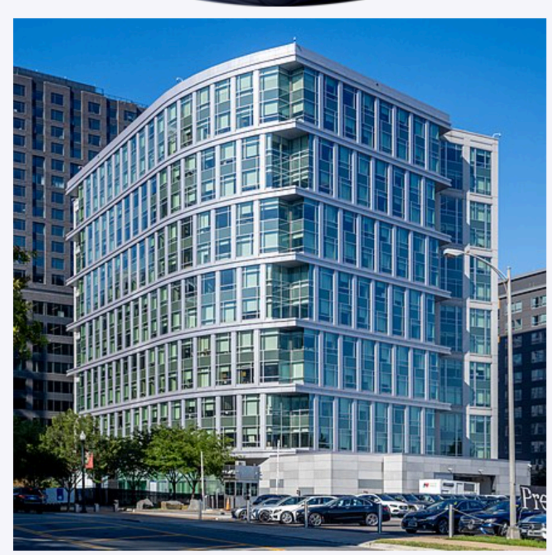
CSE215
Foundations of Computer Science

State University of New York, Korea

Why we need proof in CS?

- Reliability
- Security
- Optimization
- Limitation of Computation

Real-World Application: Proof in DARPA (US Defense Advanced Research Projects Agency)



This following part is not confidential.

Project Motivation

- C memory error contribute to 85% bugs in Microsoft
- Rust language is, by design, free of most memory bugs
- *Trust* Large Language Models to translate C into Rust
- *But verify* the translation with state-of-the-art software techniques
- Formal proof is usually considered the very best verification.
- Reddit: https://www.reddit.com/r/rust/comments/1efvfrm/darpas_translating_all_c_to_rust_tractor_program/

Proposition we aim to prove

- Let C be the original C program
- Let R be the translated Rust program
- For any input of the original C program x, C(x) = R(x)
- “=” for observational run-time behavior

Final 2021

Problem 5. [5 points]

Prove using contradiction that the cube root of an irrational number is irrational.

Definitions and facts about numbers

Symbols

- Integers Z
- Natural numbers N
- Real numbers R
- $| x |$
- sum Σ
- $a \mid b$
- b mod a

Formal definitions

- Even/Odd numbers
- Rational/Irrational numbers
- Prime/Composite numbers

Even/odd numbers

We say an integer n is even if: $\exists k \in \mathbf{Z}$ such that $n = 2k$

How can you define an odd number?

Rational/Irrational numbers

We say a real number r is rational if $\exists m, n \in \mathbf{Z}$ such that $r = n/m$

(and n and m have no common divisor).

Prime/Composite numbers

We say a natural number n is prime if $n > 1$, and

$$\forall r, s \in \mathbf{N}, n = rs \to (r = 1 \vee s = 1)$$

d | n

We say a non-zero integer d divides an integer n, if

$$\exists k \in \mathbf{Z}, \text{ such that } n = k * d.$$

Direct proof

Methods of mathematical proof

Statements	Method of proof
Proving existential statements (Disproving universal statements)	Constructive proof Non-constructive proof
Proving universal statements (Disproving existential statements)	Direct proof Proof by mathematical induction Well-ordering principle Proof by exhaustion Proof by cases Proof by contradiction

What can Direct Proof prove?

- For all x, P(x)
- For all x, P(x) -> Q(x)
- There exists x, P(x)

- **Prove: If p is an even number, then p^2 is an even number**

- Proof.

  - Assume p is an even integer. By definition of an even number, $p = 2k$ for some integer k

  - Squaring both sides of “$p=2k$”, we get $p^2 = 4k^2$

  - Thus $p^2 = 2(2k^2)$ which is twice an integer

  - Thus p^2 is even

- QED.

Even + odd = odd

Proposition

- Sum of an even integer and an odd integer is odd.

- Proof.
  - Suppose n is an even number, and m is an odd number, we need to show n+m is odd
  - since n is an even number, n = 2k for some integer k
  - since m is an odd number, m = 2k'+1 for some integer k'
  - Thus n+m = 2(k+k')+1 which shows n+m is odd.
- QED.

n is odd $\Rightarrow n^2$ is odd

Proposition

- The square of an odd integer is odd.

- Proof.
  - Suppose n is an odd number. We want to show that n^2 is an odd number.
  - Since n is odd, $n = 2k+1$ for some integer k
  - $n^2 = 4k^2+4k+1= 2(2k^2+2k) + 1$
  - Thus n^2 is odd
- QED.

If $a|b$ and $b|c$, then $a|c$

Proposition

- (Transitivity) For integers a, b, c, if $a|b$ and $b|c$, then $a|c$.

- Proof.
  - Suppose a, b, c are three integers and a|b, b|c.
  - Since a|b, we have b = ak for some integer k
  - Since b|c, we have c = bk’ for some integer k’
  - Thus, c = a (k*k’)
  - Thus a|c.
- QED.

Summary

- Proof techniques — direct proof. **Commonly used for proving “for all x, P(x) -> Q(x)”.**

- Also used in many variants

Direct proof Variation 1

- How to prove “If A, then B”
  - Suppose A, … Therefore B.

Direct proof Variation 2

- How to prove “for all real number x, P(x)”
  - Let x be a real number. …Therefore P(x).

Direct proof Variation 3

- How to prove “for all real number x, P(x) -> Q(x) ”
  - Let x be a real number. Suppose P(X). … Therefore Q(x).

Direct proof Variation 4

- How to prove “there exists x, P(x)”
  - Let x be <something you choose>. …. We have P(x) holds.

Direct Proof Exercises

Problem 4. [5 points]

Prove that the sum of the squares of any two consecutive odd integers is even.

- Proof.
  - We need to prove the following:
    - for any integer n, $(2n+1)^2 + (2n+3)^2$ is even.
  - Let n be an arbitrary integer.
  - We have $(2n+1)^2 + (2n+3)^2 = 8n^2 + 20n + 2 = 2(4n^2 + 10n+1)$ following algebraic Identities.
  - Therefore, $(2n+1)^2 + (2n+3)^2$ is even.
- QED.

Problem 5. Direct proof (points = 5)

Suppose a, b and c are integers. If $a^2|b$ and $b^3|c$, then $a^6|c$.

- Proof.
    - Let a, b, and c be three integers.
    - Suppose $a^2 \mid b$ and $b^3 \mid c$
    - By definition, we have $b = k a^2$ for some integer k, and $c = k' b^3$ for some integer k'.
    - Thus, $c = (k' k^3) a^6$
    - Therefore $a^6 \mid c$.
- QED

Prove: For any natural number n, $n^2 + 3n + 2$ is composite

For any integer x, y, if x is even, then xy is even.

Prove: there exist two irrational number r1, r2, such that r1*r2 is a rational number.

Prove: Suppose a is an integer. If $7|4a$, then $7|a$.