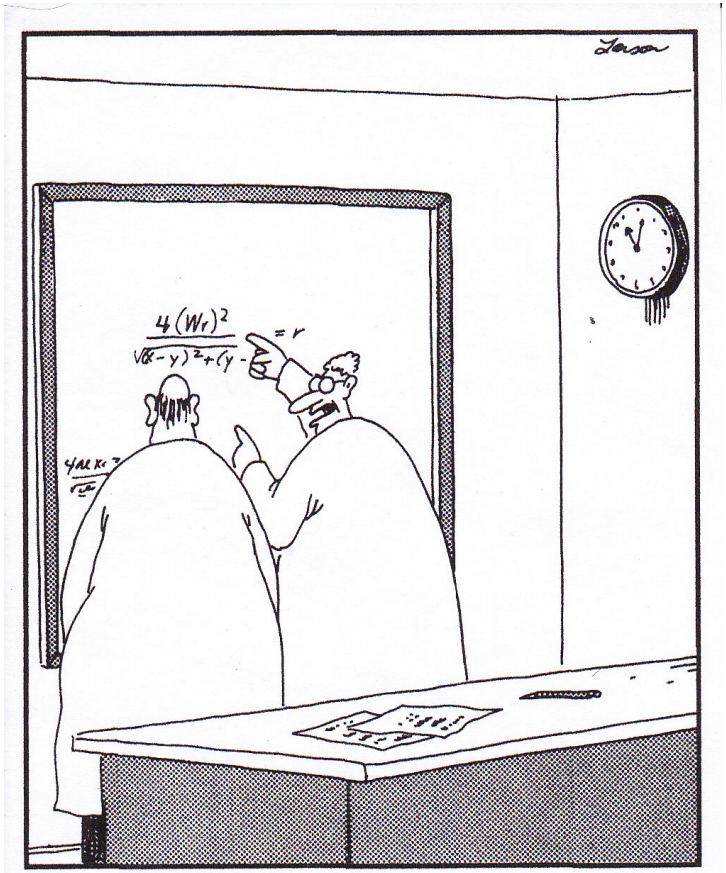
CSE 311: Foundations of Computing

Lecture 10: Proof Strategies & Number Theory



"Yes, yes, I *know* that, Sidney … *every*body knows *that!* … But look: Four wrongs *squared*, minus two wrongs to the fourth power, divided by this formula, *do* make a right."

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

Since x and y were arbitrary, the sum of any odd integers is even.

3. $(\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y})$
4. $\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(x+y))$ Intro $\forall$

Even and Odd

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

Suppose that both are odd.

3.1 $\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})$ Assumption

so x+y is even.

3.9 $\text{Even}(\mathbf{x+y})$

Since x and y were arbitrary, the sum of any odd integers is even.

3. $(\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y})$ DPR
4. $\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \wedge \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(x+y))$ Intro $\forall$

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

Suppose that both are odd.

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1

so x+y is even.

3.9 Even(**x+y**)

Since x and y were arbitrary, the sum of any odd integers is even.

3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	DPR
4.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y))	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove "The sum of two odd numbers is even."

Let x and y be arbitrary integers.

1. **Let x be an arbitrary integer**
2. **Let y be an arbitrary integer**

Suppose that both are odd.

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1

Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b.

3.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
3.5	**x** = 2**a**+1	Elim ∃: 2.4
3.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
3.7	**y** = 2**b**+1	Elim ∃: 2.5

so x+y is, by definition, even.

3.9	∃z (**x+y** = 2z)	Intro ∃: 2.4
3.10	Even(**x+y**)	Def of Even

Since x and y were arbitrary, the sum of any odd integers is even.

3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	DPR
4.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**))	Intro ∀

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove "The sum of two odd numbers is even."

Let x and y be arbitrary integers.

1. Let **x** be an arbitrary integer
2. Let **y** be an arbitrary integer

Suppose that both are odd.

3.1	Odd(**x**) ∧ Odd(**y**)	Assumption
3.2	Odd(**x**)	Elim ∧: 2.1
3.3	Odd(**y**)	Elim ∧: 2.1

Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b.

