Mathematical Induction

- Representation of integers

- Mathematical Induction

Reading (Epp's textbook)
5.1 – 5.3

Representations of Integers

Let b be a positive integer greater than 1.
Then if n is a positive integer, it can be expressed **uniquely** in the form:

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0,$$

where k is a nonnegative integer,
$a_0, a_1, \ldots, a_k$ are nonnegative integers less than b,
and $a_k \neq 0$.

Example for b=10:

$859 = 8 \cdot 10^2 + 5 \cdot 10^1 + 9 \cdot 10^0$

Representations of Integers

Example for b=2 (binary expansion):

$(10110)_2 = 1\cdot2^4 + 1\cdot2^2 + 1\cdot2^1 = (22)_{10}$

Example for b=16 (hexadecimal expansion):

(we use letters A to F to indicate numbers 10 to 15)

$(3A0F)_{16} = 3\cdot16^3 + 10\cdot16^2 + 15\cdot16^0 = (14863)_{10}$

$(B0C)_{16} = 11\cdot16^2 + 12\cdot16^0 = (2828)_{10} =$
$(101100001100)_2 = 1\cdot2^{11} + 1\cdot2^9 + 1\cdot2^8 + 1\cdot2^3 + 1\cdot2^2$

Base b expansion

How can we construct the base b expansion of an integer n?

First, divide n by b to obtain a quotient q_0 and remainder a_0, that is,

$$n = bq_0 + a_0, \text{ where } 0 \le a_0 < b.$$

The remainder a_0 is the rightmost digit in the base b expansion of n.
Next, divide q_0 by b to obtain:

$$q_0 = bq_1 + a_1, \text{ where } 0 \le a_1 < b.$$

a_1 is the second digit from the right in the base b expansion of n.
Continue this process until you obtain a quotient equal to zero.

Example

What is the base 8 expansion of $(12345)_{10}$?

First, divide 12345 by 8:

- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$

The result is: $(12345)_{10} = (30071)_8$.

Base b expansion Algorithm

n: positive integer

b: positive integer, greater than 1

procedure base_b_expansion(n, b)

q := n

k := 0

while (k = 0 or q $\neq$ 0)

    a_k := q mod b

    q := $\lfloor q/b \rfloor$

    k := k + 1

end while

{the base b expansion of n is $(a_{k-1} \dots a_1 a_0)_b$ }

Proof Methods (seen so far)

Many different strategies for proving theorems:

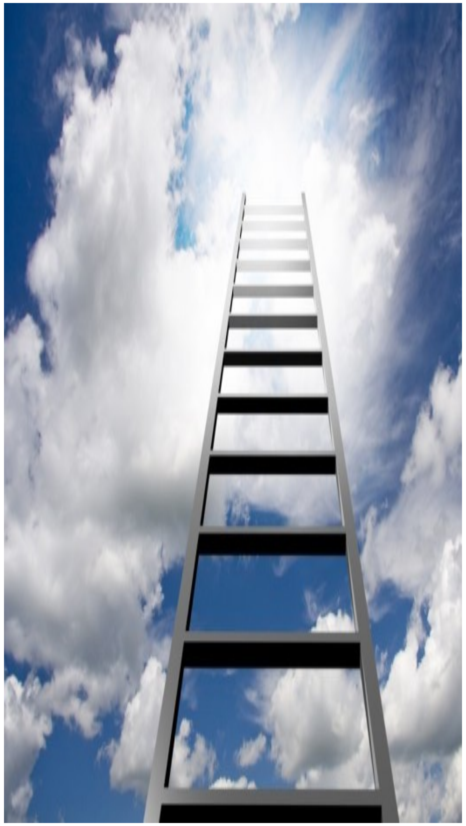
- **Direct proof:** p → q proved by directly showing that if p is true, then q must follow.
- **Proof by contraposition:** Prove p → q by proving ¬q → ¬p
- **Proof by contradiction:** Prove that the negation of the theorem yields a contradiction.
- **Proof by cases:** Exhaustively enumerate different possibilities, and prove the theorem for each case In many proofs, one needs to combine several different strategies!

