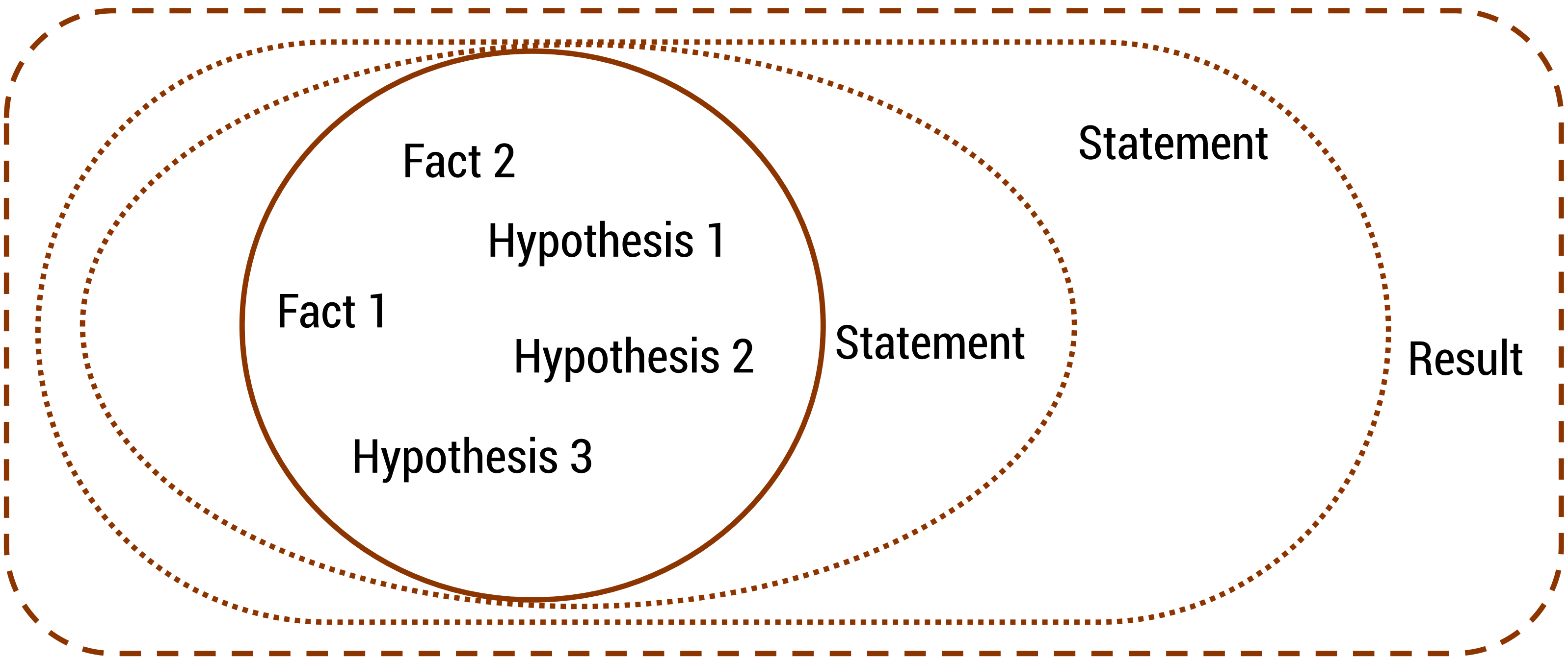
homework #3 out

- Homework #3 is up today. It's all about proofs.
- James is back on Monday.
- Proof recap session Wed at 6pm in EE 105.

- Start with hypotheses and facts
- Use rules of inference to extend set of facts
- Result is proved when it is included in the set



proof by contradiction: one way to prove $\neg p$

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

	1. p	assumption
	...	
	3. $\mathbf{F}$	
4.	$p \to \mathbf{F}$	direct Proof rule
5.	$\neg p \vee \mathbf{F}$	equivalence from 4
6.	$\neg p$	equivalence from 5

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

English proof of: $\neg \exists x\,(\mathrm{Even}(x) \wedge \mathrm{Odd}(x))$

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

We proceed 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 $k=m+\frac{1}{2}$.

