Musa Al-hassy and Wolfram Kahl November 16, 2020

Reference Sheet for Discrete Maths

Propositional Calculus

Order of decreasing binding power: $=$, $\neg$, $\wedge/\vee$, $\Rightarrow/\Leftarrow$, $\equiv/\not\equiv$.

Equivales is the only equivalence relation that is associative $((p \equiv q) \equiv r) \quad \equiv \quad (p \equiv (q \equiv r))$, and it is symmetric and has identity true.

Discrepancy (difference) '$\not\equiv$' is symmetric, associative, has identity 'false', mutually associates with equivales $((p \not\equiv q) \equiv r) \quad \equiv \quad (p \not\equiv (q \equiv r))$, and mutually interchanges with it as well $(p \not\equiv q \equiv r) \quad \equiv \quad (p \equiv q \not\equiv r)$. Finally, negation commutes with difference: $\neg(p \equiv q) \equiv \neg p \equiv q$.

Implication has the alternative definition $p \Rightarrow q \;\equiv\; \neg p \vee q$, thus having true as both left identity and right zero; it distributes over $\equiv$ in the second argument, and is self-distributive; and has the properties:

Shunting $p \wedge q \Rightarrow r \;\equiv\; p \Rightarrow (q \Rightarrow r)$

Contrapositive $p \Rightarrow q \quad\equiv\quad \neg q \Rightarrow \neg p$

Leibniz $e = f \;\Rightarrow\; E[z \coloneqq e] = E[z := f]$

Modus Ponens

$$p \wedge (p \Rightarrow q) \quad \equiv \quad p \wedge q$$
$$p \wedge (q \Rightarrow p) \quad \equiv \quad p$$
$$p \wedge (p \Rightarrow q) \quad \Rightarrow \quad q$$

It is a *linear* order relation generated by '$\mathsf{false} \Rightarrow \mathsf{true}$'; whence "from false, follows anything": $\mathsf{false} \Rightarrow p$. Moreover it has the useful properties "(3.62) Contextualisation": $p \Rightarrow (q \equiv r) \quad\equiv\quad p \wedge q \quad\equiv\quad p \wedge r$ —we *have* the context p in each side of the equivalence— and $p \Rightarrow (q \Rightarrow r) \quad\equiv\quad p \wedge q \;\Rightarrow\; p \wedge r$. Implication is "Sub-associative": $((p \Rightarrow q) \Rightarrow r) \;\Rightarrow\; (p \Rightarrow (q \Rightarrow r))$. Finally, we have "$\equiv$-$\equiv$ Elimination": $(p \equiv q \equiv r) \Rightarrow s \;\equiv\; p \Rightarrow s \;\equiv\; q \Rightarrow s \;\equiv\; r \Rightarrow s$.

Conjunction and disjunction distribute over one another, are both associative and symmetric, $\vee$ has identity false and zero true whereas $\wedge$ has identity true and zero false, $\vee$ distributes over $\vee, \equiv, \wedge, \Rightarrow, \;\Leftarrow$ whereas $\wedge$ distributes over $\equiv - \equiv$ in that $p \wedge (q \equiv r \equiv s) \;\equiv\; p \wedge q \quad\equiv\quad p \wedge r \quad\equiv\quad p \wedge s$, and they satisfy,

Excluded Middle	**Contradiction**	**Absorption**	**De Morgan**
$p \vee \neg p$	$p \wedge \neg p \equiv \mathsf{false}$	$p \wedge (q \vee \neg p) \equiv p \wedge q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
		$p \vee (q \vee \neg p) \equiv p \vee q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$

Most importantly, they satisfy the **"Golden Rule"**: $p \wedge q \equiv p \equiv q \equiv p \vee q$.

The many other properties of these operations —such as weakening laws and other absorption laws and case-analysis ($\sqcup$-char)— can be found by looking at the list of *lattice properties* —since the Booleans are a lattice.

Orders

An *order* is a relation $\_ \sqsubseteq \_ \;:\; \tau \to \tau \to \mathbb{B}$ satisfying the following three properties:

Reflexivity	**Transitivity**	**Mutual Inclusion**
$a \sqsubseteq a$	$a \sqsubseteq b \wedge b \sqsubseteq c \Rightarrow a \sqsubseteq c$	$a \sqsubseteq b \wedge b \sqsubseteq a \;\equiv\; a = b$

Indirect Inclusion is like 'set inclusion' and Indirect Equality is like 'set extensionality'.

