

THEOREMS FROM GRIES AND SCHNEIDER'S LADM

J. STANLEY WARFORD

Abstract. This is a collection of the axioms and theorems in Gries and Schneider's book *A Logical Approach to Discrete Math* (LADM), Springer-Verlag, 1993. The numbering is consistent with that text. Additional theorems not included or numbered in LADM are indicated by a three-part number. This document serves as a reference for homework exercises and taking exams.

Table of Precedences

- (a) $[x := e]$ (textual substitution) (highest precedence)
- (b) $.$ (function application)
- (c) unary prefix operators: $+$ $-$ \neg $\#$ \sim \mathcal{P}
- (d) $**$
- (e) \cdot $/$ \div **mod** **gcd**
- (f) $+$ $-$ \cup \cap \times \circ \bullet
- (g) \downarrow \uparrow
- (h) $\#$
- (i) \triangleleft \triangleright $^{\wedge}$
- (j) $=$ $<$ $>$ \in \subset \subseteq \supset \supseteq $|$ (conjunctive)
- (k) \vee \wedge
- (l) \Rightarrow \Leftarrow
- (m) \equiv (lowest precedence)

All nonassociative binary infix operators associate from left to right except $**$, \triangleleft , and \Rightarrow , which associate from right to left.

Definition of $/$: The operators on lines (j), (l), and (m) may have a slash $/$ through them to denote negation—e.g. $x \notin T$ is an abbreviation for $\neg(x \in T)$.

Some Basic Types

Name	Symbol	Type (set of values)
<i>integer</i>	\mathbb{Z}	integers: $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$
<i>nat</i>	\mathbb{N}	natural numbers: $0, 1, 2, \dots$
<i>positive</i>	\mathbb{Z}^+	positive integers: $1, 2, 3, \dots$
<i>negative</i>	\mathbb{Z}^-	negative integers: $-1, -2, -3, \dots$
<i>rational</i>	\mathbb{Q}	rational numbers: i/j for i, j integers, $j \neq 0$
<i>reals</i>	\mathbb{R}	real numbers
<i>positive reals</i>	\mathbb{R}^+	positive real numbers
<i>bool</i>	\mathbb{B}	booleans: <i>true</i> , <i>false</i>

Date: November 21, 2022.

Theorems of the Propositional Calculus

Equivalence and *true*.

- (3.1) **Axiom, Associativity of \equiv :** $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$
- (3.2) **Axiom, Symmetry of \equiv :** $p \equiv q \equiv q \equiv p$
- (3.3) **Axiom, Identity of \equiv :** $true \equiv q \equiv q$
- (3.4) *true*
- (3.5) **Reflexivity of \equiv :** $p \equiv p$

Negation, inequivalence, and *false*.

- (3.8) **Definition of *false* :** $false \equiv \neg true$
- (3.9) **Axiom, Distributivity of \neg over \equiv :** $\neg(p \equiv q) \equiv \neg p \equiv q$
- (3.10) **Definition of \neq :** $(p \neq q) \equiv \neg(p \equiv q)$
- (3.11) $\neg p \equiv q \equiv p \equiv \neg q$
- (3.12) **Double negation:** $\neg\neg p \equiv p$
- (3.13) **Negation of *false*:** $\neg false \equiv true$
- (3.14) $(p \neq q) \equiv \neg p \equiv q$
- (3.15) $\neg p \equiv p \equiv false$
- (3.16) **Symmetry of \neq :** $(p \neq q) \equiv (q \neq p)$
- (3.17) **Associativity of \neq :** $((p \neq q) \neq r) \equiv (p \neq (q \neq r))$
- (3.18) **Mutual associativity:** $((p \neq q) \equiv r) \equiv (p \neq (q \equiv r))$
- (3.19) **Mutual interchangeability:** $p \neq q \equiv r \equiv p \equiv q \neq r$
- (3.19.1) $p \neq p \neq q \equiv q$

Disjunction.

- (3.24) **Axiom, Symmetry of \vee :** $p \vee q \equiv q \vee p$
- (3.25) **Axiom, Associativity of \vee :** $(p \vee q) \vee r \equiv p \vee (q \vee r)$
- (3.26) **Axiom, Idempotency of \vee :** $p \vee p \equiv p$
- (3.27) **Axiom, Distributivity of \vee over \equiv :** $p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$
- (3.28) **Axiom, Excluded middle:** $p \vee \neg p$
- (3.29) **Zero of \vee :** $p \vee true \equiv true$
- (3.30) **Identity of \vee :** $p \vee false \equiv p$
- (3.31) **Distributivity of \vee over \vee :** $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$
- (3.32) $p \vee q \equiv p \vee \neg q \equiv p$

Conjunction.

- (3.35) **Axiom, Golden rule:** $p \wedge q \equiv p \equiv q \equiv p \vee q$
- (3.36) **Symmetry of \wedge :** $p \wedge q \equiv q \wedge p$
- (3.37) **Associativity of \wedge :** $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- (3.38) **Idempotency of \wedge :** $p \wedge p \equiv p$
- (3.39) **Identity of \wedge :** $p \wedge true \equiv p$
- (3.40) **Zero of \wedge :** $p \wedge false \equiv false$

- (3.41) **Distributivity of \wedge over \wedge :** $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$
 (3.42) **Contradiction:** $p \wedge \neg p \equiv false$
 (3.43) **Absorption:**
 (a) $p \wedge (p \vee q) \equiv p$
 (b) $p \vee (p \wedge q) \equiv p$
 (3.44) **Absorption:**
 (a) $p \wedge (\neg p \vee q) \equiv p \wedge q$
 (b) $p \vee (\neg p \wedge q) \equiv p \vee q$
 (3.45) **Distributivity of \vee over \wedge :** $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
 (3.46) **Distributivity of \wedge over \vee :** $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
 (3.46.1) **Consensus:** $(p \wedge q) \vee (\neg p \wedge r) \vee (q \wedge r) \equiv (p \wedge q) \vee (\neg p \wedge r)$
 (3.47) **De Morgan:**
 (a) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
 (b) $\neg(p \vee q) \equiv \neg p \wedge \neg q$
 (3.48) $p \wedge q \equiv p \wedge \neg q \equiv \neg p$
 (3.49) $p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$
 (3.50) $p \wedge (q \equiv p) \equiv p \wedge q$
 (3.51) **Replacement:** $(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \wedge (r \equiv q)$
 (3.52) **Equivalence:** $p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
 (3.53) **Exclusive or:** $p \not\equiv q \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$
 (3.55) $(p \wedge q) \wedge r \equiv p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r$

Implication.

- (3.57) **Definition of Implication:** $p \Rightarrow q \equiv p \vee q \equiv q$
 (3.58) **Axiom, Consequence:** $p \Leftarrow q \equiv q \Rightarrow p$
 (3.59) **Implication:** $p \Rightarrow q \equiv \neg p \vee q$
 (3.60) **Implication:** $p \Rightarrow q \equiv p \wedge q \equiv p$
 (3.61) **Contrapositive:** $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$
 (3.62) $p \Rightarrow (q \equiv r) \equiv p \wedge q \equiv p \wedge r$
 (3.63) **Distributivity of \Rightarrow over \equiv :** $p \Rightarrow (q \equiv r) \equiv (p \Rightarrow q) \equiv (p \Rightarrow r)$
 (3.63.1) **Distributivity of \Rightarrow over \wedge :** $p \Rightarrow q \wedge r \equiv (p \Rightarrow q) \wedge (p \Rightarrow r)$
 (3.63.2) **Distributivity of \Rightarrow over \vee :** $p \Rightarrow q \vee r \equiv (p \Rightarrow q) \vee (p \Rightarrow r)$
 (3.64) $p \Rightarrow (q \Rightarrow r) \equiv (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$
 (3.65) **Shunting:** $p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$
 (3.66) $p \wedge (p \Rightarrow q) \equiv p \wedge q$
 (3.67) $p \wedge (q \Rightarrow p) \equiv p$
 (3.68) $p \vee (p \Rightarrow q) \equiv true$
 (3.69) $p \vee (q \Rightarrow p) \equiv q \Rightarrow p$
 (3.70) $p \vee q \Rightarrow p \wedge q \equiv p \equiv q$
 (3.71) **Reflexivity of \Rightarrow :** $p \Rightarrow p$
 (3.72) **Right zero of \Rightarrow :** $p \Rightarrow true \equiv true$
 (3.73) **Left identity of \Rightarrow :** $true \Rightarrow p \equiv p$

- (3.74) $p \Rightarrow false \equiv \neg p$
 (3.74.1) $\neg p \Rightarrow false \equiv p$
 (3.74.2) $p \Rightarrow \neg p \equiv \neg p$
 (3.75) $false \Rightarrow p \equiv true$
 (3.76) **Weakening/strengthening:**
 (a) $p \Rightarrow p \vee q$ (Weakening the consequent)
 (b) $p \wedge q \Rightarrow p$ (Strengthening the antecedent)
 (c) $p \wedge q \Rightarrow p \vee q$ (Weakening/strengthening)
 (d) $p \vee (q \wedge r) \Rightarrow p \vee q$
 (e) $p \wedge q \Rightarrow p \wedge (q \vee r)$
 (3.76.1) $p \wedge q \Rightarrow p \vee r$ (Weakening/strengthening)
 (3.76.2) $(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$
 (3.77) **Modus ponens:** $p \wedge (p \Rightarrow q) \Rightarrow q$
 (3.77.1) **Modus tollens:** $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$
 (3.78) $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv p \vee q \Rightarrow r$
 (3.78.1) $(p \Rightarrow r) \vee (q \Rightarrow r) \equiv p \wedge q \Rightarrow r$
 (3.79) $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv r$
 (3.80) **Mutual implication:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$
 (3.81) **Antisymmetry:** $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$
 (3.82) **Transitivity:**
 (a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
 (b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
 (c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$
 (3.82.1) **Transitivity of \equiv :** $(p \equiv q) \wedge (q \equiv r) \Rightarrow (p \equiv r)$
 (3.82.2) $(p \equiv q) \Rightarrow (p \Rightarrow q)$

Leibniz as an axiom.

