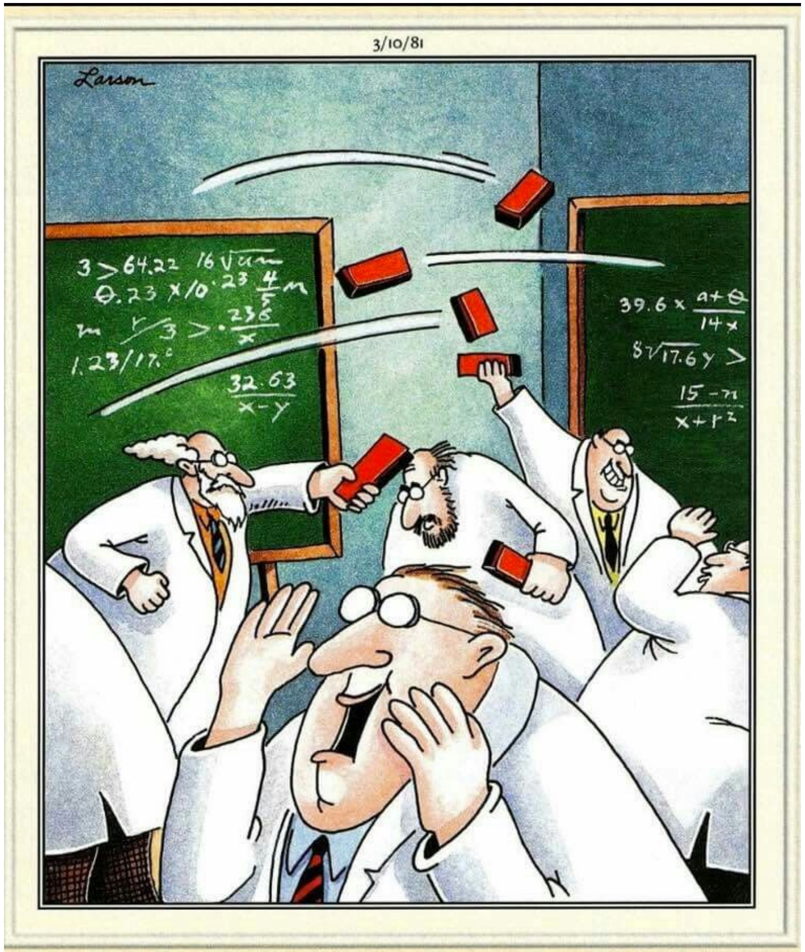
CSE 311: Foundations of Computing

Lecture 13: Set Theory



“Eraser fight!!”

Last class: 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

Last class: Definitions

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

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

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

$$A \subseteq B \;:=\; \forall x\,(x \in A \rightarrow x \in B)$$

- Notes:

$$(\boldsymbol{A} = \boldsymbol{B}) \equiv (\boldsymbol{A} \subseteq \boldsymbol{B}) \wedge (\boldsymbol{B} \subseteq \boldsymbol{A})$$

$x \leq y$ $x < y$

$A \supseteq B$ **means** $B \subseteq A$

$x \geq y$

$A \subset B$ **means** $A \subseteq B$ **but** $A \neq B$

Definition: Subset

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

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

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

D = {5, 3, 4}

B = D

QUESTIONS

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

Definition: Subset

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

$$A \subseteq B \;:=\; \forall x\, (x \in A \rightarrow x \in B)$$

Another way to write domain restriction.

We will use a shorthand for restriction to a set

$$\forall x{\in}A,\, P(x) \;:=\; \forall x\, (x \in A \rightarrow P(x))$$

Restricting all quantified variables improves *clarity*

Sets & Logic

Building Sets from Predicates

Every set S defines a predicate "x ∈ S".

We can also define a set from a predicate P:

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

{x : x is even}

S = the set of all x (in some universe U) for which P(x) is true

In other words... $x \in S \leftrightarrow P(x)$

Proofs About Sets

$A := \{x : P(x)\}$ $B := \{x : Q(x)\}$

Suppose we want to prove $\mathbf{A \subseteq B}$.

