Mathematical Prerequisites

This is a summary of basic mathematical notation and concepts which you need to be familiar with in order to take this course. Most of the material here should be familiar either from high school mathematics or first-year discrete math, and it will ***not*** *be covered in lectures.*

1 Set Theory

Common Sets

- $\mathbb{N}$: the set of all natural numbers, $\{0, 1, 2, \dots\}$
- $\mathbb{Z}$: the set of all integers, $\{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Z}^+$: the set of all positive integers, $\{1, 2, 3, \dots\}$
- $\mathbb{Q}$: the set of all rational numbers
- $\mathbb{R}$: the set of all real numbers
- $\mathbb{R}^+$: the set of all positive real numbers

Notation

You should be familiar with set-builder notation: $\{x : P(x)\}$, where $P(x)$ is some property of x. This represents the set of all elements x for which $P(x)$ is true. For example, $\{x : x^2 = 4\}$ represents the set $\{2, -2\}$. We often give the domain of x before the colon, as in $\{x \in \mathbb{N} : x^2 < 9\} = \{0, 1, 2\}$.

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

- $\varnothing$ or $\{\}$: "the empty set"
- $x \in A$: "x is an element of A".
- $x \notin A$: "x is not an element of A".
- $A \subseteq B$: "A is a subset of B"; *i.e.*, every element of A is also in B.
- $A = B$: "A equals B"; *i.e.*, $A \subseteq B$ and $B \subseteq A$.
- $A \cap B$: "A intersect B"; *i.e.*, the set $\{x : x \in A \text{ and } x \in B\}$.
- $A \cup B$: "A union B"; *i.e.*, the set $\{x : x \in A \text{ or } x \in B\}$.
- $A \setminus B$ or $A - B$: "A minus B" (*set* difference); *i.e.*, the set $\{x : x \in A \text{ and } x \notin B\}$.
- $\overline{A}$: "the complement of A". This assumes there is some domain D from which the items in A are chosen; then $\overline{A} = D - A$.
- $A \times B$: "the Cartesian product of A and B"; *i.e.*, the set $\{(x, y) : x \in A \text{ and } y \in B\}$.
- $|A|$: "cardinality of A" (intuitively, the number of elements in A)

2 Logic and Proofs

You should be familiar with the Boolean connectives ($\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$) and identities involving them.
You should be familiar with quantifiers $\exists$ ("there exists") and $\forall$ ("for all") and identities involving them.
You should be able to work with nested quantifiers. For example, you should understand the difference between the statements $\forall x \exists y L(x, y)$, $\exists x \forall y L(x, y)$ and $\forall y \exists x L(x, y)$.

You should be able to understand and use important proof techniques:

- proof by cases
- proof by contradiction: to prove A, derive a contradiction from $\neg A$.
- direct proof of an implication: to prove $A \Rightarrow B$, assume A as a hypothesis and prove B.
- proof of an implication by proving contrapositive: to prove $A \Rightarrow B$, prove $\neg B \Rightarrow \neg A$.
- proof by mathematical induction (strong and ordinary)
- proof of existence by construction: to prove $\exists x P(x)$, explicitly construct an x and show that $P(x)$ is true for it.
- uniqueness proofs (*i.e.*, proving that there exists a *unique* x such that $P(x)$ is true).
- proof of universally quantified statement by generalization: to prove $\forall x P(x)$, start with a generic item x and show that $P(x)$ holds. Note that your proof must apply to every x; it cannot use any properties of particular x's.

You should be able to combine proof techniques above to prove "if and only if" statements or statements with nested quantifiers.

3 Functions

Formally, a function $f : A \to B$ is a set $f \subseteq A \times B$, where, for all $x \in A$, there is exactly one element $y \in B$ such that $(x, y) \in f$. If $(x, y) \in f$, we use the notation $f(x)$ to denote y. This means that f associates with each value $x \in A$ a unique value $f(x)$. A is called the *domain* of the function f. Note that the domain can be a Cartesian product of other sets: in this case we use the notation $f(x, y)$ instead of $f((x, y))$.

