Math Review

Algorithms

Corazza

Students entering Compro are expected to have familiarity with basic algebra, calculus, and discrete math topics. This document reviews most of the points that should be familiar to the incoming student. The problems shown below are included to let you to test your knowledge.

Section L: Laws Of Logarithms

$$
\begin{aligned}
y = \log_b x &\text{ means } x = b^y \\
\log x &\text{ means } \log_2 x \\
\log^n x &\text{ means } (\log x)^n \\
\ln x &\text{ means } \log_e x \ (e \approx 2.71828) \\
\log_b(xy) &= \log_b x + \log_b y \\
\log_b(x^y) &= y \log_b x \\
\log_b(\frac{x}{y}) &= \log_b x - \log_b y \\
\log_b x &= \frac{\log_a x}{\log_a b} \\
0 < x < y &\Rightarrow \log_b(x) < \log_b(y) \\
\log_b 1 &= 0 \\
\log_b b &= 1 \\
\log_b x &< x \text{ (for } b \geq 2 \text{ and } x > 0) \\
\log 1024 &= 10 \\
\ln 2 &\approx .693 \text{ (in particular, } 0 < \ln 2 < 1) \\
\log e &\approx 1.44 \text{ (in particular, } 1 < \log e < 2)
\end{aligned}
$$

Problem L1. Show that the following is not true in general, for $k > 1$:

$$(\log n)^k = k \log n.$$

Problem L2. Show that the following is not true in general:

$$\log_b(x + y) = \log_b x + \log_b y$$

Problem L3. Show that, for all $n > 2$,

$$n < n \log n < n^2.$$

It is also true that for all $n > 4$, $n^2 < 2^n$. This is proved by induction. See Problem MI2.

Problem L4. Solve for n:

$$2^{3n-1} = 32.$$

Section S: Sets

A. A *set* is a collection of objects (this is only approximately correct!).
   - The notation $x \in A$ signifies that x is an element of A.
   - *Set notation.* The set containing just the elements 1, 2, 3 is denoted $\{1, 2, 3\}$. Elliptical notation can be used to denote larger sets, such as $\mathbf{N} = \{1, 2, 3, \ldots\}$. Set-builder notation defines a set by specifying properties; for instance:

     $$E = \{n \mid n \text{ is a natural number and for some } x,\ n = 2 * x\}.$$

   - Two sets are *equal* if and only if they have the same elements. Therefore, duplicate elements are not allowed in a set when viewed as a data structure.

B. B is a *subset* of A, $B \subseteq A$, if every element of B is also an element of A. The empty set, denoted $\emptyset$, is a subset of every set (but is *not* an element of every set!).

C. If A and B are sets, $A \cup B$ ("the union of A and B") consists of all objects that belong to at least one of A and B; and $A \cap B$ ("the intersection of A and B") consist of all objects that belong to both A and B. Example:

$$\{1, 2, 3\} \cup \{2, 3, 4\} = \{1, 2, 3, 4\}$$
$$\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$$

D. Suppose each of A, B is a set. Then A, B are *disjoint* if A and B have no element in common (that is, $A \cap B = \emptyset$). Similarly, $A_i (i \in I)$ are disjoint if no two of the sets have an element in common.

E. The *cardinality* or *size* of a set A is denoted $|A|$. Example: $|\{2, 7, 14\}| = 3$.

F. The *power set* of a set A, denoted $\mathcal{P}(A)$, is the set whose elements are all the subsets of A. Note: If A has n elements, $\mathcal{P}(A)$ has 2^n elements. That is, a set with n elements has 2^n subsets.

G. If a set A having n elements is totally ordered, then a *permutation* of A is a re-arrangement of the elements of A.
   - Example: The following are two of the permuations of $\{1, 2, 3, 4\}$:

     $$[1, 2, 4, 3], [4, 3, 2, 1]$$

   - The permutation of A that does not re-arrange any of the elements is called the *identity permutation.*
   - The number of permutations of an n-element set is $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$.

H. The notation $C(n, m)$ is read "the number of combinations of n things taken m at a time" and can be understood to mean "the number of m-element subsets of an n-element set."

