CS 3313: Foundations of Computing

Lab 1: Proof Techniques

http://gw-cs3313.github.io

Outline

- Math preliminaries – this should all be review
- Proof techniques
- Exercises

Sets and set operations

- Set: Collection of non-repeating items $S = \{1, a, \{c, d\}\}, |S| = 3$

Sets and set operations

- Set: Collection of non-repeating items $S = \{1, a, \{c, d\}\}, |S| = 3$
- Common sets:

  $\mathbb{Z}$ - set of integers

  $\mathbb{Z}^+$ - set of positive integers

  $\mathbb{N}$ - natural numbers

  $\mathbb{R}$ - Reals

  $\emptyset\ or\ \{\}$ – empty set

Sets and set operations

- Set: Collection of non-repeating items $S = \{1, a, \{c, d\}\}, |S| = 3$
- Common sets:

  $\mathbb{Z}$ - set of integers

  $\mathbb{Z}^+$ - set of positive integers

  $\mathbb{N}$ - natural numbers

  $\mathbb{R}$ - Reals

  $\emptyset\ or\ \{\}$ – empty set
- Set relations:
  - Membership: $5 \in \mathbb{Z}$, $3.1 \notin \mathbb{Z}$, $\{c, d\} \in \{1, a, \{c, d\}\}$
  - Subset: $\{1,2\} \subset \{1,2,3\}$
  - Union: $A \cup B$ Intersection: $A \cap B$ Complement: $\overline{A}$
  - De Morgan's Laws: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$
  - Cartesian product: If $A = \{1,2,3\}, B = \{a, b\}$

    $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$

Strings

- *<u>Alphabet</u>* Σ : set of symbols
  - Ex: $\Sigma = \{a, b\}, \Sigma = \{0,1\}$
- *<u>String</u>*: finite sequence of symbols from Σ,
  - ex: $v = aba$ and $w = abaaa$
  - ex: $v = 001$ and $w = 11001$
  - Empty string (λ)
  - Substring, prefix, suffix

Strings

- *Alphabet* Σ : set of symbols
  - Ex: $\Sigma = \{a, b\}$, $\Sigma = \{0,1\}$
- *String*: finite sequence of symbols from Σ,
  - ex: $v = aba$ and $w = abaaa$
  - ex: $v = 001$ and $w = 11001$
  - Empty string (λ)
  - Substring, prefix, suffix
- *Operations on strings*:
  - *Concatenation*: $vw = abaabaaa$
  - *Reverse*: $w^R = aaaba$
  - *Repetition*: $v^2 = abaaba$ *and* $v^0 = \lambda$
- *Length of a string:* $|v| = 3$ and $|\lambda| = 0$

Languages

- Language L: Set of strings

- Σ^* = set of all strings formed by concatenating zero or more symbols in Σ
  - Ex: if $\Sigma = \{0,1\}$ *then* $\Sigma^* = \{$*all binary strings, including empty string*$\}$
- **A *language* is any subset of Σ***

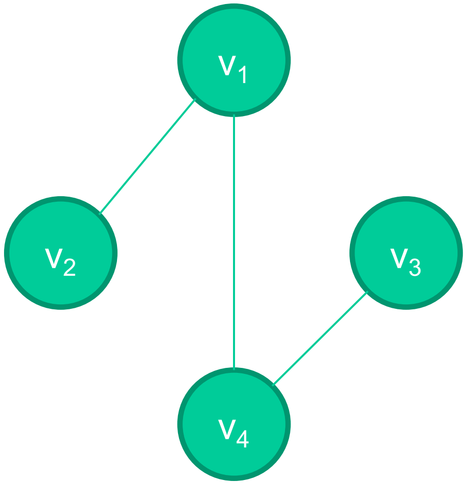
Examples: $L_1 = \{ a^n b^n : n \geq 0 \}$ and $L_2 = \{ ab, aa \}$

- A string in a language is also called a *sentence* of the language

Graphs

- A graph G consists of a
  - vertex set $V(G) = \{v_1, v_2, \ldots\}$ and
  - edge set $E(G) \subset \{(x, y) | x, y \in V(G)\}$
    i.e., an edge connects a pair of vertices
- Directed vs. undirected graphs
- Degree of a vertex – number of edges coming out of the vertex
  e.g. $\deg(v_1) = 2$

Graph G



Outline

- Math preliminaries – this should all be review
- Proof techniques
- Exercises

Proofs

This class will involve a lot of proofs.