3.4	∃**z** (**x** = 2**z**+1)	Def of Odd: 2.2
3.5	**x** = 2**a**+1	Elim ∃: 2.4
3.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
3.7	**y** = 2**b**+1	Elim ∃: 2.5

Their sum is x+y = ... = 2(a+b+1)

3.8	**x+y** = 2(**a**+**b**+**1**)	Algebra

so x+y is, by definition, even.

3.9	∃z (**x+y** = 2z)	Intro ∃: 2.4
3.10	Even(**x+y**)	Def of Even

Since x and y were arbitrary, the sum of any odd integers is even.

3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**)	DPR
4.	∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**))	Intro ∀

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Proof: Let x and y be arbitrary integers.

Suppose that both are odd. Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b. Their sum is x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1), so x+y is, by definition, even.

Since x and y were arbitrary, the sum of any two odd integers is even. ■

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Integers

Prove "The sum of two odd numbers is even."

Proof: Let x and y be arbitrary **odd** integers.

Then, x = 2a+1 for some integer a and y = 2b+1 for some integer b. Their sum is x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1), so x+y is, by definition, even.

Since x and y were arbitrary, the sum of any two odd integers is even.

■

$\forall x\ \forall y\ ((\text{Odd}(x) \wedge \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Rational Numbers

Domain of Discourse
Real Numbers

- A real number x is *rational* iff there exist integers a and b with $b \neq 0$ such that $x = a/b$.

$$\text{Rational}(x) := \exists a\, \exists b\, (((\text{Integer}(a) \wedge \text{Integer}(b)) \wedge (x = a/b)) \wedge b \neq 0)$$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

Formally, prove $\forall x\ \forall y\ ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary reals.

Suppose x and y are rational.

Thus, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

Thus, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Thus, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

By definition, then, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

Proof: Let x and y be arbitrary rationals.

Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (a/b)(c/d) = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational.

Since x and y were arbitrary, we have shown that the product of any two rationals is rational. ■

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "The product of two rationals is rational."

OR "If x and y are rational, then xy is rational."

Recall that unquantified variables (not constants) are implicitly for-all quantified.

$\forall x\ \forall y\ ((\text{Rational}(x) \wedge \text{Rational}(y)) \rightarrow \text{Rational}(xy))$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) := $\exists a\ \exists b\ (\text{Integer}(a) \wedge \text{Integer}(b) \wedge (x = a/b) \wedge (b \neq 0))$

Prove: "If x and y are rational, then xy is rational."

Proof: ~~Let x and y be arbitrary rationals.~~

Suppose x and y are rational.

Then, x = a/b for some integers a, b, where b≠0, and y = c/d for some integers c,d, where d≠0.

Multiplying, we get that xy = (a/b)(c/d) = (ac)/(bd). Since b and d are both non-zero, so is bd. Furthermore, ac and bd are integers. By definition, then, xy is rational.

~~Since x and y were arbitrary, we have shown that the product of any two rationals is rational.~~ ■

Last class: English Proofs

- High-level language let us work more quickly
  - should not be necessary to spill out every detail
  - examples so far

    skipping Intro ∧ and Elim ∧ (and hence, Commutativity and Associativity)

    skipping Double Negation

    not stating existence claims (immediately apply Elim ∃ to name the object)

    not stating that the implication has been proven ("Suppose X... Thus, Y." says it already)
  - (list will grow over time)

- English proof is correct if the reader believes they could translate it into a formal proof
  - the reader is the "compiler" for English proofs

Proof Strategies

Proof Strategies: Counterexamples

To prove $\neg\forall x\, P(x)$, prove $\exists\neg P(x)$:

- Equivalent by De Morgan's Law
- All we need to do that is find an x where $P(x)$ is **false**
- This example is called a ***counterexample*** to $\forall x\, P(x)$.

e.g. Prove "Not every prime number is odd"

Proof: 2 is a prime that is not odd — a counterexample to the claim that every prime number is odd. ■

An English proof does not need to cite De Morgan's law.