- For small values of n, m, $C(n,m)$ can be computed by inspection. Example: Compute $C(3,2)$. To do the computation, take any 3-element set $\{a,b,c\}$ and write out the 2-element subsets:

  $$\{\{a,b\},\{b,c\},\{a,c\}\}.$$

  The resulting collection now contains 3 two-element subsets of $\{a,b,c\}$. Therefore, $C(3,2)=3$.
- Formula for computing $C(n,m)$

  $$C(n,m)=\frac{n!}{m!(n-m)!}.$$

  Example:

  $$C(10,2)=\frac{10!}{2!8!}=\frac{10\cdot 9\cdot 8\cdot 7\cdot 6\cdots 2\cdot 1}{(2\cdot 1)(8\cdot 7\cdot 6\cdots 2\cdot 1)}=\frac{10\cdot 9}{2\cdot 1}=45.$$

I. The notation $P_{n,m}$ is read "the number of permutations of n things taken m at a time." The meaning is this: We have a set S with n elements, and we want to arrange m of the elements of S in a particular order.

- The computation is easier to understand in a simple case. We want to compute $P_{3,2}$. Let $S=\{a,b,c\}$. We want to arrange two elements from S in a particular order. We can think that there are two "slots" to fill—positions 1 and positions 2—with elements from S:

  $$\underset{1}{\underline{\qquad}}\qquad\underset{2}{\underline{\qquad}}$$

  To fill these slots, we perform two tasks in succession:

  Task 1: Pick a 2-element subset from S

  Task 2: Arrange it so one element is in position 1, the other in position 2.

  There are $C(3,2)$ ways to perform Task 1. After a set has been selected, there are 2! ways to arrange that set—that is, 2! ways to place the elements into position 1 and position 2. Therefore:

  $$P_{3,2}=C(3,2)\cdot 2!$$
- The same logic gives the formula for $P_{n,m}$:

  $$P_{n,m}=C(n,m)m!=\frac{n!}{(n-m)!}.$$
- Example: Compute $P_{10,2}$.

  $$P_{10,2}=\frac{10!}{(10-2)!}=\frac{10!}{8!}=10\cdot 9=90.$$

Problem S1. Are the following sets equal? Explain.

$$\{1,1,2\},\{1,2\},\{2,1\}.$$

Problem S2. Is the following statement true or false?

$$\{1, \{2, 3\}\} \subseteq \{1, 2, 3, 4, 5, \ldots\}$$

Solution. False. The first set contains an element that is *not* an element of the second set — namely, $\{2, 3\}$.

Problem S3. What is the powerset of the set $\{1, 2\}$?

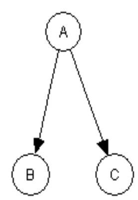
Problem S4. List all the permutations of the set $\{1, 3, 4\}$.

Problem S5. In how many ways can 5 students, from a group of 9 students, be seated in a row of 5 chairs?

Problem S6. A committee of three representatives is to be chosen from a larger group of 20 people. In how many ways can this committee be formed?

Section DGF: Directed Graphs and Functions

A directed graph is a set of objects (called *vertices* or *nodes*) together with a set of arrows that join some of the vertices. Here is a simple example:



A function from a set X to a set Y—written $f : X \to Y$—is a special kind of directed graph f (we usually denote functions using typical letters f, g, h, etc.) with the following characteristics:

- The objects of the graph f are the elements of X together with the objects of Y.
- Each arrow of f always starts at an element of X and points to an element of Y. If, in f, x points to y, we write $x \to y$ or $f(x) = y$.
- In f, no $x \in X$ ever points to more than one element of Y
- In f, every element of X does point to *at least one* element of Y.

When $f : X \to Y$ is a function, X is called its *domain*, Y its *codomain*.

Concepts Related to Functions. Suppose $f : X \to Y$ is a function.

(1) *Onto*. A f is *onto* if for each $y \in Y$ there is an element $x \in X$ so that $x \to y$.

(2) *Range*. The range of f is the set of all $y \in Y$ that are pointed to by one or more x in X; the range is the set of all *output values* of f. If the range of f is Y itself, f is onto.

(3) *1-1*. A function $f : X \to Y$ is *1-1* if, whenever x and x' are distinct elements of X, and $x \to y$ and $x' \to y'$, then y and y' are also distinct elements of Y.

