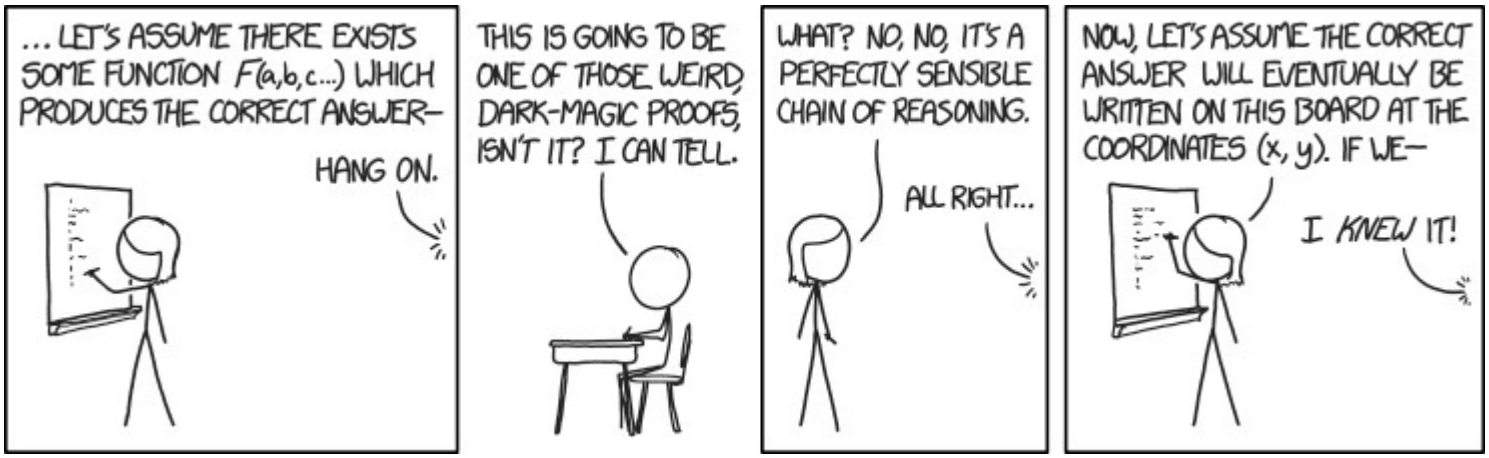
CSE 311: Foundations of Computing

Lecture 9: English Proofs, Strategies, Set Theory



Last class: Inference Rules for Quantifiers

Intro ∃

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

Elim ∀

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

Intro ∀

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

Elim ∃

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

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

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

Last class: Even and Odd

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

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

Formal proof of: $\forall x\,(Even(x) \rightarrow Even(x^2))$

1. Let **a** be an arbitrary integer
   - 2.1 Even(**a**) — Assumption
   - 2.2 ∃y (**a** = 2y) — Definition of Even
   - 2.3 **a** = 2**b** — Elim ∃: **b** special depends on **a**
   - 2.4 $a^2 = (2b)^2 = 2(2b^2)$?
   - 2.5 ∃y ($\mathbf{a}^2$ = 2y) — Intro ∃ rule
   - 2.6 Even($\mathbf{a}^2$) — Definition of Even
2. Even(**a**)→Even($\mathbf{a}^2$) — Direct proof rule
3. ∀x (Even(x)→Even(x^2)) — Intro ∀: 1,2

Last class: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: 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 an arbitrary integer
   - 2.1 Even(**a**) — Assumption
   - 2.2 $\exists y\,(\mathbf{a} = 2y)$ — Definition of Even
   - 2.3 $\mathbf{a} = 2\mathbf{b}$ — Elim ∃: **b** special depends on **a**
   - 2.4 $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$ — Algebra
   - 2.5 $\exists y\,(\mathbf{a}^2 = 2y)$ — Intro ∃ rule
   - 2.6 Even($\mathbf{a}^2$) — Definition of Even
2. Even(**a**)→Even($\mathbf{a}^2$) — Direct proof rule
3. $\forall x\,(\text{Even}(x) \rightarrow \text{Even}(x^2))$ — Intro ∀: 1,2

English Proof: Even and Odd

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

Prove "The square of every even integer is even."

