CSE 311 Foundations of Computing I

Lecture 15

Induction

Autumn 2012

Announcements

- Reading assignments
  - Today:
    - 5.2, 5.3 7th Edition
    - 4.2, 4.3 6th Edition
    - 3.3, 3.4 5th Edition
  - Monday: 5.3 (7th), 4.3 (6th), 3.4 (5th)
- Midterm next Friday, Nov 2
  - Closed book, closed notes
  - Practice midterm questions available on the Web
  - Extra office hours Thursday (midterm review)
    - 3:30 pm, Dan Suciu, Gowen 201
    - 4:30 pm, Richard Anderson, Gowen 201

Highlights from last lecture

- Shift cipher
  - $F(x) = (x + c) \bmod 26$; $F^{-1}(x) = (x - c) \bmod 26$
- Multiplicative cipher
  - Suppose $ab \equiv 1 \pmod{26}$ (i.e, ab mod 26 = 1)
  - $F(x) = ax \bmod 26$; $F^{-1}(x) = bx \bmod 26$
- Composite cipher
  - $F(x) = (ax + c) \bmod 26$; $F^{-1}(x) = (bx - bc) \bmod 26$
- Examples
  - $F(x) = (x + 5) \bmod 26$; $F^{-1}(x) = (x - 5) \bmod 26$
  - $G(x) = 7x \bmod 26$; $G^{-1}(x) = 15x \bmod 26$
  - $H(x) = (7x + 5) \bmod 26$; $H^{-1}(x) = (15x + 3) \bmod 26$

Induction Example

- Prove $3 \mid 2^{2n} - 1$ for all $n \geq 0$
  - n=0
  - n=1
  - n=2
  - n=3
  - ...

Induction as a rule of Inference

Domain: integers ≥ 0

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

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

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

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. $P(k) \rightarrow P(k+1)$ — Direct Proof Rule
7. $\forall k\, (P(k) \rightarrow P(k+1))$ — Intro ∀ from 2-6
8. $\forall n\, P(n)$ — Induction Rule 1&7

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

$P(0)$
$\forall k\,(P(k) \to P(k+1))$
$\therefore \forall n\, P(n)$

1. Prove P(0) — **Base Case**
2. Let k be an arbitrary integer ≥ 0 — **Inductive Hypothesis**
3. Assume that P(k) is true
4. ... — **Inductive Step**
5. Prove P(k+1) is true
6. P(k) → P(k+1) — Direct Proof Rule
7. ∀ k (P(k) → P(k+1)) — Intro ∀ from 2-6
8. ∀ 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

- 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 $n \geq 1$

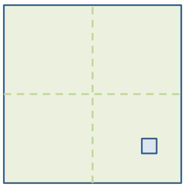
Harmonic Numbers

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

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: 



Strong Induction

$P(0)$
$\forall\, k\, ((P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)) \rightarrow P(k+1))$
$\therefore\ \forall\, n\, P(n)$

Follows from ordinary induction applied to
$Q(n) = P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(n)$

Strong Induction English Proofs

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 for some arbitrary integer k ≥ 0, P(j) is true for every j from 0 to k
4. Inductive Step: Prove that P(k+1) is true using Inductive Hypothesis that P(j) is true for all values ≤ k
5. Conclusion: Result follows by induction

Every integer ≥ 2 is the product of primes