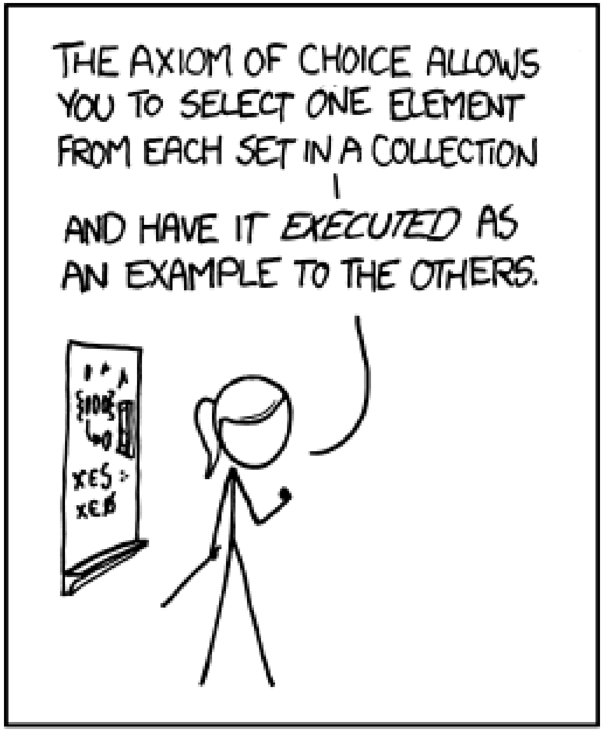
But two integers cannot differ by ½ so this is a contradiction.

So, no integer is both even an odd.

□

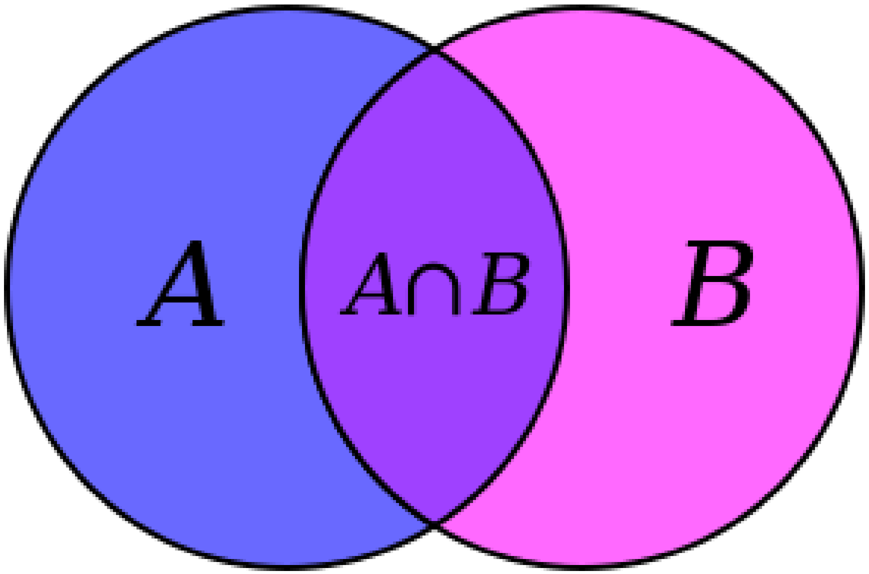
Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Spring 2015
Lecture 9: Set theory



MY MATH TEACHER WAS A BIG BELIEVER IN PROOF BY INTIMIDATION.

