Proofs

CSC 1300 – Discrete Structures
Villanova University
Proofs in Computer Science

• Establishing correctness and efficiency of algorithms
• Verification of program correctness
• Establishing that an operating system is secure
• Establishing that certain goals cannot be achieved (e.g., creating a universal program-correctness checker or finding a more efficient algorithm)
• Making inferences in AI
• Establishing the integrity of a database
Basic Terminology

**Axiom (postulate)** – underlying assumption, does not require a proof

**Rules of inference** – used to draw conclusions from other assertions

**Proof** of a statement **A** – a sequence of statements, each of which is:
- an axiom or
- follows from one or more earlier statements
  and the last statement in the sequence is **A**

**Theorem** – a statement that has been proved

**Lemma** – a theorem used in the proof of other theorems

**Corollary** – a theorem that immediately follows from another theorem

**Conjecture** – a statement that we would like to prove
Famous Conjectures

_Fermat’s Last Theorem_ (17th century)
Equation $x^n + y^n = z^n$ has no non-zero integer solutions for $n > 2$.
– a conjecture for over 300 years → proved by Andrew Wiles (Princeton, 1994)

_Goldbach’s Conjecture_ (18th century)
Every even integer greater than 4 is the sum of two primes.
– still neither proved nor disproved

_P ≠ NP Conjecture_ (1970s)
There are problems that cannot be solved by any polynomial-time algorithm (i.e., running time grows slower than exponentially with input size), but whose guessed solutions can be verified by a such an algorithm.
– still neither proved nor disproved

_3x + 1 Conjecture_ (1950s)
If we repeatedly apply the transformation that sends an even integer $x$ to $x/2$ and an odd integer to $x \rightarrow 3x + 1$ we will eventually reach 1. (eg: 13 → 40 → 20 → 10 → 5 → 16 → 8 → 4 → 2 → 1)
– still neither proved nor disproved
Open Sentences

Declarative sentences containing \textit{variable(s)} representing objects from some set \(D\) called the \textit{domain of discourse} (or just the \textit{domain})

- Truth of open sentence depends on value(s) of variables
- Notation: \(P(x)\) or \(Q(x,y,z)\)
- Also called \textit{Propositional functions} or \textit{open propositions}

Examples

- \(P(x) = \text{“x is even” with domain the Natural numbers}\)
  \(P(2) = \quad P(3) = \)
- \(Q(x) = \text{x is enrolled in CSC 1051 and CSC 1300 this semester}\)
- \(R(x,y) = \text{x loves y}\)
- \(M(x,y) = \text{x loves y and y loves z}\)
- \(S(x) = \text{x is even or x is odd}\)
Universal quantifier

Definition: *universal quantification* of $P(x)$

“$P(x)$ is true for all values of $x$ in the domain of discourse $S$”

“for all $x \in S$, $P(x)$”

“for every $x \in S$, $P(x)$”

$\forall x \in S, P(x)$
Examples of universal quantification

\[ \forall x \in \mathbb{N}, (x + 0 = x) \]

\[ \forall x \in \mathbb{N}, (x^2 > x) \]

\[ \forall x \in D, P(x) \]
where \( D = \{ x: x \text{ is a CSC 1300 student} \} \) and

\[ P(x): “x \text{ loves CS}” \]

Let \( S = \text{set of all sentient beings} \)
\( M(x): “x \text{ is mortal}” \) and
\( H(x): “x \text{ is a human}” \)

Express the proposition: “\textit{every human is mortal}”
Existential quantifier

Definition: *existential quantification* of $P(x)$

“There exists an element $x$ in the domain of discourse $S$ such that $P(x)$ is true”

“there is an $x \in S$ such that $P(x)$”

“for some $x \in S$, $P(x)$”

$\exists x \in S, P(x)$

*existential quantifier.*
Examples of existential quantification

**True or false?**

\[ \exists x \in \mathbb{N}, \ (x + x = x \times x) \]

\[ \exists x \in \mathbb{N}, \ (x = x + 1) \]

\[ \exists x \in D, P(x) \]

where domain \( D = \{x: x \text{ is a CSC 1300 student}\} \) and \( P(x): \text{“}x \text{ loves CS”} \)

Let \( Q(x) \) denote \text{“}x \text{ is a sophomore”} with domain D. Express the sentence: \text{“}there is a sophomore who loves CS” \text{“}
Example

Let $S = \{1, 2, 3\}$ and let $R(x): \frac{(x^2 + 3x)}{2}$ is even be an open sentence over the domain $S$.

What are the truth values of $R(x)$ for each $x$ in $S$?

State $\forall x \in S, R(x)$ ... is it true?

