Discrete Mathematics and Statistics - CPT107

Xi'an Jiaotong-Liverpool University

西交利物浦大学

Part 1. Number Systems and Proof Techniques

Reading:

Discrete Mathematics for Computer Scientists, J.K. Truss, Sections 1.1 Number Systems and 1.3 Mathematical Induction (Subsections 1.3.1 and 1.3.2 only).

Discrete Mathematics for Computing R. Haggarty, Section 2.4.

Contents

- The most basic datatypes
  - Natural Numbers
  - Integers
  - Rationals
  - Real Numbers
  - Prime Numbers
- Proof Techniques
  - Finding a counter-example
  - Proof by contradiction
  - Proof by Induction

The Natural Numbers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

We say that $\mathbb{N}$ is closed under addition because if you take any two numbers in $\mathbb{N}$ and add them, you always get another number in $\mathbb{N}$.

Key property: Any natural number can be obtained from 0 by applying the operation $S(n) = n + 1$ some number times.

Examples: $S(0) = 1$. $S(S(0)) = 2$. $S(S(S(0))) = 3$.

The Integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

The positive integers: $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.

The Rational Numbers

$\mathbb{Q}$ is the set of all numbers that can be written as x/y where x and y are integers and y is not 0.

The Real Numbers

$\mathbb{R}$ is the set of all (decimal) numbers — distances to points on a number line.

Examples.

- -3.0
- 0
- 1.6
- $\pi = 3.14159\ldots$

A real number that is not rational is called irrational.

Prime Numbers

A prime number is a integer greater than 1 which has exactly two divisors that are positive integers: 1 and itself.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$$

Every integer greater than 1 can be written as a unique product of prime numbers.

Examples: $6 = 2 \times 3$. $15 = 3 \times 5$. $1400 = 2^3 \times 5^2 \times 7$.

A positive integer is even if it has 2 as a factor. Otherwise, it is odd.

The prime numbers reconsidered

Let $f(n) = n^2 + n + 41$

Statement: For every natural number n, $f(n)$ is prime.

Is the statement true or false?

$f(0)$ is 41, which is prime.

$f(1)$ is 43, which is prime.

$f(2)$ is 47, which is prime.

How can we either prove that the statement is true, or show that it is false?

Let $f(n) = n^2 + n + 41$

Statement: For every natural number n, $f(n)$ is prime.

To prove that the statement is false, we just have to find a natural number that is a counter-example. $f(0)$ is prime. $f(1)$ is prime. $f(2)$ is prime. $f(3)$ is prime $\ldots$ $f(39)$ is prime.

But $f(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 41 \cdot 41$. So $n = 40$ is a counter-example, and the statement is false.

Finding a counter-example can be difficult (Example: The Perrin Numbers)

$P(0) = 3$

$P(1) = 0$

$P(2) = 2$

$P(n) = P(n-2) + P(n-3)$ for $n > 2$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$P(n)$	3	0	2	3	2	5	5	7	10	12	17	22	29

n	13	14	15	16	17	18
$P(n)$	39	51	68	90	119	158

$P(0) = 3$

$P(1) = 0$

$P(2) = 2$

$P(n) = P(n-2) + P(n-3)$

An integer $n > 1$ is a Perrin Numbers if $P(n)$ is divisible by n.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$P(n)$	3	0	2	3	2	5	5	7	10	12	17	22	29
			2	3		5		7				11	

n	13	14	15	16	17	18
$P(n)$	39	51	68	90	119	158
	13				17	

- 1899 Are the Perrin numbers the same as the prime numbers?
- proved shortly afterwards: Every prime number is a Perrin number.
- 1995 There are Perrin numbers that are not prime. The smallest Perrin number that is not prime is 271 441.

The moral of the story

We can't believe a statement just because it is true for the first 271 440 examples that we try.

We need a proof that the statement is true or a proof that it is false. To prove that a statement like the one that we looked at earlier is false, we just need to find a counter-example, but sometimes this is difficult (because there are too many examples to check), so we have other methods. . .

$\sqrt{2}$ is not a rational number

Proof by contradiction.

