Adam Blank    Spring 2016

# CSE 311

# Foundations of Computing I

## Even and Odd

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

| Domain of Discourse |
|---|
| Integers |

**Prove: "The square of every even number is even."**

**Formal proof of: $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$**

| | | |
|---|---|---|
| 1. | Let $a$ be arbitrary | Defining a |
| 2.1. | $\text{Even}(a)$ | Assumption |
| 2.2. | $\exists y\ (a = 2y)$ | Definition of Even by 2.1 |
| 2.3. | $a = 2c$ | ∃ Elim: 2.2 |
| 2.4. | $a^2 = 4c^2 = 2(2c^2)$ | Algebra |
| 2.5. | $\exists y\ (a^2 = 2y)$ | ∃ Intro: 2.4 |
| 2.6. | $\text{Even}(a^2)$ | Definition of Even by 2.5 |
| 2. | $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$ | Direct Proof Rule |

## Even and Odd

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

| Domain of Discourse |
|---|
| Integers |

| | |
|---|---|
| Initialize variables. [Header/Intro of the proof] | Let a be an arbitrary even number. |
| Explain why $a^2$ is even. [Body of the proof] | Then, a = 2c for some c, by definition of even. Squaring both sides, we see $a^2 = 4c^2 = 2(2c^2)$. |
| Conclude the sub-proof ["Return" "Inner Result"] | It follows that $a^2$ is even by definition of even. |
| Conclude the proof ["What have we shown?" | Since a was arbitrary, we've shown the square of every even number is even. |

Now, Prove "The square of every odd number is odd."

## Even and Odd

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

| Domain of Discourse |
|---|
| Integers |

**Prove: "The square of every odd number is odd."**

Let x be an arbitrary odd number.

Then, x = 2k+1 for some integer k (depending on x).

Therefore, $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Since $2k^2+2k$ is an integer, $x^2$ is odd.

## Counterexamples

To *disprove* ∀x P(x) prove ¬∀x P(x) :

- $\neg\forall x\ P(x) \equiv \exists x \neg P(x)$
- To prove the existential, find an x for which P(x) is **false**
- This example is called a **counterexample.**

## Counterexample...example

Disprove "Every non-negative integer has another number smaller than it."

$$\forall x\ \exists y\ (y < x)$$

| | |
|---|---|
| Tell the reader that we're about to use a "counterexample". | We claim $\forall x\ \exists y\ (y < x)$ is false. So, we show the negation, $\exists x\ \forall y\ (y \geq x)$, is true. |
| Use ∃ Intro. | Consider x = 0. |
| Use ∀ Intro. | Let y be arbitrary. |
| Prove the ∀ statement. | Since y is non-negative, $y \geq 0$. So, the claim is true. |
| Conclude the proof. | Thus, the original claim is false. |

## Reminder for HW

For Elim ∃...

**Your "c" has to be new (e. g. cannot be used previously in the proof)**
**You should say what variables your "c" depends on.**

---

**The order you use Elim ∃ and Elim ∀ in DOES matter!**

**Reminder: ∃x ∀y P(x,y) IS DIFFERENT FROM ∀y∃x P(x,y)**

## Proof by Contrapositive: One Strategy for implications

If we assume ¬q and derive ¬p, then we have proven ¬q → ¬p, which is the same as p → q.

1.1. ¬q  Assumption
...
1.3. ¬p
1. ¬q → ¬p  Direct Proof Rule
2. p → 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 → F  Direct Proof rule
2. ¬p ∨ F  Law of Implication: 4
3. ¬p  Identity: 5

## Even and Odd

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

| Domain of Discourse |
|---|
| Integers |

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

English proof: ¬ ∃x (Even(x)∧Odd(x))
≡∀x ¬(Even(x)∧Odd(x))

We go by contradiction. Let x be any integer and suppose that it is both even and odd. Then x=2k for some integer k and x=2m+1 for some integer m. Therefore 2k=2m+1 and hence k=m+½.

But two integers cannot differ by ½ so this is a contradiction. So, no integer is both even and odd.

## Rational Numbers

| Domain of Discourse |
|---|
| Real Numbers |

- A real number x is *rational* iff there exist integers p and q with q≠0 such that x=p/q.

Rational(x) ≡ ∃p ∃q ((x=p/q) ∧ Integer(p) ∧ Integer(q) ∧ q≠0)

## Rationality

| Domain of Discourse |
|---|
| Real Numbers |

| Predicate Definitions |
|---|
| Rational(x) ≡ $\exists p\ \exists q\ ((x = \frac{p}{q} \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0$ |

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

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

Note that xy = (ac)/(bd).

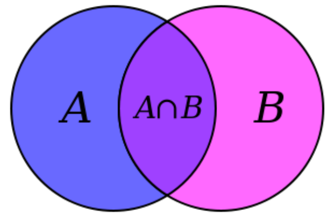
Since b and d are both non-zero, so is bd; furthermore, ac and bd are integers. It follows that xy is rational, by definition of rational.