This is a predicate:

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

Typically: use direct proof of the implication

Proofs About Sets

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

$A := \{x : P(x)\}$ $B := \{x : Q(x)\}$

Prove that $A \subseteq B$ for P(x):= "x>2" and Q(x):="x^2>3"

Proof: Let x be an arbitrary object (in the universe).

Suppose that $x \in A$. By definition, this means $P(x)$.

... Therefore $x > 2$ so $x^2 > 4$ which implies $x^2 > 3$.

Thus, we have $Q(x)$. By definition, this means $x \in B$.

Since x was arbitrary, we have shown, by definition, that $A \subseteq B$. ∎

Operations on Sets

Set Operations and $\vee$ $\wedge$

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

$A - B$

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

QUESTIONS

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

[6] = $\{1,2,3,4,5,6\} = A \cup B \cup C$

{3} = $A \cap B = A \cap C = B \cap C$

{1,2} = $A \setminus (B \cap C) = A \setminus \{3\} = \{1,2\}$

$A \setminus B = A \setminus C$

More Set Operations

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

Symmetric Difference

$$\overline{A} = A^C := \{\, x : x \in U \wedge x \notin A \,\}$$

(with respect to universe U)

Complement

Equivalently $x \in \overline{A} \leftrightarrow x \notin A \leftrightarrow \neg(x \in A)$

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

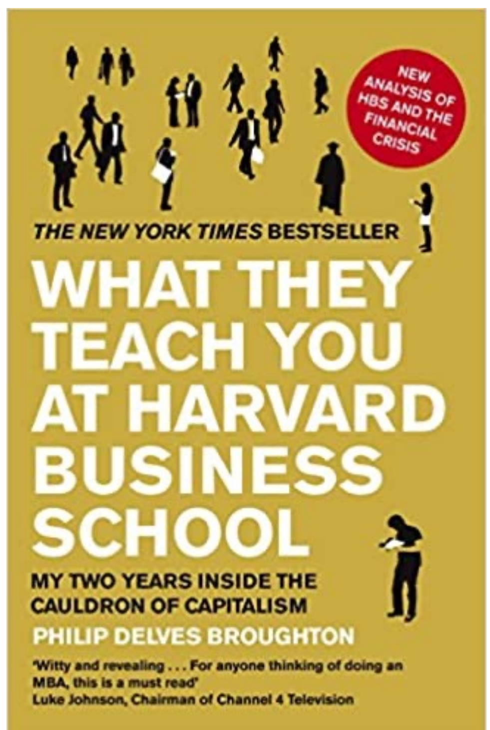
$A \oplus B$ = {3, 4, 6}
$\overline{A}$ = {4,5,6}

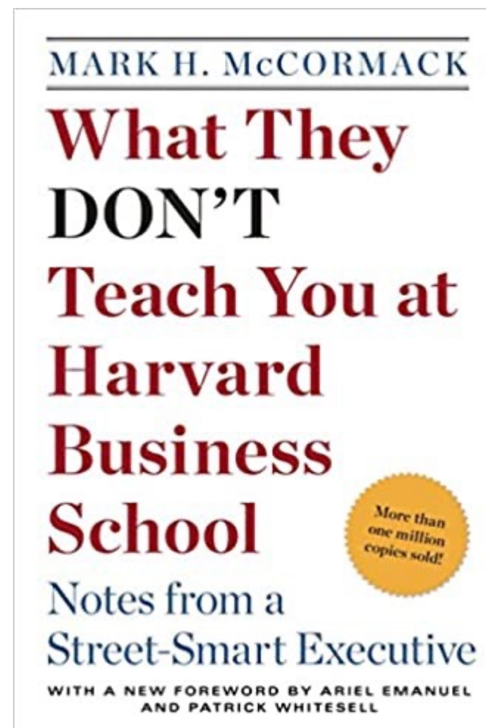
Set Complement

Erik Brynjolfsson
@erikbryn

It's remarkable that as recently as 11 years ago, the sum of all human knowledge could be provided in just two books.

1:55 PM · Sep 10, 2021





De Morgan's Laws

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

$$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$$

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

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x\ \left(x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B}\right)$

Proof: Let x be an arbitrary object.

($\Rightarrow$) Suppose that $x \in \overline{A \cup B}$.

…

Thus, we have $x \in \overline{A} \cap \overline{B}$.

