CS 13: Mathematical Foundations of Computer Science

Definitions and Theorems

What Is This?

This is a complete[1] listing of definitions and theorems relevant to CS 13. The goal of this document is less as a reference and more as a way of indicating what is and is not allowed to be assumed in proofs.

Contents

[1] It's not actually complete. It's probably missing a lot. If you find an error or a missing theorem, please let us know! We will give you a rubber ducky.

1 Arithmetic

This section is all about arithmetic. You'll find that you can basically assume anything about arithmetic that you learned in high school algebra or earlier.

1.1 Definitions

Arithmetic Expression of Real Numbers — DEFINITION

An arithmetic expression of real numbers is an expression made up of real numbers, variables representing real numbers, addition, multiplication, subtraction, division, exponentiation, and logarithms.

Zero — CONSTANT

Zero (0, the additive identity) is the constant real number such that for any arithmetic expression X, $0 + X = X = X + 0$.

One — CONSTANT

One (1, the multiplicative identity) is the constant real number such that for any arithmetic expression X, $1 \cdot X = X = X \cdot 1$.

2 Equality

This section is all about equalities. You'll find that you can basically assume anything about arithmetic that you learned in high school algebra or earlier.

2.1 Definitions

Equality for Real Numbers — DEFINITION

If X and Y are two real numbers, then $X = Y$ ("X equals Y") when both expressions "evaluate" to the same real number.
(This means you should use what you learned in high school about these types of expressions.)

Inequality for Real Numbers — DEFINITION

If X and Y are two real numbers, then $X \neq Y$ ("X does not equal Y") when $\neg(X = Y)$.

2.2 Theorems

Reflexivity of Equality for Real Numbers — THEOREM

If x is a real number, then $x = x$.

Symmetry of Equality for Real Numbers — THEOREM

If x, y are real numbers, then $x = y \iff y = x$.

Transitivity of Equality for Real Numbers — THEOREM

If x, y, and z are real numbers, then $(x = y \wedge y = z) \implies x = z$.

Identities for Real Numbers — THEOREM

If x is a real number, then:

- $x + 0 = x = 0 + x$
- $x \cdot 1 = x = 1 \cdot x$
- $x^0 = 1$ (unless x evaluates to 0, in which case x^0 is undefined)
- $0^x = 0$ (unless x evaluates to 0, in which case 0^x is undefined)
- $1^x = 1$
- $x/1 = x$

Domination for Real Numbers — THEOREM

If x is a real number, then:

- $x \cdot 0 = 0 = 0 \cdot x$
- $x \cdot 1 = x = 1 \cdot x$

Inverse Operations for Real Numbers — THEOREM

If a and b are real numbers, then:

- $a - b = a + (-b)$
- $a \cdot \frac{b}{a} = b$

Inverses for Real Numbers — THEOREM

If x and b are real numbers, then:

- $x + (-x) = 0 = (-x) + x$
- $x \cdot \frac{1}{x} = 1 = \frac{1}{x} \cdot x$ (unless x evaluates to 0)
- $b^{\log_b(x)} = x$
- $\log_b(b^x) = x$
- $-(-x) = x$

Associativity of Arithmetic Expressions — THEOREM

If x, y, and z are real numbers, then:

- $(x + y) + z = x + (y + z)$
- $(xy)z = x(yz)$

As a consequence, we can omit the parentheses in these expressions.

Commutativity of Arithmetic Expressions — THEOREM

If x and y are real numbers, then:

- $x + y = y + x$
- $xy = yx$

Distributivity of Arithmetic Expressions — Theorem

If $a, b, c,$ and d are real numbers, then:

- $a(b+c) = ab + ac$
- $(a+b)(c+d) = ac + ad + bc + bd$

Algebraic Properties of Real Numbers — Theorem

If a, b, c, and d are real numbers, then:

- $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$
- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
- $(a^b)(a^c) = a^{b+c}$
- $\left(a^b\right)^c = a^{bc}$
- $\log_c(ab) = \log_c(a) + \log_c(b)$
- $\log_c\left(\frac{a}{b}\right) = \log_c(a) - \log_c(b)$

Adding Equalities — Theorem

If a and b are real numbers, $a = b$, and $c = d$, then $a + c = b + d$.

