Mathematical Proofs

Mathematical Proofs

- An argument that something is true
  - If X, then Y
- Types of proofs
  - Direct/Constructive proofs
  - Proof by contradiction
  - Proof by induction
    - Mathematical induction
    - Structural induction

Direct Proofs

- If X, then Y
- Assume X is true, show directly that Y is true.

Direct Proofs

- Example:
  - For integers *a,b*: If *a* and *b* are odd, then ab is odd.
  - Given: a and b are odd integers
    - There exists integer x such that a= 2x +1
    - There exists integer y such that b = 2y + 1
  - Must prove: a times b is also odd
    - There exists integer z such that ab = 2z + 1

Direct Proofs

- Perform the multiplication directly
  - ab = (2x + 1)(2y + 1)
    = 4xy + 2x + 2y + 1
    = 2(2xy + x + y) + 1

  So z = 2xy + x + y

Not only did you prove that a z exists, you constructed an "algorithm" for generating this z.

This is an example of a <u>constructive</u> proof.

Proof by contradiction

- If X, then Y
- With proof by contraction
  - You assume that Y is false
  - Then derive a contradiction to a fact known to be true
  - If we find a contradiction, then we know our initial assumption (I.e. Y is false) must be invalid and thus Y must be true.

Proof by contradiction

- Example
  - A, B, and C are sets. If $A \cap B = \varnothing$ and $C \subseteq B$, then $A \cap C = \varnothing$
  - Given:
    - A and B have nothing in common
    - C is a subset of B
  - Must show:
    - A and C have nothing in common

Proof by contradiction

- If X, then Y -- Assume Y is false
  1. Assume that $A \cap C \neq \varnothing$
     - Meaning, there is an element x which is in both A and C
  2. Since C is a subset of B then x, being a member of C must a member of B as well.
  3. However, by #1, $x \in A$.
  4. $x \in A$ and $x \in B$ implies that $A \cap B \neq \varnothing$
  5. This contradicts X
  6. The assumption in #1 must be invalid and as such $A \cap C = \varnothing$

Proof by Induction

- Used to prove statements involving an integer that we wish to prove true for all integers greater than a given integer
  - Example:

$$\sum_{i=1}^{n} i = 1+2+3+4+\cdots+n = \frac{n(n+1)}{2}$$

For all $n \geq 0$

Proof by Induction

- Notice there are two elements to the problem to be proven:
  - Statement involving an integer, P(n)
  - A specific integer n_0 for which we are trying to show that P(n) is true for all values greater than or equal to.

Proof by induction

- How :
  - Let P(n) is some statement involving an integer, n. To prove that P(n) is true for every integer $\geq$ a given integer n_0, it is sufficient to show these two things:
    1. $P(n_0)$ is true
    2. For any $k \geq n_0$, if P(k) is true, then P(k+1) is true.

Proof by induction

- Steps to an inductive proof:
  1. Basis step:
     Show P(n) is true when $n=n_0$
  2. Induction hypothesis
     Assume that P(n) is true for some $k \geq n_0$
  3. Inductive step
     Prove P(n) is true for n = k+1 using the induction hypothesis.

Proof by induction

- Example:
  - Show that for n ≥ 0
    $$\sum_{i=1}^{n} i = 1+2+3+4+\cdots+n = \frac{n(n+1)}{2}$$
  1. Basis step: Show true for n = 0

$$\sum_{i=1}^{0} i = 0 \qquad \frac{0(0+1)}{2} = 0$$

Proof by Induction

2. Inductive Hypothesis: Assume true for n=k

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

3. Inductive Step: Show true for n=k +1

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

Proof by induction

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

By the induction hypothesis

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2} \qquad \text{so…}$$

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

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

Proof by Induction

- An inductive proof on languages
  - Recall the recursive definition of the rev function:
    1. $\Lambda^r = \Lambda$
    2. For any $x \in \Sigma^*$ and $a \in \Sigma$, $(xa)^r = ax^r$

  Recall the recursive definition of |x|
    1. $|\Lambda| = 0$
    2. For any $x \in \Sigma^*$ and $a \in \Sigma$, $|xa| = |x| + 1$

Proof by induction

- Show that $|x^r| = |x|$
- We can prove by induction based on the length of x.
- Restate the problem as
  - For all n ≥ 0, where n = |x|, $|x^r| = |x|$

Proof by induction

1. Basis step: Show true for n = 0

   When |x| = 0, then x = Λ.

   By definition $\Lambda^r = \Lambda$ and $|\Lambda| = 0$

2. Inductive Hypothesis: Assume true for n=k

   For all strings x where |x| = k, $|x^r| = |x|$

Proof by induction

3. Inductive Step: Show true for n=k +1

Must show that $|x^r| = |x|$ for all strings x with length of k+1

- Let x = ya where $a \in \Sigma$ and $y \in \Sigma^*$ and $|y| = k$
- By definition $x^r = (ya)^r = ay^r$ Since $|y| = k$. by the inductive hypothesis $|y^r| = |y| = k$
- By definition of length $|x^r| = |ay| = |y| + 1 = k+1$

Strong Principal of Induction

- Stronger than the basic induction :
  - Let P(n) is some statement involving an integer, n. To prove that P(n) is true for every integer ≥ a given integer n_0, it is sufficient to show these two things:
    1. $P(n_0)$ is true
    2. For any $k \geq n_0$, if P(n) is true for all n such that $k \geq n \geq n_0$, then P(k+1) is true

Strong Principal of Induction

- Example:
  - Recall this recursive definition of a language L
    1. $\Lambda \in L$
    2. For any $x \in L$, both $0x$ and $0x1 \in L$
    3. No strings are in L unless it can be obtained using rules 1-2.