- Formal treatment dates from late 19th century
- Direct ties between set theory and logic
- Important foundational language



$\mathbb{N}$ 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, π
$[n]$ is the set $\{1, 2, \ldots, n\}$ when n is a natural number
$\{\} = \varnothing$ is the **empty set**; the *only* set with no elements

EXAMPLES
Are these sets?
$A = \{1, 1\}$
$B = \{1, 3, 2\}$
$C = \{\square, 1\}$
$D = \{\{\}, 17\}$
$E = \{1, 2, 7, \text{cat}, \text{dog}, \varnothing, \alpha\}$

Set membership:
We write $2 \in E$; $3 \notin E$.

- 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

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

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

QUESTIONS

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

- 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: $\boldsymbol{(A = B) \equiv (A \subseteq B) \land (B \subseteq A)}$

building sets from predicates

- The following says "S is the set of all x's where P(x) is true."

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

- The following says "S is the set of those elements of A for which P(x) is true."

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

- "The set of all the real numbers less than one"

$$\{x \in \mathbb{R} : x < 1\}$$

- "The set of all powers of two"

$$\{x \in \mathbb{N} : \exists j\ (x = 2^j)\}$$

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] = ? $A \cup B$

{3} = ? $A \cap C$

{1,2} = ? $A \setminus C$

{1,3} = ? (Can we ever separate 1 and 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, 4, 2, 6}
C = {1, 2, 3, 4}

QUESTIONS

Let S = {1, 2}.

If the universe is A, then $\overline{S}$ is... {3}

If the universe is B, then $\overline{S}$ is... {4, 6}

If the universe is C, then $\overline{S}$ is... {3, 4}

it's Boolean algebra again! (yay…?)

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

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

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

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

- Complement works like $\neg$

$$\overline{A} = \{x : \neg(x \in A)\}$$

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

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

e.g. $\text{Days} = \{M, W, F\}$

$$\begin{aligned}\mathcal{P}(\text{Days}) = \{\, & \varnothing, \\ & \{M\}, \{W\}, \{F\}, \\ & \{M, W\}, \{W, F\}, \{M, F\}, \\ & \{M, W, F\} \quad \}\end{aligned}$$

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

cartesian product

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

$A = \{1, 2\}$ $B = \{a, b, c\}$

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

$A \times \emptyset = \emptyset$

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

de Morgan's laws

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

$x \in \overline{A \cup B} \leftrightarrow \neg(x \in A \vee x \in B)$

$\leftrightarrow (\neg(x \in A) \wedge \neg(x \in B))$

$\leftrightarrow (x \in \bar{A} \wedge x \in \bar{B}) \leftrightarrow x \in \bar{A} \cap \bar{B}$

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

$x \in \overline{A \cap B} \leftrightarrow \neg(x \in A \wedge x \in B)$

$\leftrightarrow (\neg(x \in A) \vee \neg(x \in B))$

$\leftrightarrow (x \in \bar{A} \vee x \in \bar{B})$

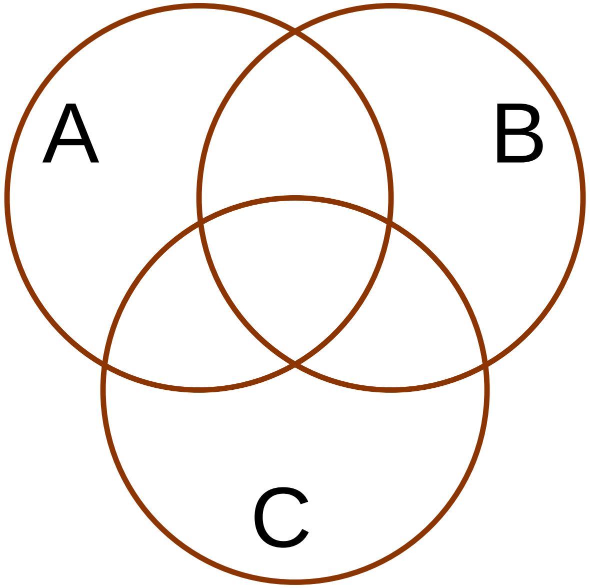
$\leftrightarrow x \in \bar{A} \cup \bar{B}$

