MA352 Midterm Study Guide

Jonathan Lam

March 18, 2020

Contents

1 Sets

This can be seen as a boolean algebra $(S, \cup, \cap, \bar{}, \varnothing, U)$.

1.1 Properties

- Involution: $\bar{\bar{A}} = A$
- Absorption: $A \cup (A \cup B) = A \cup B$, $A \cap (A \cap B) = A \cap B$
- Bound: $A \cup U = U$, $A \cap \varnothing = \varnothing$
- Idempotent: $A \cup A = A$, $A \cap A = A$
- Complement: $A \cup \bar{A} = U$, $A \cap \bar{A} = \varnothing$

- Identity: $A \cup \varnothing = A$, $A \cap U = A$
- (Distributive law both ways)
- 0/1: $\bar{\varnothing} = U$, $\bar{U} = \varnothing$
- De Morgan's: $\bar{A} \cup \bar{B} = \overline{A \cap B}$, $\bar{A} \cap \bar{B} = \overline{A \cup B}$

A collection S of nonempty subsets (i.e., S is a set of sets) of X is said to be a partition of X if every element in X belongs to exactly 1 member o S (i.e., S pairwise disjoint, but $\cup_i S = X$).

If X and Y are sets, define the Cartesian product $X \times Y = \{(x, y) : x \in X, y \in Y\}$.

2 Relations

Define $\varnothing = R \subseteq X \times Y$ to be a relation from X to Y (any nonempty subset of the Cartesian product). If from a set to itself, call it a relation on X. $\text{Dom}(R)) \subseteq X$ set of elements $x \in X$ s.t. $(x, y) \in R$; the analogous definition also exists for Range(R). The inverse is the set $R^{-1} = \{(y, x) : (x, y) \in R\} \subseteq Y \times X$.

Can define function composition, $R_2 \circ R_1$ is R_2 composed with R_1. A relation is a function if $\text{Dom}(R) = X$, and if it is injective.

Injective, surjective, bijective.

Binary and unary operators.

Denote operators on elements of sets with (S, op). (E.g., $(\mathbb{R}, +)$).

Can represent a relation on a set with a digraph.

2.1 Classifications of relations

These all apply to relations on a set, not from one set to another.

- Reflexive: $(x, x) \in R \; \forall x \in X$
- Symmetric: $(x, y) \in R \Rightarrow (y, x) \in R$
- Antisymmetric: $x \neq y, (x, y) \in R \Rightarrow (y, x) \notin R$ (in other words, $(x, y), (y, x) \in R \Rightarrow x = y$)
- Transitive: $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$
- Partial ordering: reflexive, antisymmetric, and transitive
- Total ordering: partial ordering, and every pair of elements is comparable
- Equivalence: reflexive, symmetric, and transitive

2.2 Equivalence relations

Let R be an equivalence relation on X. Then the equivalence class of $a \in X$ is $[a] = \{b : (a, b) \in R\}$.

The set of equivalence classes of X is a partition of X.

2.3 Matrices of relations

The matrix of relation is a transformation matrix. Each column is the transformation of an input element to the output elements, where 1 denotes a relation and 0 doesn't. I.e., line up the input set along the horizontal direction, output direction along the vertical direction, draw 1's where relations happen. Composition is multiplication, just like a transformation matrix, and multiplication by an element of the input set gives you the elements it is related to.

3 Mathematical induction

1. Basis step: Prove that $S(1)$ is true.
2. Inductive step: Prove that $S(k) \to S(k+1)$ is true.

Sometimes you can avoid mathematical induction; not the only way to prove things like these (e.g., geometric series, or using a similar, known mathematical rule and applying some (usually linear) rule like differentiation.)

4 Groups

... TODO ...

5 Modular arithmetic and elementary number theory

5.1 Basic rules of divisibility and modular arithmetic

Division algorithm:

$$\forall a, b \in \mathbb{Z},\ b > 0\ \exists! q, r \in \mathbb{Z} : a = bq + r,\ 0 \leq r < b$$

$$a|b \Rightarrow a|nb$$

$$a|b, c|d \Rightarrow (a+c)|d$$

$$a_1 \equiv a_2 \mod b \Leftrightarrow r_1 = r_2$$

where r_1 and r_2 come from the division algorithm of a_1 and a_2 with b.

$$a \equiv b \mod n, c \equiv d \mod n \Rightarrow a + b \equiv (b + c) \mod n$$

5.2 GCD and LCM

$$a = \prod_i^k p_i^{\alpha_i},\ b = \prod_i^k p_i^{\beta_i}$$

where $\{p_i\}$ denotes the set of distinct prime factors that divide a or b. Then:

$$\gcd(a,b) = \prod_i^k p_i^{\min \alpha_i, \beta_i}$$

$$\text{lcm}(a,b) = \prod_i^k p_i^{\max \alpha_i, \beta_i}$$

$$\gcd(a,b)\text{lcm}(a,b) = ab$$

Another way to characterize gcd is: for any integer d s.t. $d|a$ and $d|b$, then $d|\gcd(a,b)$.

5.3 Euclid's algorithm

To find $\gcd(a,b)$: let $m = \max(a,b)$, $n = \min(a,b)$. If $n = 0$, then $\gcd(a,b) = \gcd(m,n) = \gcd(m,0) = m$. If not, then $\gcd(a,b) = \gcd(n, m \mod n)$.

5.3.1 Linear diophantine equations

Given $a, b \in \mathbb{Z}$ linear Diophantine equations $ax + by = c,\ x, y \in \mathbb{Z}$ always has a solution x, y if $\gcd(a,b)|c$, and Euclid's algorithm can help discover it. Namely, this involves the recurrence relation $x = y'$, $y = x' - y'q$ at any given step; at the basis step, $x = 1$, $y = 0$ (since $1(m) + 0(0) = \gcd(a,b)$ at the last step of Euclid's algorithm).

It's easier to understand by going the full depth of Euclid's algorithm, and then expressing $\gcd(a)b$ as a linear combination of the m and n from that step; again, on the bottom-most step, $1(m) + 0(n) = m = \gcd(a,b)$; work your way up from here. However, this can often be found by inspection.

This gives you a particular solution of x, y. To find the general solution, find the associated homogeneous solution and go from there. I.e., solve $ax = -by$. Thus $x = \frac{-b}{\gcd(a,b)}t$, $y = \frac{a}{\gcd(a,b)}t$. Thus the general solution is

$$x = x_0 - \frac{b}{\gcd(a,b)}t,\ y = y_0 + \frac{a}{\gcd(a,b)}t$$

5.3.2 Computing inverse modulo n

In general, $ax \equiv 1 \mod p$ has $\gcd(a,p)$ solutions. I.e., a has a unique solution to this equation $x = a^{-1}$ (inverse) iff $\gcd(a,p) = 1$.