This is the ‘official’ collection of need-to-know definitions for the CSc 245 final exam. I can’t recall the last time I didn’t ask a definition question on an 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 an exam in this class, it will come from this list.

Once in a while a student will express disappointment that I ask definition questions on exams. I think it’s important that you know what core terms mean so that you can use them correctly and effectively. At the same time, I don’t require that you memorize the exact wording of the definitions you see here. If you provide a definition in your own words that captures all of the detail found here, that’s great.

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

**Topic 1: Course Background**

- *Discrete Mathematics* is the study of collections of distinct objects.

**Topic 2: Logic**

- *Philosophical Logic* is the classical notion of ‘logic’: The study of thought and reasoning, including arguments and proof techniques.
- *Mathematical Logic* is the use of formal languages and grammars to represent the syntax and semantics of computation.
- A *Well-Formed Formula* (wff) is a correctly structured expression of a language.
- A *proposition* (a.k.a. *statement*) is a claim that is either true or false with respect to an associated context.
- A *simple proposition* is a proposition containing no logical operators.
- A claim that is a logical combination of multiple simple propositions is a *compound proposition*.
- Two propositions $p$ and $q$ are *Logically Equivalent* ($p \equiv q$) when both evaluate to the same result when presented with the same input. [Note: An alternate, equally-correct definition is given below.]
- A *Tautology* is a proposition that always evaluates to true.
- A *Contradiction* is a proposition that always evaluates to false.
- A *Contingency* is a proposition that is neither a tautology nor a contradiction.
- The *Inverse* of $p \rightarrow q$ is $\overline{p} \rightarrow \overline{q}$.
- The *Converse* of $p \rightarrow q$ is $q \rightarrow p$.
- The *Contraposition* of $p \rightarrow q$ is $\overline{q} \rightarrow \overline{p}$.
- $p$ and $q$ are *Logically Equivalent*, written $p \equiv q$, if $p \leftrightarrow q$ is a tautology. [Note: An alternate, equally-correct definition is given above.]
Topic 3: Quantification

- A statement that includes at least one variable and will evaluate to either true or false when the variable(s) are assigned value(s) is a **Predicate** (a.k.a. **Propositional Function**).
- The collection of values from which a variable’s value is drawn is known as the **Domain of Discourse** (a.k.a. **Universe of Discourse**).
- A quantified variable in a predicate is a **Bound** variable.
- Unquantified variables are **Free** (a.k.a. **Unbound**) variables.
- The **Generalized De Morgan’s Laws** are the equivalences $\forall x P(x) \equiv \exists x \neg P(x)$ and $\exists x Q(x) \equiv \forall x \neg Q(x)$.

Topic 4: Arguments

- “An **Argument** is a connected series of statements to establish a definite proposition.” [Thanks to Monty Python!]
- An argument that moves from specific observations to a general conclusion is an **Inductive Argument**.
- An argument that uses accepted general principles to explain a specific situation is a **Deductive Argument**.
- Any deductive argument of the form $(p_1 \land p_2 \land \ldots \land p_n) \rightarrow q$ is **Valid** if the conclusion must follow from the hypotheses.
- A valid argument that also has true premises is a **Sound** argument.
- Any unsupported or improperly constructed argument demonstrates **Specious Reasoning**.
- A **Fallacy** is an argument constructed with an improper inference.

Topic 5: Proofs of $p \rightarrow q$

- A **Conjecture** is a statement with an unknown truth value.
- A **Theorem** is a conjecture that has been shown to be true.
- A sound argument that establishes the truth of a theorem is a **Proof**.
- A **Lemma** is a simple theorem whose truth is used to construct more complex theorems.
- A **Corollary** is a theorem whose truth follows directly from another theorem.

Prolog

- A **Horn Clause** is a disjunction of predicates in which at most one of the predicates is not negated.

