CS 173: Discrete Structures

Eric Shaffer
Office Hour: Wed. 1-2, 2215 SC
shaffer1@illinois.edu

Agenda

- Quickly revisiting propositional logic
- What you can do with what you now know
  - Logic
  - Number Theory
- Set Theory
  - Section 2.1 : Definitions and Notation
  - Section 2.2 : Operations on Sets

Revisiting Propositional Logic

- Informally, a "predicate" P(x) is a function
  - It returns a Boolean value (i.e. T or F)
  - The value depends on an input variable(s)
  - It is used with quantifiers
- Example:

"If you don't know where you are going, you will wind up somewhere else."

$\forall x \in People, \neg KnowsWhereGoing(x) \rightarrow EndsUpElsewhere(x)$

- A predicate must take on a TF value
- A propositional variable must take on a TF value
  - e.g. saying Q = "somewhere else" would be wrong

capital

$P(x, y)$

$p \vee q$ ← lower case

Things you can do with predicate logic

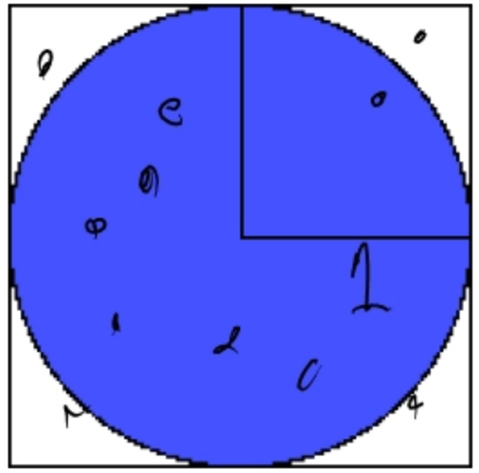
- Build an artificially intelligent super-brain! (maybe)
- "Intelligence is ten million rules."
  - Douglas Lenat CEO of Cycorp

- Cyc™ is an automatic reasoning system consisting of
  - an inference engine
  - a knowledge-base of rules
    - E.g. “All trees are plants”

- "one of the most controversial endeavors of the artificial intelligence history” -- Wikipedia entry

Things you can do with number theory

- Implement a Random Number Generator
  - Lots of uses
    - Cryptography
    - Randomized algorithms
    - Monte Carlo methods



$$\frac{\#\text{ points in circle}}{\#\text{ points}} \approx \frac{\text{area circ}}{\text{area sqr}}$$

$$\approx \frac{\pi}{4}$$

    - Instigating a financial system collapse (maybe)

  - Can you really write a program that generates RNs?

Random Number Generation

- Linear Congruential generators are common
  - Most C/C++ standard library "rand()" implementations
    - "random()" and "rand48()" are usually better if available

- Introduced by D.H. Lehmer (1949)

  Sequence $X_{n+1} = (aX_n + c)$ **mod** m
    - m>0 (usually a prime)
    - 0<a<m
    - 0≤ c < m
    - 0≤ X_0< m
- *How many distinct values can be generated?*

m , the will be in [0, m-1]

Random Number Generation

$X_{n+1} = (aX_n + c) \bmod m$

- How many distinct values can be generated?
- What should we try to maximize?
- Is choosing X_0 important ?

"period" = how many values do you generate before repeating

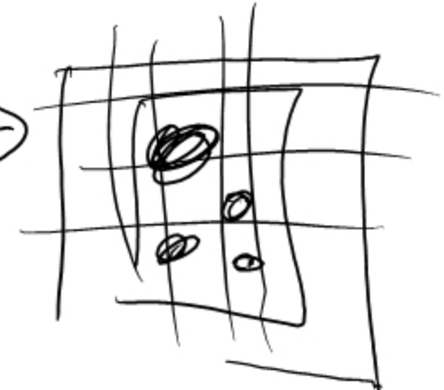
X_0 = "seed"

often
Clock time used for seed

- **US Patent 5732138 - Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system**

Lava lamp

image



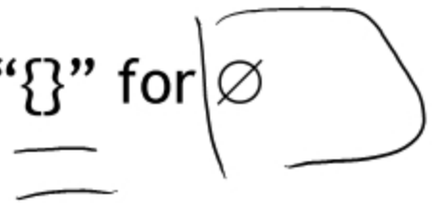
Set Theory - Definitions and notation

A set is an unordered collection of elements.