## Proofs

- Formal proofs follow simple well-defined rules and should be easy to check
  - In the same way that code should be easy to execute
- English proofs correspond to those rules but are designed to be easier for humans to read
  - Easily checkable in principle
- Simple proof strategies already do a lot
  - Later we will cover a specific strategy that applies to loops and recursion (mathematical induction)

## CSE 311: Foundations of Computing

### Lecture 9: Set Theory




## Sets

- Mathematical sets are a lot like Java sets:
  - `Set<T> s = new HashSet<T>();`
  - …with the following exceptions:
    - They are untyped: {"string", 123, 1.2} is a valid set
    - They are immutable: you can't add/remove from them
    - They are built differently
    - They have one fundamental operation:
      - Contains: $x \in S$

## Some Common Sets

ℕ is the set of **Natural Numbers;** N = {0, 1, 2, …}
ℤ is the set of **Integers**; Z = {…, -2, -1, 0, 1, 2, …}
ℚ is the set of **Rational Numbers**; e.g. ½, -17, 32/48
ℝ is the set of **Real Numbers**; e.g. 1, -17, 32/48, π
[n] is the set {1, 2, …, n} when n is a natural number
{} = ∅ is the **empty set**; the *only* set with no elements

EXAMPLES
Are these sets?
A = {1, 1}
B = {1, 3, 2}
C = {☐, 1}
D = {{}, 17}
E = {1, 2, 7, cat, dog, ∅, α}

We say $2 \in E$; $3 \notin E$.

They're all sets.
Note {1} = {1, 1}.

## Definition: Equality

A and B are *equal* if they have the same elements

$$A = B \equiv \forall x\, (x \in A \leftrightarrow x \in B)$$

```
boolean equal(Set A, Set B) {
    boolean result = true;
    for (x : A) {
        if (x ∉ B) { result = false; }
    }
    for (x : B) {
        if (x ∉ A) { result = false; }
    }
    return result;
}
```

A = {4, 3, 3}
B = {3, 4, 3}
C = {3, 4}

Are any of A, B, C equal?

They all are!
(dups, order don't matter!)

## Definition: Subset

A is a *subset* of B if every element of A is also in B

$$A \subseteq B \equiv \forall x\, (x \in A \rightarrow x \in B)$$

```
boolean subset(Set A, Set B) {
    boolean result = true;
    for (x : A) {
        if (x ∉ B) { result = false; }
    }
    return result;
}
```

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}

QUESTIONS
$\varnothing \subseteq A$? **Yes. In fact, $\varnothing \subseteq X$ for any set X.**
$A \subseteq B$? **No. $3 \in A$, but that's not true for B.**
$C \subseteq B$? **Yes, $3 \in B$, $4 \in B$.**

## Definitions

- A and B are *equal* if they have the same elements

$$A = B \equiv \forall x\,(x \in A \leftrightarrow x \in B)$$

- A is a *subset* of B if every element of A is also in B

$$A \subseteq B \equiv \forall x\,(x \in A \rightarrow x \in B)$$

- Note: $(A = B) \equiv (A \subseteq B) \wedge (B \subseteq A)$

## Building Sets from Predicates

- The following says "S is the set of all x's where P(x) is true." $S = \{x : P(x)\}$
- The following says "those elements of A for which P(x) is true." $S = \{x \in A : P(x)\}$
- "All the real numbers less than one."
  - $\{x \in \mathbb{R} : x < 1\}$
- "All the powers of two that happen to be odd."
  - $\{x \in \mathbb{N}: \exists k\ (x = 2k+1) \wedge \exists j\ (x = 2^j)\}$
- "All natural numbers between 1 and n" ("brackets n")
  - $[n] = \{x \in \mathbb{N} : 1 \leq x \leq n\}$

## Set Operations

$A \cup B = \{\, x : (x \in A) \vee (x \in B)\}$ Union

$A \cap B = \{\, x : (x \in A) \wedge (x \in B)\}$ Intersection

$A \setminus B = \{\, x : (x \in A) \wedge (x \notin B)\}$ Set Difference

A = {1, 2, 3}
B = {4, 5, 6}
C = {3, 4}

QUESTIONS

Using A, B, C and set operations, make…

[6] = A ∪ B = A ∪ B ∪ C

{3} = C ∖ B = A ∖ B = A ∩ B

{1,2} = A ∖ C = (A ∪ B) ∖ C

## More Set Operations

$A \oplus B = \{\, x : (x \in A) \oplus (x \in B)\}$ Symmetric Difference

$\bar{A} = \{\, x : x \notin A\,\}$ (with respect to universe U) Complement

A = {1, 2, 3}
B = {1, 4, 2, 6}
C = {1, 2, 3, 4}

QUESTIONS

Let $S$ = {1, 2}.

If the universe is A, then $\bar{S}$ is… **A ∖ S =** {3}

If the universe is B, then $\bar{S}$ is… **B ∖ S =** {4, 6}

If the universe is C, then $\bar{S}$ is… **C ∖ S =** {3, 4}