Adam Blank Spring 2017

CSE 311

Foundations of Computing I

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 square of every odd number is odd."

Do this problem
OR
Start reading the gold handout.

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

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

Domain of Discourse: Integers

$\forall x\ (\text{odd}(x) \rightarrow \text{odd}(x^2))$

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.

"How can I USE a statement?"

Known Statements

Domain of Discourse: Integers

$\forall x\ (\text{Even}(x) \vee \text{Odd}(x))$

Choose a particular x we care about.

Even(5) ∨ Odd(5)

0 = 2x
?
0 = 2x+1

$\exists y\ (16 = 4y)$

*Assert that one exists. *We can't assert any other properties though!!!!**

choose 7 s.t. 16 = 4·7

"How can I USE a statement?"

Known Statements

Domain of Discourse: Integers

$\forall x\ (\text{Even}(x) \vee \text{Odd}(x))$

Choose a particular x we care about.

"Since every integer is either even or odd, it follows that 5 is even or odd..."

$\exists y\ (16 = 4y)$

*Assert that one exists. *We can't assert any other properties though!!!!**

"Choose z such that 16 = 4z..."

Unknown Statements

$(\exists y\ (16 = 4y)) \rightarrow (\exists y\ (16 = 2y))$

Domain of Discourse: Integers

Suppose the left side and prove the right side.

Suppose $\exists y(16 = 4y)$. Choose a s.t. $16 = 4a = 2(2a)$. So, there is an l s.t. $16 = 2l$ (it's $2a$).

$\forall x\ \left((\exists y\ (x = 4y)) \rightarrow (\exists y\ (x = 2y))\right)$

Define an "arbitrary x" and prove it for that x.

Unknown Statements

$(\exists y\ (16 = 4y)) \rightarrow (\exists y\ (16 = 2y))$

Domain of Discourse: Integers

Suppose the left side and prove the right side.

"Suppose 16 = 4y for some y. Then, note that 16 = 2(2y). Thus, there is an x such that 16 = 2x (namely, 2y)."

$\forall x\ \left((\exists y\ (x = 4y)) \rightarrow (\exists y\ (x = 2y))\right)$

Define an "arbitrary x" and prove it for that x.

"Let x be arbitrary. Suppose x = 4y for some y. Then, note that x = 2(2y). Thus, there is a z such that x = 2z (namely, 2y)."

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 arb non-neg. int.

Prove the ∀ statement. {

Conclude the proof. {

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

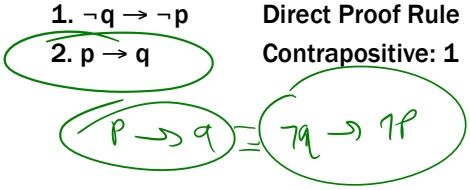
If we assume ¬q and derive ¬p, then we have proven ¬q → ¬p, which is the same as p → q.

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))

Let x be an arb. integer.
Suppose for contradiction that x is odd and even
$x = 2k+1$, $x = 2\ell$
$2k+1 = 2\ell \rightarrow k + \frac{1}{2} = \ell$

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))

Let x be an arbitrary integer. We go by contradiction. Suppose that x 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."

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

Let x, y be arb. rationals. $xy =$
Choose p_x, q_x, p_y, q_y, all ints.
s.t. $q_x \neq 0$, $q_y \neq 0$ and $x = \frac{p_x}{q_x}$
and $y = \frac{p_y}{q_y}$

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).

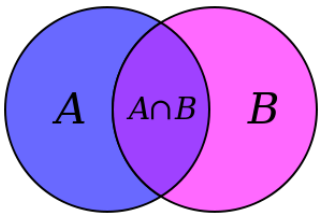
Since b and d are both non-zero, so is bd; furthermore, ac and bd are integers. It follows that xy is rational, by definition of rational.

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)**

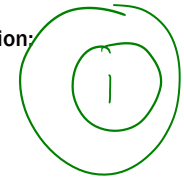
CSE 311: Foundations of Computing

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 ∈ E; 3 ∉ E.

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 ∈ E; 3 ∉ 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 = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}

Are any of A, B, C equal?

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
∅ ⊆ A?
A ⊆ B?
C ⊆ B?

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
∅ ⊆ A? **Yes. In fact, ∅ ⊆ X for any set X.**
A ⊆ B? **No. 3 ∈ A, but that's not true for B.**
C ⊆ B? **Yes, 3 ∈ B, 4 ∈ 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."

$$S = \{x \in A : P(x)\}$$

$\forall x\,(x \in \mathbb{R} \rightarrow x \leq 0)$
$\forall (x \in \mathbb{R})\, x \leq 0$

- "All the real numbers less than one."
  - $\{x : x < 1 \wedge x \in \mathbb{R}\} \simeq \{x \in \mathbb{R} : x < 1\}$
- "All the powers of two that happen to be odd."
  -
- "All natural numbers between 1 and n" ("brackets n")
  - $\{x \in \mathbb{N} : 1 \leq x \leq n\}$

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] =
{3} =
{1,2} =

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 = {3, 5, 6}
C = {3, 4}

QUESTIONS
Using A, B, C and set operations, make...
[6] = $A \cup B = A \cup B \cup C$
{3} = $C \setminus B = A \cap B$
{1,2} = $A \setminus C$

More Set Operations

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

$\overline{A} = \{ x : x \notin A \}$ (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 $\overline{S}$ is...
If the universe is B, then $\overline{S}$ is...
If the universe is C, then $\overline{S}$ is...