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

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x \ (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

($\Rightarrow$) Suppose that $x \in \overline{A \cup B}$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$.

…

Thus, we have $x \in \overline{A} \cap \overline{B}$.

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x \ (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

($\Rightarrow$) Suppose that $x \in \overline{A \cup B}$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \lor x \in B)$.

…

Thus, we have $x \in \overline{A} \cap \overline{B}$.

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x \ (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

($\Rightarrow$) Suppose that $x \in \overline{A \cup B}$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \lor x \in B)$.

…

Thus, $x \in \overline{A}$ and $x \in \overline{B}$.

Then $x \in \overline{A} \cap \overline{B}$ by the definition of intersection.

De Morgan’s Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x \; (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

(⇒) Suppose that $x \in \overline{A \cup B}$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$.

…

Thus, $\neg(x \in A)$ and $\neg(x \in B)$, so $x \in \overline{A}$ and $x \in \overline{B}$ by the definition of complement, and then $x \in \overline{A} \cap \overline{B}$ by the definition of intersection.

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x \ (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

($\Rightarrow$) Suppose that $x \in \overline{A \cup B}$. Then, by the definition of complement, we have $\neg(x \in A \cup B)$. The latter says, by the definition of union, that $\neg(x \in A \vee x \in B)$, or equivalently $\neg(x \in A) \wedge \neg(x \in B)$ by De Morgan's law. Thus, we have $x \in \overline{A}$ and $x \in \overline{B}$ by the definition of complement, and then $x \in \overline{A} \cap \overline{B}$ by the definition of intersection.

To show C = D show
$x \in C \rightarrow x \in D$ and
$x \in D \rightarrow x \in C$

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall\, x\ \ (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

(⇒) Suppose that $x \in \overline{A \cup B}$.... Then, $x \in \overline{A} \cap \overline{B}$.

(⇐) Suppose that $x \in \overline{A} \cap \overline{B}$. Then, by the definition of intersection, we have $x \in \overline{A}$ and $x \in \overline{B}$. That is, we have $\neg(x \in A) \land \neg(x \in B)$, which is equivalent to $\neg(x \in A \lor x \in B)$ by De Morgan's law. The last is equivalent to $\neg(x \in A \cup B)$, by the definition of union, so we have shown $x \in \overline{A \cup B}$, by the definition of complement. ■

Proofs About Set Equality

A lot of *repetitive* work to show $\rightarrow$ and $\leftarrow$.

Do we have a way to prove $\leftrightarrow$ directly?

Recall that $P \equiv Q$ and $(P \leftrightarrow Q) \equiv T$ are the same

We can use an equivalence chain to prove that a biconditional holds.

De Morgan's Laws

Prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

Formally, prove $\forall x \ (x \in \overline{A \cup B} \leftrightarrow x \in \overline{A} \cap \overline{B})$

Proof: Let x be an arbitrary object.

The stated biconditional holds since:

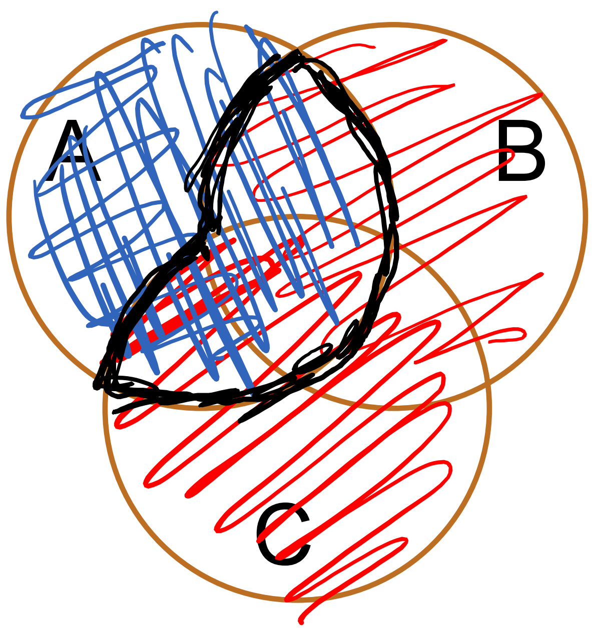
$$
\begin{aligned}
x \in \overline{A \cup B} \quad & \equiv \neg(x \in A \cup B) && \text{Def of Comp} \\
& \equiv \neg(x \in A \vee x \in B) && \text{Def of Union} \\
& \equiv \neg(x \in A) \wedge \neg(x \in B) && \text{De Morgan} \\
& \equiv x \in \overline{A} \wedge x \in \overline{B} && \text{Def of Comp} \\
& \equiv x \in \overline{A} \cap \overline{B} && \text{Def of Union}
\end{aligned}
$$

