Intro to Discrete Structures Study Guide

Propositions

(¬) negation NOT
(∧) conjunction AND
(∨) disjunction OR
(⊕) xor XOR
(→) implication If Then
(↔) biconditional IFF

$p \to q$ ≡ all equivalent
converse $q \to p$
contrapositive $\neg q \to \neg p$
inverse $\neg q \to \neg p$

Truthtable

$p \vee q \to \neg r$

p	q	r	p∨q	¬r	p∨q → ¬r
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	T	T
F	T	T	T	F	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	F	T	T

≡ ↳ final

- 2 propositions equiv if final truth values same
- n variables → 2^n rows

English → Prop

① Identify atomic props & label w/ variables
② Determine logical connectives

Satisfiability

↳ iff there exists at least 1 set of values for prop vars to make the whole prop true
- Consistant - if possible to make all props in a list of props true

Predicates & Quantifiers

- predicate → ie P(x) where x is in domain U

(∀) universal FOR ALL
(∃) existential THERE EXISTS

$\neg \forall x J(x) = \exists x \neg J(x)$
$\neg \exists x J(x) = \forall x \neg J(x)$

Arguments

$\frac{p \to q \quad p}{q}$ $\frac{p \to q \quad \neg q}{\neg p}$ $\frac{p \to q \quad q \to r}{p \to r}$ $\frac{p \vee q \quad \neg p}{q}$

$\frac{p}{p \vee q}$ $\frac{p \wedge q}{p}$ $\frac{p \quad q}{p \wedge q}$ $\frac{\neg p \vee r}{p \to q \vee r}$

$\frac{\forall x P(x)}{P(c)}$ $\frac{P(c)}{\forall x P(x)}$ $\frac{\exists x P(x)}{P(c)}$ $\frac{P(c)}{\exists x P(x)}$

Proof Methods

① Direct proof
② Contrapositive ($p \to q$)
↳ assume $\neg q$ to prove $\neg p$
③ Contradiction
↳ assume $\neg q$ and prove $\neg p$ while assuming p is true
④ Biconditional
↳ prove $p \to q$ and $q \to p$

Proof Strategies

- by cases
$(p_1 \vee p_2 \vee \dots p_n) \to q$
prove ∀
$(p_1 \to q) \wedge (p_2 \to q) \wedge \dots$
- w/o loss of generality able to avoid repetitive proofs
- existence proofs
↳ constructive
$\exists x P(x)$
assume at least 1 element exists to satisfy P(x)
↳ nonconstructive
no x to satisfy P(x)
prove by contradic
- Counterexample
prove ¬p is true
- Uniqueness
① prove element x ∀ property exists
② show if $y \neq x$, y does not have the property
- Universally Quantified
$\forall x P(x)$
Regular proof but keep x as x

Sets $S = \{x \mid P(x)\}$

U ⇒ contains all in domain
∅ ⇒ contains nothing
↳ $\emptyset \subseteq$ all S
- proper subset ($A \subset B$)
↳ $A \subseteq B$ but $A \neq B$
- cardinality $|A|$
↳ # elements in A
- power set $\mathcal{P}(A)$
↳ set of all subsets of A
$|\mathcal{P}(A)| = 2^{|A|}$ (includes ∅)
- cartesian product $A \times B$
$A = \{a, b, c\}$ $B = \{1, 2, 3\}$
$A \times B = \{(a,1), (a,2), \dots (c,3)\}$
$B \times A = \{(1,a) \dots (3,c)\}$
$|A \times B| = |A| \cdot |B|$
- truth set
set of elems in domain D where P(x) is true

≡
→ A ∪ B or (INCL)
→ A ∩ B and
→ $\bar{A}$ / A^c not
→ A − B / $A \cap \bar{B}$
→ $A \oplus B$ / $(A-B) \cup (B-A)$ (EXCL)
≡
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (A \cap B) = A = A \cap (A \cup B)$
$(A \cup B) \cup C = A \cup (B \cup C)$

Functions ($f: A \to B$)

range f(A) = corresponding B
- injection - one to one
- onto - all elements of B are mapped to
- bijection - injection & onto, every element A & B used
- inverse - $f: A \to B$, $f^{-1}: B \to A$
↳ bijection
- reverse connections

f	f^{-1}
0 → 4	0 ← 4
* → x	* ← x
△ → y	△ ← y

→ $f(x) = y$, solve for x, $f^{-1}(x) = x$
- composition $f \circ g$
$f \circ g = f(g(x))$
$A \xrightarrow{g} B \xrightarrow{f} C = A \xrightarrow{f \circ g} C$
domain f ⊆ codomain g
- floor $\lfloor x \rfloor$
↳ largest int ≤ x
- ceiling $\lceil x \rceil$
↳ smallest int ≥ x

Sequence & Summation

- sequence - ordered list
- geometric - $a, ar, ar^2 \dots$
- arithmetic - $a, a+d, a+2d$
- closed formula - formula for n^{th} term
- Summation
$\sum_{j=m}^{n} a_i = a_m + a_{m+1} + \dots + a_n$
- Product notation
$\prod_{j=m}^{n} a_i = a_m \cdot a_{m+1} \cdot \dots \cdot a_n$
↳ See notes pg 2 for table

Countability

↳ set ∀ finite elems or same cardinality as $\mathbb{Z}^+$
- prove countability
→ prove one to one & onto
① $\mathbb{Z}^+$: 1 2 3 ...
S : a b c ...
② ∀ yes S, $f(x) = -$, $y = f(x)$
solve $x = z$, $f(z) = y$
→ prove values can be put in a sequence
★ subset of countable set is countable
- $\mathbb{R}$ is not countable

