Some mathematical prerequisites for CSC165

Danny Heap and François Pitt
heap@cs.toronto.edu

Here are some mathematical concepts, and notation, that I'll assume you are comfortable with during the course. I won't necessarily be teaching this material, so the onus is on you to make sure you really are comfortable with this material, and if not to ask about it.

You may also want to refer to these as justification for conclusions you derive in proofs you write up for this course.

Set theory and notation

$\mathbb{Z}$: The integers, or whole numbers, $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

$\mathbb{N}$: the natural numbers or non-negative integers $\{0, 1, 2, \ldots\}$. Notice that the convention in Computer Science is to include 0 in the natural numbers, unlike in some other disciplines.

$\mathbb{Z}^+$: The positive integers $\{1, 2, 3, \ldots\}$.

$\mathbb{Z}^-$: The negative integers $\{-1, -2, -3, \ldots\}$.

$\mathbb{Q}$: The rational numbers (ratios of integers), comprised of $\{0\}$, $\mathbb{Q}^+$ (positive rationals), and $\mathbb{Q}^-$ (the negative rationals).

$\mathbb{R}$: The real numbers, comprised of $\{0\}$, $\mathbb{R}^+$ (positive reals), and $\mathbb{R}^-$ (negative reals).

$x \in A$: "x is an element of A," or "x is in A."

$A \subseteq B$: "A is a subset of B." Every element of A is also an element of B.

$A = B$: "A equals B." A and B contain exactly the same elements, in other words $A \subseteq B$ and $B \subseteq A$.

$A \cup B$: "A union B." The set of elements that are in either A, or B, or both.

$A \cap B$: "A intersection B." The set of elements that are in both A and B.

$A \setminus B$ OR $A - B$: "A minus B." The set of elements that are in A but not in B (the set difference).

$|A|$: "cardinality of A." The number of elements in A.

$\emptyset$ OR $\{\}$: "The empty set." Convince yourself that for *any* set A, $\emptyset \subseteq A$.

$\mathcal{P}(A)$: "The power set of A." The set of all subsets of A. For example, suppose $A = \{73, \diamond\}$, the $\mathcal{P}(A) = \{\emptyset, \{73\}, \{\diamond\}, \{73, \diamond\}\}$.

$\{x | P(x)\}$: "The set of all x for which $P(x)$ is true." For example, $\{x \in \mathbb{Z} | \cos(\pi x) > 0\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ (even integers).

NUMBER THEORY

If m and n are natural numbers, $n \neq 0$, then there is exactly one pair of natural numbers (q, r) such that:

$$m = qn + r, \qquad n > r \geq 0.$$

We say that q is the QUOTIENT of m divided by n, and r is the REMAINDER. We also say that $m \bmod n = r$.

In the special case where the remainder r is zero (so $m = qn$) we say that n DIVIDES m, written $n \mid m$. We say that n is a DIVISOR of m (e.g. 4 is a divisor of 12). Convince yourself that any natural number is a divisor of 0, and that 1 is a divisor of any natural number.

A natural number, p, is prime if it has exactly two positive divisors. Thus $2, 3, 5, 7, 11$ are all prime but 1 isn't (too few positive divisors) and 9 isn't (too many positive divisors). There are infinitely many primes, and any integer greater than 1 can be expressed (in exactly one way) as a product of primes (if we allow unary products such as $2 = 2$).

FUNCTIONS

We'll use the standard notation $f : A \mapsto B$ to say that f is a function from set A to B. In other words, for every $x \in A$ there is an associated $f(x) \in B$. Here are some common number-theoretic functions along with their properties. We'll use the convention that variables $x, y \in \mathbb{R}$ whereas $k, m, n \in \mathbb{Z}^+$.

$\min\{x, y\}$: "minimum of x or y." The smallest of x or y. Properties: $\min\{x, y\} \leq x$ and $\min\{x, y\} \leq y$.

$\max\{x, y\}$: "maximum of x or y." The largest of x or y. Properties: $x \leq \max\{x, y\}$ and $y \leq \max\{x, y\}$.

$|x|$: "absolute value of x," which is $\begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$

Notice that the same notation is used for the cardinality of a set, so you have to pay attention to the context.

$\gcd(m, n)$: "greatest common divisor of m and n." The largest positive integer that divides both m and n.

LCM(m, n): "least common multiple of m and n." The smallest positive integer that is a multiple of m and n. Property: $\gcd(m, n) \times \text{lcm}(m, n) = mn$.

$\lfloor x \rfloor$: The largest integer that is not larger than x,

$$\forall x \in \mathbb{R}, y = \lfloor x \rfloor \Leftrightarrow y \in \mathbb{Z} \wedge y \leq x \wedge (\forall z \in \mathbb{Z}, z \leq x \Rightarrow z \leq y)$$

$\lceil x \rceil$: The smallest integer that is not smaller than x,

$$\forall x \in \mathbb{R}, y = \lceil x \rceil \Leftrightarrow y \in \mathbb{Z} \wedge y \geq x \wedge (\forall z \in \mathbb{Z}, z \geq z \Rightarrow z \geq y)$$

Inequalities

The following properties hold:

If $m, n \in \mathbb{Z}$: then $m < n$ if and only if $m + 1 \leq n$, and $m > n$ if and only if $m \geq n + 1$.

If $x, y, z, w \in \mathbb{R}$:

- Then if $x < y$ and $w \leq z$, then $x + w < y + z$.
- Then if $x < y$, then $\begin{cases} xz < yz, \text{if } z > 0 \\ xz = yz, \text{if } z = 0 \\ xz > yz, \text{if } z < 0 \end{cases}$
- Then if $x < y$ and $y \leq z$ (or $x \leq y$ and $y < z$), then $x < z$.
- $|x + y| \leq |x| + |y|$. This is an instance of the triangle inequality.

Exponents and logarithms

For any $a, b, c \in \mathbb{R}^+$: $a = \log_b c$ if and only if $b^a = c$.

For any $x \in \mathbb{R}^+$: $\ln x = \log_e x$, and $\log x = \log_2 x$ (In Computer Science, base 2 outranks base 10).

For any $a, b, c \in \mathbb{R}^+$ and $n \in \mathbb{Z}^+$, the following hold:

$$\begin{array}{ll}
\sqrt[n]{b} = b^{1/n} & b^{\log_b a} = a = \log_b b^a \\
b^a b^c = b^{a+c} & \log_b(ac) = \log_b a + \log_b c \\
(b^a)^c = b^{ac} & \log_b(a^c) = c \log_b a \\
b^a / b^c = b^{a-c} & \log_b(a/c) = \log_b a - \log_b c \\
b^0 = 1 & \log_b 1 = 0 \\
a^c b^c = (ab)^c &
\end{array}$$