This section uses the following notation: E_X^z means $E[z := X]$.

- (3.83) **Axiom, Leibniz:** $e = f \Rightarrow E_e^z = E_f^z$
 (3.84) **Substitution:**
 (a) $(e = f) \wedge E_e^z \equiv (e = f) \wedge E_f^z$
 (b) $(e = f) \Rightarrow E_e^z \equiv (e = f) \Rightarrow E_f^z$
 (c) $q \wedge (e = f) \Rightarrow E_e^z \equiv q \wedge (e = f) \Rightarrow E_f^z$
 (3.85) **Replace by true:**
 (a) $p \Rightarrow E_p^z \equiv p \Rightarrow E_{true}^z$
 (b) $q \wedge p \Rightarrow E_p^z \equiv q \wedge p \Rightarrow E_{true}^z$
 (3.86) **Replace by false:**
 (a) $E_p^z \Rightarrow p \equiv E_{false}^z \Rightarrow p$
 (b) $E_p^z \Rightarrow p \vee q \equiv E_{false}^z \Rightarrow p \vee q$
 (3.87) **Replace by true:** $p \wedge E_p^z \equiv p \wedge E_{true}^z$
 (3.88) **Replace by false:** $p \vee E_p^z \equiv p \vee E_{false}^z$
 (3.89) **Shannon:** $E_p^z \equiv (p \wedge E_{true}^z) \vee (\neg p \wedge E_{false}^z)$
 (3.89.1) $E_{true}^z \wedge E_{false}^z \Rightarrow E_p^z$

Additional theorems concerning implication.

- (4.1) $p \Rightarrow (q \Rightarrow p)$
 (4.2) **Monotonicity of \vee :** $(p \Rightarrow q) \Rightarrow (p \vee r \Rightarrow q \vee r)$
 (4.3) **Monotonicity of \wedge :** $(p \Rightarrow q) \Rightarrow (p \wedge r \Rightarrow q \wedge r)$

Proof technique metatheorems.

- (4.4) **Deduction (assume conjuncts of antecedent):**
 To prove $P_1 \wedge P_2 \Rightarrow Q$, assume P_1 and P_2 , and prove Q .
 You cannot use textual substitution in P_1 or P_2 .
 (4.5) **Case analysis:** If E_{true}^z and E_{false}^z are theorems, then so is E_P^z .
 (4.6) **Case analysis:** $(p \vee q \vee r) \wedge (p \Rightarrow s) \wedge (q \Rightarrow s) \wedge (r \Rightarrow s) \Rightarrow s$
 (4.7) **Mutual implication:** To prove $P \equiv Q$, prove $P \Rightarrow Q$ and $Q \Rightarrow P$.
 (4.7.1) **Truth implication:** To prove P , prove $true \Rightarrow P$.
 (4.9) **Proof by contradiction:** To prove P , prove $\neg P \Rightarrow false$.
 (4.9.1) **Proof by contradiction:** To prove P , prove $\neg P \equiv false$.
 (4.12) **Proof by contrapositive:** To prove $P \Rightarrow Q$, prove $\neg Q \Rightarrow \neg P$.

General Laws of Quantification

For symmetric and associative binary operator \star with identity u .

- (8.13) **Axiom, Empty range:** $(\star x \mid false : P) = u$
 (8.14) **Axiom, One-point rule:** Provided $\neg occurs('x', 'E')$,
 $(\star x \mid x = E : P) = P[x := E]$
 (8.15) **Axiom, Distributivity:** Provided $P, Q : \mathbb{B}$ or R is finite,
 $(\star x \mid R : P) \star (\star x \mid R : Q) = (\star x \mid R : P \star Q)$
 (8.16) **Axiom, Range split:** Provided $R \wedge S \equiv false$ and $P : \mathbb{B}$ or R and S are finite,
 $(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
 (8.17) **Axiom, Range split:** Provided $P : \mathbb{B}$ or R and S are finite,
 $(\star x \mid R \vee S : P) \star (\star x \mid R \wedge S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
 (8.18) **Axiom, Range split for idempotent \star :** Provided $P : \mathbb{B}$ or R and S are finite,
 $(\star x \mid R \vee S : P) = (\star x \mid R : P) \star (\star x \mid S : P)$
 (8.19) **Axiom, Interchange of dummies:** Provided \star is idempotent or R and Q are finite,
 $\neg occurs('y', 'R'), \neg occurs('x', 'Q'),$
 $(\star x \mid R : (\star y \mid Q : P)) = (\star y \mid Q : (\star x \mid R : P))$
 (8.20) **Axiom, nesting:** Provided $\neg occurs('y', 'R')$,
 $(\star x, y \mid R \wedge Q : P) = (\star x \mid R : (\star y \mid Q : P))$
 (8.21) **Axiom, Dummy renaming:** Provided $\neg occurs('y', 'R, P')$,
 $(\star x \mid R : P) = (\star y \mid R[x := y] : P[x := y])$
 (8.22) **Change of dummy:** Provided $\neg occurs('y', 'R, P')$, and f has an inverse,
 $(\star x \mid R : P) = (\star y \mid R[x := f.y] : P[x := f.y])$

- (8.23) **Split off term:** For $n: \mathbb{N}$,
- (a) $(\star i \mid 0 \leq i < n+1 : P) = (\star i \mid 0 \leq i < n : P) \star P[i := n]$
 - (b) $(\star i \mid 0 \leq i < n+1 : P) = P[i := 0] \star (\star i \mid 0 < i < n+1 : P)$

Theorems of the Predicate Calculus

Universal quantification.

Notation: $(\star x \mid P)$ means $(\star x \mid \text{true} : P)$.

- (9.2) **Axiom, Trading:** $(\forall x \mid R : P) \equiv (\forall x \mid R \Rightarrow P)$
- (9.3) **Trading:**
- (a) $(\forall x \mid R : P) \equiv (\forall x \mid \neg R \vee P)$
 - (b) $(\forall x \mid R : P) \equiv (\forall x \mid R \wedge P \equiv R)$
 - (c) $(\forall x \mid R : P) \equiv (\forall x \mid R \vee P \equiv P)$
- (9.4) **Trading:**
- (a) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \Rightarrow P)$
 - (b) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : \neg R \vee P)$
 - (c) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \wedge P \equiv R)$
 - (d) $(\forall x \mid Q \wedge R : P) \equiv (\forall x \mid Q : R \vee P \equiv P)$
- (9.4.1) **Universal double trading:** $(\forall x \mid R : P) \equiv (\forall x \mid \neg P : \neg R)$
- (9.5) **Axiom, Distributivity of \vee over \forall :** Provided $\neg \text{occurs}('x', 'P')$,
- $$P \vee (\forall x \mid R : Q) \equiv (\forall x \mid R : P \vee Q)$$
- (9.6) Provided $\neg \text{occurs}('x', 'P')$, $(\forall x \mid R : P) \equiv P \vee (\forall x \mid \neg R)$
- (9.7) **Distributivity of \wedge over \forall :** Provided $\neg \text{occurs}('x', 'P')$,
- $$\neg(\forall x \mid \neg R) \Rightarrow ((\forall x \mid R : P \wedge Q) \equiv P \wedge (\forall x \mid R : Q))$$
- (9.8) $(\forall x \mid R : \text{true}) \equiv \text{true}$
- (9.9) $(\forall x \mid R : P \equiv Q) \Rightarrow ((\forall x \mid R : P) \equiv (\forall x \mid R : Q))$
- (9.10) **Range weakening/strengthening:** $(\forall x \mid Q \vee R : P) \Rightarrow (\forall x \mid Q : P)$
- (9.11) **Body weakening/strengthening:** $(\forall x \mid R : P \wedge Q) \Rightarrow (\forall x \mid R : P)$
- (9.12) **Monotonicity of \forall :** $(\forall x \mid R : Q \Rightarrow P) \Rightarrow ((\forall x \mid R : Q) \Rightarrow (\forall x \mid R : P))$
- (9.13) **Instantiation:** $(\forall x \mid P) \Rightarrow P[x := E]$
- (9.16) **Metatheorem:** P is a theorem iff $(\forall x \mid P)$ is a theorem.

