CS 173: Discrete Structures

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

Agenda

- What you should know about Number Theory
- Review pseudo-code conventions (Appendix 3)
- Introduction to Set Theory (Section 2.1)
- Quiz

But first…a word about number representations and bugs

~~Great~~ Moments in Software Engineering

- Ariane 5 is a European launch system designed to deliver payloads into low Earth orbit.
- Ariane 5's first test flight on 4 June 1996 failed, with the rocket self-destructing 37 seconds after launch because of a malfunction in the control software. A data conversion from 64-bit floating point to 16-bit signed integer value caused a processor trap. The floating point number had a value too large to be represented by a 16-bit signed integer. Efficiency considerations had led to the disabling of the software handler (in Ada code) for this trap.
- The loss of more than US$370 million makes this one of the most expensive computer bugs in history.

Number Systems
Reverse Conversion

- Conversion of integer *n* to base *b*
- Let $a_k, a_{k-1}, \ldots, a_0$ be the "digits" of the base b number

Procedure convert(n,b:integers)
$i := 0$
while $(n > 0)$
begin
$a_i := n \bmod b$
$n := n \div b$
$i := i+1$
end

Number Theory things you should know

- $a|b$
- division algorithm
- mod function
- congruence mod *m*
  - definition
  - Thm: $a \equiv b$ mod m iff $a = b + km$
- GCD and LCM
- Fundamental Theorem of Arithmetic
- Euclidean Algorithm
- number representations and conversions

Pseudo-code

- You should understand the pseudo-code used in the book
- Read Appendix 3 in the textbook
- It's a very, very simple imperative language
- "Procedure" is like a function of method
  - Includes a list of input variables and their types
- Conditionals: "if…then…else"
- Assignment is ":="
- Testing equality "="
- Blocks of code "begin … end"
- Loops
  - "for <variable> := <initial value> to <final value>
  - In final iteration, variable will be assigned final value
    - E.g. "for i:=0 to 100" will iterate __101__ times

a := 5

if (a = 3) then

Pseudo-code

- while loops

while <condition>
    <statement>

-- or --

while <condition>
begin
    <statement**S**>
end

Pseudo-code

- Some procedures operate on "Lists"
  - You saw an example in HW 0
- For this class, a list is
  - An **ordered** set of values or variables
  - **procedure** *some_sort* ($l_1,\ldots,l_n$: integers)
  - "interchange l_1 and l_2" is used to reorder list elements
  - the text treats them like arrays

- Comments are in braces: "{this is a comment}"

2, 3, 5

3, 2, 5

Set Theory - Definitions and notation

A set is an unordered collection of elements.

Some examples:

{1, 2, 3} is the set containing "1" and "2" and "3."
{1, 1, 2, 3, 3} = {1, 2, 3} since repetition is irrelevant.
{1, 2, 3} = {3, 2, 1} since sets are unordered.
{1, 2, 3, …} is a way we denote an infinite set (in this case, the natural numbers).
$\emptyset$ = {} is the empty set, or the set containing no elements.

Note: $\emptyset \neq \{\emptyset\}$

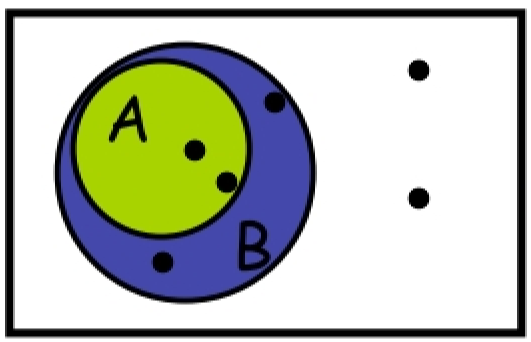
$\emptyset \neq \{\emptyset\}$

Set Theory - Definitions and notation

$x \in S$ means "x is an element of set S."
$x \notin S$ means "x is not an element of set S."

$A \subseteq B$ means "A is a subset of B."

or, "B contains A."
or, "every element of A is also in B."
or, $\forall x\ ((x \in A) \rightarrow (x \in B))$.



Venn Diagram

Set Theory - Definitions and notation

$A \subseteq B$ means "A is a subset of B."
$A \supseteq B$ means "A is a superset of B."

$A = B$ if and only if A and B have exactly the same elements.

iff, $A \subseteq B$ and $B \subseteq A$
iff, $A \subseteq B$ and $A \supseteq B$
iff, $\forall x \, ((x \in A) \leftrightarrow (x \in B))$.

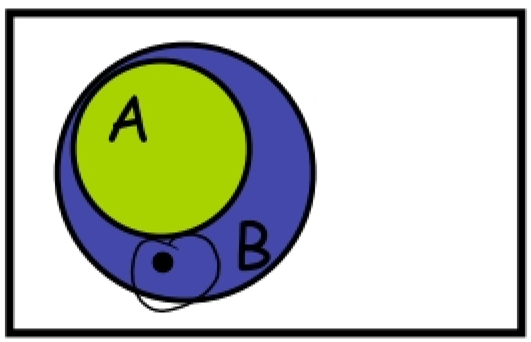
So to show equality of sets A and B, show:

- $A \subseteq B$
- $B \subseteq A$

Set Theory - Definitions and notation

$A \subset B$ means "A is a proper subset of B."

- $A \subseteq B$, and $A \neq B$.
- $\forall x\,((x \in A) \rightarrow (x \in B)) \wedge \neg\forall x\,((x \in B) \rightarrow (x \in A))$
- $\forall x\,((x \in A) \rightarrow (x \in B)) \wedge \exists x\,\neg(\neg(x \in B) \vee (x \in A))$
- $\forall x\,((x \in A) \rightarrow (x \in B)) \wedge \exists x\,((x \in B) \wedge \neg(x \in A))$
- $\forall x\,((x \in A) \rightarrow (x \in B)) \wedge \exists x\,((x \in B) \wedge (x \notin A))$



Set Theory - Definitions and notation

Quick examples:

- $\{1,2,3\} \subseteq \{1,2,3,4,5\}$
- $\{1,2,3\} \subset \{1,2,3,4,5\}$

Is $\emptyset \subseteq \{1,2,3\}$?

Yes! $\forall x\ (x \in \emptyset) \rightarrow (x \in \{1,2,3\})$ Vacuously

~~holds, because $(x \in \emptyset)$ is false.~~

Is $\emptyset \in \{1,2,3\}$? No

Is $\emptyset \subseteq \{\emptyset,1,2,3\}$? Yes!

Is $\emptyset \in \{\emptyset,1,2,3\}$? Yes!

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"

": or |" "such that"

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 $S = \{a\}$, $2^S = \{\varnothing, \{a\}\}$.

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

If $S = \varnothing$, $2^S = \{\varnothing\}$.

If $S = \{\varnothing,\{\varnothing\}\}$, $2^S = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing,\{\varnothing\}\}\}$.

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

Set Theory - Cartesian Product

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

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

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>}

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

A,B finite → |AxB| = ?

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