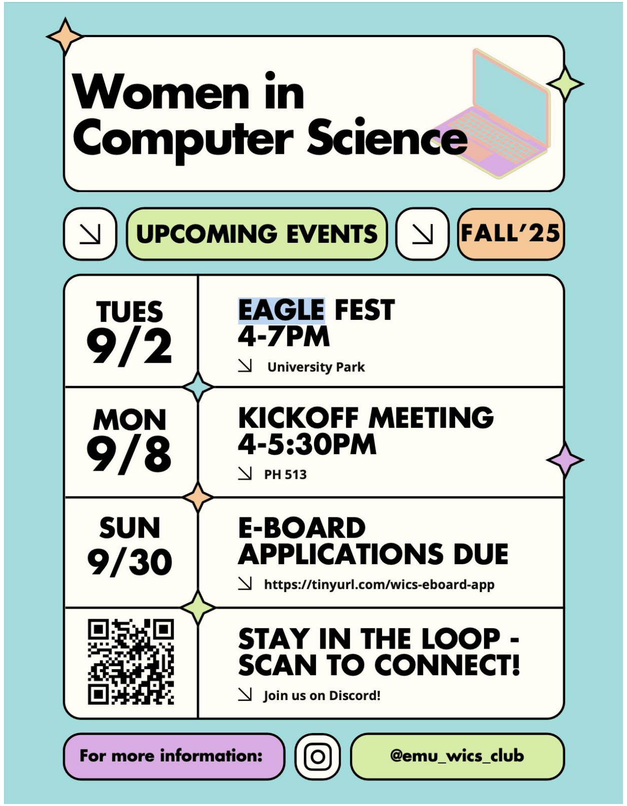
COSC 444/541: Automata

Lecture 2: Proof Techniques

Announcements



Today's Agenda

- Proofs (Chapter 1.1)
- Break at 1:50 PM
- Continue Proofs (Chapter 1.1)
- If we have time:
  - Three Basic Concepts (Chapter 1.2)
    - Languages, Grammars, Automata
- Exit Token

Proofs

Automata is a theoretical field, so results must be proven.

Proofs give us absolute guarantees

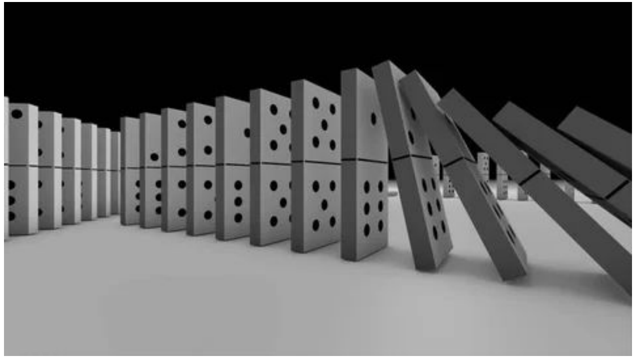
- whether a problem is solvable or not
- what machines can and cannot compute

Proof by Induction

A powerful, rigorous technique for proving that a predicate P(n) is true for every natural number n, no matter how large.

Based on a predicate-logic inference rule:

$$\frac{\begin{array}{l} P(0) \\ \forall n \geq 0\ (P(n) \rightarrow P(n+1)) \end{array}}{\therefore \forall n \geq 0\ P(n)}$$



Proof by Induction

Outline of an inductive proof:

Want to prove $\forall n\, P(n) \ldots$

Base case (or basis step): Prove P(0).

Inductive step: Prove $\forall n\, P(n) \rightarrow P(n+1)$

Let $n \in \mathbf{N}$, assume P(n). (inductive hypothesis)

Under this assumption, prove P(n+1).

Inductive inference rule then gives $\forall n\, P(n)$

Proof by Induction

Example 1: Prove that the sum of the first n odd positive integers is n^2.

That is, prove:

$$\forall n \geq 1 : \underbrace{\sum_{i=1}^{n} (2i - 1) = n^2}_{P(n)}$$

Proof by Induction

Example 1: Prove

$$\forall n \geq 1 : \underbrace{\sum_{i=1}^{n} (2i - 1) = n^2}_{P(n)}$$

Base case:

Let n=1.

The sum of the first 1 odd positive integer is 1 which equals 1^2.