- If $\sqrt{2}$ were rational then we could write it as $\sqrt{2} = x/y$ where x and y are integers and y is not 0.
- By repeatedly cancelling common factors, we can make sure that x and y have no common factors so they are not both even.
- Then $2 = x^2/y^2$ so $x^2 = 2y^2$ so x^2 is even. This means x is even, because the square of any odd number is odd.

the proof continued

- Let $x = 2w$ for some integer w.
- Then $x^2 = 4w^2$ so $4w^2 = 2y^2$ so $y^2 = 2w^2$ so y^2 is even so y is even.
- This contradicts the fact that x and y are not both even, so our original assumption, that $\sqrt{2}$ is rational, must have been wrong.

Induction

One domino for each natural number, arranged in order.

- I will push domino 0 (the one at the front of the picture) towards the others.
- For every natural number m, if the m'th domino falls, then the $(m+1)$st domino will fall.

Conclude: All of the dominos will fall.

Proving by induction that a property holds for every natural number *n*

- Prove that the property holds for the natural number $n = 0$.
- Prove that if the property holds for $n = m$ (for any natural number m) then it holds for $n = m + 1$.

A proof of a property by induction looks like this

Base Case: Show that the property holds for $n = 0$.

Inductive Step: Assume that the property holds for $n = m$. Show that it holds for $n = m + 1$.

Conclusion: You can now conclude that the property holds for every natural number n.

Example: Proof by Induction

For every natural number n,

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

Base Case: Take $n = 0$. The left-hand-side and the right-hand-side are both 0 so they are equal.

Inductive Step: Assume that the property holds for $n = m$, so

$$0 + 1 + \cdots + m = \frac{m(m+1)}{2}.$$

Now consider $n = m + 1$. We must show that

$$0 + 1 + \cdots + m + (m+1) = \frac{(m+1)(m+2)}{2}.$$

Proof continued

Since

$$0 + 1 + \cdots + m = \frac{m(m+1)}{2}.$$

$$\begin{aligned} 0 + 1 + \cdots + m + (m+1) &= \frac{m(m+1)}{2} + m + 1 \\ &= \frac{m(m+1) + 2(m+1)}{2} \\ &= \frac{(m+1)(m+2)}{2} \end{aligned}$$

Other starting values

Suppose you want to prove a statement not for all natural numbers, but for all integers greater than or equal to some particular natural number b

Base Case: Show that the property holds for $n = b$.

Inductive Step: Assume that the property holds for $n = m$ for any $m \geq b$. Show that it holds for $n = m + 1$.

Conclusion: You can now conclude that the property holds for every integer $n \geq b$.

Example: Proof by Induction

For every integer $n \geq 3$, $n^2 \geq 3n$.

Base Case: Take $n = 3$. Then $3^2 \geq 3 \times 3$.

Inductive Step: Assume that the statement is true for $n = m$ for $m \geq 3$ so $m^2 \geq 3m$. Now consider $n = m + 1$. We must show that $(m + 1)^2 \geq 3(m + 1)$.

$(m + 1)^2 = m^2 + 2m + 1 \geq 3m + 2m + 1$ and since $m \geq 1$, the right-hand-side is at least $3m + 3 = 3(m + 1)$.

Digression: Algebraic manipulation (Reminder from school)

$w^y \times w^z = ?$

- w^{yz}?
- w^{y+z}?
- w^{y^z}?

Example: Another proof by Induction

For every natural number n, $2^{n+2} + 3^{2n+1}$ is divisible by 7.

Base Case: Take $n = 0$. Then $2^{n+2} + 3^{2n+1} = 2^2 + 3^1 = 7$, which is divisible by 7.

Inductive Step: Assume that the property holds for $n = m$ so $2^{m+2} + 3^{2m+1}$ is divisible by 7. Now consider $n = m + 1$. We must show that $2^{(m+1)+2} + 3^{2(m+1)+1}$ is divisible by 7.

Proof continued

$$
\begin{aligned}
2^{(m+1)+2} + 3^{2(m+1)+1} &= 2^1 \times 2^{m+2} + 3^2 \times 3^{2m+1} \\
&= 2 \times 2^{m+2} + 9 \times 3^{2m+1} \\
&= 2 \times (2^{m+2} + 3^{2m+1}) + 7 \times 3^{2m+1}.
\end{aligned}
$$

Since $2^{m+2} + 3^{2m+1}$ is divisible by 7, the first term of the right-hand-side is divisible by 7. So is the second term. So the whole thing is divisible by 7.