Multiplying Equalities — Theorem

If a and b are real numbers, $a = b$, and $c = d$, then $ac = bd$.

Dividing Equalities — Theorem

If a and b are real numbers, $a = b$, and $c \neq 0$, then $\frac{a}{c} = \frac{b}{c}$

Subtracting Equalities — Theorem

If a and b are real numbers, $a = b$, and $c = d$, then $a - c = b - d$.

Raising Equalities To A Power — Theorem

If a and b are real numbers and $a = b$, then $a^c = b^c$.

Log Change-Of-Base Formula — Theorem

If x, a, and b are real numbers, $x, a, b > 0$, $a \neq 1$, $b \neq 1$, then $\log_a(x) = \frac{\log_b(x)}{\log_b(a)}$

Powers of -1 — Theorem

For any $n \in \mathbb{N}$, $(-1)^{2n} = 1$ and $(-1)^{2n+1} = -1$.

3 Inequalities

This section is all about inequalities. You'll find that you can basically assume anything about arithmetic that you learned in high school algebra or earlier.

3.1 Definitions

Less-Than for Real Numbers DEFINITION

If x and y are two real numbers, then $x < y$ ("x is less than y") when x "evaluates" to a smaller real number than y evaluates to.
(This means, use what you learned in high school about these types of expressions.)

Greater-Than for Real Numbers DEFINITION

If x and y are two real numbers, then $x > y$ ("x is greater than y") when $y < x$.

Less-Than-Or-Equal-To for Real Numbers DEFINITION

If x and y are two real numbers, then $x \leq y$ ("x is less than or equal to y") when $\neg(x > y)$.

Greater-Than-Or-Equal-To for Real Numbers DEFINITION

If x and y are two real numbers, then $x \geq y$ ("x is greater than or equal to y") when $\neg(x < y)$.

3.2 Theorems

Trichotomy for Real Numbers THEOREM

If x and y are two real numbers, then $x = y \vee x < y \vee x > y$.

Antisymmetry of Inequality for Real Numbers THEOREM

If x, y are real numbers, then $(x \leq y \wedge y \leq x) \implies x = y$.

Transitivity of Inequality for Real Numbers THEOREM

If x, y, and z are real numbers, then $(x < y \wedge y < z) \implies x < z$.

Adding Inequalities THEOREM

If a and b are real numbers, $a < b$ and $c < d$, then $a + c < b + d$.

Subtracting Inequalities THEOREM

If a and b are real numbers and $a < b$ and $c > d$, then $a - c < b - d$.

Multiplying (Positive) Inequalities THEOREM

If a and b are real numbers, $0 < a < b$ and $0 < c < d$, then $0 < ac < bd$.

Multiplying (Negative) Inequalities THEOREM

If a and b are real numbers, $a < 0$, and $b < 0$, then $ab > 0$.

Inverting Inequalities THEOREM

If a and b are real numbers and $0 < a < b$, then $\frac{1}{a} > \frac{1}{b} > 0$.

Same Sign THEOREM

If a and b are real numbers and $ab > 0$, then a and b are both positive or a and b are both negative.

Squares Are Non-negative THEOREM

If a is a real number, then $a^2 \geq 0$.

4 Absolute Value

This section is all about absolute values. In general, we don't care much about absolute values, but they're something easy to prove things about. So, we list out a bunch of theorems you may use here.

4.1 Definitions

Absolute Value DEFINITION

If x is a real number, then

$$|X| = \begin{cases} X & \text{if } X \geq 0 \\ -X & \text{if } X < 0 \end{cases}$$

4.2 Theorems

Absolute Value Magnitude THEOREM

If x and M are real numbers and $M \geq 0$, then $|x| \leq M \iff -M \leq x \leq M$.

Positive Definite THEOREM

If x is a real number, then $|x| \geq 0$ and $|x| = 0 \iff x = 0$.