Existential quantification.

- (9.17) **Axiom, Generalized De Morgan:** $(\exists x \mid R : P) \equiv \neg(\forall x \mid R : \neg P)$
- (9.18) **Generalized De Morgan:**
- (a) $\neg(\exists x \mid R : \neg P) \equiv (\forall x \mid R : P)$
 - (b) $\neg(\exists x \mid R : P) \equiv (\forall x \mid R : \neg P)$
 - (c) $(\exists x \mid R : \neg P) \equiv \neg(\forall x \mid R : P)$
- (9.19) **Trading:** $(\exists x \mid R : P) \equiv (\exists x \mid R \wedge P)$
- (9.20) **Trading:** $(\exists x \mid Q \wedge R : P) \equiv (\exists x \mid Q : R \wedge P)$
- (9.20.1) **Existential double trading:** $(\exists x \mid R : P) \equiv (\exists x \mid P : R)$

- (9.20.2) $(\exists x |: R) \Rightarrow ((\forall x | R : P) \Rightarrow (\exists x | R : P))$
- (9.21) **Distributivity of \wedge over \exists :** Provided $\neg occurs('x', 'P')$,
 $P \wedge (\exists x | R : Q) \equiv (\exists x | R : P \wedge Q)$
- (9.22) Provided $\neg occurs('x', 'P')$, $(\exists x | R : P) \equiv P \wedge (\exists x |: R)$
- (9.23) **Distributivity of \vee over \exists :** Provided $\neg occurs('x', 'P')$,
 $(\exists x |: R) \Rightarrow ((\exists x | R : P \vee Q) \equiv P \vee (\exists x | R : Q))$
- (9.24) $(\exists x | R : false) \equiv false$
- (9.25) **Range weakening/strengthening:** $(\exists x | R : P) \Rightarrow (\exists x | Q \vee R : P)$
- (9.26) **Body weakening/strengthening:** $(\exists x | R : P) \Rightarrow (\exists x | R : P \vee Q)$
- (9.26.1) **Body weakening/strengthening:** $(\exists x | R : P \wedge Q) \Rightarrow (\exists x | R : P)$
- (9.27) **Monotonicity of \exists :** $(\forall x | R : Q \Rightarrow P) \Rightarrow ((\exists x | R : Q) \Rightarrow (\exists x | R : P))$
- (9.28) **\exists -Introduction:** $P[x := E] \Rightarrow (\exists x |: P)$
- (9.29) **Interchange of quantification:** Provided $\neg occurs('y', 'R')$ and $\neg occurs('x', 'Q')$,
 $(\exists x | R : (\forall y | Q : P)) \Rightarrow (\forall y | Q : (\exists x | R : P))$
- (9.30) Provided $\neg occurs('x', 'Q')$,
 $(\exists x | R : P) \Rightarrow Q$ is a theorem iff $(R \wedge P)[x := \hat{x}] \Rightarrow Q$ is a theorem.

A Theory of Sets

- (11.2) **Axiom, Enumeration:** $\{e_0, e_1, \dots, e_{n-1}\} = \{x | x = e_0 \vee x = e_1 \vee \dots \vee x = e_{n-1} : x\}$
- (11.3) **Axiom, Set membership:** Provided $\neg occurs('x', 'F')$,
 $F \in \{x | R : E\} \equiv (\exists x | R : F = E)$
- (11.4) **Axiom, Extensionality:** $S = T \equiv (\forall x |: x \in S \equiv x \in T)$
- (11.4.1) **Axiom, Empty set:** $\emptyset = \{x | false : E\}$
- (11.4.2) $e \in \emptyset \equiv false$
- (11.4.3) **Axiom, Universe:** $\mathbf{U} = \{x |: x\}$, $\mathbf{U} : set(t) = \{x : t |: x\}$
- (11.4.4) $e \in \mathbf{U} \equiv true$, for $e : t$ and $\mathbf{U} : set(t)$
- (11.5) $S = \{x | x \in S : x\}$
- (11.5.1) **Axiom, Abbreviation:** For x a single variable, $\{x | R\} = \{x | R : x\}$
- (11.6) Provided $\neg occurs('y', 'R')$ and $\neg occurs('y', 'E')$,
 $\{x | R : E\} = \{y | (\exists x | R : y = E)\}$
- (11.7) $x \in \{x | R\} \equiv R$
 R is the characteristic predicate of the set.
- (11.7.1) $y \in \{x | R\} \equiv R[x := y]$ for any expression y
- (11.9) $\{x | Q\} = \{x | R\} \equiv (\forall x |: Q \equiv R)$
- (11.10) $\{x | Q\} = \{x | R\}$ is valid iff $Q \equiv R$ is valid.
- (11.11) **Methods for proving set equality $S = T$:**
- (a) Use Leibniz directly.
 - (b) Use axiom Extensionality (11.4) and prove the (9.8) Lemma
 $v \in S \equiv v \in T$ for an arbitrary value v .
 - (c) Prove $Q \equiv R$ and conclude $\{x | Q\} = \{x | R\}$.

Operations on sets.

- (11.12) **Axiom, Size:** $\#S = (\sum x \mid x \in S : 1)$
- (11.13) **Axiom, Subset:** $S \subseteq T \equiv (\forall x \mid x \in S : x \in T)$
- (11.14) **Axiom, Proper subset:** $S \subset T \equiv S \subseteq T \wedge S \neq T$
- (11.15) **Axiom, Superset:** $T \supseteq S \equiv S \subseteq T$
- (11.16) **Axiom, Proper superset:** $T \supset S \equiv S \subset T$
- (11.17) **Axiom, Complement:** $v \in \sim S \equiv v \in \mathbf{U} \wedge v \notin S$
- (11.18) $v \in \sim S \equiv v \notin S$, for v in \mathbf{U}
- (11.19) $\sim \sim S = S$
- (11.20) **Axiom, Union:** $v \in S \cup T \equiv v \in S \vee v \in T$
- (11.21) **Axiom, Intersection:** $v \in S \cap T \equiv v \in S \wedge v \in T$
- (11.22) **Axiom, Difference:** $v \in S - T \equiv v \in S \wedge v \notin T$
- (11.23) **Axiom, Power set:** $v \in \mathcal{P}S \equiv v \subseteq S$
- (11.24) **Definition.** Let E_s be a set expression constructed from set variables, \emptyset , \mathbf{U} , \sim , \cup , and \cap .
Then E_p is the expression constructed from E_s by replacing:
 \emptyset with *false*, \mathbf{U} with *true*, \cup with \vee , \cap with \wedge , \sim with \neg .
The construction is reversible: E_s can be constructed from E_p .
- (11.25) **Metatheorem.** For any set expressions E_s and F_s :
 - (a) $E_s = F_s$ is valid iff $E_p \equiv F_p$ is valid,
 - (b) $E_s \subseteq F_s$ is valid iff $E_p \Rightarrow F_p$ is valid,
 - (c) $E_s = \mathbf{U}$ is valid iff E_p is valid.

Basic properties of \cup .

- (11.26) **Symmetry of \cup :** $S \cup T = T \cup S$
- (11.27) **Associativity of \cup :** $(S \cup T) \cup U = S \cup (T \cup U)$
- (11.28) **Idempotency of \cup :** $S \cup S = S$
- (11.29) **Zero of \cup :** $S \cup \mathbf{U} = \mathbf{U}$
- (11.30) **Identity of \cup :** $S \cup \emptyset = S$
- (11.31) **Weakening:** $S \subseteq S \cup T$
- (11.32) **Excluded middle:** $S \cup \sim S = \mathbf{U}$

Basic properties of \cap .

- (11.33) **Symmetry of \cap :** $S \cap T = T \cap S$
- (11.34) **Associativity of \cap :** $(S \cap T) \cap U = S \cap (T \cap U)$
- (11.35) **Idempotency of \cap :** $S \cap S = S$
- (11.36) **Zero of \cap :** $S \cap \emptyset = \emptyset$
- (11.37) **Identity of \cap :** $S \cap \mathbf{U} = S$
- (11.38) **Strengthening:** $S \cap T \subseteq S$
- (11.39) **Contradiction:** $S \cap \sim S = \emptyset$

Basic properties of combinations of \cup and \cap .

