ECS 20 — Lecture 7 — Fall 2013 —18 Oct 2013

Phil Rogaway

Today: o **Sets** and
- o Writing sets
- o Some operations on sets
- o Some important sets for math and CS

S = {dog, cat}. Order we write elements (points) in a set doesn't matter.
= {cat, dog}. Repetitions don't matter, either:
= {cat, dog, cat}.

$S = \emptyset$

Often many ways to write a set

$A = \{2i+1 : i \in \mathbf{Z}\}$
$= \{\ldots,-5,-3,-1, 1, 3, 5,\ldots\}$
$= \{x : x$ is an odd integer$\}$
$= \{n : n \in \mathbf{Z}$ and $\neg (\exists j \in \mathbf{Z})(2j=n)\}$

Or

Let P be the set of prime numbers.
$P = \{n : n$ *is* a prime number$\}$
$P = \{n \in \mathbf{N} : i \mid n \implies i \in \{-n,-1,1,n\}\}$
$P = \{2,3,5,7,11,\ldots\}$

Can a set contain a set? **Sure**.
Can a set contain the emptyset? **Sure**
$S = \{\mathbf{N}, \{2,3\}, [0,1]\}$.
$S = \{ \emptyset, \{\emptyset\}, \{\{ \emptyset\}\} \}$

Naïve set theory, where we describe sets with natural language, can sometime run into trouble.
Can a set contain itself? **No**
Can a set contain "everything"? **No**
Russell's paradox: Let $R = \{ x \mid x \notin x\}$ *Problem*: is $R \in R$ iff $R \notin R$?

Def: $S = T$ iff $x \in S \leftrightarrow x \in T$

Def: $S \subseteq T$ if $x \in S \rightarrow x \in T$

{a, b} ⊆{a,b,c} YES
{a, b} ⊆{a,b} YES

{a b} $\subseteq${a,d,e}   NO
$\emptyset \subseteq$ {a,b,c}   YES (explain)
{$\emptyset$} $\subseteq$ {a,b,c}   NO
{$\emptyset$} $\subseteq$ {{$\emptyset$}}   YES
T/F: for all S, $\emptyset \subseteq$ S: True

Some important sets for math and computer science
N = {1, 2, 3, ...} // some books include 0, some don't
R = {*x*: *x* is a real number}
Z = {...,-2,-1, 0, 1, 2, ,...}
Q = {*m*/*n*:   *m*, *n*\in **Z**, *n*≠ 0}

[*a*.. *b*] integers between *a* and *b*, inclusive.
[*a*, *b*] reals between *a* and *b*, inclusive

[1..*N*] = {1, 2, …, *N*}
[*N*] = $\mathbf{Z}_N$ = {0, 1, …, *N*-1}

Sometimes sets come with operations on them, these operations satisfying simple algebraic properties.

Example:
Group This is a set A and an operation * where:
1) (x*y)*z = x*(y*z);
2) there exists an element 1 in A such that *x**1=1**x* = *x*;
3) for every element *x* there is an element *y* such that *x***y* = 1 = *y***x*]

But let me emphasize that a set, all by itself, does **not** have operations defined on its elements.

- Ask questions about making **N**, **R**, **Z** into groups.
- Later: ask questions about making BITS, BYTES, WORDS32 into a group, by either XOR and Modular addition operation

For computers, important sets correspond to those things that our architectures natively manipulate:

BITS = {0,1}
BYTES = $\{0,1\}^8$ Signed, unsigned
WORDS32 = $\{0,1\}^{32}$ Signed, unsigned
WORDS64 = $\{0,1\}^{64}$ Signed, unsigned
IEEEFLOAT64 = $\{0,1\}^{64}$ = representing exponents -1022 .. 1023 (about 16 digits of accuracy)
Weirder than you may think

- **sign**, **significand** (=coefficient), **exponent** $(-1)^{\text{sign}} \cdot$ *signficand*$\cdot\, 2^{exponent}$EEF
- **+ ∞** and **−∞**
- NaN (of various kinds)
- Zero can be +0 or −0

William Kahan. A primary architect of the IEEE 754 floating-point standard

Or particular language:
 The set of all valid C programs
 The set of valid URLs
 The set of valid http programs

$|S|$ = the number of element in S if S is finite, ∞ otherwise

$A = \{\{a\}, b, \emptyset\}$. $|A| = 3$
A = $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ $|A|$=3.