Multiplying Absolute Values THEOREM

If x and y are real numbers, then $|xy| = |x||y|$

Triangle Inequality THEOREM

If x and y are real numbers, then $|x + y| \leq |x| + |y|$.

5 Parity

This section is all about parity (even-ness/odd-ness) of integers. Unlike all the previous sections, we will use this as a starting point for discussing proofs. This means that you may *only* assume what is written here explicitly and nothing more.

5.1 Definitions

Even — DEFINITION

An integer n is *even* iff $\exists k\ (n = 2k)$

Odd — DEFINITION

An integer n is *odd* iff $\exists k\ (n = 2k + 1)$

Perfect Square — DEFINITION

An integer n is a *perfect square* iff there exists an integer x for which $n = x^2$.

Closure Under $\star$ — DEFINITION

A set S is *closed* under a binary operation $\star$ iff $x \star x$ is an element of S.

5.2 Theorems

$\mathbb{Z}$ is closed under $+$ — THEOREM

The integers are closed under addition.

$\mathbb{Z}$ is closed under $\times$ — THEOREM

The integers are closed under multiplication.

The square of every even integer is even — THEOREM

If n is even, then n^2 is even.

The square of every odd number is odd — THEOREM

If n is odd, then n^2 is odd.

The sum of two odd numbers is even — THEOREM

If n and m are odd, then $n + m$ is even.

No even number is the largest even number — THEOREM

For all even numbers n, there exists a larger even number m.

$\mathbb{Z}$ is closed under $-$ — THEOREM

The integers are closed under subtraction.

$\mathbb{Z}$ is not closed under $/$ — THEOREM

The integers are *not* closed under division.

No Integer is Odd and Even — THEOREM

If n is an integer, n is not both odd and even.

Every Integer is Odd or Even — THEOREM

If n is an integer, n is even or odd.

6 Logic

6.1 Definitions

Boolean True — DEFINITION

$\top$ is a logical formula that is always true.

Boolean False — DEFINITION

$\bot$ is a logical formula that is always false.

Boolean Not — DEFINITION

If p is a logical formula, then $\neg p$ is true exactly when $p = \bot$ and false otherwise.

Boolean And — DEFINITION

If p and q are logical formulae, then $p \wedge q$ is true exactly when both $p = \top$ and $q = \top$ and false otherwise.

Boolean Or — DEFINITION

If p and q are logical formulae, then $p \vee q$ is true exactly when at least one of $p = \top$ and $q = \top$ and false otherwise.

Boolean Implication — DEFINITION

If p and q are logical formulae, then $p \implies q$ is true exactly when $\neg p \vee q$ is true.

Boolean Equivalence — DEFINITION

If p and q are logical formulae, then $p \iff q$ is true exactly when p and q have the same truth value.

6.2 Theorems

DeMorgan's Laws for Logic — THEOREM

If p and q are logical formulae, then $\neg(p \vee q) \iff \neg p \wedge \neg q$ and $\neg(p \wedge q) \iff \neg p \vee \neg q$.

Distributivity for Logic — THEOREM

If p, q, and r are logical formulae, then $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$ and $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$.

7 Rationals

This section is all about rational numbers. We also use proofs about rational numbers as a starting point for discussing proofs. This means that you may *only* assume what is written here explicitly and nothing more.

7.1 Definitions

Rational — DEFINITION

A real number x is *rational* iff there are two integers p and $q \neq 0$ such that $x = \frac{p}{q}$.

7.2 Theorems

$\mathbb{Q}$ is closed under $+$ — THEOREM

The rationals are closed under addition (and subtraction)

$\mathbb{Q}$ is closed under $\times$ — THEOREM

The rationals are closed under multiplication

$\mathbb{R} \setminus \mathbb{Q}$ is not closed under $+$ — THEOREM

The irrationals are not closed under addition.

8 Sets

8.1 Definitions

The Set of Natural Numbers — DEFINITION

$\mathbb{N} = \{0, 1, 2, \dots\}$ is the set of *Natural Numbers*
$\mathbb{N}_+ = \{1, 2, 3, \dots\}$ is the set of positive natural numbers. (Note that this is the same as $\mathbb{Z}_+$.)