Topic 6: Sets

- A **set** is an unordered collection of unique objects.
- Set $A$ is a **subset** of set $B$ (written $A \subseteq B$) if every member of $A$ can be found in $B$.
- $A$ is a **proper subset** of $B$ (written $A \subset B$) if $A \subseteq B$ and $A \neq B$.
- The **power set** of a set $A$ (written $\mathcal{P}(A)$) is the set of all of $A$’s subsets, including the empty set.
- Two sets are **disjoint** if their intersection is $\emptyset$.
- A **partition** of a set separates all of its members into disjoint subsets.
- An **ordered pair** is a group of two items $(a, b)$ such that $(a, b) \neq (b, a)$ unless $a = b$.
- The **Cartesian Product** of two sets $A$ and $B$ (written $A \times B$) is the set of all ordered pairs $(a, b)$ such that $a \in A$ and $b \in B$. 
Topic 7: Matrices

- A **matrix** is an \(n\)-dimensional collection of values, \(n \in \mathbb{Z}^+\).
- A **square** matrix is a two-dimensional matrix in which the # of rows equals the # of columns.
- Two matrices \(A\) and \(B\) are **equal** iff they share the same dimensions and each pair of corresponding elements is equal.
- The **transposition** of an \(m \times n\) matrix \(A\) is the \(n \times m\) matrix \(A^T\) in which the rows of \(A\) become the columns of \(A^T\).
- A matrix \(A\) is **symmetric** iff \(A = A^T\).
- The **matrix multiplication** of an \(m \times n\) matrix \(A\) and an \(n \times o\) matrix \(B\) is an \(m \times o\) matrix \(C = A \cdot B\) in which \(c_{ij} = \sum_{k=1}^{n} (a_{ik} \cdot b_{kj})\).
- **Identity matrices**, denoted \(I_n\), are \(n \times n\) matrices populated with 1 down the main diagonal (upper-left to lower-right) and with 0 elsewhere.
- The \(n^{th}\) **matrix power** of an \(m \times m\) matrix \(A\), denoted \(A^n\), is the matrix resulting from \(n-1\) successive matrix products of \(A\). \(A^0 = I_m\).
- The **logical matrix product** of an \(m \times n\) 0–1 matrix \(A\) and an \(n \times l\) 0–1 matrix \(B\) is an \(m \times l\) 0–1 matrix \(C = A \odot B\) in which \(c_{ij} = \bigvee_{k=1}^{n} (a_{ik} \wedge b_{kj})\).
- The \(r^{th}\) **logical matrix power** of an \(m \times m\) 0–1 matrix \(A\), denoted \(A^{|r|}\), is the matrix resulting from \(r-1\) successive logical matrix products of \(A\). \(A^{[0]} = I_m\).

Topic 8: Relations

- A **(binary) relation** from set \(X\) to set \(Y\) is a subset of the Cartesian Product of the domain \(X\) and the codomain \(Y\).
- A relation \(R\) on set \(A\) is **reflexive** if \((a, a) \in R\), \(\forall a \in A\).
- A relation \(R\) on set \(A\) is **symmetric** if, whenever \((a, b) \in R\), then \((b, a) \in R\), for \(a, b \in A\).
- A relation \(R\) on set \(A\) is **antisymmetric** if \((x, y) \in R\) and \(x \neq y\), then \((y, x) \notin R\), \(\forall x, y \in A\).
- A relation \(R\) on set \(A\) is **transitive** if whenever \((a, b) \in R\) and \((b, c) \in R\), then \((a, c) \in R\), for \(a, b, c \in A\).
- The **inverse** of a relation \(R\) on set \(A\), denoted \(R^{-1}\), contains all of the ordered pairs of \(R\) with their components exchanged. (That is, \(R^{-1} = \{(b, a) \mid (a, b) \in R\}\).)
- Let \(G\) be a relation from set \(A\) to set \(B\), and let \(F\) be a relation from \(B\) to set \(C\). The **composite of \(F\)** and \(G\), denoted \(F \circ G\), is the relation of ordered pairs \((a, c), a \in A, c \in C\), such that \(b \in B\), \((a, b) \in G\), and \((b, c) \in F\).
- A relation \(R\) on set \(A\) is a **(reflexive/weak) partial order** if it is reflexive, antisymmetric, and transitive.
- A relation \(R\) on set \(A\) is **irreflexive** if for all members of \(A\), \((a, a) \notin R\).
- A relation \(R\) on set \(A\) is an **irreflexive (or strict) partial order** if it is irreflexive, antisymmetric, and transitive.
- A relation \(R\) on set \(A\) is an **equivalence relation** if it is reflexive, symmetric, and transitive.
- The **equivalence class** of an equivalence relation \(R\) on set \(B\), and an element \(b \in B\), is \(\{c \mid c \in B \land (b, c) \in R\}\) and is denoted \([b]\). That is, the equivalence class is the set of all elements of the base relation equivalent to a given element as defined by the relation.
- Let \(R\) be a weak partial order on set \(A\). \(a\) and \(b\) are said to be **comparable** if \(a, b \in A\) and either \(a \preceq b\) or \(b \preceq a\) (that is, \((a, b) \in R\) or \((b, a) \in R\)).
- A weak partially-ordered relation \(R\) on set \(A\) is a **total order** if every pair of elements \(a, b \in A\) are comparable.
Topic 9: Functions