(11.40) **Distributivity of \cup over \cap :** $S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$

(11.41) **Distributivity of \cap over \cup :** $S \cap (T \cup U) = (S \cap T) \cup (S \cap U)$

(11.42) **De Morgan:**

(a) $\sim (S \cup T) = \sim S \cap \sim T$

(b) $\sim (S \cap T) = \sim S \cup \sim T$

Additional properties of \cup and \cap .

(11.43) $S \subseteq T \wedge U \subseteq V \Rightarrow (S \cup U) \subseteq (T \cup V)$

(11.44) $S \subseteq T \wedge U \subseteq V \Rightarrow (S \cap U) \subseteq (T \cap V)$

(11.45) $S \subseteq T \equiv S \cup T = T$

(11.46) $S \subseteq T \equiv S \cap T = S$

(11.47) $S \cup T = \mathbf{U} \equiv (\forall x \mid x \in \mathbf{U} : x \notin S \Rightarrow x \in T)$

(11.48) $S \cap T = \emptyset \equiv (\forall x \mid x \in S \Rightarrow x \notin T)$

Properties of set difference.

(11.49) $S - T = S \cap \sim T$

(11.50) $S - T \subseteq S$

(11.51) $S - \emptyset = S$

(11.52) $S \cap (T - S) = \emptyset$

(11.53) $S \cup (T - S) = S \cup T$

(11.54) $S - (T \cup U) = (S - T) \cap (S - U)$

(11.55) $S - (T \cap U) = (S - T) \cup (S - U)$

Implication versus subset.

(11.56) $(\forall x \mid P \Rightarrow Q) \equiv \{x \mid P\} \subseteq \{x \mid Q\}$

Properties of subset.

(11.57) **Antisymmetry:** $S \subseteq T \wedge T \subseteq S \equiv S = T$

(11.58) **Reflexivity:** $S \subseteq S$

(11.59) **Transitivity:** $S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$

(11.60) $\emptyset \subseteq S$

(11.61) $S \subset T \equiv S \subseteq T \wedge \neg(T \subseteq S)$

(11.62) $S \subset T \equiv S \subseteq T \wedge (\exists x \mid x \in T : x \notin S)$

(11.63) $S \subseteq T \equiv S \subset T \vee S = T$

(11.64) $S \not\subseteq S$

(11.65) $S \subset T \Rightarrow S \subseteq T$

(11.66) $S \subset T \Rightarrow T \not\subseteq S$

(11.67) $S \subseteq T \Rightarrow T \not\subseteq S$

(11.68) $S \subseteq T \wedge \neg(U \subseteq T) \Rightarrow \neg(U \subseteq S)$

$$(11.69) \quad (\exists x \mid x \in S : x \notin T) \Rightarrow S \neq T$$

(11.70) **Transitivity:**

$$(a) \quad S \subseteq T \wedge T \subseteq U \Rightarrow S \subseteq U$$

$$(b) \quad S \subset T \wedge T \subseteq U \Rightarrow S \subset U$$

$$(c) \quad S \subset T \wedge T \subset U \Rightarrow S \subset U$$

Theorems concerning power set \mathcal{P} .

$$(11.71) \quad \mathcal{P}\emptyset = \{\emptyset\}$$

$$(11.72) \quad S \in \mathcal{P}S$$

$$(11.73) \quad \#(\mathcal{P}S) = 2^{\#S} \quad (\text{for finite set } S)$$

Union and intersection of families of sets.

$$(11.74.1) \quad \textbf{Definition:} \quad v \in (\cup x \mid R : E) \equiv (\exists x \mid R : v \in E)$$

$$(11.75.1) \quad \textbf{Definition:} \quad v \in (\cap x \mid R : E) \equiv (\forall x \mid R : v \in E)$$

(11.76) **Axiom, Partition:** Set S partitions T if

(i) the sets in S are pairwise disjoint and

(ii) the union of the sets in S is T , that is, if

$$(\forall u, v \mid u \in S \wedge v \in S \wedge u \neq v : u \cap v = \emptyset) \wedge (\cup u \mid u \in S : u) = T$$

Bags.

$$(11.80) \quad \textbf{Axiom, Size:} \quad \#\{x \mid R : E\} = (\sum x \mid R : 1)$$

$$(11.81) \quad \textbf{Axiom, Number of occurrences:} \quad v\#\{x \mid R : E\} = (\sum x \mid R \wedge v = E : 1)$$

$$(11.82) \quad \textbf{Axiom, Bag equality:} \quad B = C \equiv (\forall v \mid v\#B = v\#C)$$

$$(11.83) \quad \textbf{Axiom, Subbag:} \quad B \subseteq C \equiv (\forall v \mid v\#B \leq v\#C)$$

$$(11.84) \quad \textbf{Axiom, Proper subbag:} \quad B \subset C \equiv B \subseteq C \wedge B \neq C$$

$$(11.85) \quad \textbf{Axiom, Union:} \quad B \cup C = \{v, i \mid 0 \leq i < v\#B + v\#C : v\}$$

$$(11.86) \quad \textbf{Axiom, Intersection:} \quad B \cap C = \{v, i \mid 0 \leq i < v\#B \downarrow v\#C : v\}$$

$$(11.87) \quad \textbf{Axiom, Difference:} \quad B - C = \{v, i \mid 0 \leq i < v\#B - v\#C : v\}$$

Mathematical Induction

(12.3) **Axiom, Mathematical Induction over \mathbb{N} :**

$$(\forall n : \mathbb{N} \mid (\forall i \mid 0 \leq i < n : P.i) \Rightarrow P.n) \Rightarrow (\forall n : \mathbb{N} \mid P.n)$$

(12.4) **Mathematical Induction over \mathbb{N} :**

$$(\forall n : \mathbb{N} \mid (\forall i \mid 0 \leq i < n : P.i) \Rightarrow P.n) \equiv (\forall n : \mathbb{N} \mid P.n)$$

(12.5) **Mathematical Induction over \mathbb{N} :**

$$P.0 \wedge (\forall n : \mathbb{N} \mid (\forall i \mid 0 \leq i \leq n : P.i) \Rightarrow P(n+1)) \equiv (\forall n : \mathbb{N} \mid P.n)$$

(12.11) **Definition, b to the power n :**

$$b^0 = 1$$

$$b^{n+1} = b \cdot b^n \quad \text{for } n \geq 0$$

- (12.12) **b to the power n :**
 $b^0 = 1$
 $b^n = b \cdot b^{n-1}$ for $n \geq 1$
- (12.13) **Definition, factorial:**
 $0! = 1$
 $n! = n \cdot (n-1)!$ for $n > 0$
- (12.14) **Definition, Fibonacci:**
 $F_0 = 0, F_1 = 1$
 $F_n = F_{n-1} + F_{n-2}$ for $n > 1$
- (12.14.1) **Definition, Golden Ratio:** $\phi = (1 + \sqrt{5})/2 \approx 1.618$ $\hat{\phi} = (1 - \sqrt{5})/2 \approx -0.618$
- (12.15) $\phi^2 = \phi + 1$ and $\hat{\phi}^2 = \hat{\phi} + 1$
- (12.16) $F_n \leq \phi^{n-1}$ for $n \geq 1$
- (12.16.1) $\phi^{n-2} \leq F_n$ for $n \geq 1$
- (12.17) $F_{n+m} = F_m \cdot F_{n+1} + F_{m-1} \cdot F_n$ for $n \geq 0$ and $m \geq 1$

Inductively defined binary trees.

- (12.30) **Definition, Binary Tree:**
 \emptyset is a binary tree, called the empty tree.
 (d, l, r) is a binary tree, for $d: \mathbb{Z}$ and l, r binary trees.
- (12.31) **Definition, Number of Nodes:**
 $\# \emptyset = 0$
 $\#(d, l, r) = 1 + \#l + \#r$
- (12.32) **Definition, Height:**
 $height.\emptyset = 0$
 $height.(d, l, r) = 1 + \max(height.l, height.r)$
- (12.32.1) **Definition, Leaf:** A leaf is a node with no children (i.e. two empty subtrees).
- (12.32.2) **Definition, Internal node:** An internal node is a node that is not a leaf.
- (12.32.3) **Definition, Complete:** A binary tree is complete if every node has either 0 or 2 children.
- (12.33) The maximum number of nodes in a tree with height n is $2^n - 1$ for $n \geq 0$.
- (12.34) The minimum number of nodes in a tree with height n is n for $n \geq 0$.
- (12.35) (a) The maximum number of leaves in a tree with height n is 2^{n-1} for $n > 0$.
(b) The maximum number of internal nodes in a tree with height n is $2^{n-1} - 1$ for $n > 0$.
- (12.36) (a) The minimum number of leaves in a tree with height n is 1 for $n > 0$.
(b) The minimum number of internal nodes in a tree with height n is $n - 1$ for $n > 0$.
- (12.37) Every nonempty complete tree has an odd number of nodes.

