Concepts Notes

@saffron

Logic

logical operators

– $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$

quantifiers

– $\forall, \exists$

helpful equivalences

– $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
– $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
– $\neg(p \wedge q) \equiv \neg p \vee \neg q$
– $\neg(p \vee q) \equiv \neg p \wedge \neg q$
– $\neg(p \Rightarrow q) \equiv p \wedge \neg q$
– $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ ("contrapositive form")
– $\neg(\forall x \in S, p(x)) \equiv \exists x \in S, \neg p(x)$
– $\neg(\exists x \in S, p(x)) \equiv \forall x \in S, \neg p(x)$

definitions

truth tables can prove equivalences

tautology: always true / contradiction: always false

divisibility: Let $a, b \in \mathbb{Z}$. Then $a \mid b \iff (\exists k \in \mathbb{Z}, ak = b)$

parity: an integer a is even iff $2 \mid a$ and odd otherwise (i.e. $2 \mid a + 1$).

Proof Strategies

TODO AFSOC, contraposition, etc etc from your old notes.

– $(p \Rightarrow q)$ assume p, prove q
– $(p \vee q \Rightarrow r)$ by cases: assume p, prove r. assume q, prove r
– we find a contradiction

Sets

– list notation: $A = \{1, 2, 3, ...\}$
– set builder notation: $B = \{n : n \text{ is prime}\}$
– number sets
  – naturals $\mathbb{N} = \{0, 1, 2, ...\}$
  – integers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
  – rationals $\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z} \wedge b \neq 0\right\}$
  – reals $\mathbb{R} = \{\text{the number line}\}$
  – closure properties
    – $+ / \times$ of two $\mathbb{N}$ is still $\mathbb{N}$
    – $+ / - / \times$ of two $\mathbb{Z}$ is still $\mathbb{Z}$

  - $+/-/\times/\div$ (except 0) of two $\mathbb{Q}/\mathbb{R}$ is still $\mathbb{Q}/\mathbb{R}$

definitions
- $x \notin X$ iff $\neg(x \in X)$
- $X = \emptyset$ iff $\forall x, x \notin X$
- $A \subseteq B$ iff $\forall x \in A, x \in B$
- $X \cap Y = \{a : a \in X \wedge a \in Y\}$
- $X \cup Y = \{a : a \in X \vee a \in Y\}$
- $X \setminus Y = \{a : a \in X \wedge a \notin Y\}$
- $X \times Y = \{(x, y) : x \in X \wedge y \in Y\}$
- $X = Y$ iff $X \subseteq Y \wedge Y \subseteq X$
- $\bigcap_{i \in I} X_i = \{a : \forall i \in I, a \in X_i\}$
- $\bigcup_{i \in I} X_i = \{a : \exists i \in I, a \in X_i\}$
- $\mathcal{P}(A) = \{X : X \subseteq A\}$

de Morgan's for sets
- $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$
- $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$
- $X \setminus \left(\bigcap_{i \in I} Y_i\right) = \bigcup_{i \in I} (X \setminus Y_i)$
- $X \setminus \left(\bigcup_{i \in I} Y_i\right) = \bigcap_{i \in I} (X \setminus Y_i)$