Invalid Proof Methods

- Proof by obviousness: "The proof is so clear, it need not be mentioned!"
- Proof by intimidation: "Don't be stupid – of course it's true!"
- Proof by confusion: $\forall \alpha \in \theta \, \exists \, \beta \in \alpha \rightarrow \beta \approx \gamma$
- Proof by intuition: "I have this gut feeling.."
- Proof by resource limits: "Due to lack of space, we omit this part of the proof..."

Don't ever use anything like these!!

Induction



- Suppose we have an infinite ladder, and we know two things:
  I. We can reach the first rung of the ladder.
  II. If we reach a particular rung, then we can also reach the next rung.
- From these two facts, can we conclude that we can reach every step of the infinite ladder?
- Answer is yes, and mathematical induction allows us to make arguments like this.

Induction

- The **principle of mathematical induction** is a useful tool for proving that a certain property is true for **all integers $n \geq a$**.
- It cannot be used to discover theorems, but only to prove them.

- If we have a propositional function $P(n)$, and we want to prove that $P(n)$ is true for any integer $n \geq a$, we do the following:
  1. Show that $P(a)$ is true. (basis step)
  2. Show that if $P(k)$ then $P(k + 1)$ for any $k \geq a$. (inductive step)
  3. Then $P(n)$ must be true for any $n \geq a$. (conclusion)

Mathematical Induction

- Used to prove statements of the form $\forall x \in Z^+, P(x)$.

- An inductive proof has two steps:

  1. **Base case:** Prove that P(1) is true.

  2. **Inductive step:** Prove $\forall$n $\in Z^+$, P(k) → P(k + 1).

- Induction says if you can prove (1) and (2), you can **conclude**:

  $\boldsymbol{\forall x \in Z^+, P(x).}$

Inductive Hypothesis

- In the **inductive step**, need to show:

  $$\forall k \in Z^+, P(k) \rightarrow P(k + 1)$$

- To prove this, we assume P(k) holds, and based on this assumption, prove P(k + 1).

- The assumption that P(n) holds is called the **inductive hypothesis.**

Example 1 (Proving an Inequality)

Show that $n < 2^n$ for all positive integers n.

Let P(n) be the propositional function "$n < 2^n$."

Prove that $\forall n \in Z^+, P(n)$

1. Base case: Show that P(1) is true.

$$1 < 2^1 \text{ (True)}$$

2. Inductive step: Show that if P(k) is true, then P(k + 1) is true.

Assume that $k < 2^k$ is true **(Inductive Hypothesis).**

We need to show that P(k + 1) is true, i.e.

Show: $k + 1 < 2^{k+1}$

We start from $k < 2^k$:

$$k + 1 < 2^k + 1 < 2^k + 2^1 \leq 2^k + 2^k = 2^{k+1}$$

Therefore, if $k < 2^k$ then $k + 1 < 2^{k+1}$

Example 1 (Cont.)

3. (Conclusion) Then P(n) must be true for any positive integer.
   - ✓ $n < 2^n$ is true for any positive integer.
   - ✓ End of proof.

Example 2

Prove the following statement by induction: $\forall n \in Z^{+}, \quad 1+2+3+\cdots+n = {}^{n\times(n+1)}/_{2}$.

- Let P(n) be the propositional function "$1+2+3+\cdots+n = {}^{n\times(n+1)}/_{2}$"
- Prove that $\forall\, n \in Z^{+}, P(n)$

1. **Base case:** n = 1. In this case, $\frac{1\times(1+1)}{2} = 1$; thus, the base case holds.
2. **Inductive step:** By the inductive hypothesis, we assume P(k):

$$1+2+3+\cdots+k = {}^{k\times(k+1)}/_{2}$$

Now, we want to show P(k + 1):

$$1+2+3+\cdots+(k+1) = {}^{(k+1)\times(k+2)}/_{2}$$

Example 2 (Cont.)

The left-hand side of *P(k+1)* is

$$1 + 2 + 3 + \cdots + (k+1)$$

$$= 1 + 2 + 3 + \cdots + k + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1)$$

$$= \frac{k(k+1)}{2} + \frac{2(k+1)}{2}$$

$$= \frac{k^2 + k}{2} + \frac{2k+2}{2}$$

$$= \frac{k^2 + 3k + 1}{2}$$

Example 2 (Cont.)