The Set of Integers — DEFINITION

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of *Integers*.
$\mathbb{Z}_+ = \{1, 2, 3, \dots\}$ is the set of positive integers.

The Set of Rationals — DEFINITION

$\mathbb{Q} = \left\{ \dfrac{p}{q} : p, q \in \mathbb{Z} \wedge q \neq 0 \right\}$ is the set of *Rational Numbers*.
$\mathbb{Q}_+ = \left\{ \dfrac{p}{q} : p, q \in \mathbb{Z} \wedge p, q > 0 \right\}$ is the set of positive rational numbers.

The Set of Reals — DEFINITION

$\mathbb{R}$ is the set of *Real Numbers*.
$\mathbb{R}_+$ is the set of positive real numbers.

Set Inclusion — DEFINITION

If A and B are sets, then $x \in A$ ("x is an *element* of A") means that x is an element of A, and $x \notin A$ ("x is *not* an *element* of A") means that x is *not* an element of A.

The Empty Set — DEFINITION

$\varnothing$, also written as $\emptyset$ or $\{\}$, is the *empty set*. It contains nothing; that is, for all x, $x \notin \varnothing$.

Set Equality — DEFINITION

If A and B are sets, then $A = B$ iff $\forall x\,(x \in A \iff x \in B)$.

Subset and Superset — DEFINITION

If A and B are sets, then $A \subseteq B$ ("A is a *subset* of B") means that all the elements of A are also in B, and $A \supseteq B$ ("A is a *superset* of B") means that all the elements of B are also in A.

Set Comprehension — DEFINITION

If $P(x)$ is a predicate, then $\{x : P(x)\}$ is the set of all elements for which $P(x)$ is true. Also, if S is a set, then $\{x \in S : P(x)\}$ is the subset of all elements of S for which $P(x)$ is true.

Set Union — DEFINITION

If A and B are sets, then $A \cup B$ is the *union* of A and B. $A \cup B = \{x : x \in A \vee x \in B\}$.

Set Intersection — DEFINITION

If A and B are sets, then $A \cap B$ is the *intersection* of A and B. $A \cap B = \{x : x \in A \wedge x \in B\}$.

Set Difference — DEFINITION

If A and B are sets, then $A \setminus B$ is the *difference* of A and B. $A \setminus B = \{x : x \in A \wedge x \notin B\}$.

Set Symmetric Difference — DEFINITION

If A and B are sets, then $A \oplus B$ is the *symmetric difference* of A and B. $A \oplus B = \{x : x \in A \oplus x \in B\}$.

Set Complement — DEFINITION

If A is a set, then $\overline{A}$ is the *complement* of A. If we restrict ourselves to a "universal set", $\mathcal{U}$ (a set of all possible things we're discussing), then $\overline{A} = \{x \in \mathcal{U} : x \notin A\}$.

Brackets n — DEFINITION

If $n \in \mathbb{N}$, then $[n]$ ("*brackets* n") is the set of natural numbers from 1 to n. $[n] = \{x \in \mathbb{N} : 1 \leq x \leq n\}$.

Cartesian Product — DEFINITION

If A and B are sets, then $A \times B$ is the *cartesian product* of A and B. $A \times B = \{(a, b) : a \in A,\ b \in B\}$.

Powerset — DEFINITION

If A is a set, then $\mathcal{P}(A)$ is the *power set* of A. $\mathcal{P}(A) = \{S : S \subseteq A\}$.

Disjoint Sets — DEFINITION

Two sets A and B are disjoint if they share no elements, i.e., they are disjoint if

$$A \cap B = \varnothing.$$

8.2 Theorems

Subset Containment — THEOREM

If A and B are sets, then $(A = B) \iff (A \subseteq B \wedge B \subseteq A)$.

Russell's Paradox — THEOREM

The set of all sets that do not contain themselves does not exist. That is, $\{x : x \notin x\}$ does not exist.

DeMorgan's Laws for Sets — THEOREM

If A and B are sets, then $\overline{A \cup B} = \overline{A} \cap \overline{B}$ and $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

Distributivity for Sets — THEOREM

If A and B are sets, then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

$A \cap B \subseteq A$ — THEOREM

If A and B are sets, then $A \cap B \subseteq A$.

