CS 2742 (Logic in Computer Science) – Fall 2008
Lecture 18

Antonina Kolokolova

November 3, 2011

6.1 Power sets

A *power set* of a set A, denoted 2^A, is a set of all subsets of A. For example, if $A = \{1, 2, 3\}$ then $2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$.

Let $|A|$ denote the number of elements of A (also called *cardinality*, especially when talking about infinite sets.) The size of the power set, as notation suggests, is $2^{|A|}$.

Theorem 1. *Let A be a finite set. Then the cardinality of 2^A is $2^{|A|}$.*

Proof. Suppose A has n elements. Now, every subset S of A can be represented by a binary string of length n, which would have a 1 in the positions corresponding to an element in S, and a 0 in places corresponding to elements not in S. For example, if $A = \{1, 2, 3\}$ as above, then $S\{1, 3\}$ is represented by a string 101, and $\emptyset$ is represented by a string 000. Now, the number of binary strings of length n is 2^n. Therefore, the number of possible subsets of A (and thus the elements of 2^A) is also 2^n. □

What if A is infinite? Still the size of the powerset (called *cardinality* in this context) will be larger. In the next lecture we will talk about a technique called Diagonalization, due to Cantor, that can be used to show this.

7 Cartesian products, functions, relations

Cartesian product of sets $A_1 \dots A_n$, denoted $A_1 \times \cdots \times A_n$ is a set of ordered tuples $< a_1, a_2, ...a_n >$ such that $a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n$. Note that an *ordered tuple* (a, b) is not the same as a set $\{a, b\}$: here the order of elements matters, so the tuple

$< 1, 2 >$ is not the same as the tuple $< 2, 1 >$. For two sets, their Cartesian product is $A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$.

For example, a cartesian product of sets $\{3, 4\}$ and $\{1, 2, 3\}$ is the set of pairs $\{(3, 1), (3, 2), (3, 3), (4, 1), (4, 2)$ Note that the pair $(4, 3)$ is in the set, but the pair $(3, 4)$ is not, because 4 is not an element of $\{1, 2, 3\}$.

Proof that cartesian product $\mathbb{N} \times \mathbb{N}$ is countable: exactly the rational numbers.

Definition 1. *A relation on n variables $R(x_1, \ldots, x_n)$ is a subset of the Cartesian product of domains of $x_1, \ldots, x_n$.*

A predicate is true if the corresponding tuple of values is in the relation. Example: $Parent(x, y)$.

A *function* is a special kind of relation that has exactly value of x_n for any tuple of values of $x_1 \ldots x_{n-1}$. Usually we write $f(x_1 \ldots x_{n-1}) = x_n$ to mean that R is a function and $R(x_1, \ldots, x_{n-1}, x_n)$ holds.

So just as we defined numbers using sets, we now defined functins and relations on numbers (and not just numbers: the variables can be anything).

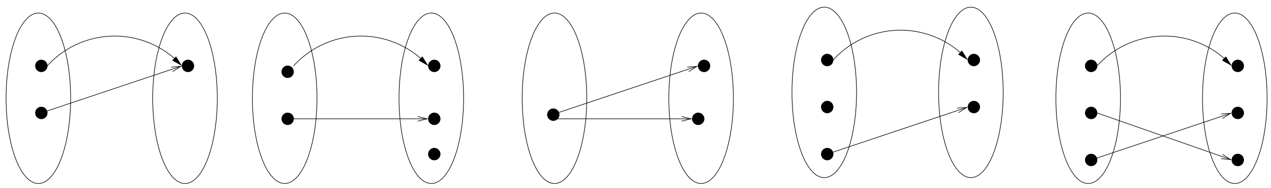
Example 1. $f(x) = Mother(x)$ is a function, so is $f(x) = x^2$, so is $f(x) = x/y$.

Definition 2. *We often write functions as $f : X \to Y$ (read as "function f from X to Y") meaning that the tuples of variables of f come from X, and that the output value of f comes from Y. We call X the* domain *of f, and $\{y | x \in X \wedge f(x) = y\}$ a* range *of f, or* image *of X under f. A set Y is called* codomain*; the range of f is a subset of the codomain,*

Domain and range can be different sets: e.g., function counting the number of a's in a string $f : \Sigma^* \to \mathbb{N}$.

- Identity function: $f(x) = x$. Can be defined for any domain=codomain.
- Constant function: $f(x) = a$,where s does not change when x does. For example, $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = 0$.
- Arithmetic functions: logarithmic function $f(x, y) = \log_x y$, exponential $f(x, y) = x^y$, addition, multiplication, division,subtraction,etc.
- Boolean functions: a function from strings of 0s and 1s of length n (denoted $\{0, 1\}^n$) to $\{0, 1\}$.

A function is defined by a formula if there is a formula which is true exactly on tuples of inputs + output of the function. E.g., a function $F : \mathbb{N} \to \mathbb{N}$ $f(x) = x + 1$ can be defined by $y > x \wedge \forall z\ (z \leq x \vee z \geq y)$. Sometimes a function is not well defined on a certain domain: e.g., $\sqrt{x}$ is not well-defined when both the domain and the range are natural numbers.



Definition 3. *Let $f : X \to Y$ be a function. Then f is* one-to-one *(or* injective*) iff $\forall x, y \in X$ $(f(x) = f(y) \to x = y)$. A function is* onto *(or* surjective*) if $\forall y \in Y \exists x \in X(f(x) = y)$. A function is* bijective *if it is both one-to-one and onto.*

To prove that two sets are the same size, give a bijection (or give two functions, one a surjection and one an injection).

To prove that a function is one-to-one show that $f(x) = f(y) \to x = y$.

Example 2. For example, $f(x) = 4x + 1$, $f(x) = f(y)$ so 4x+1=4y+1 so $x = y$. On the other hand, $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n^2$ is not one-to-one: as a counterexample take $x = -1$ and $y = 1$. Then $x \neq y$, but $x^2 = y^2$.

To prove that a function is onto, show that every element has a *preeimage*. To prove that it is not onto, show that there is an element in the codomain such that nothing maps into it.

Example 3. Consider again $f(x) = 4x+1$ over real numbers. There it is onto. Now consider it over integers. It is not onto integers.