Proof by Induction

Example 1: Prove $$\forall n \geq 1 : \underbrace{\sum_{i=1}^{n}(2i-1) = n^2}_{P(n)}$$

Inductive step:

Prove $\forall n \geq 1 : P(n) \rightarrow P(n+1)$

Let $n \geq 1$, assume P(n), and prove P(n+1).

$$\sum_{i=1}^{n+1}(2i-1) = \left(\sum_{i=1}^{n}(2i-1)\right) + (2(n+1)-1)$$

Proof by Induction

Example 2: [Textbook page 16, exercise 36]

Show that

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Proof by Induction

Example 3: [Textbook page 16, exercise 37]

Show that

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

Proof by Induction

In-class exercise:

[Textbook page 16, exercise 38]

Prove that for all $n \geq 4$ the inequality $2^n < n!$ holds.

Proof by Contradiction

Sometimes you want to show that something is impossible

- Square root of 2 cannot be written as a ratio of integers
- A cycle with an odd number of nodes can’t be colored with two colors

Difficult to prove non-existence directly, and can’t prove by example

Solution: show that the negation of the claim leads to a contradiction

Proof by Contradiction

Outline of proof by contradiction:

We need to show proposition p.

Suppose, instead, that p is false.

Then, we can see that both q and $\neg q$ follow, which is a contradiction.

Therefore, p must be true.

Proof by Contradiction

A set of propositions is a contradiction if their conjunction is always false.

1. $p \land \neg p$
2. $p \lor \neg p$
3. $(x > 5) \land (x > 21)$
4. $x = 20$ and x is odd
5. $(x > 5) \land (x < 21)$
6. $(x < 5) \land (x > 21)$
7. x is negative number and the square root of x is real

Proof by Contradiction

A set of propositions is a contradiction if their conjunction is always false.

❌: not contradiction

1. $p \land \neg p$
2. $p \lor \neg p$ ❌
3. $(x > 5) \land (x > 21)$ ❌
4. $x = 20$ and x is odd
5. $(x > 5) \land (x < 21)$ ❌
6. $(x < 5) \land (x > 21)$
7. x is negative number and the square root of x is real

Proof by Contradiction

Example 1:

Claim: If p is even and q is odd,then p does not divide q.

Proof by Contradiction

Example 1:

Claim: If p is even and q is odd,then p does not divide q.

Proof:

Assume that the claim is false.

Consider some $p|q$. Then $q = pk$ for some integer k.

Now p is even, so $p = 2n$, for some n. Thus $q = 2nk$.

This means q is even which means the premise ("q is odd") cannot be true thus contradicting the statement that the claim is false.

Proof by Contradiction

Example 2:

Claim: If n is an integer, then $n^2 + 2$ is not divisible by 4

Proof by Contradiction

Example 3: [textbook page 16 exercise 40]

Show that $\sqrt{8}$ is not a rational number.

Proof by Induction

In-class exercise:

[Textbook page 16, exercise 42]

Show that $\sqrt{3}$ is irrational.

Three Basic Concepts

Language

Grammar

Automata

What is a language?

Natural languages: English, French, …

Formal languages require precise definitions.

- Start with an alphabet Σ = finite, nonempty set of symbols
- Build strings that are finite sequences of symbols from Σ
- A language = any subset of Σ^*

Strings

Example: $\Sigma = \{a, b\}$

Strings: abab, aaabbba, λ (empty string)

Notion of strings: u, v, w

Operations:

- Concatenation: uv
- Reverse: w^R
- Length: $|w|$
- Empty string: λ, with $|\lambda|=0$ and $\lambda w = w\lambda = w$

Strings

Σ^* = all strings (including λ) from Σ

Languages = subsets of Σ^*

Standard set operations on languages: Union, intersection, difference, complement

Reverse: $L^R = \{w^R : w \in L\}$
Concatenation: $L_1L_2 = \{xy : x \in L_1, y \in L_2\}$

Grammar

Informal descriptions (English) are ambiguous.

Grammar is a precise way to define languages.

A grammar $G = (V, T, S, P)$:

- V = variables (nonterminals)
- T = terminals (alphabet symbols)
- $S \in V$ = start symbol
- P = productions (rewrite rules)

Automata

An automata is an abstract model of computation

Components:

- Input mechanism (reads symbols)
- Control unit
- Optional storage (stack, etc.)
- Transition function

Output:

Accepter (yes/no)
Transducer (produces output string)

Today’s Takeaways

We have seen/reviewed two proof techniques today:

Proof by Induction:

Useful for reasoning about infinite structures

Proof by Contradiction:

Helps prove impossibility results

Exit Token

- Write on a piece of paper:
  - Name
  - Answer one of the following questions:
    - How was your first week?
    - Weekend plans?