Mathematical Induction

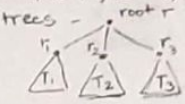
① Prove base step = true
② Induction hypothesis = P(n)
③ Prove $P(k) \to P(k+1)$

Strong Induction

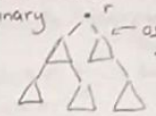
- with propositions
① Prove as many base cases as needed
② Show $[P(1) \wedge P(2) \wedge \dots \wedge P(n)] \to P(n+1)$
(kinda like recursion)
- well ordering - every nonempty set of nonnegative ints has a least element

Recursion / Structural

① Identify base / exit value
② Give rule to find new elements using existing elements
- exclusion rule - set only contains whats specified in base step & generated recursively
- well formed formulae → extremely clear (¬E), (E ∧ F), (E ∨ F), (E → F), (E ↔ F) using ( )
- trees - root r



binary



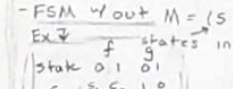
- structural induction
↳ proved property of elements in recursive set
① Prove for base step
② Prove if true for base, true for all new elements
- generalized induction
↳ prove results ∀ well ordering property
① Verify bases
② Verify result for all cases ∀ substitution

Boolean Functions

- degree n = # bits ✓ & 2^n rows
- 2^{2^n} diff boolean functions of degree n
- 2 functions equiv only if all outputs equiv
OR (+) AND (·) NOT ($^-$) NAND (|) NOR (↓)
- Sum of products - boolean product of literals
↳ when F(x) = 1, sum boolean expressions
- think DLD
- functional completeness - subset capable of expressing a whole set
↳ ie {·, +, ⁻}
b/c $\{\cdot, ^-\}$ $x+y = \overline{\bar{x}\bar{y}}$ & $\{+, ^-\}$ $xy = \overline{\bar{x}+\bar{y}}$

Language, Grammar & FSMs

grammar → $G = (V, T, S, P)$ ← productions/rules
vocab, terminals, start
- Language L(G) generated by G = set of all strings / terminals derivable from S
- derivation tree

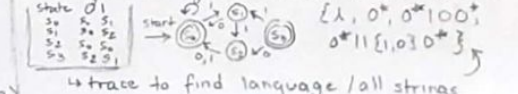


- Backus-Naur (BNF)
↳ ex $A \to Aa$ $A \to a$ $A \to AB$ ⇒ ⟨A⟩ ::= ⟨A⟩a | a | ⟨A⟩⟨B⟩
- FSM w/ out $M = (S, I, O, f, g, S_0)$ output
Ex

	f		g	
state	0	1	0	1
S_0	S_1	S_0	1	0
S_1	S_3	S_0	1	0
S_2	S_1	S_2	0	1
S_3	S_2	S_1	0	1

- FSM w/o Out → language recognition
↳ FS Automata $M = (S, I, f, s_0, F)$ final state ⓒ

state	0	1
s_0	s_0	s_1
s_1	s_2	s_3
s_2	s_0	s_2
s_3	s_2	s_1



$\{\lambda, 0^*, 0^*100^*, 0^*11 \{1,0\}^* 0^*\}$
↳ trace to find language / all strings
↳ solve
① write down states leading to final states
② garbage collection
③ verify all states have 2 outputs
- nondeterministic, 1 output has 2+ options
- Concatenation $A = \{0, 1\}$ $B = \{1, 10, 110\}$
$AB = \{01, 010, 0110, 11, 110, 1110\}$
$BA = \{01, 11, 100, 101, 1100, 1101\}$

Regular Set

- kleene's theorem - set as FSA ↔ regular set
- reg expressions are
↳ ∅, λ, x when $x \in I$
↳ AB and A ∪ B and A^*

★ Symbols = states
Edges = rules
Double check!

$\mathbb{Z}$ = int

Number Theory

- a divides b if exists int c such that $b = ac \rightarrow a|b$
  - ↳ $a|b$ & $a|c \rightarrow a|(b+c)$
  - ↳ $a|b \rightarrow a|bc$
  - ↳ $a|b$ & $b|c \rightarrow a|c$
  - ↳ $a|b$ & $a|c \rightarrow a|mb+nc$
- division algo → $a = dq + r$ where $0 \leq r < d$ $q = d|a$ $r = a \bmod d$
- congruence - $a \equiv b \bmod m$ if $m|a-b$
  - ↳ 2 ints congruent if $a \bmod m = b \bmod m$
    $a = b + km$
  - ↳ $a \equiv b \bmod m \rightarrow ca \equiv cb \bmod m$
    $\rightarrow c+a \equiv c+b \bmod m$
  - ↳ $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
    $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

* more rules in "9_Number Theory"

- Base b → $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$
  where $a_k \ldots a_0$ = nonnegative ints $< b$
- Construct expansion
  1. divide n by b → $n = bq_0 + r_0$
  2. now $q_0 = bq_1 + a_1$
  3. repeat until $q = 0$
- int is prime when only +factors are itself & 1
- fund theorem arith - every int $n > 1$ can be written as a prime or product of primes
- $f(n) = n^2 - n + 41$ is prime $n = 1$ to 40

Greatest Common Divisor

- Largest int d such that $d|a$ & $d|b$, $a \& b \neq 0$
  ↳ $d = \gcd(a, b)$
- euclidian ↓

$287 = 91 \cdot 3 + 14$
$91 = 14 \cdot 6 + 7$
$14 = 7 \cdot 2 + 0$

ex $\gcd(91, 287)$
$\gcd(287, 91)$
$(91, 14)$
$(14, 7)$
$(7, 0) = 7$