A Theory of Programs

- (p.1) **Axiom, Excluded miracle:** $wp.S.false \equiv false$
- (p.2) **Axiom, Conjunctivity:** $wp.S.(X \wedge Y) \equiv wp.S.X \wedge wp.S.Y$

- (p.3) **Monotonicity:** $(X \Rightarrow Y) \Rightarrow (wp.S.X \Rightarrow wp.S.Y)$
- (p.4) **Definition, Hoare triple:** $\{Q\} S \{R\} \equiv Q \Rightarrow wp.S.R$
- (p.4.1) $\{wp.S.R\} S \{R\}$
- (p.5) **Postcondition rule:** $\{Q\} S \{A\} \wedge (A \Rightarrow R) \Rightarrow \{Q\} S \{R\}$
- (p.6) **Definition, Program equivalence:** $S = T \equiv (\text{For all } R, wp.S.R \equiv wp.T.R)$
- (p.7) $(Q \Rightarrow A) \wedge \{A\} S \{R\} \Rightarrow \{Q\} S \{R\}$
- (p.8) $\{Q0\} S \{R0\} \wedge \{Q1\} S \{R1\} \Rightarrow \{Q0 \wedge Q1\} S \{R0 \wedge R1\}$
- (p.9) $\{Q0\} S \{R0\} \wedge \{Q1\} S \{R1\} \Rightarrow \{Q0 \vee Q1\} S \{R0 \vee R1\}$
- (p.10) **Definition, skip:** $wp.skip.R \equiv R$
- (p.11) $\{Q\} skip \{R\} \equiv Q \Rightarrow R$
- (p.12) **Definition, abort:** $wp.abort.R \equiv false$
- (p.13) $\{Q\} abort \{R\} \equiv Q \equiv false$
- (p.14) **Definition, Composition:** $wp.(S;T).R \equiv wp.S.(wp.T.R)$
- (p.15) $\{Q\} S \{H\} \wedge \{H\} T \{R\} \Rightarrow \{Q\} S;T \{R\}$
- (p.16) **Identity of composition:**
 (a) $S ; skip = S$ (b) $skip ; S = S$
- (p.17) **Zero of composition:**
 (a) $S ; abort = abort$ (b) $abort ; S = abort$
- (p.18) **Definition, Assignment:** $wp.(x := E).R \equiv R[x := E]$
- (p.19) **Proof method for assignment:** (p.19) is (10.2)
 To show that $x := E$ is an implementation of $\{Q\}x := ?\{R\}$,
 prove $Q \Rightarrow R[x := E]$.
- (p.20) $(x := x) = skip$
- (p.21) $IFG :$ (p.21) is (10.6)
if $B1 \rightarrow S1$
 $\parallel B2 \rightarrow S2$
 $\parallel B3 \rightarrow S3$
fi
- (p.22) **Definition, IFG:** $wp.IFG.R \equiv (B1 \vee B2 \vee B3) \wedge$
 $B1 \Rightarrow wp.S1.R \wedge B2 \Rightarrow wp.S2.R \wedge B3 \Rightarrow wp.S3.R$
- (p.23) **Empty guard:** **if fi** = *abort*
- (p.24) **Proof method for IFG:** (p.24) is (10.7)
 To prove $\{Q\}IFG\{R\}$, it suffices to prove
 (a) $Q \Rightarrow B1 \vee B2 \vee B3$,
 (b) $\{Q \wedge B1\} S1 \{R\}$,
 (c) $\{Q \wedge B2\} S2 \{R\}$, and
 (d) $\{Q \wedge B3\} S3 \{R\}$.
- (p.25) $\neg(B1 \vee B2 \vee B3) \Rightarrow IFG = abort$
- (p.26) **One-guard rule:** $\{Q\} \text{if } B \rightarrow S \text{ fi } \{R\} \Rightarrow \{Q\} S \{R\}$
- (p.27) **Distributivity of program over alternation:**
if $B1 \rightarrow S1; T \parallel B2 \rightarrow S2; T$ **fi** = **if** $B1 \rightarrow S1 \parallel B2 \rightarrow S2$ **fi** ; T

(p.28) **DO :** $\text{do } B \rightarrow S \text{ od}$

(p.29) **Fundamental Invariance Theorem.** (p.29) is (12.43)

Suppose

- $\{P \wedge B\} S \{P\}$ holds—i.e. execution of S begun in a state in which P and B are *true* terminates with P *true*—and
- $\{P\} \text{do } B \rightarrow S \text{ od } \{true\}$ —i.e. execution of the loop begun in a state in which P is *true* terminates.

Then $\{P\} \text{do } B \rightarrow S \text{ od } \{P \wedge \neg B\}$ holds.

(p.30) **Proof method for DO:** (p.30) is (12.45)

To prove $\{Q\} \text{initialization}; \{P\} \text{do } B \rightarrow S \text{ od } \{R\}$,
it suffices to prove

- (a) P is *true* before execution of the loop: $\{Q\} \text{initialization}; \{P\}$,
- (b) P is a loop invariant: $\{P \wedge B\} S \{P\}$,
- (c) Execution of the loop terminates, and
- (d) R holds upon termination: $P \wedge \neg B \Rightarrow R$.

(p.31) **False guard:** $\text{do } false \rightarrow S \text{ od} = \text{skip}$

Relations and Functions

(14.2) **Axiom, Pair equality:** $\langle b, c \rangle = \langle b', c' \rangle \equiv b = b' \wedge c = c'$

(14.2.1) **Ordered pair one-point rule:** Provided $\neg \text{occurs}('x, y', 'E, F')$,
 $(\star x, y \mid \langle x, y \rangle = \langle E, F \rangle : P) = P[x, y := E, F]$

(14.3) **Axiom, Cross product:** $S \times T = \{b, c \mid b \in S \wedge c \in T : \langle b, c \rangle\}$

(14.3.1) **Axiom, Ordered pair extensionality:**
 $U = V \equiv (\forall x, y \mid \langle x, y \rangle \in U \equiv \langle x, y \rangle \in V)$

Theorems for cross product.

(14.4) **Membership:** $\langle x, y \rangle \in S \times T \equiv x \in S \wedge y \in T$

(14.5) $\langle x, y \rangle \in S \times T \equiv \langle y, x \rangle \in T \times S$

(14.6) $S = \emptyset \Rightarrow S \times T = T \times S = \emptyset$

(14.7) $S \times T = T \times S \equiv S = \emptyset \vee T = \emptyset \vee S = T$

(14.8) **Distributivity of \times over \cup :**

(a) $S \times (T \cup U) = (S \times T) \cup (S \times U)$

(b) $(S \cup T) \times U = (S \times U) \cup (T \times U)$

(14.9) **Distributivity of \times over \cap :**

(a) $S \times (T \cap U) = (S \times T) \cap (S \times U)$

(b) $(S \cap T) \times U = (S \times U) \cap (T \times U)$

(14.10) **Distributivity of \times over $-$:**

$S \times (T - U) = (S \times T) - (S \times U)$

(14.11) **Monotonicity:** $T \subseteq U \Rightarrow S \times T \subseteq S \times U$

(14.12) $S \subseteq U \wedge T \subseteq V \Rightarrow S \times T \subseteq U \times V$

- (14.13) $S \times T \subseteq S \times U \wedge S \neq \emptyset \Rightarrow T \subseteq U$
 (14.14) $(S \cap T) \times (U \cap V) = (S \times U) \cap (T \times V)$
 (14.15) For finite S and T , $\#(S \times T) = \#S \cdot \#T$

Relations.

(14.15.1) **Definition, Binary relation:**

A *binary relation* over $B \times C$ is a subset of $B \times C$.

(14.15.2) **Definition, Identity:** The identity relation i_B on B is $i_B = \{x: B \mid \langle x, x \rangle\}$

(14.15.3) **Identity lemma:** $\langle x, y \rangle \in i_B \equiv x = y$

(14.15.4) **Notation:** $\langle b, c \rangle \in \rho$ and $b \rho c$ are interchangeable notations.

(14.15.5) **Conjunctive meaning:** $b \rho c \sigma d \equiv b \rho c \wedge c \sigma d$

The *domain* $Dom.\rho$ and *range* $Ran.\rho$ of a relation ρ on $B \times C$ are defined by

(14.16) **Definition, Domain:** $Dom.\rho = \{b: B \mid (\exists c \mid b \rho c)\}$

(14.17) **Definition, Range:** $Ran.\rho = \{c: C \mid (\exists b \mid b \rho c)\}$

The *inverse* ρ^{-1} of a relation ρ on $B \times C$ is the relation defined by

(14.18) **Definition, Inverse:** $\langle b, c \rangle \in \rho^{-1} \equiv \langle c, b \rangle \in \rho$, for all $b: B, c: C$

(14.19) Let ρ and σ be relations.