Functions

definitions
- a function $f : X \to Y$ is an assignment that satisfies
  - totality: $\forall x \in X, f(x)$ is defined (i.e. domain $= X$)
  - existence: $\forall x \in X, f(x) \in Y$ (i.e. codomain $= Y$)
  - uniqueness: $\forall x, x' \in X, (x = x' \Rightarrow f(x) = f(x'))$ (i.e. VLT)
- $\mathrm{Gr}(f) = \{(x, y) \in X \times Y : f(x) = y\}$
- let $f : X \to Y, g : Y \to Z$. then $g \circ f : X \to Z = g(f(x))$
- $f = g$ iff same domain, same codomain, and $\forall x \in X, f(x) = g(x)$
- $\mathrm{id}_X : X \to X$ is $\mathrm{id}_X(x) = x$
- characteristic function of U in X is $\chi_U(a)$ is 1 if $a \in U$, 0 if not.
- image of U under f is $f[U] = \{y \in Y : \exists x \in U, y = f(x)\}$
- preimage of V under f is $f^{-1}[V] = \{x \in X : f(x) \in V\}$
- f is injective iff $\forall a, b \in X, (f(a) = f(b) \Rightarrow a = b)$
- f is surjective iff $\forall y \in Y, \exists x \in X, f(x) = y$
- f is bijective iff f is both injective and surjective
- a left inverse for f is a function $g : Y \to X$ s.t. $g \circ f = \mathrm{id}_X$
  - this implies f is injective
- a right inverse for f is a function $g : Y \to X$ s.t. $f \circ g = \mathrm{id}_Y$
  - this implies f is surjective
- an inverse (two-sided) for f is a function g that is both left and right inverse, also denoted f^{-1}
  - this implies f is bijective

Induction

The Fundamental Theorem of Arithmetic (Existence)

– Every natural number $n \geq 2$ can be expressed as a product of primes

recursive function definitions

$$\sum_{k=1}^{n} a_k = \begin{cases} \sum_{k=1}^{0} a_k = 0 \\ \sum_{k=1}^{m+1} a_k = a_{m+1} + \sum_{k=1}^{m} a_k \text{ if } n = m+1 \end{cases}$$

$$\prod_{k=1}^{n} a_k = \begin{cases} \prod_{k=1}^{0} a_k = 1 \\ \prod_{k=1}^{m+1} a_k = a_{m+1} \cdot \prod_{k=1}^{m} a_k \text{ if } n = m+1 \end{cases}$$

$$n! = \sum_{k=1}^{n} k$$

weak induction formula

– to prove $\forall n \in \mathbb{N}$ with $n \geq n_0$, $p(n)$:
  – (Base Case) Verify $p(n_0)$ holds
  – (Inductive Step) Verify $\forall n \geq n_0, p(n) \Rightarrow p(n+1)$

strong induction formula

– to prove $\forall n \in \mathbb{N}$ with $n \geq n_0$, $p(n)$:
  – (Base Case) Verify $p(n_0)$ holds
  – (Inductive Step) Verify $\forall n \geq n_0, (p(i) \text{ is true for all } i \text{ such that } n_0 \leq i \leq n) \Rightarrow p(n+1)$

strong induction, multiple base cases formula

– to prove $\forall n \in \mathbb{N}$ with $n \geq n_0$, $p(n)$ with base cases from n_0 to n_1:
  – (Base Case) Verify all base cases hold
  – (Inductive Step) Verify $\forall n \geq n_1, (p(i) \text{ is true for all } i \text{ such that } n_0 \leq i \leq n) \Rightarrow p(n+1)$

Relations

relation equivalence

– relations $R = S$ iff same domain, codomain, and $\forall x, y \in X \times Y, xRy \Leftrightarrow xSy$

properties of relations (let R be a relation on X)

– R is reflexive iff $\forall x \in X, xRx$
– R is symmetric iff $\forall x, y \in X, xRy \Rightarrow yRx$
– R is antisymmetric iff $\forall x, y \in X, xRy \wedge yRx \Rightarrow y = x$
– R is transitive iff $\forall x, y, z \in X, xRy \wedge yRz \Rightarrow xRz$
– R is an equivalence relation iff R is reflexive, symmetric, and transitive
– R is a partial order iff R is reflexive, antisymmetric, and transitive (may be denoted $\preccurlyeq$)
  – if $\preccurlyeq$ is a partial order of X, we say $(X, \preccurlyeq)$ is a poset

- R is total iff $\forall x, y \in X, (x \neq y \Rightarrow xRy \vee yRx)$ (every two distinct elements are relatable)
- R is a total order iff R is a partial order and total