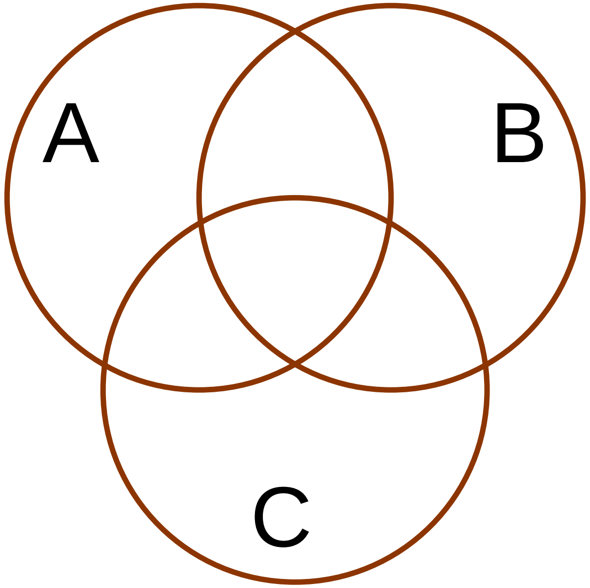
Proof technique:
To show C = D show
$x \in C \rightarrow x \in D$ and
$x \in D \rightarrow x \in C$

distributive laws

just like $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

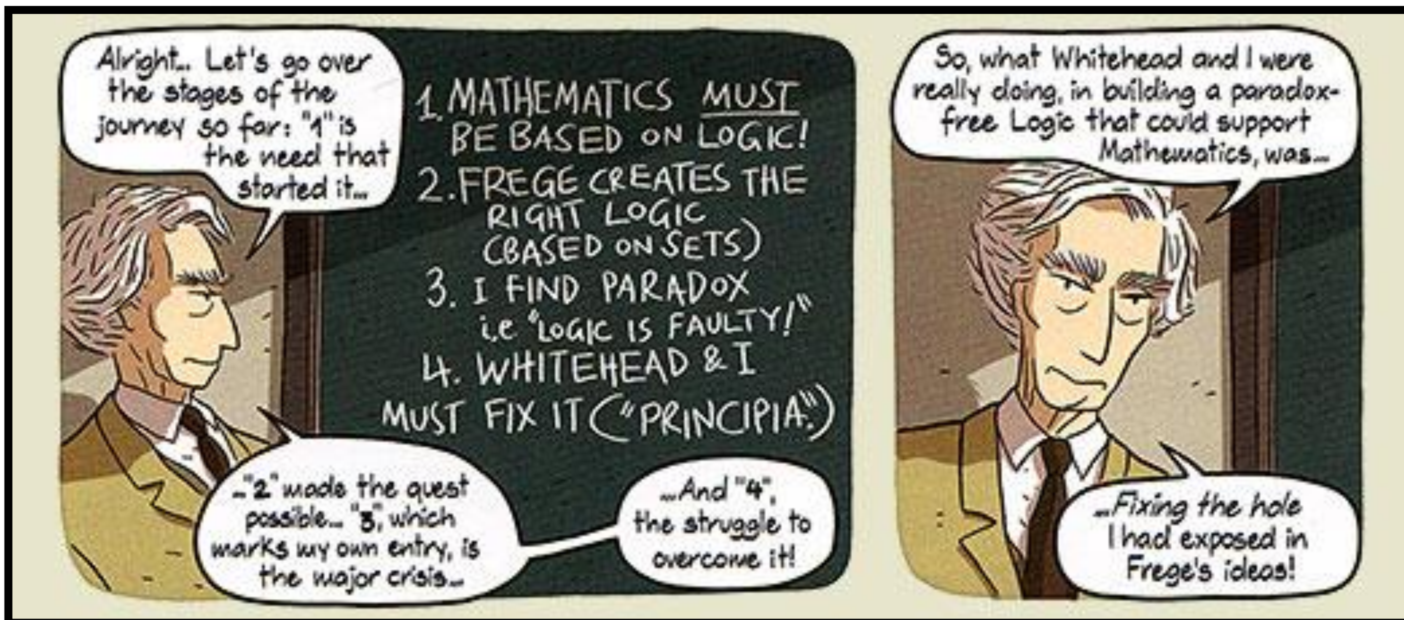
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$