- (a) $Dom(\rho^{-1}) = Ran.\rho$
- (b) $Ran(\rho^{-1}) = Dom.\rho$
- (c) If ρ is a relation on $B \times C$, then ρ^{-1} is a relation on $C \times B$
- (d) $(\rho^{-1})^{-1} = \rho$
- (e) $\rho \subseteq \sigma \equiv \rho^{-1} \subseteq \sigma^{-1}$

Let ρ be a relation on $B \times C$ and σ be a relation on $C \times D$. The *product* of ρ and σ , denoted by $\rho \circ \sigma$, is the relation defined by

(14.20) **Definition, Product:** $\langle b, d \rangle \in \rho \circ \sigma \equiv (\exists c \mid c \in C: \langle b, c \rangle \in \rho \wedge \langle c, d \rangle \in \sigma)$

or, using the alternative notation by

(14.21) **Definition, Product:** $b (\rho \circ \sigma) d \equiv (\exists c \mid b \rho c \sigma d)$

Theorems for relation product.

(14.22) **Associativity of \circ :** $\rho \circ (\sigma \circ \theta) = (\rho \circ \sigma) \circ \theta$

(14.23) **Distributivity of \circ over \cup :**

- (a) $\rho \circ (\sigma \cup \theta) = (\rho \circ \sigma) \cup (\rho \circ \theta)$
- (b) $(\sigma \cup \theta) \circ \rho = (\sigma \circ \rho) \cup (\theta \circ \rho)$

(14.24) **Distributivity of \circ over \cap :**

- (a) $\rho \circ (\sigma \cap \theta) \subseteq (\rho \circ \sigma) \cap (\rho \circ \theta)$
- (b) $(\sigma \cap \theta) \circ \rho \subseteq (\sigma \circ \rho) \cap (\theta \circ \rho)$

Theorems for powers of a relation.(14.25) **Definition:**

$$\rho^0 = i_B$$

$$\rho^{n+1} = \rho^n \circ \rho \quad \text{for } n \geq 0$$

$$(14.26) \quad \rho^m \circ \rho^n = \rho^{m+n} \quad \text{for } m \geq 0, n \geq 0$$

$$(14.27) \quad (\rho^m)^n = \rho^{m \cdot n} \quad \text{for } m \geq 0, n \geq 0$$

(14.28) For ρ a relation on finite set B of n elements,

$$(\exists i, j \mid 0 \leq i < j \leq 2^{n^2} : \rho^i = \rho^j)$$

(14.29) Let ρ be a relation on a finite set B . Suppose $\rho^i = \rho^j$ and $0 \leq i < j$. Then

$$(a) \quad \rho^{i+k} = \rho^{j+k} \quad \text{for } k \geq 0$$

$$(b) \quad \rho^i = \rho^{i+p \cdot (j-i)} \quad \text{for } p \geq 0$$

Table 14.1 Classes of relations ρ over set B

Name	Property	Alternative
(a) reflexive	$(\forall b \mid b \rho b)$	$i_B \subseteq \rho$
(b) irreflexive	$(\forall b \mid \neg(b \rho b))$	$i_B \cap \rho = \emptyset$
(c) symmetric	$(\forall b, c \mid b \rho c \equiv c \rho b)$	$\rho^{-1} = \rho$
(d) antisymmetric	$(\forall b, c \mid b \rho c \wedge c \rho b \Rightarrow b = c)$	$\rho \cap \rho^{-1} \subseteq i_B$
(e) asymmetric	$(\forall b, c \mid b \rho c \Rightarrow \neg(c \rho b))$	$\rho \cap \rho^{-1} = \emptyset$
(f) transitive	$(\forall b, c, d \mid b \rho c \wedge c \rho d \Rightarrow b \rho d)$	$\rho = (\cup i \mid i > 0 : \rho^i)$

(14.30.1) **Definition:** Let ρ be a relation on a set. The *reflexive closure* of ρ is the relation $r(\rho)$ that satisfies:(a) $r(\rho)$ is reflexive;(b) $\rho \subseteq r(\rho)$;(c) If any relation σ is reflexive and $\rho \subseteq \sigma$, then $r(\rho) \subseteq \sigma$.(14.30.2) **Definition:** Let ρ be a relation on a set. The *symmetric closure* of ρ is the relation $s(\rho)$ that satisfies:(a) $s(\rho)$ is symmetric;(b) $\rho \subseteq s(\rho)$;(c) If any relation σ is symmetric and $\rho \subseteq \sigma$, then $s(\rho) \subseteq \sigma$.(14.30.3) **Definition:** Let ρ be a relation on a set. The *transitive closure* of ρ is the relation ρ^+ that satisfies:(a) ρ^+ is transitive;(b) $\rho \subseteq \rho^+$;(c) If any relation σ is transitive and $\rho \subseteq \sigma$, then $\rho^+ \subseteq \sigma$.(14.30.4) **Definition:** Let ρ be a relation on a set. The *reflexive transitive closure* of ρ is the relation ρ^* that is both the reflexive and the transitive closure of ρ .

- (14.31) (a) A reflexive relation is its own reflexive closure.
 (b) A symmetric relation is its own symmetric closure.
 (c) A transitive relation is its own transitive closure.
- (14.32) Let ρ be a relation on a set B . Then,
 (a) $r(\rho) = \rho \cup i_B$
 (b) $s(\rho) = \rho \cup \rho^{-1}$
 (c) $\rho^+ = (\cup i \mid 0 < i : \rho^i)$
 (d) $\rho^* = \rho^+ \cup i_B$

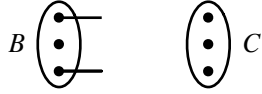



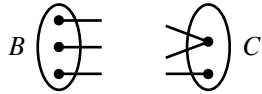
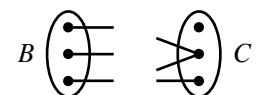
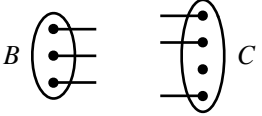
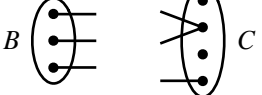
Equivalence relations.

- (14.33) **Definition:** A relation is an *equivalence relation* iff it is reflexive, symmetric, and transitive
- (14.34) **Definition:** Let ρ be an equivalence relation on B . Then $[b]_\rho$, the *equivalence class* of b , is the subset of elements of B that are equivalent (under ρ) to b :
 $x \in [b]_\rho \equiv x \rho b$
- (14.35) Let ρ be an equivalence relation on B , and let b, c be members of B . The following three predicates are equivalent:
 (a) $b \rho c$
 (b) $[b] \cap [c] \neq \emptyset$
 (c) $[b] = [c]$
 That is, $(b \rho c) = ([b] \cap [c] \neq \emptyset) = ([b] = [c])$
- (14.35.1) Let ρ be an equivalence relation on B . The equivalence classes partition B .
- (14.36) Let P be the set of sets of a partition of B . The following relation ρ on B is an equivalence relation:
 $b \rho c \equiv (\exists p \mid p \in P : b \in p \wedge c \in p)$

Functions.

- (14.37) (a) **Definition:** A binary relation f on $B \times C$ is *determinate* iff
 $(\forall b, c, c' \mid b f c \wedge b f c' : c = c')$
 (b) **Definition:** A binary relation is a *function* iff it is determinate.
- (14.37.1) **Notation:** $f.b = c$ and $b f c$ are interchangeable notations.
- (14.38) **Definition:** A function f on $B \times C$ is *total* if $B = \text{Dom}.f$.
 Otherwise it is *partial*.
 We write $f : B \rightarrow C$ for the type of f if f is total and $f : B \rightsquigarrow C$ if f is partial.
- (14.38.1) **Total:** A function f on $B \times C$ is total if, for an arbitrary element b : B ,
 $(\exists c : C \mid f.b = c)$
- (14.39) **Definition, Composition:** For functions f and g , $f \bullet g = g \circ f$.
- (14.40) Let $g : B \rightarrow C$ and $f : C \rightarrow D$ be total functions.
 Then the composition $f \bullet g$ of f and g is the total function defined by
 $(f \bullet g).b = f(g.b)$

ρ a relation on $B \times C$
 f a function, $f : B \rightarrow C$

<p>Determinate (14.37)</p>  <p>Determinate: f is a function</p>  <p>Not determinate: ρ is not a function</p>	<p>Total (14.38)</p>  <p>Total</p>  <p>Not total (partial)</p>
<p>Onto (14.41a)</p>  <p>Onto</p>  <p>Not onto</p>	<p>One-to-one (14.41b)</p>  <p>One-to-one</p>  <p>Not one-to-one</p>

Inverses of total functions.

(14.41) Definitions:

- (a) Total function $f : B \rightarrow C$ is *onto* or *surjective* if $\text{Ran}.f = C$.
- (b) Total function f is *one-to-one* or *injective* if
 $(\forall b, b' : B, c : C) : b f c \wedge b' f c \equiv b = b'$.
- (c) Total function f is *bijective* if it is one-to-one and onto.