UNION

A $\cup$B = $\{x: x\in A$ or $x\in B\}$ // not really very rigorous:
{x : blah} before the colon, the universe should be clear, with
what comes after a narrowing of that. Books don't all stick to this, but that's what learned!

{dog, cat} $\cup$ {cat, fish}
$\{a,b\} \cup \{\emptyset,a\} = \{a,b, \emptyset\}$

$A \cup \emptyset = A$

Can union up infinitely many things

$\bigcup_{n\in \mathbf{N}} [0,n] = \mathbf{R}$
∪_{i∈I} A_i eg, \cup{$i\in$**N**} {2i–1} = the set of odd positive number

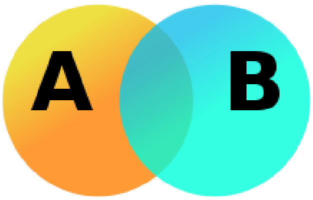
∪_{$a\in N$} $\{a^i: i\in \mathbf{N}\}$
"powers of integers"

INTERSECTION

$\{1,2,3\} \cap \{2,5,8\} = \{2\}$
$\{1,2,3\} \cap \{4,5,8\} = \emptyset$
$\{1,2,3\} \cap \emptyset = \emptyset$ **True**/False
$S \cap \emptyset = \emptyset$ **True**/False
Can intersect infinitely many things, too:

$\bigcap_{n \in \mathbf{N}} \ [0, n] = \{0\}$

Venn Diagrams



Set Difference

A \ B or A – B

Symmetric Difference

A ⊕ B

Algebra of sets

Commutative laws:

- $A \cup B = B \cup A$
- $A \cap B = B \cap A$

Associative laws:

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

Distributive laws:

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

Proof: $x \in A \cup (B \cap C)$ means

$(x \in A) \vee ((x \in B) \wedge (x \in C))$ But $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$. So

$= ((x \in A) \vee (x \in B)) \wedge (x \in A) \vee ((x \in C))$

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

Identity laws:

- $A \cup \varnothing = A$
- $A \cap U = A$

Complement laws:

- $A \cup A^C = U$
- $A \cap A^C = \varnothing$
-

idempotent laws:

- $A \cup A = A$
- $A \cap A = A$

domination laws:

- $A \cup U = U$
- $A \cap \varnothing = \varnothing$

absorption laws:

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

double complement or Involution law:

- $(A^C)^C = A$

complement laws for the universal set and the empty set:

- $\varnothing^C = U$
- $U^C = \varnothing$

De Morgan's laws:

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

Proof (of first claim): $x \in (A \cup B)^c$

iff $\neg (x \in (A \cup B))$

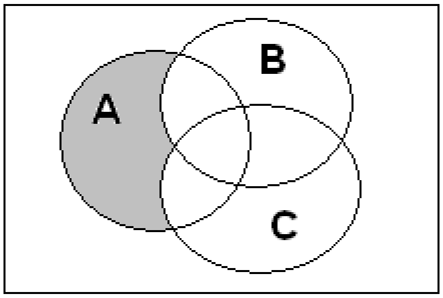
iff $\neg (x \in A \lor x \in B)$

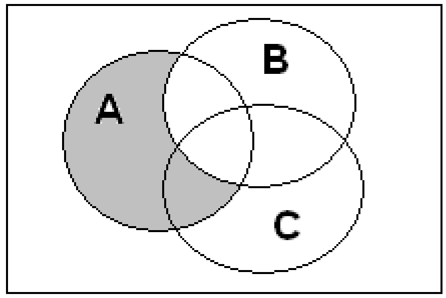
iff $\neg (x \in A) \land \neg (x \in B)$

iff $x \in A^c \land x \in B^c$

Be careful!!

$$(A \setminus B) \setminus C \stackrel{?}{=} A \setminus (B \setminus C)$$





Cartesian Product (= Cross product) ← Did get here, continue next time

A × B = {(a,b): A∈A, B∈ B}

$\mathbf{R}^2$ points in the plane
An array of chessmen might be represented by BYTES^{64}

Power Set

$\mathcal{P}$ – Power set operator, unary operator (takes 1 input). ***P***(x) is the "set of all subsets of x"
$\mathcal{P}(X) = \{A: A \subseteq X\}$

Example: X = {a, b, c}
Example:
Variant notation: $\mathcal{P}(X) = 2^X$

Notation is suggestive of size –
For X finite, $|\mathcal{P}(X)| = 2^{|X|}$

…