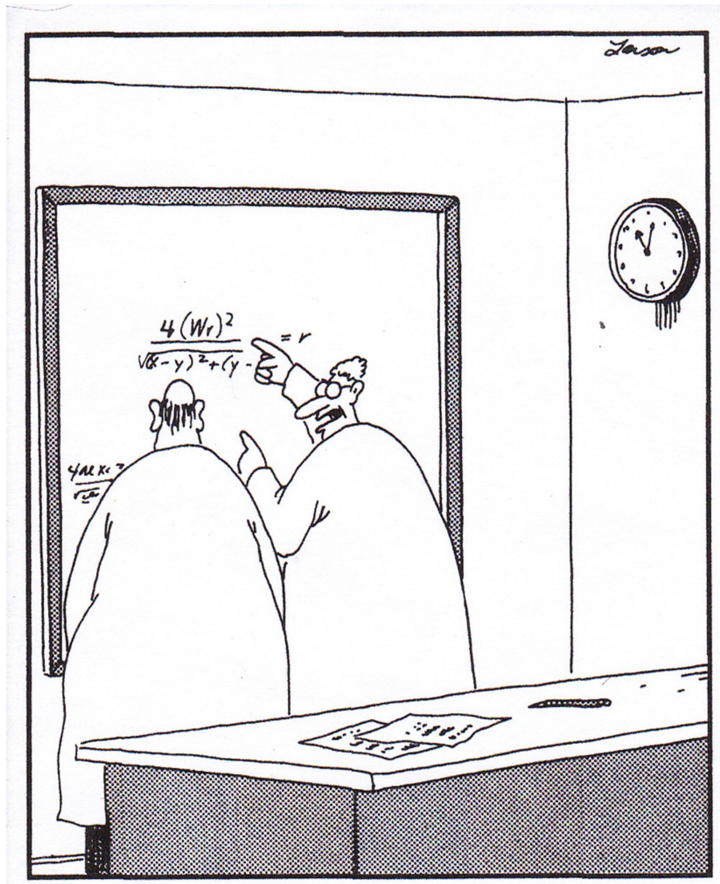
CSE 311: Foundations of Computing

Lecture 9: English Proofs, 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."

cozy.cs.
is up.

13 1.

$$\frac{A,\ A \to B}{\therefore B}$$

Last class: Inference Rules for Quantifiers

Intro ∃

$$\frac{P(c) \text{ for some } c}{\therefore \quad \exists x\, P(x)}$$

Elim ∀

$$\frac{\forall x\, P(x)}{\therefore \quad P(a) \quad \textbf{(for any } a\textbf{)}}$$

Cannot set constants equal to other after they are defined

Elim ∃

$$\frac{\exists x\, P(x)}{\therefore\ P(c) \textbf{ for some } \textbf{\textit{special}}^{**}\ c}$$

Intro ∀

$$\frac{\text{“}\textbf{Let } a \textbf{ be arbitrary}^{*}\text{”} \ldots P(a)}{\therefore \quad \forall x\, P(x)}$$

** c is a NEW name.
List all dependencies for c.

* in the domain of P. No other name in P depends on a.

dependencies:
other named arbitrary constants in ∃x P(x)

Last class: Formal & English Proofs: Even and Odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
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: **a** depend **x**
	3.6	∃**z** (**y** = 2**z**+1)	Def of Odd: 2.3
	3.7	**y** = 2**b**+1	Elim ∃: 2.5: **b** depend **y**
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 two odd integers is even.	3.	(Odd(**x**) ∧ Odd(**y**)) → Even(**x**+**y**)	DPR
	4.	∀y ((Odd(x) ∧ Odd(y)) → Even(x+y))	Intro ∀
	5.	∀x∀y ((Odd(x) ∧ Odd(y)) → Even(x+y))	Intro ∀

Last class: Even and Odd

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

Domain of Discourse
Integers

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

Let x and y be arbitrary odd integers

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. ■

$\forall x\ \forall y\ ((\mathrm{Odd}(x) \land \mathrm{Odd}(y)) \rightarrow \mathrm{Even}(x+y))$

Rational Numbers

Domain of Discourse
Real Numbers

- A real number x is *rational* iff there exist integers a and b with b≠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) := $\exists a\ \exists b\ (\text{Integer}(a) \land \text{Integer}(b) \land (x = a/b) \land (b \neq 0))$

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

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

Let x and y be arbitrary real #'s

Assum x y are ratnl

$\therefore$ xy is rational

Since x and y were arbitrary the

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. ■

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

Rationality

Domain of Discourse
Real Numbers

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

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. ■

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

Rationality

Domain of Discourse
Real Numbers

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

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 $b \neq 0$, and $y = c/d$ for some integers c, d, where $d \neq 0$.

Thus, xy is rational.

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

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

Rationality

Domain of Discourse
Real Numbers

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

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. ■

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

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 rationals.