(14.42) Let f be a total function, and let f^{-1} be its relational inverse.

- (a) Then f^{-1} is a function, i.e. is determinate, iff f is one-to-one.
- (b) And, f^{-1} is total iff f is onto.

(14.43) Definitions: Let $f : B \rightarrow C$.

- (a) A *left inverse* of f is a function $g : C \rightarrow B$ such that $g \bullet f = i_B$.
- (b) A *right inverse* of f is a function $g : C \rightarrow B$ such that $f \bullet g = i_C$.
- (c) Function g is an *inverse* of f if it is both a left inverse and a right inverse.

(14.44) Function $f : B \rightarrow C$ is onto iff f has a right inverse.

(14.45) Let $f : B \rightarrow C$ be total. Then f is one-to-one iff f has a left inverse.

- (14.46) Let $f : B \rightarrow C$ be total. The following statements are equivalent.
- (a) f is one-to-one and onto.
 - (b) There is a function $g : C \rightarrow B$ that is both a left and a right inverse of f .
 - (c) f has a left inverse and f has a right inverse.

Order relations.

- (14.47) **Definition:** A binary relation ρ on a set B is called a *partial order on B* if it is reflexive, antisymmetric, and transitive. In this case, pair $\langle B, \rho \rangle$ is called a *partially ordered set* or *poset*.

We use the symbol \preceq for an arbitrary partial order, sometimes writing $c \succeq b$ instead of $b \preceq c$.

- (14.47.1) **Definition, Incomparable:** $\text{incomp}(b, c) \equiv \neg(b \preceq c) \wedge \neg(c \preceq b)$
- (14.48) **Definition:** Relation \prec is a *quasi order* or *strict partial order* if \prec is transitive and irreflexive
- (14.48.1) **Definition, Reflexive reduction:** Given \preceq , its *reflexive reduction* \prec is computed by eliminating all pairs $\langle b, b \rangle$ from \preceq .
- (14.48.2) Let \prec be the reflexive reduction of \preceq . Then,
 $\neg(b \preceq c) \equiv c \prec b \vee \text{incomp}(b, c)$
- (14.49) (a) If ρ is a partial order over a set B , then $\rho - i_B$ is a quasi order.
 (b) If ρ is a quasi order over a set B , then $\rho \cup i_B$ is a partial order.

Total orders and topological sort.

- (14.50) **Definition:** A partial order \preceq over B is called a *total* or *linear* order if $(\forall b, c \in B : b \preceq c \vee c \preceq b)$, i.e. iff $\preceq \cup \preceq^{-1} = B \times B$.
 In this case, the pair $\langle B, \preceq \rangle$ is called a *linearly ordered set* or a *chain*.
- (14.51) **Definitions:** Let S be a nonempty subset of poset $\langle U, \preceq \rangle$.
- (a) Element b of S is a *minimal element of S* if no element of S is smaller than b , i.e. if $b \in S \wedge (\forall c \mid c \prec b : c \notin S)$.
 - (b) Element b of S is the *least element of S* if $b \in S \wedge (\forall c \mid c \in S : b \preceq c)$.
 - (c) Element b is a *lower bound of S* if $(\forall c \mid c \in S : b \preceq c)$.
 (A lower bound of S need not be in S .)
 - (d) Element b is the *greatest lower bound of S* , written $\text{glb}.S$ if b is a lower bound and if every lower bound c satisfies $c \preceq b$.
- (14.52) Every finite nonempty subset S of poset $\langle U, \preceq \rangle$ has a minimal element.
- (14.53) Let B be a nonempty subset of poset $\langle U, \preceq \rangle$.
- (a) A least element of B is also a minimal element of B (but not necessarily vice versa).
 - (b) A least element of B is also a greatest lower bound of B (but not necessarily vice versa).

(c) A lower bound of B that belongs to B is also a least element of B .

((14.54) **Definitions:** Let S be a nonempty subset of poset $\langle U, \preceq \rangle$.

- (a) Element b of S is a *maximal element* of S if no element of S is larger than b , i.e. if $b \in S \wedge (\forall c \mid b \prec c : c \notin S)$.
- (b) Element b of S is the *greatest element* of S if $b \in S \wedge (\forall c \mid c \in S : c \preceq b)$.
- (c) Element b is an *upper bound* of S if $(\forall c \mid c \in S : c \preceq b)$.
(An upper bound of S need not be in S .)
- (d) Element b is the *least upper bound* of S , written $\text{lub}.S$, if b is an upper bound and if every upper bound c satisfies $b \preceq c$.

Relational databases.

(14.56.1) **Definition, select:** For Relation R and predicate F , which may contain names of fields of R , $\sigma(R, F) = \{t \mid t \in R \wedge F\}$

(14.56.2) **Definition, project:** For A_1, \dots, A_m a subset of the names of the fields of relation R , $\pi(R, A_1, \dots, A_m) = \{t \mid t \in R : \langle t.A_1, t.A_2, \dots, t.A_m \rangle\}$

(14.56.3) **Definition, natural join:** For Relations R_1 and R_2 , $R_1 \bowtie R_2$ has all the attributes that R_1 and R_2 have, but if an attribute appears in both, then it appears only once in the result; further, only those tuples that agree on this common attribute are included.

Growth of Functions

(g.1) **Definition of asymptotic upper bound:** For a given function $g.n$, $O(g.n)$, pronounced “big-oh of g of n ”, is the set of functions

$$\{f.n \mid (\exists c, n_0 \mid c > 0 \wedge n_0 > 0 : (\forall n \mid n \geq n_0 : 0 \leq f.n \leq c \cdot g.n))\}$$

(g.2) **O -notation:** $f.n = O(g.n)$ means function $f.n$ is in the set $O(g.n)$.

(g.3) **Definition of asymptotic lower bound:** For a given function $g.n$, $\Omega(g.n)$, pronounced “big-omega of g of n ”, is the set of functions

$$\{f.n \mid (\exists c, n_0 \mid c > 0 \wedge n_0 > 0 : (\forall n \mid n \geq n_0 : 0 \leq c \cdot g.n \leq f.n))\}$$

(g.4) **Ω -notation:** $f.n = \Omega(g.n)$ means function $f.n$ is in the set $\Omega(g.n)$.

(g.5) **Definition of asymptotic tight bound:** For a given function $g.n$, $\Theta(g.n)$, pronounced “big-theta of g of n ”, is the set of functions

$$\{f.n \mid (\exists c_1, c_2, n_0 \mid c_1 > 0 \wedge c_2 > 0 \wedge n_0 > 0 : (\forall n \mid n \geq n_0 : 0 \leq c_1 \cdot g.n \leq f.n \leq c_2 \cdot g.n))\}$$

(g.6) **Θ -notation:** $f.n = \Theta(g.n)$ means function $f.n$ is in the set $\Theta(g.n)$.

(g.7) $f.n = \Theta(g.n)$ if and only if $f.n = O(g.n)$ and $f.n = \Omega(g.n)$

Comparison of functions.**(g.8) Reflexivity:**

(a) $f.n = O(f.n)$

(b) $f.n = \Omega(f.n)$

(c) $f.n = \Theta(f.n)$

(g.9) Symmetry: $f.n = \Theta(g.n) \equiv g.n = \Theta(f.n)$ **(g.10) Transpose symmetry:** $f.n = O(g.n) \equiv g.n = \Omega(f.n)$ **(g.11) Transitivity:**

(a) $f.n = O(g.n) \wedge g.n = O(h.n) \Rightarrow f.n = O(h.n)$

(b) $f.n = \Omega(g.n) \wedge g.n = \Omega(h.n) \Rightarrow f.n = \Omega(h.n)$

(c) $f.n = \Theta(g.n) \wedge g.n = \Theta(h.n) \Rightarrow f.n = \Theta(h.n)$

(g.12) Define an *asymptotically positive polynomial* $p.n$ of degree d to be $p.n = (\Sigma i \mid 0 \leq i \leq d : a_i n^i)$ where the constants a_0, a_1, \dots, a_d are the *coefficients* of the polynomial and $a_d > 0$. Then $p.n = \Theta(n^d)$.**(g.13)** (a) $O(1) \subset O(\lg n) \subset O(n) \subset O(n \lg n) \subset O(n^2) \subset O(n^3) \subset O(2^n)$

(b) $\Omega(1) \supset \Omega(\lg n) \supset \Omega(n) \supset \Omega(n \lg n) \supset \Omega(n^2) \supset \Omega(n^3) \supset \Omega(2^n)$

A Theory of Integers**Minimum and maximum.****(15.53) Definition of \downarrow :** $(\forall z \mid: z \leq x \downarrow y \equiv z \leq x \wedge z \leq y)$ **Definition of \uparrow :** $(\forall z \mid: z \geq x \uparrow y \equiv z \geq x \wedge z \geq y)$ **(15.54) Symmetry:**

(a) $x \downarrow y = y \downarrow x$

(b) $x \uparrow y = y \uparrow x$

(15.55) Associativity:

(a) $(x \downarrow y) \downarrow z = x \downarrow (y \downarrow z)$

(b) $(x \uparrow y) \uparrow z = x \uparrow (y \uparrow z)$

Restrictions. Although \downarrow and \uparrow are symmetric and associative, they do not have identities over the integers. Therefore, axiom (8.13) empty range does not apply to \downarrow or \uparrow . Also, when using range-split axioms, no range should be *false*.

