Discreet Fall 2023 Notes

Samuel Lindskog

December 14, 2023

Relations

Definition 1.1 (Relation)**.** Suppose A and B are sets. Then a set $R \subseteq A \times B$ is called a relation from A to B. A set $R \subseteq A \times A$ is called a relation on A.

Definition 1.2 (Relation Dom)**.** Suppose R is a relation from A to B. Then the domain of R is the set:

$$\text{Dom}(R) = \{a \in A \mid \exists b \in B((a, b) \in R)\}$$

Definition 1.3 (Relation Range)**.** Suppose R is a relation from A to B. Then the domain of R is the set:

$$\text{Ran}(R) = \{b \in B \mid \exists a \in A((a, b) \in R)\}$$

Definition 1.4 (Inverse Relation)**.** The inverse of a relation R from A to B is the relation R^{-1} from B to A defined:

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$$

Definition 1.5 (Composition)**.** Suppose R a relation from A to B, and S a relation from B to C. Then the composition of S and R is the relation $S \circ R$ from A to C defined as follows:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B((a, b) \in R \wedge (b, c) \in S)\}$$

Definition 1.6. Suppose R is a relation on A

1. R is *reflexive* if $\forall x \in A(xRx)$.
2. R is *symmetric* if $\forall x, y \in A(xRy \Rightarrow yRx)$.
3. R is *transitive* if $\forall x, y, z \in A((xRy \wedge yRz) \Rightarrow xRz)$.
4. R is *antisymmetric* if $\forall x \in A \forall y \in A((xRy \wedge yRx) \Rightarrow x = y)$.

Definition 1.7 (Partial and Total Orders)**.** Suppose R is a relation on set A. Then R is called a *partial order* on A if it is reflexive, transitive, and antisymmetric. It is called a *total order* on A if it is a partial order, and $\forall x, y \in A(xRy \vee yRx)$.

Definition 1.8 (R-smallest and R-minimal)**.** Suppose R is a partial order on a set A and $B \subseteq A$. Then $b \in B$ is called an *R-smallest* element of B if $\forall x \in B(bRx)$. It is called an *R-minimal* element of B if $\forall x \in B(xRb \Rightarrow x = b)$.

Definition 1.9 (R-greatest and R-maximal)**.** Suppose R is a partial order on a set A and $B \subseteq A$. Then $b \in B$ is called an *R-greatest* element of B if $\forall x \in B(xRb)$. It is called an *R-maximal* element of B if $\forall x \in B(bRx \Rightarrow x = b)$.

Definition 1.10 (Upper and Lower Bound)**.** Suppose R is partial order on A, $B \subseteq A$. Then $a \in A$ is called an *R-lower bound* for B if $\forall x \in B(aRx)$. Similarly, $a \in A$ is an *R-upper bound* for B if $\forall x \in B(xRa)$.

Definition 1.11 (l.u.b and g.l.b)**.** Suppose R is a partial order on A, and $B \subseteq A$. Let U be the set of all upper bounds for B, and L the set of all lower bounds. If U has a smallest element, then this smallest element is called the *least upper bound* of B. If L has a largest element, then this largest element is called the *greatest lower bound* of B.

Definition 1.12 (Equivalence Relation)**.** Suppose that R is a relation of a set A. Then R is called an *equivalence relation* on A if it is reflexive, symmetric, and transitive.

Definition 1.13 (Equivalence Class)**.** Suppose R is an equivalence relation of set A, and $x \in A$. Then the *equivalence class* of x with respect to R is the set:

$$[x]_R = \{y \in A \mid yRx\}$$

The set of all equivalence classes of elements of A is called *A modulo R*, and is denoted A/R. Thus:

$$A/R = \{[x]_R \mid x \in A\}$$

Definition 1.14 (Pairwise Disjoint)**.** Let $\mathcal{F}$ be a family of sets. We will say that $\{$ is *pairwise disjoint* if every pair of distinct elements of $\mathcal{F}$ are disjoint, or in other words:

$$\forall X, Y \in \mathcal{F}(X \neq Y \Rightarrow X \cap Y = \emptyset)$$

Definition 1.15 (Congruence)**.** Suppose $m \in \mathbb{Z} \setminus \{0\}$. for any $x, y \in \mathbb{Z}$, we will say that x is congruent to y modulo m if $\exists k \in \mathbb{Z}(x - y = km)$, denoted as $x \equiv y \pmod{m}$.