English Proof:
(translate from right)

1. Let **a** be an arbitrary integer
   - 2.1 Even(**a**) Assumption
   - 2.2 ∃y (**a** = 2y) Definition
   - 2.3 **a** = 2**b** **b** special depends on **a**
   - 2.4 $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$ Algebra
   - 2.5 ∃y ($\mathbf{a}^2$ = 2y)
   - 2.6 Even($\mathbf{a}^2$) Definition
2. Even(**a**)→Even($\mathbf{a}^2$)
3. ∀x (Even(x)→Even(x^2))

■

English Proof: Even and Odd

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

Prove "The square of every even integer is even."

Proof: Let **a** be an arbitrary even integer.

1. Let **a** be an arbitrary integer
   - 2.1 Even(**a**) — Assumption

Then, by definition, **a** = 2**b** for some integer **b** (depending on **a**).

- 2.2 ∃y (**a** = 2y) — Definition
- 2.3 **a** = 2**b** — **b** special depends on **a**

Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.

- 2.4 $a^2 = 4b^2 = 2(2b^2)$ — Algebra

Since $2b^2$ is an integer, by definition, a^2 is even.

- 2.5 ∃y (a^2 = 2y)
- 2.6 Even(a^2) — Definition

Since **a** was arbitrary, it follows that the square of any even integer is even. ■

2. Even(**a**)→Even(a^2)
3. ∀x (Even(x)→Even(x^2))

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 integer is odd."

Proof: Let ~~a~~ b be an arbitrary odd integer. By definition, $a = 2b + 1$ for some b (dep. on a). Then,

$a^2 = (2b+1)^2 = 4b^2 + 4b + 1 = 2(2b^2 + 2b) + 1.$

That shows that a^2 is odd, by definition. Since a was arbitrary, this shows that the square of any odd integer is odd. □

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 square of every odd integer is odd."

Proof: Let b be an arbitrary odd integer.

Then, b = 2c+1 for some integer c (depending on b).

Therefore, $b^2 = (2c+1)^2 = 4c^2 + 4c + 1 = 2(2c^2 + 2c) + 1$.

Since $2c^2+2c$ is an integer, b^2 is odd. Since b was arbitrary, the square of every odd integer is odd. ■

Proof Strategies: Counterexamples

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

- Works by de Morgan's Law: $\neg \forall x\, P(x) \equiv \exists x \neg P(x)$
- All we need to do that is find an x for which $P(x)$ is false
- This example is called a ***counterexample*** to $\forall x\, P(x)$.

$P(x) = Prime(x) \rightarrow Odd(x)$
$\equiv \neg Prime(x) \vee Odd(x)$

$\forall x P(x)$

e.g. Disprove "Every prime number is odd"

$Prime(2) \wedge \neg Odd(2)$

$\neg P(x) \equiv \neg(Prime(x) \rightarrow Odd(x))$
$\equiv \neg(\neg Prime(x) \vee Odd(x))$
$\equiv Prime(x) \wedge \neg Odd(x)$.

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 $p \rightarrow q$.

1.1. $\neg q$ Assumption

...

1.3. $\neg p$

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

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: "No integer is both even and odd."

English proof: $\neg\ \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

$\equiv \forall x\ \neg(\text{Even}(x) \wedge \text{Odd}(x))$

Proof: Suppose, to the contrary, there is some integer x that is both even and odd. By definition, $x = 2a$ for some a (dep. on x) and $x = 2b+1$ for some b (dep. on x). Thus, $2a = x = 2b+1$. Dividing both sides by 2, we get $a = b + 1/2$, which is impossible since a & b are integers. Therefore, there is no such x. □

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: "No integer is both even and odd."

English proof: $\neg\ \exists x\ (\text{Even}(x) \wedge \text{Odd}(x))$

$\equiv \forall x\ \neg(\text{Even}(x) \wedge \text{Odd}(x))$

Proof: We work by contradiction. Let x be an arbitrary integer and suppose that it is both even and odd. Then x=2a for some integer a and x=2b+1 for some integer b. Therefore 2a=2b+1 and hence a=b+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 $q \neq 0$ such that $x = p/q$.

$$\text{Rational}(x) \equiv \exists p \, \exists q \; ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0)$$

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
$\text{Rational(x)} \equiv \exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

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

Proof: Let x and y be rational. That means for some $a+b$, $x = a/b$, where a & b are integers and $b \neq 0$; and $y = c/d$ for some integers c & $d \neq 0$.

Multiplying them, $xy = (a/b)(c/d) = (ac)/(bd)$.

