Collected Definitions for Exam #4

I can’t recall the last time I didn’t ask a definition question on a 245 exam. To help you better prepare yourself for such questions, I’ve assembled this list. My pledge to you: If I ask you for a definition on the exam, the term will come from this list. Note that this is not a complete list of the definitions given in class. You should know the others, too, but I won’t specifically ask you for their definitions on the exam.

Once in a while a student will express disappointment that I ask definition questions on exams. My justification is that I think it’s important for you to know what the core terms mean so that you can use them correctly for such questions, I’ve assembled this list. My pledge to you: If I ask you for a definition on the exam, the term will come from this list. Note that this is not a complete list of the definitions given in class. You should know the others, too, but I won’t specifically ask you for their definitions on the exam.

The definitions are grouped by lecture topic, and should be in an order within each topic that is at least close to the order in which the definitions appeared in class.

### Topic 10: Integers

- Let $i$ and $j$ be positive integers. $j$ is a factor of $i$ when $i \% j = 0$.
- A positive integer $p$ is prime if $p \geq 2$ and the only factors of $p$ are 1 and $p$.
- A positive integer $p$ is composite if $p \geq 2$ and $p$ is not prime.
- Let $x$ and $y$ be integers such that $x \neq 0$ and $y \neq 0$. The Greatest Common Divisor (GCD) of $x$ and $y$ is the largest integer $i$ such that $i | x$ and $i | y$. That is, $gcd(x, y) = i$.
- If the GCD of $a$ and $b$ is 1, then $a$ and $b$ are relatively prime.
- When the members of a set of integers are all relatively prime to one another, they are pairwise relatively prime.
- Let $x$ and $y$ be positive integers. The Least Common Multiple (LCM) of $x$ and $y$ is the smallest integer $s$ such that $x | s$ and $y | s$. That is, $lcm(x, y) = s$.
- If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a$ and $b$ are congruent modulo $m$ (written $a \equiv b \pmod{m}$) iff $a \% m = b \% m$ (or, iff $m | (a - b)$). (This is just a different phrasing of the definition given in Topic 1. Either is acceptable.)
  - $a$ and $b$ are said to be members of the same congruence class.

### Topic 11: Sequences and Strings

- A sequence is the ordered range of a function from a set of integers to a set $S$.
- In an arithmetic sequence (a.k.a. arithmetic progression) $a$, $a_{n+1} - a_n$ is constant. This constant is called the common difference of the sequence.
- In a geometric sequence (a.k.a. geometric progression) $g$, $\frac{g_{n+1}}{g_n}$ is constant. This constant is called the common ratio of the sequence.
- An increasing (a.k.a. non-decreasing) sequence $i$ is ordered such that $i_n \leq i_{n+1}$.
- A strictly increasing sequence $i$ is ordered such that $i_n < i_{n+1}$.
- A non-increasing (a.k.a. decreasing) sequence $i$ is ordered such that $i_n \geq i_{n+1}$.
- A strictly decreasing sequence $i$ is ordered such that $i_n > i_{n+1}$.
- Sequence $x$ is a subsequence of sequence $y$ when the elements of $x$ are found within $y$ in the same relative order.
- A string is a contiguous finite sequence of zero or more elements drawn from a set called the alphabet.
- A set is finite if there exists a bijective mapping between it and a set of cardinality $n$, $n \in \mathbb{Z}^+$.
- A set is countably infinite (a.k.a. denumerably infinite) if there exists a bijective mapping between the set and either $\mathbb{Z}^+$ or $\mathbb{Z}^+$.
- A set is countable if it is either finite or countably infinite. If neither, the set is uncountable.

(Continued ...)
Topic 12: Induction

- The First Principle of Mathematical Induction: if (i) $P(a)$ is true for the starting point $a \in \mathbb{Z}^+$, and (ii) if $P(k)$ is true for any $k \in \mathbb{Z}^+$, then $P(k+1)$ is true, then $P(n)$ is true for all $n \in \mathbb{Z}^+$, $n \geq a$.

- The Second Principle of Mathematical Induction: if (i) $P(a)$ is true for the starting point $a \in \mathbb{Z}^+$, and (ii) (for any $k \in \mathbb{Z}^+$) if $P(j)$ is true for any $j \in \mathbb{Z}^+$ such that $a \leq j \leq k$, then $P(k+1)$ is true, then $P(n)$ is true for all $n \in \mathbb{Z}^+$, $n \geq a$.

Topic 13: Counting

- I provided two definitions of the (Generalized) Pigeonhole Principle: learn either one:
  1. If $n$ items are placed in $k$ boxes, then at least one box contains at least $\left\lceil \frac{n}{k} \right\rceil$ items.
  2. Let $f : X \to Y$, where $|X| = n$ and $|Y| = k$, and let $m = \left\lceil \frac{n}{k} \right\rceil$. There are at least $m$ values $(a_1, a_2, \ldots, a_m)$ such that $f(a_1) = f(a_2) = \ldots = f(a_m)$.

- The Multiplication Principle (a.k.a. the Product Rule): If there are $s$ steps in an activity, with $n_1$ ways of accomplishing the first step, $n_2$ of accomplishing the second, etc., and $n_s$ ways of accomplishing the last step, then there are $n_1 \cdot n_2 \ldots \cdot n_s$ ways to complete all $s$ steps.

- The Addition Principle (a.k.a. the Sum Rule): If there are $t$ tasks, with $n_1$ ways of accomplishing the first, $n_2$ ways of accomplishing the second, etc., and $n_t$ ways of accomplishing the last, then there are $n_1 + n_2 + \ldots + n_t$ ways to complete one of these tasks, assuming that no two tasks interfere with one another.

- The Principle of Inclusion-Exclusion for Two Sets says that the cardinality of the union of sets $M$ and $N$ is the sum of their individual cardinalities excluding the cardinality of their intersection. That is: $|M \cup N| = |M| + |N| - |M \cap N|$

- The Principle of Inclusion-Exclusion for Three Sets says that the cardinality of the union of sets $M$, $N$, and $O$ is the sum of their individual cardinalities excluding the sum of the cardinalities of their pairwise intersections and including the cardinality of their intersection. That is: $|M \cup N \cup O| = |M| + |N| + |O| - (|M \cap N| + |M \cap O| + |N \cap O|) + |M \cap N \cap O|$

- An ordering of $n$ distinct elements is called a permutation.
- An ordering of an $r$-element subset of $n$ distinct elements is called an $r$-Permutation.
- An $r$-Combination of an $n$-element set $X$ is an $r$-element subset of $X$. The quantity of $r$-element subsets is denoted $C(n, r)$ or $\binom{n}{r}$, and is read “$n$ choose $r$.”

Topic 14: Algorithms

- An algorithm is a finite set of instructions for performing a task.

- A recursive definition has two (sometimes three) parts:
  1. The basis clause determines how trivial cases are to be handled.
  2. The inductive clause explains how complex problems are answered in terms of simpler versions of the same problem.
  3. The extremal clause says that only cases covered by the basis and inductive clauses are covered by the recursive definition. That is, the extremal clause provides boundaries for the definition.

- A recursive algorithm expresses the solution to a task in terms of a simpler case of the same problem.

- The factorial of a non-negative integer $n$, denoted $n!$, is the product of all integer values from 1 through $n$, inclusive. By definition, $0! = 1$.

- The $n^{th}$ term of the Fibonacci sequence is the sum of terms $n-1$ and $n-2$, where $F(0) = 0$ and $F(1) = 1$. 