9 Modular Arithmetic

9.1 Definitions

$a \mid b$ ("a *divides* b") — DEFINITION

For $a, b \in \mathbb{Z}$, where $a \neq 0$:

$$a \mid b \text{ iff } \exists (k \in \mathbb{Z})\ b = ka$$

$a \equiv_m b$ ("a *is congruent to* b *modulo* m) — DEFINITION

For $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$:

$$a \equiv_m b \text{ iff } m \mid (a - b)$$

Multiplicative group of integers mod m — DEFINITION

The multiplicative group of integers mod m is made up of the set of integers relatively prime to m from the set $\{0, 1, \ldots, m-1\}$ with multiplication performed mod m, and is denoted $\mathbb{Z}_m$.

Multiplicative inverse — DEFINITION

The multiplicative inverse of an element $n \in \mathbb{Z}_m$ is the unique element $a \in \mathbb{Z}_m$ such that $an \equiv 1$.

9.2 Theorems

Mod is idempotent — Theorem

$E_1 \text{ mod } m = a$, then $a \text{ mod } m = a$ for any $m \in \mathbb{Z}^+$.

Mod preserves equality — Theorem

If you have an equality $E_1 = E_2$, then $E_1 \text{ mod } m = E_2 \text{ mod } m$ for any $m \in \mathbb{Z}^+$.

Division Theorem — Theorem

If $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, then there exist unique $q, r \in \mathbb{Z}$, where $0 \leq r < d$ such that $a = dq + r$.
We call $q = a$ **div** d and $r = a$ **mod** d.

Relation Between Mod and Congruences — Theorem

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv_m b \iff a \text{ mod } m = b \text{ mod } m$.

Adding Congruences — Theorem

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(a \equiv_m b \wedge c \equiv_m d) \implies a + c \equiv_m b + d$.

Multiplying Congruences — Theorem

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(a \equiv_m b \wedge c \equiv_m d) \implies ac \equiv_m bd$.

Squares are congruent to 0 or 1 mod 4 — Theorem

If $n \in \mathbb{Z}$, then $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$.

Additivity of mod — Theorem

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(a + b) \text{ mod } m = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$

Multiplicativity of mod — Theorem

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $(ab) \text{ mod } m = ((a \text{ mod } m)(b \text{ mod } m)) \text{ mod } m$

Base b Representation of Integers — Theorem

Suppose n is a positive integer (in base b) with exactly m digits.
Then, $n = \sum_{i=0}^{m-1} d_i b^i$, where d_i is a constant representing the i-th digit of n.

Raising Congruences To A Power — Theorem

If $a, b, i \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv_m b \implies a^i \equiv_m b^i$.

10 Functions

10.1 Definitions

Function — DEFINITION

A *function* $f : X \to Y$ is a mapping from each element of a set X to exactly one element of Y. The set X is called the *domain* of f and the set Y is called the *codomain*.

Injection — DEFINITION

A function $f : X \to Y$ is called an *injection* iff, for all $x, y \in X$, $f(x) = f(y) \implies x = y$ (i.e., f does not map distinct elements of its domain to the same element in its codomain).

Surjection — DEFINITION

A function $f : X \to Y$ is called a *surjection* iff for all elements $y \in Y$, there exists $x \in X$ such that $f(x) = y$ (i.e., every element in its codomain Y is mapped to by at least one element of its domain X).

Bijection — DEFINITION

A function $f : X \to Y$ is called a *bijection* iff it is injective and surjective (i.e., it defines a one-to-one correspondence between elements of X and Y).

Increasing — DEFINITION

A function $f : X \to \mathbb{R}$ defined on $X \subseteq \mathbb{R}$ is *increasing* iff $x < y \implies f(x) \leq f(y)$. If this inequality is strict (i.e. $x < y \implies f(x) < f(y)$), the function is *strictly increasing*.