Functions

Definition 1.16 (Function)**.** Suppose F is a relation from A to B. Then F is called a function from A to B if for every $a \in A$ there is exactly one $b \in B$ sucha that $(a, b) \in F$, i.e:

$$\forall a \in A \exists! b \in B((a, b) \in F)$$

Notation. Suppose $f : A \to B$. If $a \in A$, we write $f(a) = b$ for $(a, b) \in f$, where b is called "the value of f at a", or "the image of a under f".

Definition 1.17 (Function Range)**.** The definition of range for relations can be used, or:

$$\text{Ran}(f) = \{b \in B \mid \exists a \in A(f(a) = b)\}$$

Definition 1.18 (One-To-One (Injective))**.**

$$\forall a_1, a_2 \in A(f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$$

Definition 1.19 (Onto (Surjective))**.**

$$\forall b \in B \exists a \in A(f(a) = b)$$

Definition 1.20 (Image)**.** Suppose $f : A \to B$ and $X \subseteq A$. Then the *image* of X under f is the set $f(X)$ defined as follows:

$$f(X) = \{f(x) \mid x \in X)\}$$

In particular, $f(\emptyset) = \emptyset$ and $f(A) =$Ran(f).

Definition 1.21 (Inverse Image)**.** Suppose $f : A \to B$ and $Y \subseteq B$. Then the *inverse image* of Y under f is the set $f^{-1}(Y)$ defined as follows:[1]

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$$

In particular, $f^{-1}(\emptyset) = \emptyset$, and:

$$f^{-1}(B) = \{a \in A \mid f(a) \in B\} = A$$

[1] If f is not injective and surjective, then f^{-1} is not a function, so the notation "$f^{-1}(y)$" is meaningless.

Mathematical Induction

Proof by Mathematical Induction

To prove a goal of the form $\forall n \in \mathbb{N}(P(n))$, first prove $P(0)$, and then prove $\forall n \in \mathbb{N}(P(n) \to P(n+1))$. The first of these proofs is called the *base case*, and the second the *induction step*. $P(n)$ is called the *inductive hypothesis*.

Strong Induction

To prove a goal of the form $\forall n \in \mathbb{N}P(n)$, prove that $\forall n \in \mathbb{N}[(\forall k \in \mathbb{N}^{\leq n-1}P(k) \to P(n))]$, where $\mathbb{N}^{\leq n-1}$ denotes all natural numbers no larger than $n - 1$.

Theorem 1.1 (Division Algorithm)**.** For all $n, m \in \mathbb{Z}$ with $m \neq 0$, there exists unique $q, r \in \mathbb{Z}$ with $0 \leq r <|m|$ such that $n = mq + r$. The numbers q and r are called the quotient and remainder when n is divided by m.

Definition 1.22. Let $m, n \in \mathbb{Z}$.

1. If $d \mid m$ and $d \mid n$ for some $d \in \mathbb{Z} \setminus \{0\}$, we say that d is a *common divisor* of m and n.

2. Assume $m \neq 0$ or $n \neq 0$. The largest common (positive) divisior of m and n is called the *greatest common divisor* of m and n, denoted by $\gcd(m, n)$, i.e.

Infinite Sets and Counting

Definition 1.23 (Equinumerous)**.** Let A and B be sets. We'll say that A is *equinumerous* with B if there is a function $f : A \to B$ that is one-to-one and onto. We'll write $A \sim B$ to indicate that A is equinumerous with B.

Definition 1.24 (Finite)**.** For each $n \in \mathbb{N}$, let $I_n = \{1, \ldots, n\}$. A set A is called *finite* if there is an $n \in \mathbb{N}$ such that $I_n \sim A$. Otherwise, A is infinite.