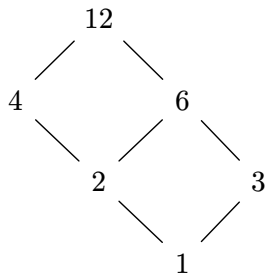

Figure 1: Hasse diagram for the poset $(\{1, 2, 3, 4, 6, 12\}, |)$

modular congruence
- let n be positive $\in \mathbb{Z}, a, b \in \mathbb{Z}$. then $a \equiv b \pmod{n}$ aka $a \equiv_n b$ iff $n \mid (b - a)$

equivalence class of a under an equivalence relation $\sim$ on X
- $[a]_{\sim} = \{b \in X : a \sim b\}$
- the set of items related to a
- $[a]_{\sim} = [b]_{\sim}$ iff $a \sim b$

the quotient (letting $\sim$ be an equivalence relation on X)
- $X/\sim = \left\{[a]_{\sim} : a \in X\right\}$
- the collection of all equivalences classes in X under $\sim$

P is a partition of X iff
- $\emptyset \notin P$
- $\forall U, V \in P, (U \neq V \Rightarrow U \cap V = \emptyset)$ i.e. different sets have no elements in common
- $\bigcup_{U \in P} U = X$ i.e. each partition together becomes P

theorem for equivalence relations/partitions, with a nonempty set X
- let $\sim$ be an equivalence relation on X. then, $X/\sim$ is a partition for X
- let P be a partition for X. then there exists a unique equivalence relation on P whose quotient is P.

Cardinality
- $[n] = \{1, 2, 3, ..., n\}$
- infinite sets
  - X is finite iff there exists a bijection $f : [n] \to X$ for some natural n
  - otherwise, X is infinite
- for finite X, then $|X|$ is the natural n where there exists bijective $f : [n] \to X$
- let X, Y be finite sets
  - $\exists$ an injection $f : X \to Y$, then $|X| \leq |Y|$
  - $\exists$ a surjection $f : X \to Y$, then $|X| \geq |Y|$
  - $\exists$ a bijection $f : X \to Y$, then $|X| = |Y|$
  - if $A \subseteq X$, then A finite and $|A| \leq |X|$
  - if $A \subseteq X$, then A finite and $|A| \leq |X|$
  - $X \cap Y$ is finite and $|X \cap Y| \leq \min\{|X|, |Y|\}$
  - $X \cup Y$ is finite and $|X \cup Y| = |X| + |Y| - |X \cap Y|$

  - $X \times Y$ is finite and $|X \times Y| = |X| \cdot |Y|$
- X is infinitely countable if $\exists$ a bijection $f : \mathbb{N} \to X$
- X is countable if X is either finite or infinitely countable
- X is uncountable if X is not countable (infinitely or otherwise)
- if X and Y are countable, then $X \times Y$ is countable
- let X be countable
  - if $\exists$ an injection $f : Y \to X$, then Y is countable
  - if $\exists$ a surjection $f : X \to Y$, then Y is countable
  - all $A \subseteq X$ are countable
- diagonalization (prove X uncountable)
  - show that every $f : \mathbb{N} \to X$ is not surjective by finding a $b \in X$ that disagrees with $f(n)$ with something involving n
- let X be any set
  - $|X| = |Y|$ iff $\exists$ a bijection $f : X \to Y$
  - $|X| \leq |Y|$ iff $\exists$ an injection $f : X \to Y$
  - $|X| < |Y|$ iff $\exists$ an injection $f : X \to Y \wedge \nexists$ a surjection $g : X \to Y$
- Cantor's: $|X| < |\mathcal{P}(X)|$