State $\exists x \in S, R(x)$ ... is it true?
Generalized De Morgan Laws of Logic

\[ \neg \forall x \in D, \ P(x) \equiv \exists x \in D, \ \neg P(x) \]

“Not everyone loves CS” \equiv “There is someone who does not love CS”

\[ \neg \exists x \in D, \ P(x) \equiv \forall x \in D, \ \neg P(x) \]

“No one who loves CS” \equiv “Everyone does not love CS”

Better example:
\[ \neg \exists x \in D, \ \neg P(x) \equiv \]
Expressions with several quantifiers

Let the universe of discourse be the set of all students (of VU).

Let

\[ C(x) \text{ means “} x \text{ has a computer”} \]
\[ F(x,y) \text{ means “} x \text{ and } y \text{ are friends”} \]

Translate the following into English:

• \( \forall x C(x) \)

• \( \forall x [C(x) \lor \exists y (F(x,y) \land C(y))] \)

• \( \exists x \neg \exists y F(x,y) \)
Does the order of the quantifiers matter?

— No, if we have several consecutive quantifiers of the same type:
\[ \forall x \forall y Q(x, y) \equiv \forall y \forall x Q(x, y) \quad \exists x \exists y Q(x, y) \equiv \exists y \exists x Q(x, y) \]

— Yes, if we have different quantifiers:
\[ \forall x \exists y Q(x, y) \not\equiv \exists y \forall x Q(x, y) \]

Example: Let \( Q(x, y) \) mean “\( x+y=0 \)”, and let the universe of discourse be the set of all real numbers. What is the truth value of:
\[ \forall x \exists y Q(x, y) \ ? \\
\exists y \forall x Q(x, y) \ ? \]
Types of proofs

- direct
- indirect (by contrapositive)
- proof of biconditional
- by contradiction
- proof by cases
- Existence proof:
  - by example for existential sentence
  - ... or by counterexample for universal (refutation)
  - non-constructive existence proof (refutation of universal)
- proof by mathematical induction
Proving \( p \rightarrow q \)

- **Direct Proof**
  
  \( p \rightarrow q \)

- **Indirect Proof / Contrapositive**
  
  \( p \rightarrow q \equiv \neg q \rightarrow \neg p \)

- **Proof by Contradiction**
  
  \( p \rightarrow q \equiv (p \land \neg q) \rightarrow (r \land \neg r) \)
Direct Proof

To prove $p \rightarrow q$:

Suppose $p$ is true; prove that $q$ must also be true

Example:
If $n$ is even, then $5n^3$ is also even

Example:
If $n$ and $m$ are rationals, $n \cdot m$ is also a rational

Example: For $x \in \mathbb{R}$, if $(x - 2)^4 \leq 0$, then $9 - x^2 \geq 0$,
Indirect Proof

Prove \( p \rightarrow q \) by proving contrapositive: \( \neg q \rightarrow \neg p \)

Examples:

Prove for Natural numbers \( n, m \):

– If \( n - 5 \) is even, then \( n \) is odd.

– If \( n \cdot m \) is odd, then an \( n \times m \) grid cannot be tiled with dominoes.
Proofs of equivalence

A \textit{proof of equivalence} of two assertions (i.e., $p \leftrightarrow q$), often stated by using “if and only if” or “necessary and sufficient,” requires two separate parts:

$p \rightarrow q \text{ and } q \rightarrow p$.

\textbf{Example:} An integer $n$ is odd iff $n^2$ is odd.
Contradiction Proof

Prove \( s \) by showing that \( \neg s \) is absurd!

- \( \neg s \rightarrow F \) \hspace{1.5em} (Reductio ad absurdum)

Famous Example: \( \sqrt{2} \) is irrational
Proofs by cases

A *proof by cases* is based on partitioning the theorem’s domain into subdomains and proving the theorem separately for each of these subdomains.

**Definition:**

\[ \lfloor x \rfloor \text{, called the *floor of* } x, \text{ is the largest integer } \leq x; \]

\[ \lceil x \rceil \text{, called the *ceiling of* } x, \text{ is the smallest integer } \geq x. \]

**Example:** \( \forall n \in \mathbb{Z}, \lfloor n/2 \rfloor + \lceil n/2 \rceil = n \)
Proofs, examples, and counterexamples: $\forall x \, P(x)$

**For universal statements:**

- **Checking validity of a theorem for specific examples does NOT constitute a proof** (unless the examples exhaust all the values in the theorem’s domain, which is impossible if the latter is infinite).

- **Just a single example suffices to disprove a theorem.** (Such an example is usually called a counterexample).
Proofs, examples, and counterexamples $\exists x \, P(x)$

**For existential statements:**

- A single example suffices to prove the theorem (constructive proof).

- Alternatively, using contradiction, prove that it is not possible for such a thing **not** to exist. (non-constructive proof)
  - Show that a player in a game has a winning strategy without actually saying what it is!
  - Famous proof: There exist irrational $x, y$ such that $x^y$ is rational
Which Proof Method?

1. Begin with a direct proof approach
2. If this fails, try either
   – indirect / contrapositive approach
   – proof by contradiction
   – proof by cases
   – a combination...
   ..... 

• If all else fails try *mathematical induction*