Russell's paradox

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



- Suppose universe U is $\{1,2, \dots, n\}$

- Can represent set $B \subseteq U$ as a vector of bits:

$$b_1 b_2 \cdots b_n \text{ where } \begin{array}{l} b_i = 1 \text{ when } i \in B \\ b_i = 0 \text{ when } i \notin B \end{array}$$

  – 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

$$\begin{array}{rr} & 01101101 \\ \vee & 00110111 \\ \hline & 01111111 \end{array}$$

Java: `z=x|y`

$$\begin{array}{rr} & 00101010 \\ \wedge & 00001111 \\ \hline & 00001010 \end{array}$$

Java: `z=x&y`

$$\begin{array}{rr} & 01101101 \\ \oplus & 00110111 \\ \hline & 01011010 \end{array}$$

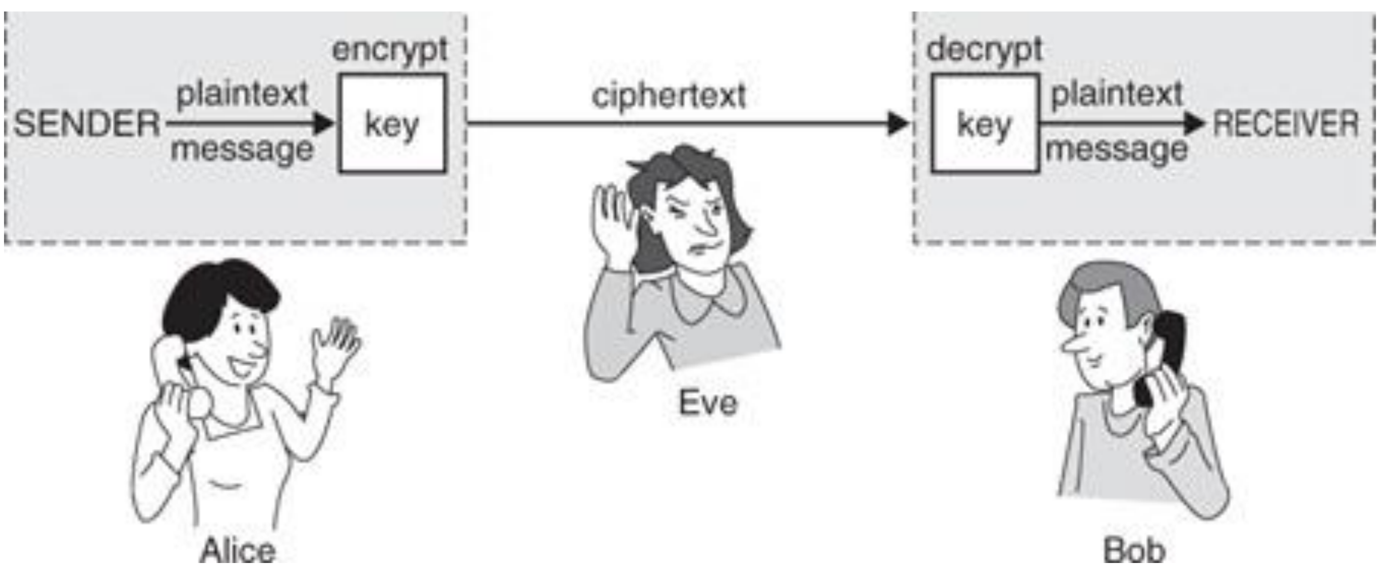
Java: `z=x^y`

a useful identity

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

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.



- 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