

Discrete Mathematical Structures
CS 3233 Lecture Eight

Prof. William Winsborough
September 19, 2006

Business

- Read Sections 2.4 for Thursday
- Recall **Homework Four**
Due Tuesday September 26:
 - Section 2.3: 4, 10, 14, 16, 38
 - Section 2.4: 4, 8
- Questions???

19 September 2006

Winsborough CS 3233 Lecture 8

2

Rules of Inference for Universally Quantified Statements

- Universal instantiation

$$\frac{\forall x. p(x)}{p(c)} \quad \text{Holds for any } c$$

- Universal generalization

$$\frac{p(c)}{\forall x. p(x)} \quad \text{Must show } p(c) \text{ for arbitrary } c$$

- Show: If $p(c)$ and $\forall x. p(x) \rightarrow q(x)$ then $q(c)$

19 September 2006

Winsborough CS 3233 Lecture 8

3

Rules of Inference for Existentially Quantified Statements

- Existential instantiation

$$\frac{\exists x. p(x)}{p(c)}$$

- c must be a new name (constant) that does not appear earlier in the proof

- Existential generalization

$$\frac{p(c)}{\exists x. p(x)}$$

- c can be any name

19 September 2006

Winsborough CS 3233 Lecture 8

4

Using Rules of Inference for Quantified Statements

- Problems 14 and 15, p.73
- We won't always be so meticulous about identifying exactly which rules of inference are being used
 - But it's important to understand the fundamentals of how proofs can be constructed

19 September 2006

Winsborough CS 3233 Lecture 8

5

Identities and Big Unions, Intersections

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

19 September 2006

Winsborough CS 3233 Lecture 8

6

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 $a \in A$, we write $f(a) = b$ if $b \in B$ is the unique element associated with a by f
- We write $f : A \rightarrow B$ to indicate that f is a function from A to B
 - $A \rightarrow B$ is called the *type* of f

19 September 2006

Winsborough CS 3233 Lecture 8

7

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 $f : A \rightarrow B$, the *graph* of f is the set of ordered pairs $\{(a,b) \mid a \in A \text{ and } b = f(a)\}$
- Formally speaking, a function **is** its graph
 - Thus, f is a subset of $A \times B$ in which each element of A occurs exactly once

19 September 2006

Winsborough CS 3233 Lecture 8

8

Terminology

- Let $f : A \rightarrow B$
 - 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 $S \subseteq A$, the *image* of S is $\{f(s) \mid s \in S\}$ and is denoted by $f(S)$
 - $f(A) = \{f(a) \mid a \in A\}$ is called the *range* of f

19 September 2006

Winsborough CS 3233 Lecture 8

9

Examples

- Successor function
 - $s : \mathbb{N} \rightarrow \mathbb{N}$
 - $s(n) = n+1$
- Floor
 - $\text{floor} : \mathbb{R} \rightarrow \mathbb{Z}$
 - $\text{floor}(x)$ = greatest integer less than x
- Square root
 - $\sqrt{\cdot} : \mathbb{R} \rightarrow \mathbb{C}$
 - The square root of a real is a complex number
- Truth assignment
 - $\sigma : \mathcal{P}^o \rightarrow \{\text{true}, \text{false}\}$

19 September 2006

Winsborough CS 3233 Lecture 8

10

Injections and Surjections

- $f : A \rightarrow B$ is *one-to-one*, or *injective*, if and only if $f(x) = f(y)$ implies $x = y$ for all $x, y \in A$
 - $f : A \overset{1-1}{\rightarrow} B$
 - $\forall x \forall y (f(x) = f(y) \rightarrow x = y)$
 - Equivalently, $\forall x \forall y (x \neq y \rightarrow f(x) \neq f(y))$
 - f is called an *injection*
- $f : A \rightarrow B$ is *onto*, or *surjective*, if for every $b \in B$, there is an $a \in A$ such that $f(a) = b$
 - f is a *function of A onto B*
 - $f : A \overset{\text{onto}}{\rightarrow} B$
 - $\forall y \exists x (f(x) = y)$
 - f is called a *surjection*

19 September 2006

Winsborough CS 3233 Lecture 8

11

More Examples

- Square
 - $f : \mathbb{Z} \rightarrow \mathbb{Z}$
 - $f(x) = x^2$
 - Neither one-to-one nor onto
- Double
 - $\text{twice} : \mathbb{Z} \rightarrow \mathbb{Z}$
 - $\text{twice}(x) = 2x$
 - One-to-one, but not onto
- Absolute value
 - $|\cdot| : \mathbb{Z} \rightarrow \mathbb{N}$
 - $|x| = \begin{cases} x & \text{if } 0 \leq x; \\ -x, & \text{otherwise} \end{cases}$
 - Onto, but not one-to-one

19 September 2006

Winsborough CS 3233 Lecture 8

12

Still More Examples

- Integer successor
 - $zs : \mathbb{Z} \rightarrow \mathbb{Z}$
 - $zs(n) = n+1$
 - Both one-to-one and onto
- Mapping of 32-bit words to \mathbb{Z}
 - Injective, but not surjective
- Successor in $\mathbb{Z}_3 = \{0, 1, 2\}$
 - $s(0) = 1$
 - $s(1) = 2$
 - $s(2) = 0$
 - Injective and surjective

19 September 2006

Winsborough CS 3233 Lecture 8

13

Bijections

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

19 September 2006

Winsborough CS 3233 Lecture 8

14

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

19 September 2006

Winsborough CS 3233 Lecture 8

15

Function Inverses

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

$$f : A \xrightarrow[1-1]{\text{onto}} B$$

- $f^{-1} : B \rightarrow A$ is the *inverse* of f
- $f^{-1}(b) = a$ iff $f(a) = b$

19 September 2006

Winsborough CS 3233 Lecture 8

16

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

19 September 2006

Winsborough CS 3233 Lecture 8

17

Equinumerous Infinite Sets

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

19 September 2006

Winsborough CS 3233 Lecture 8

18

Countability

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

19 September 2006

Winsborough CS 3233 Lecture 8

19

Uncountability of the Reals

- Theorem
 - \mathbb{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 \mathbb{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

19 September 2006

Winsborough CS 3233 Lecture 8

20

Conclusion

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