Decreasing — DEFINITION

A function $f : X \to \mathbb{R}$ defined on $X \subseteq \mathbb{R}$ is *decreasing* iff $x < y \implies f(x) \geq f(y)$. If this inequality is strict (i.e. $x < y \implies f(x) > f(y)$), the function is *strictly decreasing*.

Monotonic — DEFINITION

A function $f : X \to \mathbb{R}$ defined on $X \subseteq \mathbb{R}$ is *monotonic* if it is increasing or decreasing. It is *strictly monotonic* if it is strictly increasing or strictly decreasing.

11 Summations

11.1 Closed Forms

Gauss Summation — THEOREM

For all $n \in \mathbb{N}$, $\displaystyle\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Infinite Geometric Series — THEOREM

For $-1 < x < 1$, $\displaystyle\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$.

Finite Geometric Series — THEOREM

For $x \in \mathbb{R}, n \in \mathbb{N}$, $\sum_{i=0}^{n} x^i = \left(\frac{1}{1-x}\right) - \left(\frac{x^{n+1}}{1-x}\right) = \frac{1-x^{n+1}}{1-x}$

11.2 Theorems

Binomial Theorem — THEOREM

For all $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

12 Primes

12.1 Definitions

Factor — DEFINITION

A *factor* of an integer n is an integer f such that $\exists x\ (n = fx)$. Alternatively, f is a factor of n iff $f \mid n$.

Prime — DEFINITION

A integer $p > 1$ is *prime* iff the only positive factors of p are 1 and p.

Composite — DEFINITION

A integer $p > 1$ is *composite* iff it's not prime. That is, an integer $p > 1$ is composite iff it has a factor other than 1 and p.

Trivial Factor — DEFINITION

A *trivial factor* of an integer n is 1 or n. We call it a "trivial factor", because all numbers have these factors.

Coprime / Relatively Prime — DEFINITION

Two integers, a and b, are *coprime* (or *relatively prime*) if the only positive integer that divides both of them is 1. That is, their prime factorizations don't share any primes.

12.2 Theorems

Fundamental Theorem of Arithmetic — THEOREM

Every natural number can be *uniquely* expressed as a product of primes raised to powers.

All Composite Numbers Have a Small Non-Trivial Factor — THEOREM

If n is a composite number, then it has a non-trivial factor $f \in \mathbb{N}$ where $f \leq \sqrt{n}$.

Euclid's Theorem — THEOREM

There are infinitely many primes.

13 GCD

13.1 Definitions

GCD (Greatest Common Divisor) — DEFINITION

The *gcd* of two integers, a and b, is the largest integer d such that $d \mid a$ and $d \mid b$.

Euclidean Algorithm — ALGORITHM

```
gcd(a, b) {
   if (b == 0) {
      return a;
   }
   else {
      return gcd(b, a mod b);
   }
}
```

13.2 Theorems

GCD Property — THEOREM

For any $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = \gcd(b, a \text{ mod } b)$.

GCD Equation — THEOREM

For any $a, b \in \mathbb{Z}$,

$$\gcd(a, b) = \min\{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$$

14 Structures

14.1 Definitions

Lists — DEFINITION

A list L defined over a set A is either empty (denoted $[]$) or $x :: L'$ where $x \in A$ and L' is also a list over A. The operator :: is denoted "concatenation".

Trees — DEFINITION

A tree defined over a set A is either empty (denoted `Nil`) or is defined and **Tree**(x, L, R) where L and R are also trees over A.

14.2 Theorems

15 Counting

15.1 Definitions

Size — DEFINITION

The *size* of a finite set A, denoted $|A|$, is the number of elements in the set.

Counting Permutations — DEFINITION

The number of ways to order a set A with $|A| = n$ elements is denoted by $n!$. This quantity is called the *factorial* of n.

Counting Choices — DEFINITION

The number of ways to choose a subset B of a set A where $|B| = k$ and $|A| = n$ is denoted by $\binom{n}{k}$. This quantity is called n *choose* k.

15.2 Theorems

Rule of Product — THEOREM

For any two finite sets A, B, the size of their Cartesian product is the product of their sizes, i.e.,

$$|A \times B| = |A| \cdot |B|$$

Rule of Sum — THEOREM

A and B are disjoint finite sets if and only if $|A \cup B| = |A| + |B|$.

