Complexity Theory and Algorithms

Proof of Correctness

Disclaimer

The presentation is an amalgamation of information obtained from books and different internet resources and is intended for educational purposes only and does not replace independent professional judgement, statements of fact and opinions.

Proof of Correctness

Proof technique 1 - Contradiction

- Proof by contradiction, also known as indirect proof, consists of demonstrating the truth of a statement by proving that its negation yields a contradiction.

Example: Prove that for all integers n, if $n^3 + 5$ is odd then n is even

Let n be any integer and suppose, for the sake of contradiction, that $n^3 + 5$ and n are both odd. In this case integers j and k exist such that $n^3 + 5 = 2k + 1$ and $n = 2j + 1$. Substituting for n we have

$2k + 1 = n^3 + 5$

$2k + 1 = (2j + 1)^3 + 5$

$2k + 1 = 8j^3 + 3(2j)^2(1) + 3(2j)(1)^2 + 1^3 + 5$

$2k = 8j^3 + 12j^2 + 6j + 5.$

We found $2k = 8j^3 + 12j^2 + 6j + 5.$

Dividing by 2 and rearranging we have $k - 4j^3 - 6j^2 - 3j = 5/2$.

This, however, is impossible: 5/2 is a non-integer rational number, while $k - 4j^3 - 6j^2 - 3j$ is an integer by the closure properties for integers. Therefore, it must be the case that our assumption that when $n^3 + 5$ is odd then n is odd is false, so n must be even.

Prove that √2 is irrational

Proof.

Suppose $\sqrt{2}$ is rational. Then integers a and b exist so that $\sqrt{2} = a/b$.

Without loss of generality we can assume that a and b have no factors in common (i.e., the fraction is in simplest form). Squaring both sides and simplifying, we have

$$2b^2 = a^2$$

So we see that a^2 is even. This means that a is even. So, $a = 2m$ for some $m \in Z$. Then

$$2b^2 = a^2 = (2m)^2 = 4m^2$$

which, after dividing by 2, gives $b^2 = 2m^2$ so b^2 is even. This means $b = 2n$ for some $n \in Z$.

We have seen that if $\sqrt{2} = a/b$ then both a and b must be even and so are both multiples of 2.

This contradicts the fact that we know a and b can be chosen to have no common factors. Thus, $\sqrt{2}$ must not be rational, so $\sqrt{2}$ is irrational.

Proof of Correctness

Proof technique 2 - Mathematical Induction

- **Mathematical Induction** is a mathematical technique which is used to prove a statement, a formula or a theorem is true for every natural number.

It has 2 steps:

Step 1 − Prove that the statement is true for the initial value.

Step 2 − Show that, for any positive integer k, $k \leq n$, if S_k is true, then $S_k + 1$ is also true.

Is 3^n-1 a multiple of 2?

Example: Is 3^n-1 a multiple of 2?

1. Show it is true for **n=1:** $3^1-1 = 3-1 = 2$. Yes 2 is a multiple of 2. 3^1-1 is true

2. Assume it is true for **n=k:** 3^k-1 is true

Now, prove that $3^{k+1}-1$ is a multiple of 2

$3^{k+1}-1 = 3*3^k - 1 = (2+1)*3^k - 1 = 2*3^k + 3^k - 1$

Because: • 2×3^k is a multiple of 2 (we are multiplying by 2)

• **3^k-1 is true** (we said that in the assumption above)

So: $3^{k+1}-1$ is a multiple of 2 is true.

Show that the sum of integers from 1 to n = n(n+1)/2

- **Example: Sum of integers from 1 to n = n(n+1)/2**

What we are trying to prove: $P(n) = n(n+1)/2$

1. Show that P(n) is true for **n=1:** P(1) = 1 **and** 1(1+1)/2 = 1(2)/2 = 1(1) = 1

2. Assume it is true for **n=k:** P(k) = k(k+1)/2 is true

Now consider P(k+1)= 1 + 2 + … + k + (k+1)= k(k+1)/2 + (k+1)

= k(k+1)/2 + 2(k+1)/2= (k(k+1) + 2(k+1))/2

=(k+1)(k+2)/2

= (k+1)((k+1)+1)/2

Show that the sum of the first n powers of 2 is $2^n - 1$.

Example: The sum of the first n powers of 2 is $2^n - 1$.

1. Show that it is true for **n=1: Sum of first 1^{st} power of 2 is 2^0 , which equals $1 = 2^1 - 1$.**

2. Assume the sum of the first k powers of 2 is 2^k-1

Now, show that the sum of the first (k+1) powers of 2 is $2^{k+1}-1$

The sum of the first k+1 powers of 2 is

$$2^0 + 2^1 + 2^2 + \ldots + 2^{(k-1)} + 2^k$$

$$= \quad 2^k-1 + 2^k$$

$$= \quad 2(2^k) -1 = 2^{k+1} - 1$$


Thank You!