CSE 311 Foundations of Computing I

Lecture 13

Mathematical Induction

Spring 2013

Announcements

- Reading assignment
  - 5.1-5.2 7th Edition
  - 4.1-4.2 6th Edition
  - Today's lecture: 5.1 (7th), 4.1 (6th)

Highlights from last lecture

- Greatest common divisor (gcd)
  - Definition and computation via prime factorization
  - Euclid's algorithm 78 = *2* • 33 + 12
    33 = *2* • 12 + 9
    12 = *1* • 9 + 3
    9 = *3* • 3 so gcd(78,33)=3
  - Bézoit: ∃ s,t such that gcd(a,m)=sa+tm
    - E.g. 3=1•12 - 1•9 =1•12 - 1•(33 - 2•12)
      = -1•33 +3•12 = -1•33 + 3•(78 - 2•33)
      = 3•78 - 7•33

Highlights from last lecture

- Solving Modular Equations
  - Solving ax ≡ b (mod m) for unknown x when gcd(a,m)=1.

1. Find s such that sa+tm=1
2. Compute a^{-1}= s mod m, the *multiplicative inverse* of a modulo m
3. Set x = (a^{-1} • b) mod m

Solve 7x mod 26 = 1

Hint: $3 \cdot 26 - 11 \cdot 7 = 1$

Mathematical Induction

- Method for proving statements about all integers $n \geq 0$
  - Part of sound logical inference that applies only in the domain of integers
    - Not like scientific induction which is more like a guess from examples
  - Particularly useful for reasoning about programs since the statement might be "after n times through this loop, property P(n) holds"

Finding a Pattern

- $2^0 - 1 = 1 - 1 = 0 = 3 \bullet 0$
- $2^2 - 1 = 4 - 1 = 3 = 3 \bullet 1$
- $2^4 - 1 = 16 - 1 = 15 = 3 \bullet 5$
- $2^6 - 1 = 64 - 1 = 63 = 3 \bullet 21$
- $2^8 - 1 = 256 - 1 = 255 = 3 \bullet 85$
- …

How do you prove it?

- Want to prove $3 \mid 2^{2n} - 1$ for all integers $n \geq 0$
  - n=0
  - n=1
  - n=2
  - n=3
  - …

Induction as a rule of Inference

Domain: integers ≥ 0:

$$\begin{array}{l} \quad P(0) \\ \quad \underline{\forall k\, (P(k) \to P(k+1))} \\ \therefore \forall n\, P(n) \end{array}$$

How would we use the induction rule in a formal proof?

$$\begin{array}{l} \quad P(0) \\ \quad \underline{\forall k\, (P(k) \to P(k+1))} \\ \therefore \forall n\, P(n) \end{array}$$

1. Prove P(0)
2. Let k be an arbitrary integer ≥ 0
   3. Assume that P(k) is true
   4. ...
   5. Prove P(k+1) is true
6. $P(k) \to P(k+1)$ — Direct Proof Rule
7. $\forall k\, (P(k) \to P(k+1))$ — Intro $\forall$ from 2-6
8. $\forall n\, P(n)$ — Induction Rule 1&7

How would we use the induction rule in a formal proof?

$$\begin{array}{l} \quad P(0) \\ \quad \underline{\forall k\, (P(k) \to P(k+1))} \\ \therefore \forall n\, P(n) \end{array}$$

1. Prove P(0) — **Base Case**
2. Let k be an arbitrary integer ≥ 0
   3. Assume that P(k) is true — **Inductive Hypothesis**
   4. ...
   5. Prove P(k+1) is true — **Inductive Step**
6. $P(k) \to P(k+1)$ — Direct Proof Rule
7. $\forall k\, (P(k) \to P(k+1))$ — Intro $\forall$ from 2-6
8. $\forall n\, P(n)$ — Induction Rule 1&7

Conclusion

5 Steps to Inductive Proofs in English

Proof:

1. "By induction we will show that P(n) is true for every n≥0"
2. "Base Case:" Prove P(0)
3. "Inductive Hypothesis: Assume that P(k) is true for some arbitrary integer k ≥ 0"
4. "Inductive Step:" Want to prove that P(k+1) is true:
   Use the goal to figure out what you need.
   Make sure you are using I.H. and point out where you are using it. (Don't assume P(k+1)!)
5. "Conclusion: Result follows by induction"

Induction Example

- Want to prove $3 \mid 2^{2n} - 1$ for all $n \geq 0$

$1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$ for all $n \geq 0$

$1+2+\ldots+n = \sum_{i=1}^{n} i = n(n+1)/2$ for all $n \geq 1$

Harmonic Numbers

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}$$

Prove $H_{2^n} \geq 1 + \frac{n}{2}$ for all $n \geq 1$

Cute Application: Checkerboard Tiling with Trinominos

Prove that a $2^n \times 2^n$ checkerboard with one square removed can be tiled with: