CSC 238H — May 13 1998
St. George Campus — University of Toronto

Review of Basic Prerequisite Mathematics

This handout contains a summary of basic mathematical notation and concepts which you need to be familiar with in order to take this course. Please read it carefully *and make sure that you are very familiar with the material. Most of the material should be familiar from high school mathematics, and it will* **not** *be covered or reviewed in lectures or in tutorial.*

Set Theory

Common Sets

- $\mathbb{N}$: the natural numbers, or non-negative integers ($= \{0, 1, 2, \dots\}$)
  NOTE: 0 **is** a natural number!
- $\mathbb{Z}$: the integers ($= \{\dots, -2, -1, 0, 1, 2, \dots\}$)
- $\mathbb{Z}^+$: the positive integers ($= \{1, 2, 3, \dots\}$)
- $\mathbb{Z}^-$: the negative integers ($= \{-1, -2, -3, \dots\}$)
- $\mathbb{Q}$: 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"
- $A \subseteq B$: "A is a subset of 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)
- $A \times B$: "the Cartesian product of A and B"
- $|A|$: "cardinality of A" (the number of elements in 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, $\{x \in \mathbb{Z} \mid \cos(\pi x) > 0\}$ represents the set of integers x for which $\cos(\pi x)$ is greater than zero, *i.e.*, it is equal to $\{\dots, -4, -2, 0, 2, 4, \dots\} = \{x \in \mathbb{Z} \mid x \text{ is even}\}$.

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 distinct positive divisors. For example, 2 is prime since its positive divisors are 1 and 2 but 1 is **not** prime since it only has one positive divisor: 1. 4 is not prime, since it has three distinct positive divisors: 1, 2 and 4. 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.*, $8 = 2^3$, $77 = 7 \times 11$, $3 = 3$).

Inequalities

For any integers m and n, $m < n$ if and only if $m + 1 \leq n$ and $m > n$ if and only if $m \geq n + 1$. For any real numbers w, x, y, and z, the following properties always hold (they also hold when $<$ and $\leq$ are exchanged throughout with $>$ and $\geq$, respectively).

- if $x < y$ and $w \leq z$, then $x + w < y + z$
- if $x < y$, then $\begin{cases} xz < yz & \text{if } z > 0 \\ xz = yz & \text{if } z = 0 \\ xz > yz & \text{if } z < 0 \end{cases}$
- if $x \leq y$ and $y < z$ (or if $x < y$ and $y \leq z$), then $x < z$

Functions

We will use the standard notation

$$f : A \to B$$

to say that f is a function from set A to set B (*i.e.*, to every element $x \in A$, f associates one element $f(x) \in B$).

Let $g : A \to B$, where A and B are subsets of $\mathbb{R}$.
If $g(b) > g(a)$ whenever $b > a$, then g is a (strictly) *increasing* function.
If $g(b) < g(a)$ whenever $b > a$, then g is a (strictly) *decreasing* function.
If $g(b) \geq g(a)$ whenever $b > a$, then g is a *non-decreasing* function.
If $g(b) \leq g(a)$ whenever $b > a$, then g is a *non-increasing* function.
The function g is called *monotone* if it is either increasing or decreasing.

Now, here are some common functions together with their definition and properties (unless noted otherwise, x and y stand for arbitrary real numbers and k, m, and n stand for arbitrary positive integers in what follows).

- $\min(x, y)$: "minimum of x and y" (the smallest of x or y)

  Properties: $\min(x, y) \leq x$, $\min(x, y) \leq y$.
- $\max(x, y)$: "maximum of x and y" (the largest of x or y)

  Properties: $x \leq \max(x, y)$, $y \leq \max(x, y)$.