- A function from set $X$ to set $Y$, denoted $f : X \rightarrow Y$, is a relation from $X$ to $Y$ such that $f(x)$ is defined $\forall x \in X$ and, for each $x \in X$, there is exactly one $(x, y) \in f$.
- For each of the following, let $f : X \rightarrow Y$ be a function, and assume $f(n) = p$.
  - $X$ is the domain of $f$.
  - $Y$ is the codomain of $f$.
  - $f$ maps $X$ to $Y$.
  - $p$ is the image of $n$.
  - $n$ is the pre-image of $p$.
  - The range of $f$ is the set of all images of elements of $X$. (Note that the range need not equal the codomain.)
- A function $f : X \rightarrow Y$ is injective (a.k.a. one-to-one) if, for each $y \in Y$, $f(x) = y$ for at most one member of $X$.
- A function $f : X \rightarrow Y$ is surjective (a.k.a. onto) if $f$’s range is $Y$ (the range = the codomain).
- A bijective function (a.k.a. a one-to-one correspondence) is both injective and surjective.
- The inverse of a bijective function $f$, denoted $f^{-1}$, is the relation $\{(y, x) \mid (x, y) \in f\}$.
- Let $f : Y \rightarrow Z$ and $g : X \rightarrow Y$. The composition of $f$ and $g$, denoted $f \circ g$, is the function $h = f(g(x))$, where $h : X \rightarrow Z$.
- A function $f : X \times Y \rightarrow Z$ (or $f(x, y) = z$) is a binary function.

Topic 10: Properties of 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 $a \equiv b \ (\text{mod } m)$) 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) $g$, $\frac{a_{n+1}}{a_n}$ 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.

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:
  (a) if $n$ items are placed in $k$ boxes, then at least one box contains at least $\left\lceil \frac{n}{k} \right\rceil$ items.
  (b) Let $f : X \rightarrow Y$, 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 $n_1 \cdot n_2 \cdot \ldots \cdot n_s$ 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 \(F(1) = 1\).

Topic 15: Recurrence Relations

- A recurrence relation for the sequence \(a_0, a_1, \ldots\) is an equation that expresses term \(a_k\) in terms of one or more of its preceding sequence members, one of more of which are explicitly stated initial conditions of the sequence.
- A linear homogeneous recurrence relation with constant coefficients of degree (or order) \(k\) (abbreviated: LHRRWCC of degree \(k\)) has the form \(R(n) = c_1R(n-1) + c_2R(n-2) + \ldots + c_kR(n-k)\), where \(c_i \in \mathbb{R}\) and \(c_k \neq 0\).

Topic 16: Finite Probability

- The probability that a specific event will occur is the ratio of the number of occurrences of interest to the number of possible occurrences.

  NOTE: The next two definitions are included just in case I have time in lecture to talk about them. If I don’t cover them in class, you don’t have to know them.

- Let \(X\) and \(Y\) be events. The conditional probability of \(X\) given \(Y\), denoted \(p(X|Y)\), is \(\frac{p(X \cap Y)}{p(Y)}\).
- If \(p(A|B) = p(A)\), then the events \(A\) and \(B\) are independent.