- Order and repetition are irrelevant
  {1, 1, 2, 3, 3} = {1, 2, 3} since repetition is irrelevant.
  {1, 2, 3} = {3, 2, 1} since sets are unordered.
- Sets can be finite or infinite
  {1, 2, 3, …} is a way we denote an infinite set

- ∅ = {} is the empty set, or the set containing no elements.

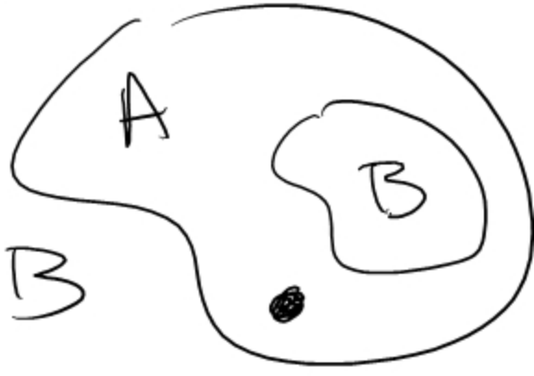
  Note: ∅ ≠ {∅}
  Also, don't use the notation "{}" for ∅



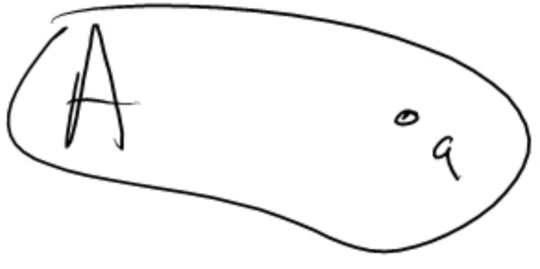
Set Theory - Definitions and notation

$\supset$ $A \supset B$ A proper superset of

$\supseteq$ $A \supseteq B$, A could be $\equiv B$



$\in$ $a \in A$



: and |

↳ "such that" $\{x : x > 0\}$

Set Theory - Definitions and notation

Quiz time:

Is $\{x\} \subseteq \{x\}$? Yes

Is $\{x\} \in \{x,\{x\}\}$? Yes

Is $\{x\} \subseteq \{x,\{x\}\}$? Yes

Is $\{x\} \in \{x\}$? No

Set Theory - Ways to define sets

- Explicitly: {John, Paul, George, Ringo}
- Implicitly: {1,2,3,…}, or {2,3,5,7,11,13,17,…}
- Set builder: { x : x is prime }, { x | x is odd }. In general { x : P(x) is true }, where P(x) is some description of the set.

: and | are read "such that" or "where"

Ex. Let D(x,y) denote "x is divisible by y."

Give another name for

$$\{ x : \forall y ((y > 1) \wedge (y < x)) \rightarrow \neg D(x,y) \}.$$

Primes

Can we use **any** predicate P to define a set S = { x : P(x) }?

Set Theory - Russell's Paradox

Can we use **any** predicate P to define a set
$S = \{ x : P(x) \}$?

Define $S = \{ x : x \text{ is a set where } x \notin x \}$ No!

Then, if $S \in S$, then by defn of S, $S \notin S$.

But, if $S \notin S$, then by defn of S, $S \in S$.

There is a town with a barber who shaves all the people (and only the people) who don't shave themselves.

Who shaves the barber?

Set Theory - Cardinality

If S is finite, then the *cardinality* of S, |S|, is the number of distinct elements in S.