Example Let $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$. Let's define $f : A \to B$ as follows:

$$\begin{array}{ccc} \underline{A} & f & \underline{B} \\ 1 & \to & 4 \\ 2 & \to & 5 \\ 3 & \to & 6 \end{array}$$

In other words, in the directed graph f, $1 \to 4, 2 \to 5, 3 \to 6$. Another way to say this is that f takes the number 1 to 4, the number 2 to 5, and the number 3 to 6. Here is notation that can be used to state this fact:

$$f(1) = 4$$
$$f(2) = 5$$
$$f(3) = 6$$

Example. We define a function g, also having domain A and codomain B (defined in the previous example), as follows:

$$g(1) = 4$$
$$g(2) = 4$$
$$g(3) = 4$$

Here g is also a function. In the previous example, the function f was *1-1*—no two elements of the domain were assigned the same value by f. Clearly, g does not have that property; in fact, all elements of the domain A of g are assigned the single value 4.

Example. Returning to the functions f and g of the previous examples, notice that the range of f is precisely equal to B, so f is onto. On the other hand, the range of g is just the singleton set $\{4\}$, and so g is *not* onto.

Problem DGF1. Consider the function $f(n) = n^2$, where the domain of f is the set $\mathbf{N}$ of all natural numbers. Is f 1-1? What is the range of f? Is f onto?

Some functions from $\mathbf{N}$ to $\mathbf{N}$ have the convenient property of being *increasing*. This means that as input values increase, output values also increase. More precisely, we have the following definition:

Definition. A function $f : \mathbf{N} \to \mathbf{N}$ is said to be *increasing* if, whenever $m < n$, we have $f(m) < f(n)$. A function $g : \mathbf{N} \to \mathbf{N}$ is said to be *nondecreasing* if, whenever $m < n$, we have $g(m) \leq g(n)$.

Example. Obviously, the identity function $f(n) = n$ is increasing. It is equally easy to see that the function $g(n) = kn$ for any integer $k > 1$ is also increasing. This can be verified by simple algebra: if $m < n$, then multiplying on both sides by k gives us $km < kn$, which establishes that $g(m) < g(n)$.

Problem DGF2. Show that the function $f(n) = n^2$, with domain $\mathbf{N}$, is increasing.

Section SUM: Summations

$$\sum_{i=1}^{N} 1 = N$$

$$\sum_{i=1}^{N} i = \frac{N(N+1)}{2}$$

$$\sum_{i=1}^{N} i^2 = \frac{N(N+1)(2N+1)}{6}$$

$$\sum_{i=0}^{N} 2^i = 2^{N+1} - 1$$

$$\sum_{i=0}^{N} a^i = \frac{a^{N+1} - 1}{a - 1}$$

$$\sum_{i=0}^{N} a^i < \frac{1}{1-a} \text{ (whenever } 0 < a < 1\text{)}$$

$$\sum_{i=1}^{N} \frac{1}{i} \approx \ln 2 \, \log N \text{ (the difference between these falls below 0.58 as } N \text{ tends to infinity)}$$

Problem SUM1. Rewrite the following in terms of the variable N, using the formulas above.

$$\sum_{i=1}^{N} 2i^2 + 3i - 4.$$

Section MI: Mathematical Induction

Mathematical induction is a technique for proving mathematical results having the general form "for all natural numbers n, ..." For example, suppose you would like to prove that for all natural numbers $n > 1$, $n^2 > n+1$. You might try a few values for n to see if the statement makes sense. Certainly $2^2 > 2+1, 3^2 > 3+1, 10^2 > 10+1$. These examples suggest that the statement always holds true. But how do we know for sure? It is at least conceivable that for certain very large numbers that we are unlikely to consider, the statement is no longer true. Mathematical induction is a technique for demonstrating that such a formula must hold true for every natural number > 1, without exception.

The intuitive idea behind Mathematical Induction is this: Suppose you wish to prove that some statement $\phi(n)$, which asserts something about each whole number n, is true for every n. For example, to prove that for all $n \geq 0$, $n < 2^n$, we would use "$n < 2^n$" as our statement $\phi(n)$. We wish to show that this statement holds for every n. Suppose now that we can prove two things:

(1) that $\phi(0)$ is true (in our example, this would mean that we can prove $0 < 2^0$);
(2) that, for any n, if $\phi(n)$ happens to be true, then $\phi(n+1)$ must also be true (in our example, this would mean that, if it happens to be true that $n < 2^n$, then it must be true that $n+1 < 2^{n+1}$).