Properties of Functions

A function $f : A \to B$ is called

- *surjective* (or *onto*) if, for every $z \in B$, there is some $x \in A$ such that $f(x) = z$.
- *injective* (or *one-to-one*) if $x \neq y$ implies $f(x) \neq f(y)$.
- *bijective* (or *a one-to-one correspondence*) if it is surjective and injective.

Let $f : A \to B$, where A and B are subsets of $\mathbb{R}$. The function f is called

- *(strictly) increasing* if $f(x) < f(y)$ whenever $x < y$.

- *(strictly) decreasing* if $f(x) > f(y)$ whenever $x < y$.
- *non-decreasing* if $f(x) \leq f(y)$ whenever $x < y$.
- *non-increasing* if $f(x) \geq f(y)$ whenever $x < y$.
- *monotone* if it is either increasing or decreasing.

Common Functions

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). More generally, if A is a set of real numbers, $\min(A)$ denotes the smallest element in set A, if such a smallest element exists.
- $\max(x, y)$: "maximum of x and y" (the largest of x or y). More generally, if A is a set of real numbers, $\max(A)$ denotes the largest element in set A, if such a largest element exists.
- $\lfloor x \rfloor$: "floor of x" (the greatest integer less than or equal to x. For example, $\lfloor 5.67 \rfloor = 5$ and $\lfloor -2.01 \rfloor = -3$).

  Properties: $x - 1 < \lfloor x \rfloor \leq x$, $\lfloor -x \rfloor = -\lceil x \rceil$, $\lfloor x + k \rfloor = \lfloor x \rfloor + k$, $\left\lfloor \frac{k}{m} \right\rfloor \geq \frac{k}{m} - \frac{m-1}{m}$.
- $\lceil x \rceil$: "ceiling of x" (the smallest integer greater than or equal to x. For example, $\lceil 5.67 \rceil = 6$ and $\lceil -2.01 \rceil = -2$).

  Properties: $x \leq \lceil x \rceil < x + 1$, $\lceil -x \rceil = -\lfloor x \rfloor$, $\lceil x + k \rceil = \lceil x \rceil + k$, $\left\lceil \frac{k}{m} \right\rceil \leq \frac{k}{m} + \frac{m-1}{m}$.

  Additional property of $\lfloor\ \rfloor$ and $\lceil\ \rceil$: $\lfloor k/2 \rfloor + \lceil k/2 \rceil = k$; prove this by considering two cases, when k is even or odd.
- $|x|$: "absolute value of x" ($|x| = x$ if $x \geq 0$; $-x$ if $x < 0$, *e.g.*, $|5.67| = 5.67$, $|-2.01| = 2.01$)

  Do not confuse this with the notation for the cardinality of a set.
- $m \operatorname{div} n = \lfloor m/n \rfloor$, the integer portion of m divided by n. For example, $5 \operatorname{div} 6 = 0$ and $27 \operatorname{div} 4 = 6$.
- $m \bmod n = m - n \cdot \lfloor m/n \rfloor$: the remainder of m divided by n. For example, $5 \bmod 6 = 5$ and $27 \bmod 4 = 3$.

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

4 Sums

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

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

Computing Sums

You should know some common sums:

- $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$
- $\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$
- $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$ for $r \neq 1$

Some identities are useful in computing sums:

- $\sum_{i=a}^{b} (ct_i + s_i) = c \sum_{i=a}^{b} t_i + \sum_{i=a}^{b} s_i$
- $\sum_{i=a}^{b} t_i = \sum_{i=0}^{b} t_i - \sum_{i=0}^{a-1} t_i$ (where $b \geq a \geq 0$).

Two simple kinds of changes of variables are also useful in computing sums (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, $k = c - i$).

Bounding Sums

See Section A.2 of the textbook.

5 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.

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

6 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 $4 = (100)_2$.
- Each positive integer has a unique binary representation whose leftmost bit is 1.
- The smallest number of bits required to represent natural number n in binary is called the *binary length* of n and is equal to $\lceil \log_2(n+1) \rceil$.

7 Asymptotic Notation

See Chapter 3 of the textbook