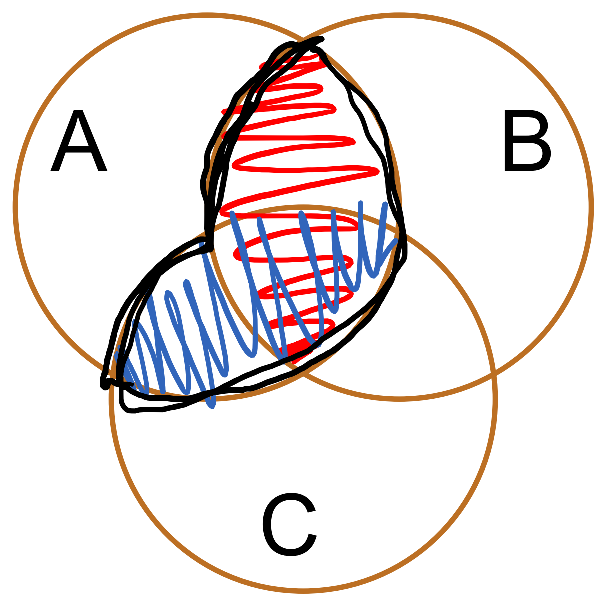
Chains of equivalences are often easier to read like this rather than as English text

Since x was arbitrary, we have shown the sets are equal. ■

Distributive Laws

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





It's Propositional Logic Again!

Meta-Theorem: Translate any Propositional Logic equivalence into "=" relationship between sets by replacing $\cup$ with $\vee$, $\cap$ with $\wedge$, and complement with $\neg$.

"Proof": Let x be an arbitrary object.

The stated bi-condition holds since:

$x \in$ left side $\equiv$ replace set ops with propositional logic

$\equiv$ apply Propositional Logic equivalence

$\equiv$ replace propositional logic with set ops

$\equiv x \in$ right side

Since x was arbitrary, we have shown the sets are equal. ■

It's Boolean Algebra Again!

- Usual notation used in circuit design
- Boolean algebra
  - a set of elements B containing {0, 1}
  - binary operations { + , • }
  - and a unary operation { ' }
  - such that the following axioms hold:

+ is ∪

• is ∩

0 is ∅

1 is universe

A' is $\overline{A}$

For any a, b, c in B:

1. closure:	a + b is in B	a • b is in B
2. commutativity:	a + b = b + a	a • b = b • a
3. associativity:	a + (b + c) = (a + b) + c	a • (b • c) = (a • b) • c
4. distributivity:	a + (b • c) = (a + b) • (a + c)	a • (b + c) = (a • b) + (a • c)
5. identity:	a + 0 = a	a • 1 = a
6. complementarity:	a + a' = 1	a • a' = 0
7. null:	a + 1 = 1	a • 0 = 0
8. idempotency:	a + a = a	a • a = a
9. involution:	(a')' = a	

Note on Proofs of Set Equality

Even though it was overly tedious in the De Morgan case…

… the best strategy for proving other cases of set equality $A = B$ is often:

Let x be an arbitrary object.

Show $A \subseteq B$: Assume that $x \in A$ and show that $x \in B$

Show $B \subseteq A$: Assume that $x \in B$ and show that $x \in A$

Power Set

$|A| :=$ the # of elements in A

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

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

$$|P(A)| = 2^{|A|}$$

- 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)=? $\{\emptyset, \{M,W,F\}, \{M\}, \{W\}, \{F\}, \{M,W\}, \{M,F\}, \{W,F\}\}$

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

$|P(\emptyset)| = 2^0 = 1$

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**

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

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

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**

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

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

Cartesian Product

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

$\mathbb{R}^2$

$\mathbb{R} \times \mathbb{R}$ 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)}.