Number Theory

- Well Ordering Principle: Any nonempty subset $X \subseteq \mathbb{N}$ has the least element
  - use in "let n be the least element, AFSOC something, wait a minute $m < n$" proofs
- division theorem: Let $a, b \in \mathbb{Z}, b \neq 0$. There is a quotient and a remainder.
  - (59 and 8? $59 = 8 \cdot 7 + 3$)
- let $a, b \in \mathbb{Z}$
  - $c \in \mathbb{Z}$ is a common divisor of a and b if c divides both a and b
  - $d \in \mathbb{Z}$ is a greatest common divisor of a and b if
    1. d divides a and b
    2. if c is a common divisor of a and b, then $c \mid d$
  - a and b are coprime iff $\gcd(a, b) = 1$
- Euclidean Algorithm
  - lemma: $a = qb + r \Rightarrow \gcd(a, b) = \gcd(b, r)$
  - let us use an example. find $\gcd(148, 40)$.

$$\begin{aligned} 148 &= 40 \cdot 3 + 28 \\ 40 &= 28 \cdot 1 + 12 \\ 28 &= 12 \cdot 2 + \mathbf{4} \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

    the last nonzero remainder, 4, is the gcd.
- Linear Diophantine Equations
  - Bézout's Lemma: let $a, b, c \in \mathbb{Z}$. the equation $ax + by = c$ has integer solutions for x, y iff $\gcd(a, b) \mid c$
  - let us use an example, via the backwards Euclidean Algorithm. find $252x + 198y = 36$.

    we first find $\gcd(a, b) = \gcd(252, 198)$.

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 && (1) \\ 198 &= 54 \cdot 3 + 36 && (2) \\ 54 &= 36 \cdot 1 + 18 && (3) \\ 36 &= 18 \cdot 2 + 0 \end{aligned}$$

    Thus, $\gcd(252, 198) = 18$. Since $18 \mid 36$, by Bézout's, we have an integer solution. We proceed by backtracking (starting from the most recent iterations).

$$\begin{aligned} 18 &= 54 - 36 \cdot 1 && \text{(from 3)} \\ 18 &= 54 - (198 - 54 \cdot 3) && \text{(from 2)} \\ 18 &= (252 - 198) - (198 - (252 - 198) \cdot 3) && \text{(from 1)} \\ 18 &= 252 \cdot 4 - 198 \cdot 5 \\ 36 &= 252 \cdot 8 - 198 \cdot 10 \end{aligned}$$

    Thus, $x = 8$ and $y = -10$.
- Multiplicative Inverses Modulo n: let $a, n \in \mathbb{Z}$ and $n \geq 1$.
  - we say a has a multiplicative inverse for a modulo n if $ax \equiv_n 1$ has an integer solution for x. then x is that multiplicative inverse

  - a has a multiplicative inverse modulo n iff $\gcd(a, n) = 1$
  - find this inverse similarly to a Linear Dio. Euclidean to get to $\gcd = 1$ and backsolve.
  - (a normal multiplicative inverse is $ax = 1$)
- Divisibility Properties
  - Euclid's Lemma: Let $a, b \in \mathbb{Z}$ and p prime. If $p \mid ab$, then $p \mid a$ or $p \mid b$.
  - $a, b, c \in \mathbb{Z}$. If $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.
  - every integer $n \geq 2$ can be expressed as a unique product of positive primes
  - there are infinitely many primes
  - Fermat's little theorem: let $a, p \in \mathbb{N}$ with p prime. Then $a^p \equiv a \pmod{p}$
    - Corollary: let $a \in \mathbb{N}$, p prime with $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$
- Bonkers Remainders When Divided by Primes
  - use Fermat's Little Corollary
  - let us use an example. find the remainder of 3^{244886} when divided by 13.

    by Fermat's, since $13 \nmid 3$, we have $3^{12} \equiv_{13} 1$. let us use the power of 12 to simplify 3^{244886}. via long division, we have $244886 = 12 \cdot 20407 + 2$. We proceed.

    $$3^{244886} \equiv_{13} 3^{12 \cdot 20407 + 2} \equiv_{13} 3^{12 \cdot 20407} \cdot 3^2 \equiv_{13} 1 \cdot 3^2 \equiv_{13} 9$$

    Thus, the remainder is 9.