Since ac & bd are integers and $bd \neq 0$, this shows xy is rational. ∎

Rationality

Domain of Discourse
Real Numbers

Predicate Definitions
Rational(x) $\equiv \exists p\ \exists q\ ((x = p/q) \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge (q \neq 0))$

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

Proof: 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.

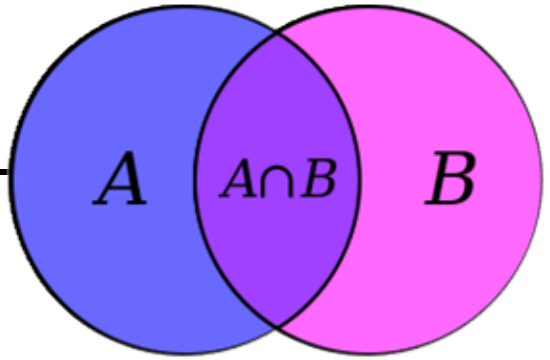
Multiplying, we get that xy = (ac)/(bd).

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)

Set Theory



Sets are collections of objects called elements.

Write $a \in B$ **to say that** a **is an element of set** B**, and** $a \notin B$ **to say that it is not.**

Some simple examples

A = {1}

B = {1, 3, 2}

C = {□, 1}

D = {{17}, 17}

E = {1, 2, 7, cat, dog, ∅, α}

Some Common Sets

$\mathbb{N}$ is the set of **Natural Numbers;** $\mathbb{N} = \{0, 1, 2, \ldots\}$

$\mathbb{Z}$ is the set of **Integers**; $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ is the set of **Rational Numbers**; e.g. ½, -17, 32/48

$\mathbb{R}$ is the set of **Real Numbers**; e.g. 1, -17, 32/48, $\pi, \sqrt{2}$

[n] is the set **{1, 2, …, n}** when **n** is a natural number

{} = $\varnothing$ is the **empty set**; the *only* set with no elements

Sets can be elements of other sets

For example

$A = \{\{1\},\{2\},\{1,2\},\emptyset\}$

$B = \{1,2\}$

Then $B \in A$.

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

Definition: Equality

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

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

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

Which sets are equal to each other?

Definition: Subset

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

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

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

QUESTIONS

$\varnothing \subseteq A$?
$A \subseteq B$?
$C \subseteq B$?

Building Sets from Predicates

S = the set of all* x for which P(x) is true

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

S = the set of all x in A for which P(x) is true

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

*in the domain of P, usually called the "universe" U

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] =

{3} =

{1,2} =

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, 2, 4, 6}
Universe:
U = {1, 2, 3, 4, 5, 6}

$A \oplus B$ = {3, 4, 6}
$\overline{A}$ = {4,5,6}

It's Boolean algebra again

- Definition for $\cup$ based on $\vee$

- Definition for $\cap$ based on $\wedge$

- Complement works like $\neg$

De Morgan's Laws

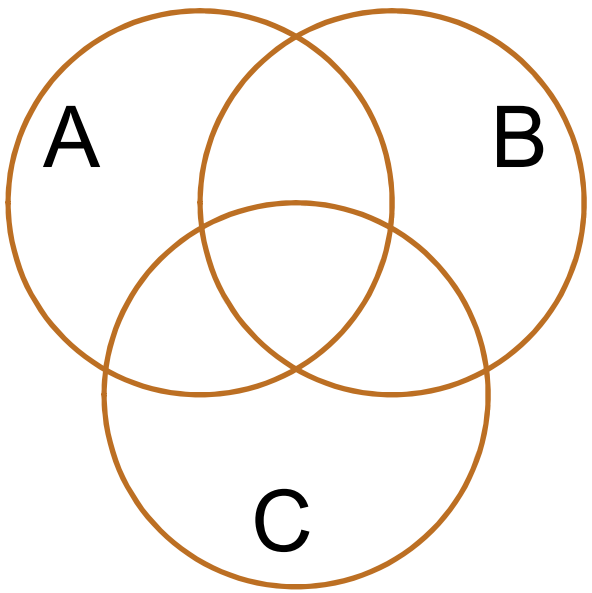
$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