(15.56) Idempotency:

(a) $x \downarrow x = x$

(b) $x \uparrow x = x$

Divisibility.**(15.77) Definition of \mid :** $c \mid b \equiv (\exists d \mid: c \cdot d = b)$

(15.78) $c \mid c$

(15.79) $c \mid 0$

(15.80) $1 \mid b$

(15.80.1) $-b \mid c \equiv b \mid c$

(15.80.2) $-1 \mid b$

- (15.81) $c \mid 1 \Rightarrow c = 1 \vee c = -1$
 (15.81.1) $c \mid 1 \equiv c = 1 \vee c = -1$
 (15.82) $d \mid c \wedge c \mid b \Rightarrow d \mid b$
 (15.83) $b \mid c \wedge c \mid b \equiv b = c \vee b = -c$
 (15.84) $b \mid c \Rightarrow b \mid c \cdot d$
 (15.85) $b \mid c \Rightarrow b \cdot d \mid c \cdot d$
 (15.86) $1 < b \wedge b \mid c \Rightarrow \neg(b \mid (c+1))$
 (15.87) **Theorem:** Given integers b, c with $c > 0$, there exist (unique) integers q and r such that $b = q \cdot c + r$, where $0 \leq r < c$.
 (15.89) **Corollary:** For given b, c , the values q and r of Theorem (15.87) are unique.

Greatest common divisor.

- (15.90) **Definition of \div and mod for operands b and $c, c \neq 0$:**
 $b \div c = q, b \bmod c = r$ where $b = q \cdot c + r$ and $0 \leq r < c$
 (15.91) $b = c \cdot (b \div c) + b \bmod c$ for $c \neq 0$
 (15.92) **Definition of gcd:**
 $b \text{ gcd } c = (\uparrow d \mid d \mid b \wedge d \mid c : d)$ for b, c not both 0
 $0 \text{ gcd } 0 = 0$
 (15.94) **Definition of lcm :**
 $b \text{ lcm } c = (\downarrow k : \mathbb{Z}^+ \mid b \mid k \wedge c \mid k : k)$ for $b \neq 0$ and $c \neq 0$
 $b \text{ lcm } c = 0$ for $b = 0$ or $c = 0$

Properties of gcd.

- (15.96) **Symmetry:** $b \text{ gcd } c = c \text{ gcd } b$
 (15.97) **Associativity:** $(b \text{ gcd } c) \text{ gcd } d = b \text{ gcd } (c \text{ gcd } d)$
 (15.98) **Idempotency:** $(b \text{ gcd } b) = \text{abs}.b$
 (15.99) **Zero:** $1 \text{ gcd } b = 1$
 (15.100) **Identity:** $0 \text{ gcd } b = \text{abs}.b$
 (15.101) $b \text{ gcd } c = (\text{abs}.b) \text{ gcd } (\text{abs}.c)$
 (15.102) $b \text{ gcd } c = b \text{ gcd } (b+c) = b \text{ gcd } (b-c)$
 (15.103) $b = a \cdot c + d \Rightarrow b \text{ gcd } c = c \text{ gcd } d$
 (15.104) **Distributivity:** $d \cdot (b \text{ gcd } c) = (d \cdot b) \text{ gcd } (d \cdot c)$ for $0 \leq d$
 (15.105) **Definition of relatively prime \perp :** $b \perp c \equiv b \text{ gcd } c = 1$
 (15.107) **Inductive definition of gcd:**
 $b \text{ gcd } 0 = b$
 $b \text{ gcd } c = c \text{ gcd } (b \bmod c)$
 (15.108) $(\exists x, y : x \cdot b + y \cdot c = b \text{ gcd } c)$ for all $b, c : \mathbb{N}$
 (15.111) $k \mid b \wedge k \mid c \equiv k \mid (b \text{ gcd } c)$

Combinatorial Analysis

- (16.1) **Rule of sum:** The size of the union of n (finite) pairwise disjoint sets is the sum of their sizes.
- (16.2) **Rule of product:** The size of the cross product of n sets is the product of their sizes.
- (16.3) **Rule of difference:** The size of a set with a subset of it removed is the size of the set minus the size of the subset.
- (16.4) **Definition:** $P(n, r) = n!/(n-r)!$
- (16.5) The number of r -permutations of a set of size n equals $P(n, r)$.
- (16.6) The number of r -permutations with repetition of a set of size n is n^r .
- (16.7) The number of permutations of a bag of size n with k distinct elements occurring n_1, n_2, \dots, n_k times is $\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_k!}$.
- (16.9) **Definition:** The *binomial coefficient* $\binom{n}{r}$, which is read as “ n choose r ”, is defined by $\binom{n}{r} = \frac{n!}{r! \cdot (n-r)!}$ for $0 \leq r \leq n$.
- (16.10) The number of r -combinations of n elements is $\binom{n}{r}$.
- (16.11) The number $\binom{n}{r}$ of r -combinations of a set of size n equals the number of permutations of a bag that contains r copies of one object and $n-r$ copies of another.

A Theory of Graphs

- (19.1) **Definition:** Let V be a finite, nonempty set and E a binary relation on V . Then $G = \langle V, E \rangle$ is called a *directed graph*, or *digraph*. An element of V is called a *vertex*; an element of E is called an *edge*.
- (19.1.1) **Definitions:**
- (a) In an *undirected graph* $\langle V, E \rangle$, E is a set of *unordered* pairs.
 - (b) In a *multigraph* $\langle V, E \rangle$, E is a *bag* of undirected edges.
 - (c) The *indegree* of a vertex of a digraph is the number of edges for which it is an end vertex.
 - (d) The *outdegree* of a vertex of a digraph is the number of edges for which it is a start vertex.
 - (e) The *degree* of a vertex is the sum of its indegree and outdegree.
 - (f) An edge $\langle b, b \rangle$ for some vertex b is a *self-loop*.
 - (g) A digraph with no self-loops is called *loop-free*.
- (19.3) The sum of the degrees of the vertices of a digraph or multigraph equals $2 \cdot \#E$.
- (19.4) In a digraph or multigraph, the number of vertices of odd degree is even.

- (19.4.1) **Definition:** A *path* has the following properties.
- (a) A path starts with a vertex, ends with a vertex, and alternates between vertices and edges.
 - (b) Each directed edge in a path is preceded by its start vertex and followed by its end vertex. An undirected edge is preceded by one of its vertices and followed by the other.
 - (c) No edge appears more than once.
- (19.4.2) **Definitions:**
- (a) A *simple path* is a path in which no vertex appears more than once, except that the first and last vertices may be the same.
 - (b) A *cycle* is a path with at least one edge, and with the first and last vertices the same.
 - (c) An undirected multigraph is *connected* if there is a path between any two vertices.
 - (d) A digraph is *connected* if making its edges undirected results in a connected multigraph.
- (19.6) If a graph has a path from vertex b to vertex c , then it has a simple path from b to c .
- (19.6.1) **Definitions:**
- (a) An *Euler path* of a multigraph is a path that contains each edge of the graph exactly once.
 - (b) An *Euler circuit* is an Euler path whose first and last vertices are the same.
- (19.8) An undirected connected multigraph has an Euler circuit iff every vertex has even degree.
- (19.8.1) **Definitions:**
- (a) A *complete graph* with n vertices, denoted by K_n , is an undirected, loop-free graph in which there is an edge between every pair of distinct vertices.
 - (b) A *bipartite graph* is an undirected graph in which the set of vertices are partitioned into two sets X and Y such that each edge is incident on one vertex in X and one vertex in Y .
- (19.10) A path of a bipartite graph is of even length iff its ends are in the same partition element.
- (19.11) A connected graph is bipartite iff every cycle has even length.
- (19.11.1) **Definition:** A *complete bipartite graph* $K_{m,n}$ is a bipartite graph in which one partition element X has m vertices, the other partition element Y has n vertices, and there is an edge between each vertex of X and each vertex of Y .
- (19.11.2) **Definitions:**
- (a) A *Hamilton path* of a graph or digraph is a path that contains each vertex exactly once, except that the end vertices of the path may be the same.
 - (b) A *Hamilton circuit* is a Hamilton path that is a cycle.

Natural Science Division, Pepperdine University, Malibu, CA 90263

Email address: Stan.Warford@pepperdine.edu

URL: <https://www.cslab.pepperdine.edu/warford/>