Mathematical Induction says that, if you can prove both (1) and (2), then you have proven that, for every n, $\phi(n)$ is indeed true.

Below are several forms of induction. Each provides a valid approach to proving the correctness of a statement about natural numbers. Different forms are useful in different contexts. We include an example of each.

Standard Induction. Suppose $\phi(n)$ is a statement depending on n. If

- $\phi(0)$ is true, and
- under the assumption that $n \geq 0$ and $\phi(n)$ is true, you can prove that $\phi(n+1)$ is also true,

then $\phi(n)$ holds true for all natural numbers n.

In Standard Induction, the step in the proof where $\phi(0)$ is verified is called the *Basis Step*. The second step, where $\phi(n+1)$ is proved assuming $\phi(n)$, is called the *Induction Step*. As we reason during this second step, we will typically need to make use of $\phi(n)$ as an assumption; in this context, $\phi(n)$ is called the *induction hypothesis*.

Note. Standard Induction allows you to establish that a statement $\phi(n)$ holds for all natural numbers 0,1,2, ... However, sometimes the objective is to show that $\phi(n)$ holds for all numbers n that are larger than a fixed number k. Standard Induction may still be used. Here is a precise statement:

Standard Induction (General Form). Let $k \geq 0$. Suppose $\phi(n)$ is a statement depending on n. If

- $\phi(k)$ is true, and

- under the assumption that $n \geq k$ and $\phi(n)$ is true, you can prove that $\phi(n+1)$ is also true,

then $\phi(n)$ holds true for all natural numbers $n \geq k$.

Problem MI1. Prove that, for every natural number $n \geq 1$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Problem MI2. Show that for every natural number $n > 4$, $n^2 < 2^n$.

Total Induction. Suppose $\phi(n)$ is a statement depending on n and $k \geq 0$. If

- $\phi(k)$ is true, and
- under the assumption that $n > k$ and that each of $\phi(k), \phi(k+1), \ldots, \phi(n-1)$ are true, you can prove that $\phi(n)$ is also true,

then $\phi(n)$ holds true for all $n \geq k$.

Problem MI3. Prove that if $f(n) = 2^n$, then f is increasing.

Finite Induction. Suppose $0 \leq k \leq n$, and suppose $\phi(i)$ is a statement depending on i, where $k \leq i \leq n$. If

- $\phi(k)$ is true, and
- under the assumption that $k \leq i < n$ and that $\phi(i)$ is true, you can prove $\phi(i+1)$ is true,

then $\phi(i)$ holds true for all i with $k \leq i \leq n$.

Note. Another equally valid variant of Finite Induction uses an induction hypothesis that is essentially the same as the one used for Total Induction.

Section BNT: Basic Number Theory

We review some basics about number theory. Assume $a, b, c, \ldots$ are integers.

- [*divides*] $a \mid b$ means a divides b, i.e., for some c, $b = ac$
- [*floor and ceiling*] $\lfloor a \rfloor$ is the largest integer not greater than a ($\lfloor \cdot \rfloor$ is called the *floor function*) and $\lceil a \rceil$ is the smallest integer not less than a ($\lceil \cdot \rceil$ is called the *ceiling function*).

  Note. The floor function applied to rational numbers a/b yields the same results as Java's integer division when both a and b are positive. However, when one is negative and the other positive, the results differ:

$$\begin{aligned} -5/4 = -(5/4) = -1 & \quad \text{(Java integer division)} \\ \lfloor -5/4 \rfloor = -2 & \quad \text{(mathematics)} \end{aligned}$$

- [*greatest common divisor*] $c = \gcd(a, b)$ means c is the largest integer that divides both a and b
- [primes] A positive integer p is *prime* if its only positive divisors are 1 and p. A positive integer c is *composite* if there are positive integers m, n, both greater than 1, such that $c = m \cdot n$.

Fact. Every integer > 1 is a product of primes. (A prime itself is considered a product of primes.)

Fact. There are infinitely many primes.

- *Fibonacci Numbers.* The sequence $F_0, F_1, F_2, \ldots, F_n, \ldots$ of Fibonacci numbers is defined by

$$\begin{aligned} F_0 &= 0; \\ F_1 &= 1; \\ F_n &= F_{n-1} + F_{n-2}. \end{aligned}$$