Counting Permutations — THEOREM

The value of $n!$ is the product $1 \cdot 2 \cdots n$.

Counting Choices — THEOREM

The value of $\binom{n}{k}$ is $\frac{n!}{k!(n-k)!}$.

Inclusion-Exclusion (two sets) — THEOREM

The size of the union of two sets is given by:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Inclusion-Exclusion (n sets) — THEOREM

The size of the union of n sets, S_i, is given by:

$$|\cup_{i=1}^{n} S_i| = \sum_{k=1}^{n} \left((-1)^{k-1} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| = k}} |S_I| \right)$$

Where S_I denotes the intersection of the events S_i for $i \in I$.

16 Probability

16.1 Definitions

Random Primitive — DEFINITION

A random primitive is a piece of code with a set of possible return values V, which it selects between using randomness.

`FlipCoin(p)` — DEFINITION

`FlipCoin(p)` is a random primitive. It returns `HEADS` with probability $0 \leq p \leq 1$ and `TAILS` otherwise.

`RollDice(N)` — DEFINITION

`RollDice(N)` is a random primitive. It returns $x \in [N]$ with probability $1/N$.

Outcome — DEFINITION

An *outcome* for a piece of code R with random primitives is a sequence of values for all random results in R.

Sample Space — DEFINITION

The *sample space* of R is the set of all possible outcomes of running R.

Event — DEFINITION

An *event* $E \subseteq S, E$ is a subset of the sample space S, i.e. a collection of possible outcomes.

Probability — DEFINITION

Let S be a sample space and $E \subseteq S$ be an event. Then, we say $\Pr(E)$ is the *probability* that running R results in an outcome in E. We define:

- $0 \leq \Pr(E) \leq 1$.
- $\Pr(S) = 1$.
- If events $E_1, E_2, \ldots, E_n \subseteq S$ are pairwise disjoint, then

$$\Pr(E_1 \cup E_2 \cup \cdots \cup E_n) = \sum_{i=1}^{n} \Pr(E_i)\,.$$

- For any set X which is not an event (i.e. $X \not\subseteq S$), $\Pr(X) = 0$.
- $\Pr(\varnothing) = 0$.

Equiprobable — DEFINITION

Let S be the sample space of R. We say that the outcomes of R are *equiprobable* if and only if, for all events $E \subseteq S$

$$\Pr(E) = \frac{|E|}{|S|}.$$

Conditional Probability — Definition

The *conditional probability* of an event A given that an event B has occurred is denoted $\Pr(A \mid B)$,

$$\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)}$$

provided that $\Pr(B) \neq 0$.

Independent Events — Definition

Two events A and B are said to be *independent* if the occurrence of one does not affect the occurrence of the other. Formally, A and B are independent if and only if the probability that both A and B occur is given by $\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$.

Random variable — Definition

A random variable is a variable whose value is dependent on a random primitive. In this class, random variables take on values in the natural numbers (in general, you can have other kinds). Formally, a random variable is a function from the sample space to the natural numbers.

Expectation — Definition

The expectation of a random variable is a weighted average over all of its outcomes. Formally, for a random variable X over a sample space Ω the expectation is,

$$\mathbb{E}[X] = \sum_{\omega \in \Omega} X(\omega) \cdot \Pr(\omega) = \sum_{x=0}^{\infty} x \cdot \Pr(X = x)$$

16.2 Theorems

Independence and Conditional Probability — Theorem

Consider any two events A and B and suppose $\Pr(B) > 0$. Then A and B are independent if and only if $\Pr(A \mid B) = \Pr(A)$.
Similarly, if $\Pr(A) > 0$, then A and B are independent if and only if $\Pr(B \mid A) = \Pr(B)$.