  We now show that:

  $L = \{x \in \{0,1\}^* \mid x = 0^i1^j \text{ and } i \geq j \geq 0\}$

Strong Principal of Induction

- Let $A = \{x \in \{0,1\}^* \mid x = 0^i1^j \text{ and } i \geq j \geq 0\}$
- We wish to prove that L = A
- Two things need to be proven
  - $L \subseteq A$
    - i.e. All strings obtainable by the recursive definition of L are of the form 0^i1^j where $i \geq j \geq 0$
  - $A \subseteq L$
    - i.e All strings of the form 0^i1^j where $i \geq j \geq 0$ can be obtained by applying the recursive definition of L.
- Can prove each by induction on the length of a string…I will go over the first ($L \subseteq A$)

Strong Principal of Induction

- $L \subseteq A$
  - Must show that for $n \geq 0$, for x such that $|x| = n$, if $x \in L$ then $x \in A$.
    - Basis step : $|x| = 0$.
      - If $|x| = 0$ then $x = \Lambda$. By definition of L, $\Lambda \in L$
      - Does Λ fit the definition 0^i1^j where $i \geq j \geq 0$?
      - Yes, it's the case where i = j = 0

Strong Principal of Induction

- $L \subseteq A$
  - Strong inductive hypothesis
    - For all x such that $k \geq |x| \geq 0$, $x= 0^i1^j$ where $i \geq j \geq 0$
  - Induction step
    - Show true for x such that $|x| = k+1$
    - L Rule 2: For any $x \in L$, both $0x$ and $0x1 \in L$
    - Thus $x=0y$ where $|y| = k$ or $x =0z1$ where $|z| = k-1$. Both cases are handled by the induction hypothesis.

Strong Principal of Induction

- Induction step
  - Show true for x such that $|x| = k+1$
  - Case 1 $x = 0y$.
    - Since $|y| = k$, by the induction hypothesis, $y=0^i1^j$ where $i \geq j \geq 0$
    - Adding a 0 to the left only makes i larger, maintaining the relationship between the number of 0s and 1s
  - Case 2 $x = 0z1$
    - Since $|z| = k-1$, by the induction hypothesis $z=0^i1^j$ where $i \geq j \geq 0$
    - Adding a 0 to the left and a 1 to the right of z will continue to maintain the relationship between 0's and 1's.

Structural Induction

- When dealing with languages, it is sometime cumbersome to restate the problems in terms of an integer.
- For languages described using a recursive definition, another type of induction, structural induction, is useful.

Structural Induction

- Principles
  - Suppose
    - U is a set,
    - I is a subset of U,
    - Op is a set of operations on U.
    - L is a subset of U defined recursively as follows:
      - $I \subseteq L$
      - L is closed under each operation in Op
      - L is the smallest set satisfying 1 & 2

Structural Induction

- Then
  - To prove that every element of L has some property P, it is sufficient to show:
    1. Every element of I has property P
    2. The set of elements of L having property P is closed under Op

    #2: If $x \in L$ has property P, Op(x) also must have property P

Structural Induction

- Recall this recursive definition of a language L
  1. $\Lambda \in L$
  2. For any $x \in L$, both $0x$ and $0x1 \in L$
  3. No strings are in L unless it can be obtained using rules 1-2.

And:

$A = \{x \in \{0,1\}^* \mid x = 0^i1^j \text{ and } i \geq j \geq 0\}$

Show $L \subseteq A$ by structural induction

Structural Induction

- Principles
  - Suppose
    - U is a set $\quad U = \{a,b\}^*$
    - I is a subset of U, $\quad I = \{\Lambda\}$
    - Op is a set of ops on U. $\quad Op = \{0x, 0x1\}$
    - L is a subset of U defined recursively as follows:
      - $I \subseteq L$
      - L is closed under each operation in Op
      - L is the smallest set satisfying 1 & 2.

Structural Induction

- To prove that every element of L has some property P:
  - Our property is:

    $A = \{x \in \{0,1\}^* \mid x = 0^i1^j \text{ and } i \geq j \geq 0\}$

    P(x) is true if $x \in A$.

Structural Induction

- To prove that every element of L has some property P, it is sufficient to show:

  1.Every element of I has property P

  In our case, must show that Λ has property P, I.e. $\Lambda \in A$, $\Lambda = 0^i1^j$, $i \geq j \geq 0$

  Once again, this is the case where i=j=0

Structural Induction

2. The set of elements of L having property P is closed under Op

   If $x \in L$ has property P, Op(x) also must have property P

Assume x has property P,

$x \in A$, $x = 0^i1^j$, $i \geq j \geq 0$

Op1(x) = 0x, which is an element of A

Op2(x) = 0x1 which is an element of A

Similar proof to induction with no mention of an integer

Summary

- Proof
  - Direct / constructive
  - Proof by contradiction
  - Proof by induction
  - Proof by strong induction
  - Proof by structural induction
- Any questions?

Reminder

- Homework #1 is due next Tuesday.
- Next class:
  - The real fun begins!
  - Regular Languages