Discrete Mathematical Structures
CS 3233 Lecture Eight

Prof. William Winsborough
September 25, 2007

Business

- Recall homework 5 due Thursday 9/27:
  - Section 1.5: 4, 8, 16
  - Section 1.6: 2 (natural-language proof), 12, 18
  - Section 1.7: 4, 6, 8
  - Section 2.1: 2a, 2b, 6, 8, 18
- Read section 2.3 for Thursday 9/27
- Homework 6 due **Tuesday** 10/2
  - Section 2.2: 2, 6, 10, 20, 26a
  - Section 2.3: 4, 10, 14, 16, 38
- **Midterm 1** will be in class Thursday 10/4 per syllabus
- Class and recitation Tuesday 10/2 will be devoted entirely to answering your questions, reviewing material, and going over homework problems
- I will post a **mock exam** by this weekend

Universal Modus Ponens

- Combines propositional modus ponens with universal instantiation:

$$\begin{array}{l} \forall x.\Phi(x)\rightarrow\Psi(x) \\ \Phi(c) \\ \hline \Psi(c) \end{array}$$

- Practice problems: 14d, p73; 11, p85

Sets

- $s\in S$ means s is an *element* of set S
- Given sets A and B,
  - $A \subseteq B$ means A is a *subset* of B
    - This means $x\in A$ implies $x\in B$
  - $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$
  - $A\subset B$ means A is a *proper subset* of B
    - $A \neq B$
  - $A = \{ a_1, a_2, \ldots \}$ means that A is enumerated by the sequence $a_1, a_2, \ldots$
- *Set comprehension:* the set of values that satisfy a given property
  - *E.g.,* EvenInts = $\{ x \mid \exists z\in Z.x=2z \}$

Basic Operators

- Empty set
  - $\emptyset = \{ \}$
- Union
  - $A\cup B = \{ x \mid x\in A \vee x\in B \}$
- Intersection
  - $A\cap B = \{ x \mid x\in A \wedge x\in B \}$
- Cartesian product:
  - $AxB = \{ (a,b) \mid a\in A \wedge b\in B \}$

Identities and Big Unions, Intersections

- Set Identities
  - Review Table 1, page 124
  - Review Example 11, page 125
- Given a collection of sets $A_1, A_2, \cdots, A_n$
  - $\bigcup_{1\leq i\leq n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$
  - $\bigcap_{1\leq i\leq n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$

Introduction to Functions

- Given sets A and B, a *function from* A *to* B is an assignment of exactly one element of B to each element of A
- For a ∈ A, we write f(a) = b if b ∈ B is the unique element associated with a by f
- We write f : A → B to indicate that f is a function from A to B
  - A → B is called the *type* of f

Function Graphs

- This is a different usage of "graph" than either of these:
  - The plot of f(x) on the Cartesian plane
  - A set of nodes and a set of edges
- Definition
  - Given a function f : A → B, the *graph* of f is the set of ordered pairs {(a,b) | a ∈ A and b = f(a)}
- Given two sets, A and B, A *binary relation* r between A and B is a subset of AxB
- Formally speaking, a function **is** its graph
  - Thus, f is a subset of A x B in which each element of A occurs exactly once

Quick Review

- Given two sets, A and B, A *binary relation* r between A and B is a subset of AxB
- What is required for r to be a function?
- If r is a function, then
  - What is required for it to be injective?
  - What is required for it to be surjective?

