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 doesn't matter. Don't write elements (points) in a set more than once. $= \{cat, dog\}$. Repetitions don't matter, either: $= \{cat, dog, cat\}$

$S = \emptyset$

Often many ways to write a set

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

Or

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

Can a set contain a set? **Sure**.
Can a set contain the empty set? **Sure**
$S = \{\mathbf{N}, \emptyset\}$
$S = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$

Naïve set theory: 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 $x \in S \Rightarrow x \in T$

$\{a, b\} \subseteq \{a, b, c\}$ TRUE
$\{a, b\} \subseteq \{a, b\}$ TRUE

{a, b} Ì {a, d, e} NO
Å Ì {a, b, c} YES (explain)
{Å} Ì {a, b, c} NO
{Å} Ì { Å } YES
T/F: for all S, Å Ì 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* ¹ 0}

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

[1..*N*] = {1, 2, ..., *N*}
[*N*] = 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) For all *x*, *y*, *z* in A, (*x***y*)**z* = *x**(*y***z*)
2) There exists an element 1 in A such that 1**x* = *x* = *x**1;
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, BYTE, WORD into a group, by either XOR and modular addition operation

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

BITS = {0, 1}
BYTE = {0, 1, ..., 255} = Signed, unsigned
WORD = {0, 1, ..., 65535} = Signed, unsigned
DWORD = {0, 1, ..., 4294967295} = Signed, unsigned
FLOAT = {0, 1, ..., 4294967295} = representing exponents -20 (about 6 digits of accuracy) in order than you may think

- **sign**, **significand** (coefficient), **exponent** (-1)^sign Ö *signficand* Ö 2^exponent
- **+** Ð and Ð
- NaN (of various kinds)
- Zero can be 0 or - 0

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

C 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, Å } |A| = 3
A = { Å , { Å }, { Å } | A| = 3

UNION

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

{dog, cat} Ç {cat, fish}
{a, b} Ç { Å , a} = { a, b, Å }

A Ç Å = A

Can union up infinitely many things

Ç n Í N [n] = 0 R,

Ç{ _ Í } Ai_ eg, \ cp{ i Í N}{2 i - 1} = the set of odd positive number

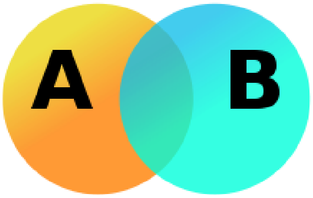
Ç{ _ a Í N}{ a^i : i Í N}
"powers of integers"

INTERSECTION

Æ
Æ = Å
Æ Å = Å True/False
S Æ Å = Å True/False
Can intersect infinitely many things, too:

Æ$_{n}$Í N n] ⇐ [0 ,

Venn Diagrams



Set Difference

A \ B or A – B

Symmetric Difference

A Ä 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* Í A Ç (B Æ C) means
(*x* Í A) Ù (*x* Í B) Ø (*x* Í C) But P Ù (Q Ø R) ⇐ (P Ù Q) Ø (P Ù R). So
⇐ (*x* Í A) Ù *x* Í (B) Ø (*x* Í A) Ù (*x* Í C)
⇐ (A Ç B) Æ (A Ç 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:

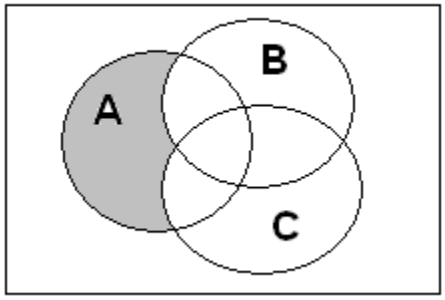
- $\varnothing^C = U$
- $U^C = \varnothing$

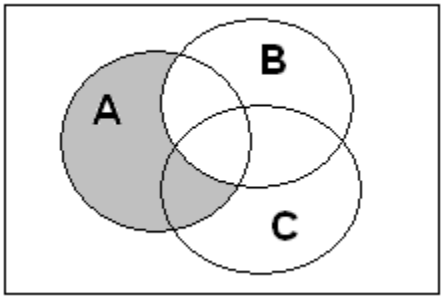
De Morgan's laws:

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

Proof (of first claim) $x \in (A \cap B)^c$
iff $x \notin (A \cap B)$
iff $x \notin A \text{ Ù } x \in B$
iff $x \notin A) \text{ Ø } x \notin B$
iff $x \in A^c \text{ Ø } x \in B^c$

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





Cartesian Product (= Cross product) ă Ddget here, continue next time

A ³ B = {(a,b) A Í A, B Í B}

R^2 points in the plane
An array of classmen might be represented by BYTE 6

Power Set

P – Power set operator, unary operator (takes 1 input) $P(x)$ is the "set of all subsets of x"

P (*X*) = { *A*: *A* Ì *X*}

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

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

...