- $\lfloor x \rfloor$: "floor of x" (the greatest integer less than or equal to x, *e.g.*, $\lfloor 5.67 \rfloor = 5$, $\lfloor -2.01 \rfloor = -3$)

  Properties: $x - 1 < \lfloor x \rfloor \le x$, $\lfloor -x \rfloor = -\lceil x \rceil$, $\lfloor x + k \rfloor = \lfloor x \rfloor + k$, $\lfloor \lfloor k/m \rfloor /n \rfloor = \lfloor k/mn \rfloor$, $(k - m + 1)/m \le \lfloor k/m \rfloor$.

- $\lceil x \rceil$: "ceiling of x" (the least integer greater than or equal to x, *e.g.*, $\lceil 5.67 \rceil = 6$, $\lceil -2.01 \rceil = -2$)

  Properties: $x \le \lceil x \rceil < x + 1$, $\lceil -x \rceil = -\lfloor x \rfloor$, $\lceil x + k \rceil = \lceil x \rceil + k$, $\lceil \lceil k/m \rceil /n \rceil = \lceil k/mn \rceil$, $\lceil k/m \rceil \le (k + m - 1)/m$.

  Additional property of $\lfloor\rfloor$ and $\lceil\rceil$: $\lfloor k/2 \rfloor + \lceil k/2 \rceil = k$.

- $|x|$: "absolute value of x" ($|x| = x$ if $x \ge 0; -x$ if $x < 0$, *e.g.*, $|5.67| = 5.67$, $|-2.01| = 2.01$)

  BEWARE! The same notation is used to represent the cardinality of a set ($|A|$) and the absolute value of a number ($|x|$) so be sure you are aware of the context in which it is used.

- $m \operatorname{div} n$: "m divided by n" (integer division of m by n, *e.g.*, $5 \operatorname{div} 6 = 0$, $27 \operatorname{div} 4 = 6$)

  Properties: $m \operatorname{div} n = \lfloor m/n \rfloor$.

- $m \bmod n$: "m modulo n" (the remainder of $m \operatorname{div} n$, *e.g.*, $5 \bmod 6 = 5$, $27 \bmod 4 = 3$)

  Properties: $m = (m \operatorname{div} n) \cdot n + m \bmod n$, $0 \le m \bmod n < n$.

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

  For example, $\gcd(3, 4) = 1$, $\gcd(12, 20) = 4$, $\gcd(3, 6) = 3$.

- $\operatorname{lcm}(m, n)$: "least common multiple of m and n" (the smallest positive integer that m and n both divide)

  For example, $\operatorname{lcm}(3, 4) = 12$, $\operatorname{lcm}(12, 20) = 60$, $\operatorname{lcm}(3, 6) = 6$.

  Properties: $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = m \cdot n$.

Calculus

Limits and Sums

A sequence of real numbers $\{a_n\} = a_0, a_1, a_2, \ldots, a_n, \ldots$ *converges* to a limit $L \in \mathbb{R}$ if for every $\varepsilon > 0$, there exists a $n_0 \ge 0$ such that $|a_n - L| < \varepsilon$ for every $n \ge n_0$. In such a case, we write $\lim_{n\to\infty} a_n = L$ or simply $\{a_n\} \to L$. Otherwise, we say that the sequence *diverges*.

If $\{a_n\}$ and $\{b_n\}$ are two sequences of real numbers such that $\{a_n\} \to L_1$ and $\{b_n\} \to L_2$, then

$$\lim_{n\to\infty} (a_n + b_n) = L_1 + L_2 \quad \text{and} \quad \lim_{n\to\infty} (a_n \cdot b_n) = L_1 \cdot L_2.$$

In particular, if c is any real number, then

$$\lim_{n\to\infty} (c \cdot a_n) = c \cdot L_1.$$

Examples:

- For any $a \in \mathbb{R}$ such that $-1 < a < 1$, $\lim_{n\to\infty} a^n = 0$.
- For any $a \in \mathbb{R}^+$, $\lim_{n\to\infty} a^{1/n} = 1$.

