Discrete Mathematical Structures
CS 3233 Lecture Fourteen

Prof. William Winsborough

September 21, 2005

Business

- Homework assignment 3 is due tomorrow by 2 at my office
- Lecture schedule:
  - No lecture next week (9/26-30)
  - Meet with TA during lecture time ALL the following week (10/3-7)
- Questions??
- Outline for today
  - Composition of function and its inverse is identity
  - Cover two remaining slides from make up lecture
  - Revisit writing formulas stating that exactly one and exactly two elements of universe satisfy an arbitrary, given formula
  - Start section 2.1

Function Inverses

- Theorem: Given $f : A \xrightarrow[\text{onto}]{\text{1-1}} B$, every $b \in B$ has a unique pre-image $a \in A$
- This justifies the following definition: Given

  $f : A \xrightarrow[\text{onto}]{\text{1-1}} B$
  - $f^{-1} : B \to A$ is the *inverse of* f
  - $f^{-1}(b) = a$ iff $f(a) = b$

Compositions

- Definition
  - Given $g : A \rightarrow B$ and $f : B \rightarrow C$, the composition of f and g, $f \circ g : A \rightarrow C$, is defined by
    $f \circ g(a) = f(g(a))$
  - Note that no special properties of f and g are required for $f \circ g$ 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 $f \circ g$ special properties as well
    - Study hint: think through these relationships

Identity Function

- Given any set A, the identity function on A, $\imath : A \rightarrow A$, is defined by $\imath(a) = a$ for all $a \in A$
- Theorem
  - Given any two sets A and B such that there exists a one-to-one correspondence $f : A \rightarrow B$, $f^{-1} \circ f : A \rightarrow A$ and $f \circ f^{-1} : B \rightarrow B$ are the identity functions on A and B respecitvely

Exercise 35, Section 3.2

- Theorem: If A is an uncountable set and A is a subset of B, then B is uncountable
- Proof:
  - Suppose B is countable
  - This means there is a sequence that enumerates B
  - A sequence that enumerates A can be constructed by dropping the elements of B – A, yielding the desired contradiction

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 the real interval [0,1] is enumerated by $\{a_n\}$
    - Use $\{a_n\}$ to construct a real in [0,1] that does not occur in $\{a_n\}$
    - Idea: for each decimal place, n, in the representation of the constructed value, choose a decimal different from the n^{th} place of a_n
    - The fact that the constructed value differs from each value a_n shows that $\{a_n\}$ does not enumerate [0,1]
    - Now use Exercise 35 to complete the proof that R is uncountable

Exactly One, Two

- Construct a formula that is true just in case p(x) holds for exactly one value of x in the universe of discourse
- Do same for two values holding

Algorithms

- Read section 2.1
- Definition
  - An *algorithm* is a finite collection of precise instructions for performing a computation to solve a problem
  - Input and output values are elements of specified sets
- Desirable characteristics:
  - Definiteness: Steps are precisely defined
    - To be really precise, must use a formal *computational model,* such as a Turing machine or the lambda calculus
  - Effectiveness: It must be possible to perform each step using a bounded amount of time and storage space
    - Bounded means there is an amount of time that is always sufficient
  - Correctness, Termination, Generality

Examples

- Finding maximum value in an input sequence of integers
- Searching: Determine whether a given value is contained in an input sequence of integers