Definition 1.25 (Cardinality)**.** If A is a finite set and $A \sim I_n$ for some $n \in \mathbb{N}$, then the *cardinality* of A, denoted $|A|$, is defined to be n. In particular, $|\varnothing| = 0$.

Definition 1.26 (Denumerable)**.** A set A is called *denumerable* is $\mathbb{Z}^+ \sim A$. It is called *countable* if it is either finite of denumerable. Otherwise, it is *uncountable*.

Corollary 1.1 (Addition Rule)**.** Let A and B be finite sets and $A \cap B = \varnothing$. Then:

$$|A \cup B| = |A| + |B|$$

Theorem 1.2. Suppose A and B finite sets. Then:

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

Proof: Suppose $A \vee B$ is the empty set. Then $A \cap B = \varnothing$ and $|A \cap B| = 0$. In the case that one of A or B is not the empty set, suppose (without loss of generality) $A = \{a_1, \ldots, a_l\}$ and $B = \varnothing$ and $l \in \mathbb{N}$. Then $A \cup B = A$ and $|B| = 0$ and thus $|A \cup B| = |A| + |B| - |A \cap B| = l$. In the case $A \wedge B = \varnothing$, trivially $|A \cup B| = |A| + |B| - |A \cap B|$.

Suppose $A \wedge B$ are not the empty set. Suppose then $A = \{a_1, \ldots, a_l\}$ and $B = \{b_1, \ldots, b_r\}$, with $l, r \in \mathbb{Z}^+$ and $\forall l \forall r (a_l \neq b_r)$. Then $A \cup B = \{a_1, \ldots, a_l, b_1, \ldots, b_r\}$ and $|A| = l$ and $|B| = r$ and $A \cap B = \varnothing$ so $|A \cap B| = 0$. It follows $|A \cup B| = l + r = |A| + |B| + |A \cap B|$.

Suppose now $\exists l \exists r(a_l = b_r)$. For A with l elements and B with r elements as defined above, suppose $A = \{a_1, \ldots, a_s, x_1, \ldots, x_n\}$ and $B = \{b_1, \ldots b_t, x_1, \ldots, x_n\}$ and $s, t, n \in \mathbb{Z}^+$ with $s + n = l$ and $t + n = r$. Then, because $A \cap B = \{x_1, \ldots, x_n\}$, it follows $|A \cap B| = n$ and $|A \cup B| = s + t + n = |A| + |B| - |A \cap B| = l + r - n = s + n + t + n - n = s + t + n$. □

Corollary 1.2. Let A and B be finite sets. Then:

$$|A \setminus B| = |A| - |A \cap B|$$

Definition 1.27 (Floor Function)**.** Let $a \in \mathbb{R}$. Define the *floor* funciton of a by:

$$\lfloor a \rfloor = \max\{n \in \mathbb{Z} \mid n \leq a\}$$

Definition 1.28 (Addition Rule)**.**

Let $A_1, \ldots, A_n$ be finite sets. Then:

$$|A_1 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n|$$

Definition 1.29 (Multiplication Rule)**.** Let $A_1, \ldots, A_n$ be finite sets. Then:

$$|A_1 \times \ldots \times A_n| = \prod_{i=1}^{n} |A_i|$$

Definition 1.30 (Permutation)**.** We define a permutation to be a set of distinct symbols which are arranged in order. An r-permutation of n symbols is a permutation of r of the n symbols. The number of r-permutations is:

$$P(n, r) = \frac{n!}{(n-r)!}$$

Definition 1.31 (Combination)**.** An r-combination of n distinct objects is any collection of r objects. The number of r-combinations of n objects is:

$$\left(n//r\right) = \frac{P(n, r)}{r!}$$

or in other words:

$$\frac{n!}{r!(n-r)!}$$

Definition 1.32 (Pigeonhole Principle)**.** Let $n, m \in \mathbb{Z}^+$ and $n > m$. Suppose we have n objects that need to be placed in m boxes. Then at least one box has at least two objects in it.