General proof procedure:

1. Understand the statement – without the math lingo
2. Build up an intuition – in English or by picture, work through examples
   - This gets easier with practice
3. Construct proof
   - This part is procedural
   - Use facts and theorems you already know
   - Proof techniques will guide you

Writing proofs

- Be concise – no multi-paragraph explanations
- Be precise – use mathematic notation and logical reasoning
- Follow proof techniques – this will give you a structure for the proof

Proof techniques

- Direct proof
- Proof by contradiction
- Proof by induction

Direct Proof

- Produce a chain of logically sound deductions that justify the expected conclusion

Example

- Theorem: $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Example

- Theorem: $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- Intuition: Any element not in the union of A and B must be outside of both A and B

Example

- Theorem: $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- Intuition: Any element not in the union of A and B must be outside of both A and B
- Proof: Important, there are two directions to prove!
  1. Suppose $x \in \overline{A \cup B}$, $then\ x \in \overline{A} \cap \overline{B}$

     If $x \in \overline{A \cup B}$, $then\ x \notin A \cup B$ *(by definition of complement)*

     So, $x \notin A$ and $x \notin B$ (by definition of union)

     Thus, $x \in \overline{A}$ and $x \in \overline{B}$ (by definition of complement)

     Therefore, $x \in \overline{A} \cap \overline{B}$ *(by definition of intersection)*

Example

- Theorem: $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- Intuition: Any element not in the union of A and B must be outside of both A and B
- Proof: Important, there are two directions to prove!
  1. Suppose $x \in \overline{A \cup B}$ *, then* $x \in \overline{A} \cap \overline{B}$
     If $x \in \overline{A \cup B}$ *, then* $x \notin A \cup B$ *(by definition of complement)*
     So, $x \notin A$ and $x \notin B$ (by definition of union)
     Thus, $x \in \overline{A}$ and $x \in \overline{B}$ (by definition of complement)
     Therefore, $x \in \overline{A} \cap \overline{B}$ *(by definition of intersection)*
  2. Suppose $x \in \overline{A} \cap \overline{B}$*, then* $x \in \overline{A \cup B}$
     If $x \in \overline{A} \cap \overline{B}$, then $x \in \overline{A}$ *and* $x \in \overline{B}$ (by definition of intersection)
     So, $x \notin A$ and $x \notin B$ (by definition of complement)
     thus, $x \notin A \cup B$ (by definition of union)
     implying that $x \in \overline{A \cup B}$ (by definition of complement)

Proof by contradiction

Proof Outline:

1. Assume the opposite of what you want to try to prove
2. Show that it leads to a contradiction
3. Thus, the original assumption must be false

Example

- Theorem: For any integer n, if n^2 is odd then n is odd

Example

- Theorem: For any integer n, if n^2 is odd then n is odd
- Intuition: The product of two odd numbers has no factors of 2, so it will be odd

Example

- Theorem: For any integer n, if n^2 is odd then n is odd
- Intuition: The product of two odd numbers has no factors of 2, so it will be odd
- Proof:
    1. Assume there exists an even n s.t. n^2 is odd (very important to get the negation of the statement correct!)
       Then, $n=2m$ for some integer m (by definition of even)
       So, $n^2 = 4m^2 = 2(2m^2)$ which is even

       Contradiction!!!

Proof by induction

Proof Outline:

1. **Base case**: Verify that statement holds for base case (e.g., true for i=1)
2. **Inductive hypothesis**: Assume that if the statement holds for i=n for some value n
3. **Induction step:** Prove that the statement holds for i=n+1

<u>Why this works:</u>

P(1) is true implies P(2) is true

P(2) is true implies P(3) is true

…

P(n-1) is true implies P(n) is true

Therefore, P(n) is true

Example

- Theorem: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{(n+1)n}{2}$

Example

- Theorem: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{(n+1)n}{2}$
- Intuition: Test it for some small values of n

Example

- Theorem: $1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \frac{(n+1)n}{2}$
- Intuition: Test it for some small values of n
- Proof:

Base case: n $=$ 1 – 1=(1+1)*1/2 = 2/2 = 1

Hypothesis: Assume $\sum_{i=1}^{k} i = \frac{(k+1)k}{2}$ for some k

Induction: Show that $\sum_{i=1}^{k+1} i = \frac{\left((k+1)+1\right)(k+1)}{2}$

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

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

Outline

- Math preliminaries – this should all be review
- Proof techniques
- Exercises

Exercises

- Prove each of the following statements
- Work in groups – make sure you put down all the names
- Scan your solutions and submit on Blackboard by end of day

Exercises

1. Prove that in any graph G, the sum of degrees of the nodes of G is an even number
2. Prove that $\sqrt{2}$ is irrational
3. Prove that

$$1^2 + 2^2 + \cdots n^2 = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$