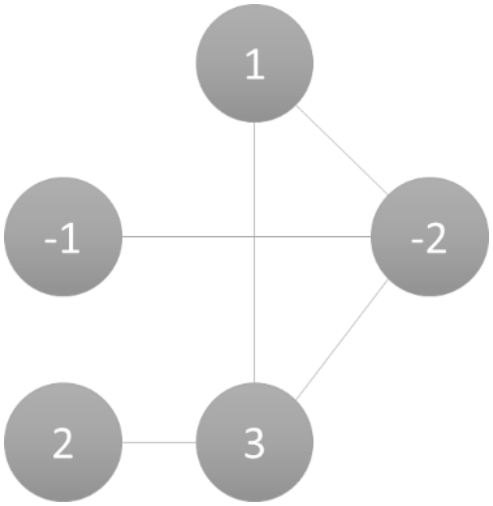
We shall prove that some infinities are larger than others! Please see section 7.2.1 of (Moore and Mertens, 2011) for more details on this problem.

Following Georg Cantor, we can examine the set of natural numbers $\mathbb{N}$ and the set of all subsets S of $\mathbb{N}$, i.e. the power set $\wp = \{S : S \subseteq \mathbb{N}\}$. We know that the set of $\mathbb{N}$ is infinite and therefore the power set is infinite as well. We would like to show that the power set $\wp$ has a larger infinity than $\mathbb{N}$.

a) What must then be our initial assumption for our proof in order to prove by contradiction?
b) We can use a table to compare the sizes of two sets with the rows representing one set and the columns representing the other. How can you tell if a set is larger than another by drawing a table?
c) Using a bit to represent whether the number is part of the set, draw an initial table of the set $\mathbb{N}$ as columns and $\wp$ as rows of a table for a small set of numbers and for a few examples of S such as the even numbers, odd numbers and prime numbers.
d) Imagine that your table contains all possible subsets. Now select the diagonal elements of the table and negate the bits. Why does this give us a new subset that can be added to the table?
e) Why can the idea of selecting and negating bits be used to create arbitrary new rows in the table?
f) How does this show that the set $\wp$ has a larger infinity than $\mathbb{N}$?

Use the answers of the above points to write your proof as a series of logical statements in several sentences.

Problem 3



Let the graph represent the amount of wealth distributed among 5 different interested parties. Negative values mean that party is in debt. Let each party be represented as a node and the funds owed/are owed to other parties as edges. If the parties have to share their wealth or debt with everyone else they owe/are owed money to simultaneously when distributing funds:

a) Is it possible that the wealth can be distributed across everyone so that no one is in debt?
b) Can one determine a general expression for how this can be determined for arbitrary graphs that represent wealth this way by looking at the edges and without computing the entire solution?

(Hint: This is the dollar game explained in this Numberphile video)

Problem 4

Show that a consequence of Fermat's little theorem below is that it *always* produces a *unique* integer sequence β_i of length $N = p - 1$ comprising of the residue classes $\{0, 1, 2, \dots, p - 1\}$ of p in some cyclic order when p is prime.

$$\alpha^N \equiv 1 \pmod{p}$$

You may validate this expression and theorem initially either by hand or by a program. An example of a value of p that produces a length that is a power of two is the Fermat primes, which are a subset of the Fermat numbers. The α here is known as a primitive root and $\alpha = 3$ is a value that is valid for Fermat primes.

The expression above is called an Nth root of unity and forms the basis of the Number Theoretic Transform (Agarwal and Burrus, 1975; Nussbaumer, 1981), an integer-only, real equivalent of the discrete Fourier transform, where the convolution theorem also applies.

References

Agarwal, R.C., Burrus, C.S., 1975. Number theoretic transforms to implement fast digital convolution. Proc. IEEE 63, 550–560.

Moore, C., Mertens, S., 2011. The Nature Of Computation. Oxford University Press.

Nussbaumer, H.J., 1981. Fast Fourier Transform and Convolution Algorithms by Henri J. Nussbaumer., Springer Series in Information Sciences, 2. Springer Berlin Heidelberg : Imprint: Springer, Berlin, Heidelberg.