Inclusion-Exclusion (two events) — Theorem

The probability that either of two events A or B occurs (or both) is given by:

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) - \Pr(A \cap B)\,.$$

Inclusion-Exclusion (n events) — Theorem

The probability that any of the events E_i occurs is given by:

$$\Pr(\cup_{i=1}^{n} E_i) = \sum_{k=1}^{n} \left((-1)^{k-1} \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ |I| = k}} \Pr(E_I) \right)$$

Where E_I denotes the intersection of the events E_i for $i \in I$.

Law of Total Probability — THEOREM

Let $B_1, B_2, \ldots, B_n$ be a partition of the sample space S. Then for any event A:

$$\Pr(A) = \sum_{i=1}^{n} \Pr(A \mid B_i) \times \Pr(B_i)$$

Linearity of Expectation — THEOREM

If $X_1, X_2, \ldots, X_n$ is a sequence of n arbitrary random variables and $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a sequence of real numbers,

$$\mathbb{E}\left[\sum_{k=1}^{n} \alpha_k X_k\right] = \sum_{k=1}^{n} \alpha_k \mathbb{E}\left[X_k\right]$$

Common forms of this result are when $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 1$, in which case we have

$$\mathbb{E}\left[\sum_{k=1}^{n} X_k\right] = \sum_{k=1}^{n} \mathbb{E}\left[X_k\right]$$

and the case where $n = 1$, in which case we have

$$\mathbb{E}[\alpha X] = \alpha \mathbb{E}[X].$$

If you are only using one of the two simplified forms, you can cite the simplified form directly as "linearity of expectation," you do not need to bring in the full form.

17 Graph Theory

17.1 Definitions

Graph — DEFINITION

A *graph* G is an ordered pair (V, E) where:

- V is a finite set of vertices.
- E is a finite set of edges, where each edge is a set $\{v_1, v_2\}$ containing two vertices.

Degree — DEFINITION

Given a graph $G = (V, E)$, the *degree* of a vertex $v \in V$ is the total number of edges adjacent to the vertex. Formally,

$$d(v) = \left|\{e \in E : v \in e\}\right|.$$

Neighbor — DEFINITION

Given a graph $G = (V, E)$, a vertex $v \in V$ is a *neighbor* of a vertex $w \in V$ (where $v \neq w$) if they are connected with an edge. Formally, v is a neighbor of w if and only if $\{v, w\} \in E$.

Walk — DEFINITION

A *walk* in a graph is a sequence of vertices such that each adjacent pair of vertices in the sequence is connected by an edge.

Trail — DEFINITION

A *trail* in a graph is a walk in which all connecting edges are distinct.

Path — DEFINITION

A *path* in a graph is a walk in which all vertices are distinct.

Connected — DEFINITION

A graph G is *connected* iff for every pair of vertices $u, v \in V(G)$, there exists a path in G connecting u and v.

Cycle — DEFINITION

A *cycle* in a graph is a trail that starts and ends at the same vertex.

Acyclic — DEFINITION

A graph is *acyclic* if it contains no cycles.

Tree — DEFINITION

A *tree* is a connected, acyclic graph.

Component — DEFINITION

A *component* of a graph is a maximal connected subgraph, meaning that it is not possible to add any more edges or vertices from the graph and still have a connected subgraph.

Bipartite — DEFINITION

A graph $G = (V, E)$ is *bipartite* if V can be partitioned into two disjoint sets, A and B, such that every edge connects a vertex in A to a vertex in B.

n-colorable — DEFINITION

A graph $G = (V, E)$ is *n-colorable* if there exists a function $c : V \to \{1, 2, \ldots, n\}$ such that there does not exist an edge $(u, v) \in E$ with $c(u) = c(v)$.

17.2 Theorems

Handshake Theorem — THEOREM

In any graph, the sum of all vertex degrees is equal to twice the number of edges.

Trees and Edges — THEOREM

A tree with n vertices has exactly $n - 1$ edges.

Euler's Formula — THEOREM

For any connected planar graph with n vertices, m edges, and f faces, the following equation holds:

$$n - m + f = 2.$$

Two-Colorability — THEOREM

A graph is bipartite if and only if it is two-colorable.

Existence of Cycles — THEOREM

If G is a connected graph with n vertices and $m \geq n$ edges, then G contains a cycle.

Index