And the right-hand side of *P(k+1)* is

$$\frac{(k+1)\times(k+2)}{2} = \frac{k^2+3k+1}{2}$$

Thus the two sides of *P(k* + 1*)* are equal to the same quantity and so they are equal to each other.

3. (Conclusion) Then P(n) must be true for any positive integer.

- ✓ $1+2+3+\cdots+n = {}^{n\times(n+1)}/_{2}$ is true for any positive integer.
- ✓ End of proof.

Example 3 (Geometric Series)

Prove the following statement by induction:
$\forall n \in Z^{nonneg}$ *and any real number r except than* 1,

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

- Let P(n) be the propositional function "$r^0 + r^1 + r^2 + \cdots + r^n = \frac{r^{(n+1)} - 1}{r-1}$"
- Prove that $\forall\, n \in Z^{nonneg}, P(n)$

1. **Base case:** n = 0. In this case, $\frac{r^{(0+1)} - 1}{r-1} = \frac{r-1}{r-1} = 1$; thus, the base case holds.
2. **Inductive step:** By the inductive hypothesis, we assume P(k):

   $$r^0 + r^1 + r^2 + \cdots + r^k = \frac{r^{(k+1)} - 1}{r-1}$$

   Now, we want to show P(k + 1):

   $$r^0 + r^1 + r^2 + \cdots + r^{k+1} = \frac{r^{(k+2)} - 1}{r-1}$$

Example 3 (Cont.)

The left-hand side of *P(k+1)* is

$$r^0 + r^1 + r^2 + \cdots + r^{k+1}$$

$$= r^0 + r^1 + r^2 + \cdots + r^k + r^{k+1}$$

$$= \frac{r^{(k+1)} - 1}{r - 1} + r^{k+1}$$

$$= \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r - 1)}{r - 1}$$

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

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

Example 3 (Cont.)

Thus the two sides of P(k + 1) are equal.

3. **(Conclusion)** Then P(n) must be true for any non-negative integer.
   - ✓ $r^0 + r^1 + r^2 + \cdots + r^n = \frac{r^{(n+1)}-1}{r-1}$ is true for any non-negative integer.
   - ✓ End of proof.

Example 4 (Divisibility Property)

Prove the following statement by induction: $\forall n \in Z^{+}$, $2^{2n} - 1$ is divisible by 3.

- Let P(n) be the propositional function "$2^{2n} - 1$ is divisible by 3"
- Prove that $\forall\, n \in Z^{+}, P(n)$

1. **Base case:** n = 1. In this case, $2^{2\times 1} - 1$= 3 is divisible by 3; thus, the base case holds.
2. **Inductive step:** By the inductive hypothesis, we assume P(k):

$$2^{2k} - 1 = 3r \text{ for some integer } r$$

Now, we want to show P(k + 1):

$$2^{2(k+1)} - 1 = 3s \text{ for some integer } s$$

Example 4 (Cont.)

The left-hand side of *P(k+1)* is

$$2^{2(k+1)} - 1$$

$$= 2^{2k+2} - 1$$

$$= 2^{2k}2^{2} - 1$$

$$= 2^{2k}4 - 1$$

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

$$= 2^{2k} \times 3 + 2^{2k} - 1$$

$$= 3 \times 2^{2k} + 3r$$

$$= 3 \times (2^{2k} + r) = 3s$$

But $s = 2^{2k} + r$ is an integer because it is a sum of products of integers.

Example 4 (Cont.)

Thus the two sides of P(k + 1) are equal for some integer s.

3. **(Conclusion)** Then P(n) must be true for any positive integer.
   - ✓ "$2^{2n} - 1$ is divisible by 3" is true for any positive integer n.
   - ✓ End of proof.

More Examples to practice

- Prove that 2^n < n! for all integers n ≥ 4.
- Prove that 3 | (n^3 – n) for all positive integers n.
- Prove that $7^n - 2^n$ is divisible by 5 for all positive integers n.