Proof Strategies: Proof by Contrapositive

If we assume ¬q and derive ¬p, then we have proven ¬q → ¬p, which is equivalent to proving p → q.

1.1. $\neg q$ Assumption

...

1.3. $\neg p$

1. $\neg q \rightarrow \neg p$ Direct Proof
2. $p \rightarrow q$ Contrapositive: 1

Proof Strategies: Proof by Contrapositive

If we assume $\neg q$ and derive $\neg p$, then we have proven $\neg q \rightarrow \neg p$, which is equivalent to proving $p \rightarrow q$.

We will prove the contrapositive.

Suppose $\neg q$.

…

Thus, $\neg p$.

	1.1. $\neg q$	Assumption
	…	
	1.3. $\neg p$	
1.	$\neg q \rightarrow \neg p$	Direct Proof
2.	$p \rightarrow q$	Contrapositive: 1

Proof by Contradiction: One way to prove ¬p

If we assume p and derive F (a contradiction), then we have proven ¬p.

1.1. p Assumption

...

1.3. F

1. $p \rightarrow$ F Direct Proof
2. $\neg p \vee$ F Law of Implication: 1
3. $\neg p$ Identity: 2

Proof Strategies: Proof by Contradiction

If we assume p and derive F (a contradiction), then we have proven ¬p.

We will argue by contradiction.

Suppose p.

...

This is a contradiction.

	1.1. p	Assumption
	...	
	1.3. F	
1.	$p \rightarrow$ F	Direct Proof
2.	$\neg p \vee$ F	Law of Implication: 1
3.	$\neg p$	Identity: 2

Often, we will infer ¬R, where R is a prior fact.
Putting these together, we have $R \wedge \neg R \equiv F$

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We will argue by contradiction.

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We will argue by contradiction.

Suppose that x is an integer that is both even and odd.

This is a contradiction. ■

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We will argue by contradiction.

Suppose that x is an integer that is both even and odd. Then, x=2a for some integer a, and x=2b+1 for some integer b.

This is a contradiction. ■

Even and Odd

Predicate Definitions
Even(x) $\equiv \exists y\ (x = 2y)$
Odd(x) $\equiv \exists y\ (x = 2y + 1)$

Domain of Discourse
Rationals

Prove: "No integer is both even and odd."

Formally, prove $\neg \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We will argue by contradiction.

Suppose that x is an integer that is both even and odd. Then, x=2a for some integer a, and x=2b+1 for some integer b. This means 2a=x=2b+1 and hence 2a-2b=1 and so a-b=½. But a-b is an integer while ½ is not, so they cannot be equal. This is a contradiction. ■

Formally, we've shown Integer(½) $\wedge \neg$Integer(½) $\equiv$ F.

Strategies

- Simple proof strategies already do a lot
  - counter examples
  - proof by contrapositive
  - proof by contradiction

- Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)

Applications of Predicate Logic

- Remainder of the course will use predicate logic to prove important properties of interesting objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

- Encode domain knowledge in predicate definitions
- Then apply predicate logic to infer useful results

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$

Number Theory

Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing

- Many significant applications
  - Cryptography & Security
  - Data Structures
  - Distributed Systems

- Important toolkit

Modular Arithmetic

- Arithmetic over a finite domain
- Almost all computation is over a finite domain

I’m ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            “I will be alive for at least ” +
            SEC_IN_YEAR * 101 + “ seconds.”
        );
    }
}
```

I’m ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            “I will be alive for at least ” +
            SEC_IN_YEAR * 101 + “ seconds.”
        );
    }
}
```

```
  ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

  ----jGRASP: operation complete.
```

Divisibility

Domain of Discourse
Integers

Definition: "b divides a"

For a, b with $b \neq 0$:

$$b \mid a \leftrightarrow \exists q\ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
1 | 5	5 | 25	0 | 5	2 | 3

Divisibility

Domain of Discourse
Integers

Definition: "b divides a"

For a, b with $b \neq 0$:

$$b \mid a \leftrightarrow \exists q\ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k