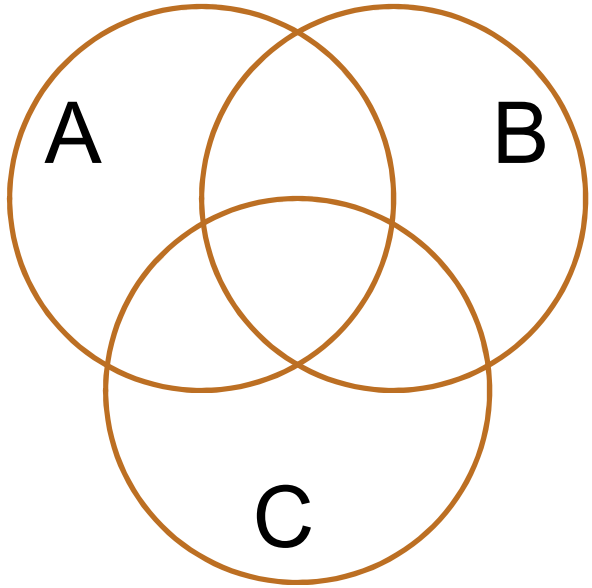
$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

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

Distributive Laws

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





Power Set

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

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

- **e.g., let Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class**

$\mathcal{P}$(Days)=?

$\mathcal{P}(\emptyset)$=?

Power Set

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

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

- **e.g., let Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class**

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

$\mathcal{P}(\emptyset) = \{\emptyset\} \neq \emptyset$

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 $A \times B$ = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

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

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
∨ 00110111
  --------
  01111111
```

Java: `z=x|y`

```
  00101010
∧ 00001111
  --------
  00001010
```

Java: `z=x&y`

```
  01101101
⊕ 00110111
  --------
  01011010
```

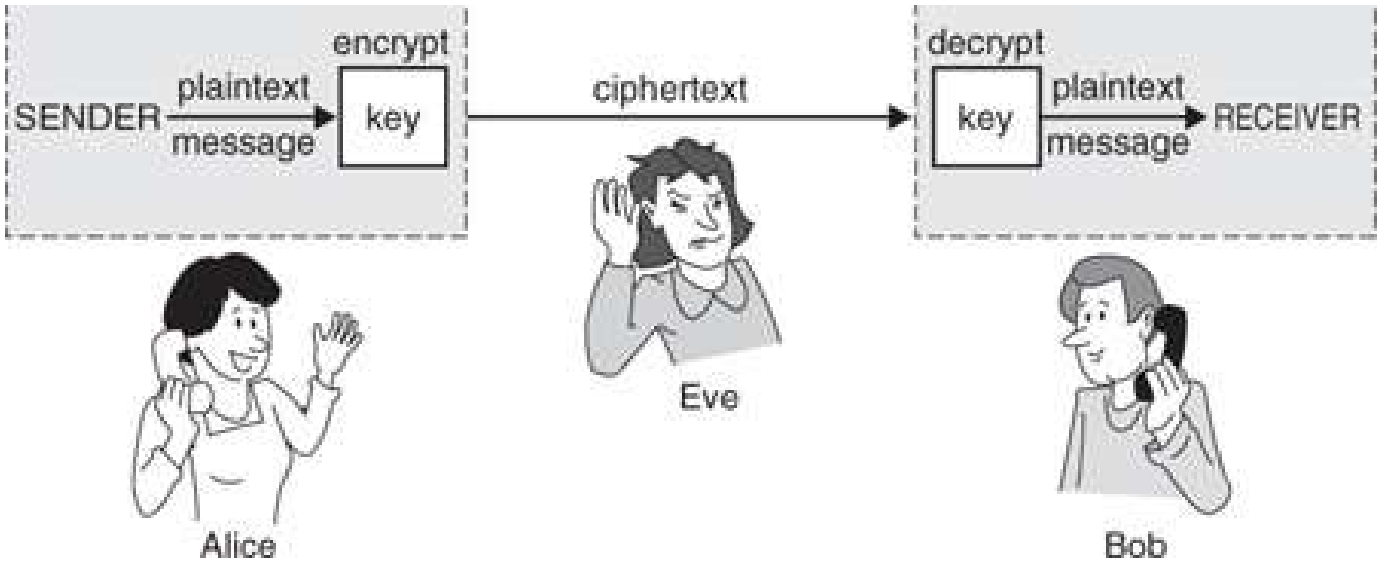
Java: `z=x^y`

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

Russell's Paradox

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

Suppose for contradiction that $S \in S$...

Russell's Paradox

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

Suppose for contradiction that $S \in S$. Then, by definition of S, $S \notin S$, but that's a contradiction.

Suppose for contradiction that $S \notin S$. Then, by definition of the set S, $S \in S$, but that's a contradiction, too.

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