$|A \times B| = |A| \cdot |B|$

Cartesian Product

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

$\mathbb{R} \times \mathbb{R}$ 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)}.

What is $A \times \emptyset$? $\emptyset$

$|A \times \emptyset| = |A| \cdot |\emptyset|$
$= |A| \cdot 0 = 0$

Cartesian Product

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

$\mathbb{R} \times \mathbb{R}$ 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)}.

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

Russell's Paradox

Frege $\forall \exists$

$S \in S$?

$S \notin S$?

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

Suppose that $S \in S$...

$\{1, 2, 3\} \in S$

Russell's Paradox

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

Suppose that $\boldsymbol{S \in S}$. Then, by the definition of $\boldsymbol{S}$, $\boldsymbol{S \notin S}$, but that's a contradiction.

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

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

Representing Sets Using Bits

- Suppose that 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 $A \cup B$? $A \cap B$?

  $\overline{A}$?

Bitwise Operations

$$\begin{array}{rl} & 01101101 \\ \vee & \underline{00110111} \\ & 01111111 \end{array}$$

Java: `z=x|y`

$$\begin{array}{rl} & 00101010 \\ \wedge & \underline{00001111} \\ & 00001010 \end{array}$$

Java: `z=x&y`

$$\begin{array}{rl} & 01101101 \\ \oplus & \underline{00110111} \\ & 01011010 \end{array}$$

Java: `z=x^y`

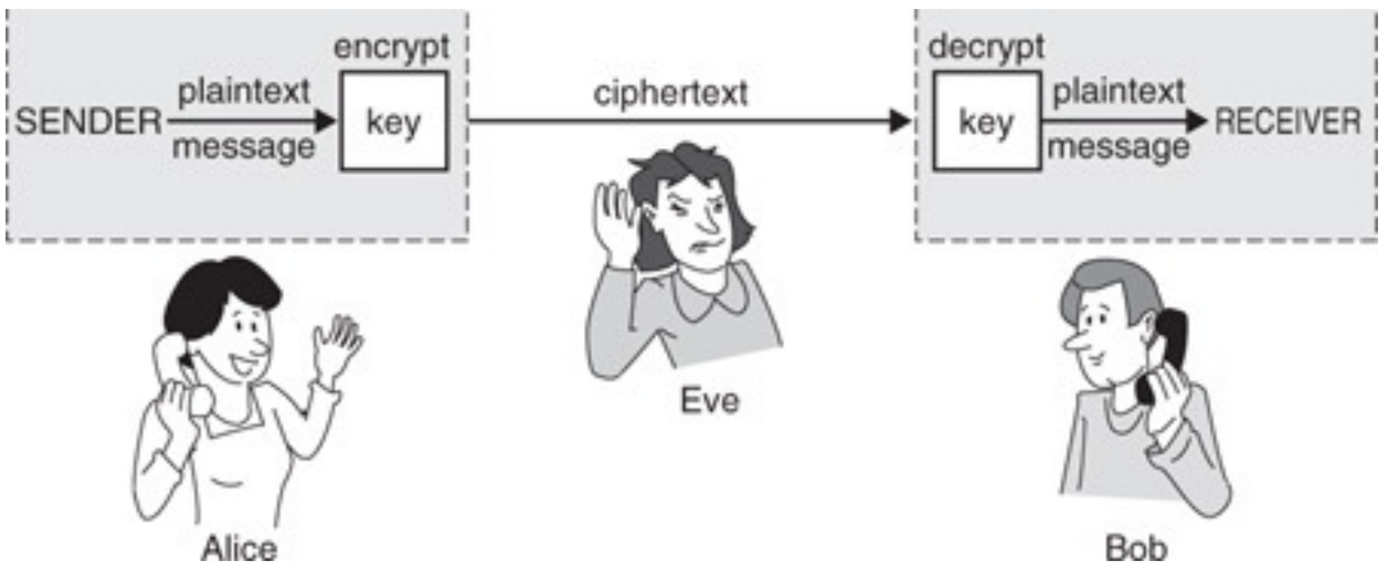
A Useful Identity

- 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