More Set Operations

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

$\overline{A} = \{ x : x \notin A \}$ (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 $\overline{S}$ is... $A \setminus S$ = {3}
If the universe is B, then $\overline{S}$ is... $B \setminus S$ = {4, 6}
If the universe is C, then $\overline{S}$ is... $C \setminus S$ = {3, 4}

Power Set

- Power Set of a set A = set of all subsets of A

  $\mathcal{P}(A) = \{ B : B \subseteq A \}$

- Let Days = {M, W, F}. Suppose we wanted to know the possible ways that we could allocate class days to be cancelled. Let's call this set $\mathcal{P}(\text{Days})$.

e.g. $\mathcal{P}(\text{Days}) = \{$

e.g. $\mathcal{P}(\varnothing) = ?$

$\}$

Power Set

- Power Set of a set A = set of all subsets of A

$$\mathcal{P}(A) = \{ B : B \subseteq A \}$$

- Let Days = {M, W, F}. Suppose we wanted to know the possible ways that we could allocate class days to be cancelled. Let's call this set $\mathcal{P}(\text{Days})$.

e.g. $\mathcal{P}(\text{Days}) = \{$
$\emptyset,$
$\{M\}, \{W\}, \{F\},$
$\{M, W\}, \{W, F\}, \{M, F\},$
$\{M, W, F\}$
$\}$

e.g. $\mathcal{P}(\emptyset) =$ {∅}

Cartesian Product

$$A \times B = \{ (a, b) : a \in A, b \in B \}$$

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

$A \times \emptyset = \{(a, b) : a \in A \wedge b \in \emptyset\} = \{(a, b) : a \in A \wedge F\} = \emptyset$

Russell's Paradox

$$S = \{ x : x \notin x \}$$

Suppose for contradiction that S ∈ S...

Russell's Paradox

$$S = \{ x : x \notin x \}$$

Suppose for contradiction that S ∈ S. Then, by definition of S, S ∉ S, but that's a contradiction.

Suppose for contradiction that S ∉ S. Then, by definition of the set comprehension, S ∈ S, but that's a contradiction.

This is reminiscent of the truth value of the statement "This statement is false."

It's Boolean algebra again

- Definition for ∪ based on ∨
- Definition for ∩ based on ∧
- Complement works like ¬

De Morgan's Laws

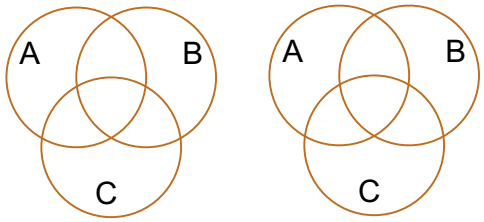
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

Proof technique:
To show C = D show
$x \in C \rightarrow x \in D$ and
$x \in D \rightarrow x \in C$

Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$



Representing Sets Using Bits

- Suppose universe U is $\{1,2,\ldots,n\}$
- Can represent set $B \subseteq U$ as a vector of bits:
  $b_1 b_2 \ldots b_n$ where $b_i = 1$ when $i \in B$
  $b_i = 0$ when $i \notin B$
  – Called the *characteristic vector* of set B
- Given characteristic vectors for A and B
  – What is characteristic vector for $A \cup B$? $A \cap B$?

UNIX/Linux File Permissions

- `ls -l`

```
drwxr-xr-x ... Documents/
-rw-r--r-- ... file1
```

- Permissions maintained as bit vectors
  – Letter means bit is 1
  – "–" means bit is 0.

Bitwise Operations

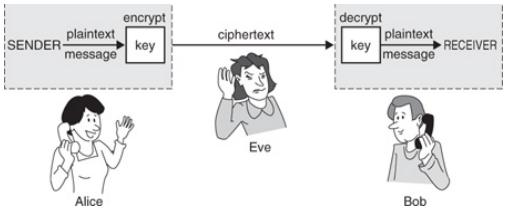
```
  01101101        Java:  z=x|y
∨ 00110111
  01111111

  00101010        Java:  z=x&y
∧ 00001111
  00001010

  01101101        Java:  z=x^y
⊕ 00110111
  01011010
```

A Useful Identity

- If x and y are bits: $(x \oplus y) \oplus y = ?$
- What if x and y are bit-vectors?

Private Key Cryptography

- **Alice** wants to communicate message secretly to **Bob** so that eavesdropper **Eve** who hears their conversation cannot tell what **Alice**'s message is.
- **Alice** and **Bob** can get together and privately share a secret key **K** ahead of time.



One-Time Pad

- Alice and Bob privately share random n-bit vector K
  - Eve does not know K
- Later, Alice has n-bit message m to send to Bob
  - Alice computes $C = m \oplus K$
  - Alice sends C to Bob
  - Bob computes $m = C \oplus K$ which is $(m \oplus K) \oplus K$
- Eve cannot figure out m from C unless she can guess K