Terminology

- Let f : A → B
  - We say f *maps* A to B
  - A is the *domain* of f
  - B is the *codomain* of f
  - If f(a) = b,
    - b is the *image* of a and
    - a is the *pre-image* of b
  - If S ⊆ A, the *image* of S is {f(s) | s ∈ S} and is denoted by f(S)
  - f(A) = {f(a) | a ∈ A} is called the *range* of f

Examples

- Successor function
  - s : N → N
  - s(n) = n+1
- Floor
  - floor : R → Z
  - floor(x) = greatest integer less than x
- Square root
  - √ : R → C
  - The square root of a real is a complex number
- Truth assignment
  - σ : $\mathcal{V}$ → {true, false}

Injections and Surjections

- f : A → B is *one-to-one*, or *injective*, if and only if f(x) = f(y) implies x = y for all x, y ∈ A
  - $f : A \xrightarrow{1-1} B$
  - ∀x∀y(f(x) = f(y) → x = y)
  - Equivalently, ∀x∀y(x ≠ y → f(x) ≠ f(y))
  - f is called an *injection*
- f : A → B is *onto,* or *surjective*, if for every b ∈ B, there is an a ∈ A such that f(a) = b
  - f is *a function of* A *onto* B
  - $f : A \xrightarrow{onto} B$
  - ∀y∃x(f(x) = y)
  - f is called a *surjection*

More Examples

- Injective and/or surjective?
  - Square
    - f : Z → Z
    - $f(x) = x^2$
  - Double
    - twice : Z → Z
    - twice(x) = 2x
  - Absolute value
    - |·| : Z → N
    - $|x| = \begin{cases} x \text{ if } 0 \le x; \\ -x, \text{ otherwise} \end{cases}$

Still More Examples

- Injective and/or surjective?
  - Integer successor
    - zs : Z → Z
    - zs(n) = n+1
  - Mapping of 32-bit words to Z
  - Successor in Z_3 = {0, 1, 2}
    - s(0) = 1
    - s(1) = 2
    - s(2) = 0

Bijections

- If f : A → B is injective and surjective, it is *bijective*
  - f is called a *one-to-one correspondence,* or a *bijection*

Compositions

- Definition
  - Given g : A → B and f : B → C, the composition of f and g, f∘g : A → C, is defined by f∘g(a) = f(g(a))
  - Note that no special properties of f and g are required for f∘g to be defined.
    - For instance, f and g need not be injective, surjective, or bijective
    - However, if f and g have special properties, it often follows that f∘g special properties as well
    - Study hint: think through these relationships

Function Inverses

- Theorem: Given $f : A \overset{\text{1-1}}{\underset{\text{onto}}{\to}} B$, every b ∈ B has a unique pre-image a ∈ A
- This justifies the following definition: Given $f : A \overset{\text{1-1}}{\underset{\text{onto}}{\to}} B$
  - f^{-1} : B → A is the *inverse* of f
  - $f^{-1}(b) = a$ iff f(a) = b

Bijections and cardinality

- Sets A and B are *equinumerous* (meaning they have the same cardinality) iff there is a one-to-one correspondence between them
  - Notice that this defines a binary relation over sets
  - Contains the ordered pairs of sets between which there exists a one-to-one correspondence
- Pretty clear for finite sets

Equinumerous Infinite Sets

- N and Z have the same cardinality
  - $f : N \to Z$
  - $f(n) = \begin{cases} 0, & \text{if } n = 0 \\ n/2, & \text{if } n \text{ is even} \\ -(n-1)/2, & \text{if } n \text{ is odd} \end{cases}$
  - Note, f is a bijection
    - Use case analysis to show f is injective based on whether x and y are odd or even
- Show N and Z^+ are equinumerous

Countability

- Definition
  - A set A is *countable* if it is finite or it is equinumerous to Z^+
  - Otherwise, A is *uncountable*
- Theorem: Q^+, the set of positive rationals, is countable

Uncountability of the Reals

- Theorem
  - R, the set of real numbers, is uncountable
- Proof
  - Uses Georg Cantor's *diagonalization argument*
  - Outline
    - Assume for contradiction that there is a one-to-one correspondence, f, between N and the real interval [0,1]
    - Use f to construct a real in [0,1] that has no preimage under f
    - Idea: for each decimal place, n, in the representation of the constructed value, choose a decimal different from the n^{th} place of f(n)
    - The fact that the constructed value differs from each value assumed by f shows that f is not onto, giving the desired contradiction

Conclusion

- So the cardinalities of N, Z, and Q are all the same
- But the cardinality of R is different