If S = {1,2,3}, |S| = 3.

If S = {3,3,3,3,3}, |S| = 1.

If S = ∅, |S| = 0.

If S = {∅, {∅}, {∅,{∅}}}, |S| = 3.

If S = {0,1,2,3,...}, |S| is infinite. (more on this later)

Set Theory - Power sets

If S is a set, then the *power set* of S is
$2^S = \{ x : x \subseteq S \}$.

aka P(S)

We say, "P(S) is the set of all subsets of S."

If S = {a}, $2^S = \{\emptyset, \{a\}\}$.

If S = {a,b}, $2^S = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$.

If S = ∅, $2^S = \{\emptyset\}$.

If S = {∅,{∅}}, $2^S = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset,\{\emptyset\}\}\}$.

Fact: ~~if S is finite,~~ $|2^S| = 2^{|S|}$. (~~if $|S| = n$,~~ $|2^S| = 2^n$)

$|2^S| = 2^{|S|}$

power set S
2^S or P(S)

$S = \{a\}$

$2^S = \{\emptyset, \{a\}\}$

$S = \{a, b\}$

$2^S = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$

---

if $S = \emptyset$, $2^S = \{\emptyset\}$

Set Theory - Cartesian Product

The *Cartesian Product* of two sets A and B is:

$$A \times B = \{ \langle a,b \rangle : a \in A \wedge b \in B \}$$

ordered pairs

If A = {Charlie, Lucy, Linus}, and
B = {Brown, VanPelt}, then

A x B = {<Charlie, Brown>, <Lucy, Brown>,
<Linus, Brown>, <Charlie, VanPelt>,
<Lucy, VanPelt>, <Linus, VanPelt>}

n-tuple

$A_1 \times A_2 \times \ldots \times A_n = \{\langle a_1, a_2, \ldots, a_n \rangle : a_1 \in A_1, a_2 \in A_2, a_n \in A_n\}$

A,B finite → |AxB| = ?

a) AxB
b) |A|+|B|
c) |A+B|
d) |A||B|

$|A \times B| = |A| \, |B|$

$A = \{1, 2\}$

$B = \{a, b\}$

$A \times B =$

$\{ \langle 1,a \rangle, \langle 1,b \rangle, \langle 2,a \rangle, \langle 2,b \rangle \}$

$C = \{9, 10\}$

$A \times B \times C =$

$\{ \langle 1,a,9 \rangle, \langle 1,a,10 \rangle, \ldots$

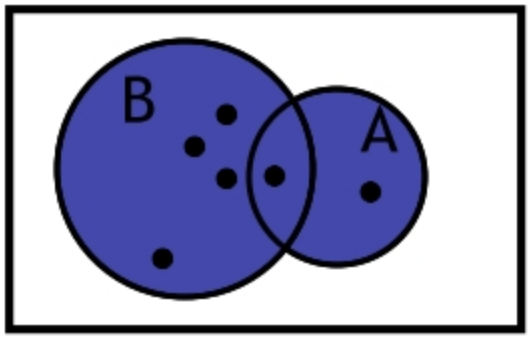
Set Theory - Operators

The *union* of two sets A and B is:

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

If A = {Charlie, Lucy, Linus}, and
B = {Lucy, Desi}, then

$A \cup B$ = {Charlie, Lucy, Linus, Desi}



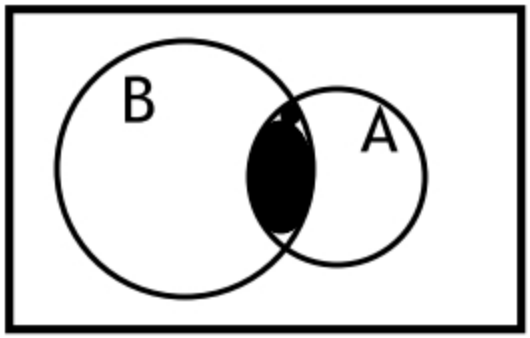
Set Theory - Operators

The *intersection* of two sets A and B is:

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

If A = {Charlie, Lucy, Linus}, and
B = {Lucy, Desi}, then

$A \cap B$ = {Lucy}



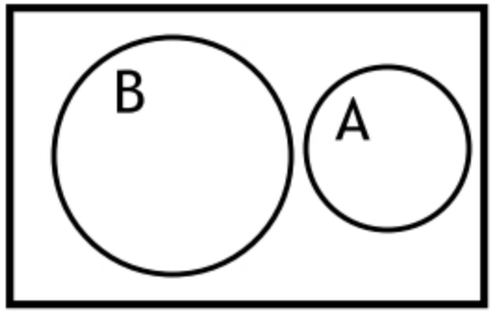
Set Theory - Operators

The *intersection* of two sets A and B is:

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

If A = {x : x is a US president}, and
B = {x : x is in this room}, then

$A \cap B$ = {x : x is a US president in this room} = $\varnothing$ ← A and B are disjoint



Sets whose intersection is empty are called *disjoint* sets

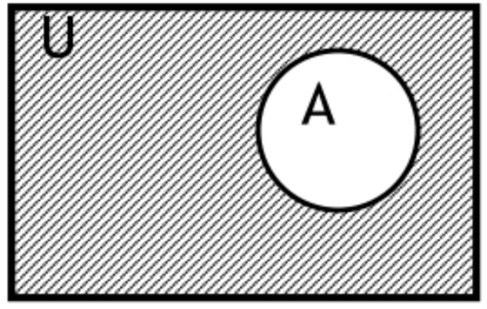
Set Theory - Operators

The *complement* of a set A is:

$$\overline{A} = \{ x : x \notin A \}$$

If A = {x : x is bored}, then

$\overline{A}$ = {x : x is not bored} = $\varnothing$



$\overline{\varnothing} = U$ and $\overline{U} = \varnothing$

U = "universe"

Let U = $\mathbb{N}$

A = {0, 1, 2}

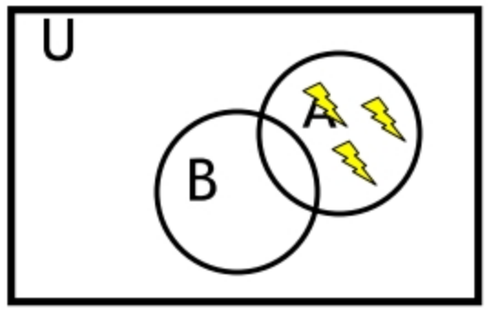
$\overline{A}$ = {3, 4, ...}

$\overline{\varnothing} = U$

$\overline{U} = \varnothing$

Set Theory - Operators

The *set difference*, A - B, is:



$$A - B = \{ x : x \in A \wedge x \notin B \}$$

$$A - B = A \cap \overline{B}$$

$A = \{1, 2, 3\}$

$B = \{2\}$

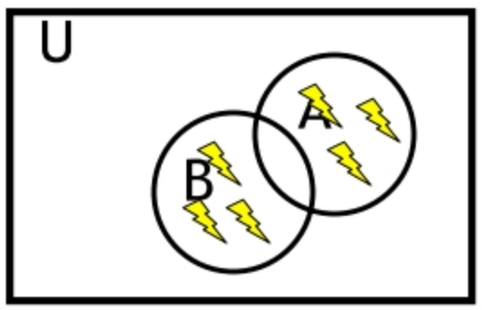
$A - B = \{1, 3\}$

Set Theory - Operators

The *symmetric difference*, $A \oplus B$, is:

$$A \oplus B = \{ x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

$$= (A - B) \cup (B - A)$$



$A = \{1, 2, 3\}$

$B = \{3, 4\}$

$A \oplus B =$

$\{1, 2, 4\}$