- For any $a \in \mathbb{R}^+$, $\lim_{n\to\infty}(1/n)^a = 0$.
- $\lim_{n\to\infty}(1+1/n)^n = e = 2.71828182845904523536\ldots$

Summation notation

The notation $\sum_{i=a}^{b} t_i$, where a and b are integers with $b \geq a$ and the t_i's are real numbers, is used to denote the sum $t_a + t_{a+1} + t_{a+2} + \cdots + t_b$. The notation is defined formally by

$$\begin{aligned}\sum_{i=a}^{b} t_i &= t_a, \text{ if } b = a, \text{ and}\\ \sum_{i=a}^{b} t_i &= t_a + \sum_{i=a+1}^{b} t_i, \text{ if } b > a.\end{aligned}$$

For example, $\sum_{i=3}^{n} 2^i = 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 8$.

Similarly, $\prod_{i=a}^{b} t_i$ represents the product $t_a \cdot t_{a+1} \cdot t_{a+2} \cdot \cdots \cdot t_b$.

Similar notation will be used for other associative operations. For example, $\bigcup_{i=a}^{b} A_i$, where the A_i's are sets, represents the union $A_a \cup A_{a+1} \cup A_{a+2} \cup \cdots \cup A_b$.

Two simple kinds of changes of variables are often useful (a, b and c are integers, with $b \geq a$):
$\sum_{i=a}^{b} t_i = \sum_{j=a+c}^{b+c} t_{j-c}$ (here, $j = c + i$).
$\sum_{i=a}^{b} t_i = \sum_{k=c-b}^{c-a} t_{c-k}$ (here, $k = c - i$).

Two of the most common sums are arithmetic and geometric sequences:

- For any $a, b \in \mathbb{R}$, the *arithmetic* sum is given by:

$$\sum_{i=0}^{n}(a+ib) = (a) + (a+b) + (a+2b) + \cdots + (a+nb) = \frac{1}{2}(n+1)(a+a+nb).$$

- For any $a, b \in \mathbb{R}^+$, the *geometric* sum is given by:

$$\sum_{i=0}^{n}(ab^i) = a + ab + ab^2 + \cdots + ab^n = a\,\frac{1-b^{n+1}}{1-b}.$$

Exponents and Logarithms

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

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

- $\sqrt[n]{b} = b^{1/n}$
- $b^a b^c = b^{a+c}$
- $(b^a)^c = b^{ac}$
- $b^a / b^c = b^{a-c}$
- $b^0 = 1$
- $a^b c^b = (ac)^b$
- $b^{\log_b a} = a = log_b b^a$
- $a^{\log_b c} = c^{\log_b a}$
- $\log_b(ac) = \log_b a + \log_b c$
- $\log_b(a^c) = c \cdot \log_b a$
- $\log_b(a/c) = \log_b a - \log_b c$
- $\log_b 1 = 0$
- $\log_b a = \log_c a / \log_c b$

Binary Notation

A *binary number* is a sequence of bits $a_k \cdots a_1 a_0$ where each bit a_i is equal to 0 or 1. Every binary number represents a natural number in the following way:

$$(a_k \cdots a_1 a_0)_2 = \sum_{i=0}^{k} a_i 2^i = a_k 2^k + \cdots + a_1 2 + a_0.$$

For example, $(1001)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 1 = 9$, $(01110)_2 = 8 + 4 + 2 = 14$.

Properties:

- If $a = (a_k \cdots a_1 a_0)_2$, then $2a = (a_k \cdots a_1 a_0 0)_2$, *e.g.*, $9 = (1001)_2$ so $18 = (10010)_2$.
- If $a = (a_k \cdots a_1 a_0)_2$, then $\lfloor a/2 \rfloor = (a_k \cdots a_1)_2$, *e.g.*, $9 = (1001)_2$ so $4 = (100)_2$.
- The smallest number of bits required to represent natural number n in binary is called the *binary length* of n and is equal to $\lceil \log_2(n+1) \rceil$.