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

Multiplying, we get that $xy = (a/b)(c/d) = (ac)/(bd)$.

By definition, then, xy is rational.

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

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

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 rationals.

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

Multiplying, we get that $xy = (a/b)(c/d) = (ac)/(bd)$.

ac and bd are integers. Also, since $b \neq 0$ and $d \neq 0$ we have $bd \neq 0$. By definition, then, xy is rational.

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

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

English Proofs

- High-level language lets 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)

\begin{proof}

\end{proof}

- English proof is correct if the <u>reader</u> is convinced 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 $\neg q$ and derive $\neg p$, then we have proven $\neg q \to \neg p$, which is equivalent to proving $p \to q$.

1.1. $\neg q$ Assumption

...

1.3. $\neg p$

1. $\neg q \to \neg p$ Direct Proof
2. $p \to q$ 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 $\neg$ p and derive F (a contradiction), then we have proven p.

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

Proof Strategies: Proof by Contradiction

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

We will argue by contradiction.

Suppose $\neg p$.

...

This is a contradiction.

1.1. $\neg p$ Assumption

...

1.3. F

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

Often, we will infer $\neg$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 $\neg\exists x\,(\text{Even}(x) \wedge \text{Odd}(x))$ $\neg P$

$\neg\neg\exists x$

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 $\neg\exists x\,(\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

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 $\mathrm{Integer}(½) \wedge \neg\mathrm{Integer}(½) \equiv \mathrm{F}$.

Proof by Cases

On Homework 3, Task 1 you are asked to show:

- Given $p \to r$ and $\neg p \to r$ derive r
- Given $p \vee q$, $p \to r$ and $q \to r$ derive r

This will mean that…

If we prove p → r and ¬ p → r then we have proven r.

If we prove p ∨ q, p → r and q → r then we have proven r.

Strategies

- Simple proof strategies already do a lot
  - counter examples
  - proof by contrapositive
  - proof by contradiction
  - proof by cases
- 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 <u>important</u> properties of <u>interesting</u> 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?

$0 = 0 * 5$

$5 \mid 1$	$25 \mid 5$	$5 \mid 0$	$3 \mid 2$
$1 \mid 5$	$5 \mid 25$	$\cancel{0 \mid 5}$	$2 \mid 3$

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?

$5 \mid 1$	$25 \mid 5$	$5 \mid 0$	$3 \mid 2$
$5 \mid 1$ iff $1 = 5k$	$25 \mid 5$ iff $5 = 25k$	$5 \mid 0$ iff $0 = 5k$	$3 \mid 2$ iff $2 = 3k$
$1 \mid 5$	$5 \mid 25$	$0 \mid 5$	$2 \mid 3$
$1 \mid 5$ iff $5 = 1k$	$5 \mid 25$ iff $25 = 5k$	$0 \mid 5$ iff $5 = 0k$	$2 \mid 3$ iff $3 = 2k$

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \mid a$, then, by definition, we have $a = qb$ for some q.
The number q is called the *quotient*.

Dividing both sides by b, we can write this as

$$\frac{a}{b} = q$$

(We want to stick to integers, though, so we'll write $a = qb$.)

Recall: Elementary School Division

$b \nmid a$

For a, b with $b > 0$, we can divide b into a.

If $b \nmid a$, then we end up with a *remainder* r with $0 < r < b$.
Now,

instead of $\dfrac{a}{b} = q$ we have $\dfrac{a}{b} = q + \dfrac{r}{b}$

Multiplying both sides by b gives us
(A bit nicer since it has no fractions.)

$$a = qb + r$$

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \mid a$, then we have $a = qb$ for some q. $r=0$

If $b \nmid a$, then we have $a = qb + r$ for some q, r with $0 < r < b$.

In general, we have $a = qb + r$ for some q, r with $0 \leq r < b$, where $r = 0$ iff $b \mid a$.

$0, \ldots, b-1$

Division Theorem

$-3 \bmod 2$

Domain of Discourse
Integers

Division Theorem $-3 = \cancel{\ } -2 \cdot 2 + 1$

For a, b with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide b **into** a**, we get a unique quotient** $q = a$ **div** b
and non-negative remainder $r = a$ **mod** b $\in \{0, \ldots, b-1\}$

$0 \leq r < b$

!

Note: $r \geq 0$ even if $a < 0$.
Not quite the same as `a % b`.

Division Theorem

Domain of Discourse
Integers

Division Theorem

For a, b with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide b into a, we get a unique quotient $q = a$ div b and non-negative remainder $r = a$ mod b

```
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

```
 ----jGRASP exec: java Test2
-1

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

Note: r ≥ 0 even if a < 0.
Not quite the same as **`a % d`**.

div and mod

$$\boxed{x = 7 \cdot (x \text{ div } 7) + (x \text{ mod } 7)}$$