Computer Science CSC 236 Winter 2006
St. George Campus University of Toronto

Basic Prerequisite Mathematics

This handout contains a review of basic mathematical notation and concepts used throughout the course. Please read it carefully *and make sure that you know the material well enough to use it from previous courses. The material will not be covered in lectures or tutorials.*

Set Theory

Common Sets

- $\mathbb{N}$: the natural numbers, or non-negative integers ($= \{0, 1, 2, \ldots\}$)

  NOTE: 0 **is** a natural number!
- $\mathbb{Z}$: the integers ($= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$)
- $\mathbb{Z}^+$: the positive integers ($= \{1, 2, 3, \ldots\}$)
- $\mathbb{Z}^-$: the negative integers ($= \{-1, -2, -3, \ldots\}$)
- $\mathbb{Q}$: the rational numbers (and $\mathbb{Q}^+$ the positive rationals, $\mathbb{Q}^-$ the negative rationals)
- $\mathbb{R}$: the real numbers (and $\mathbb{R}^+$ the positive reals, $\mathbb{R}^-$ the negative reals)

Notation

For any sets A and B, we will use the following standard notation.

- $x \in A$: "x is an element of A" or "A contains x"
- $A \subseteq B$: "A is a subset of B" or "A is included in B"
- $A = B$: "A equals B" (note that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$)
- $A \cup B$: "A union B"
- $A \cap B$: "A intersection B"
- $A \setminus B$ or $A - B$: "A minus B" (*set* difference)
- $|A|$: "cardinality of A" (the number of elements of A)
- $\varnothing$ or $\{\}$: "the empty set"
- $\mathcal{P}(A)$: "powerset of A" (the set of all subsets of A)

  For example, if $A = \{a, 34, \triangle\}$, then

  $$\mathcal{P}(A) = \big\{\{\}, \{a\}, \{34\}, \{\triangle\}, \{a, 34\}, \{a, \triangle\}, \{34, \triangle\}, \{a, 34, \triangle\}\big\}.$$
- $\{x \mid P(x)\}$ (where $P(x)$ is some property of x): "the set of elements x for which $P(x)$ is true"

  For example, $\{x \in \mathbb{Z} \mid x^2 < 9\}$ represents the set of integers x for which x^2 is less than nine, *i.e.*, it is equal to $\{-2, -1, 0, 1, 2\}$ and also to $\{x \in \mathbb{Z} \mid -7 \leq 3x \leq 6.4\}$.

Relations

- a *tuple* or vector $(x_1, \ldots, x_n)$ is an ordered collection of n objects.
  When $n = 2$, the tuple is called an *ordered pair*.
  When $n = 1$, the parentheses are usually omitted.

- for any sets $A_1, \ldots, A_n$, the *Cartesian product of* $A_1, \ldots, A_n$ is a set of tuples defined by

  $$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) \mid \text{for every } i \text{ from 1 to } n,\ x_i \in A_i\}.$$

  Example: $\{1, a\} \times \mathbb{N} = \{(1,0), (a,0), (1,1), (a,1), (1,2), (a,2), (1,3), \ldots\}$.

  Properties: when the sets A_i are all finite, $|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.

- for any set A and natural number n, the notation A^n is used to denote the Cartesian product of A with itself:

  $$\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}.$$

  When $n = 1$, A^n is the set A.
  When $n = 0$, A^n is considered to be the set $\{()\}$, which has one element, the 0-tuple, $()$.

- for any sets $A_1, \ldots, A_n$, a *relation over* $A_1, \ldots, A_n$ is any subset of $A_1 \times \cdots \times A_n$.
  When $n = 2$, the relation is called a *binary relation*.

  Example: $R = \{(x, y) \mid x < y,\ x \in \mathbb{N},\ y \in \mathbb{N}\}$ is a binary relation over $\mathbb{N}$ and $\mathbb{N}$. This R is called "the less-than relation over $\mathbb{N}$". Note that this R is also a relation over $\mathbb{R}$ and $\mathbb{Z}$.

- for any sets A and B, a *function f from A to B*, written

  $$f : A \to B$$

  is any subset of $A \times B$ where for each $x \in A$ there is a unique $y \in B$ such that $(x, y) \in f$.
  We write $f(x)$ to refer to the y associated with x by f (called the value of f at x);
  when A is the Cartesian product $A_1 \times \cdots \times A_n$, we write $f(x_1, \ldots, x_n)$.

  Example: $\min(x, y)$: "minimum of x and y" (the smallest of x or y).
  This function satisfies $\min(x, y) \leq x$, and $\min(x, y) \leq y$.

Basic Number Theory

For any two natural numbers a and b, we say that a *divides* b if there exists a natural number c such that $b = ac$. In such a case, we say that a is a *divisor* of b (*e.g.*, 3 is a divisor of 12 but 3 is not a divisor of 16). Note that any natural number is a divisor of 0 and 1 is a divisor of any natural number.

A natural number p is *prime* if it has exactly two positive divisors (*e.g.*, 2 is prime since its positive divisors are 1 and 2 but 1 is **not** prime since it only has one positive divisor: 1). There are an infinite number of prime numbers and any integer greater than one can be expressed in a unique way as a finite product of prime numbers (*e.g.*, $8 = 2^3$, $77 = 7 \times 11$, $3 = 3$).