Indirect Equality (from above)
$x = y \;\equiv\; (\forall z \bullet x \sqsubseteq z \equiv y \sqsubseteq z)$

Indirect Inclusion (from above)
$x \sqsubseteq y \;\equiv\; (\forall z \bullet y \sqsubseteq z \Rightarrow x \sqsubseteq z)$

Indirect Equality (from below)
$x = y \;\equiv\; (\forall z \bullet z \sqsubseteq x \equiv z \sqsubseteq y)$

Indirect Inclusion (from below)
$x \sqsubseteq y \;\equiv\; (\forall z \bullet z \sqsubseteq x \Rightarrow z \sqsubseteq y)$

An order is *bounded* if there are elements $\top, \bot : \tau$ being the lower and upper bounds of all other elements:

Top Element	$a \sqsubseteq \top$	**Bottom Element**	$\bot \sqsubseteq a$
Top is maximal	$\top \sqsubseteq a \;\equiv\; a = \top$	**Bottom is minimal**	$a \sqsubseteq \bot \;\equiv\; a = \top$

Lattices

A *lattice* is a pair of operations $\_ \sqcap \_,\; \_ \sqcup \_ \;:\; \tau \to \tau \to \tau$ specified by the properties:

$\sqcup$-Characterisation
$a \sqsubseteq c \wedge b \sqsubseteq c \;\equiv\; a \sqcup b \;\sqsubseteq\; c$

$\sqcap$-Characterisation
$c \sqsubseteq a \wedge c \sqsubseteq b \;\equiv\; c \;\sqsubseteq\; a \sqcap b$

The operations act as providing the greatest lower bound, 'glb', 'supremum', or 'meet', by $\sqcap$; and the least upper bound, 'lub', 'infimum', or 'join', by $\sqcup$.

Let $\Box$ be one of $\sqcap$ or $\sqcup$, then:

Symmetry of $\Box$
$a \Box b \quad=\quad b \Box a$

Associativity of $\Box$
$(a \Box b) \Box c \quad=\quad a \Box (b \Box c)$

Idempotency of $\Box$
$a \Box a \quad=\quad a$

Zero of $\Box$
$a \sqcup \top = \top$
$a \sqcap \bot = \bot$

Identity of $\Box$
$a \sqcup \bot = a$
$a \sqcap \top = a$

Absorption
$a \sqcap (b \sqcup a) = a$
$a \sqcup (b \sqcap a) = a$

Self-Distributivity of $\Box$
$a \Box (b \Box c) \;=\; (a \Box b) \Box (a \Box c)$

Weakening / Strengthening
$a \;\sqsubseteq\; a \sqcup b$
$a \sqcap b \;\sqsubseteq\; a$
$a \sqcap b \;\sqsubseteq\; a \sqcup b$

Induced Defs. of Inclusion
$a \sqsubseteq b \;\equiv\; a \sqcup b \quad=\quad b$
$a \sqsubseteq b \;\equiv\; a \sqcap b \quad=\quad a$

Monotonicity of $\Box$
$a \sqsubseteq b \wedge c \sqsubseteq d \;\Rightarrow\; a \Box c \;\sqsubseteq\; b \Box d$

Golden Rule
$a \sqcap b \;=\; a \quad\equiv\quad b = a \sqcup b$
$a \sqcap b \;=\; a \sqcup b \quad\equiv\quad a = b$
$a \sqcup b \;\sqsubseteq\; a \sqcap b \quad\equiv\quad a = b$

Duality Principle:

If a statement S is a theorem, then so is $S[(\sqsubseteq, \sqcap, \sqcup, \top, \bot) := (\sqsupseteq, \sqcup, \sqcap, \bot, \top)]$.

Conditionals

"If to ∧" may be taken as axiom from which we may prove the remaining 'alternative definitions' "if to ⋯".

if to ∧	$P[z \coloneqq \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi}]$	$\equiv$	$(b$	$\Rightarrow$	$P[z \coloneqq x])$	$\wedge$	$(\neg b$	$\Rightarrow$	$P[z := x])$
if to ∨	$P[z \coloneqq \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi}]$	$\equiv$	$(b$	$\wedge$	$P[z \coloneqq x])$	$\vee$	$(\neg b$	$\wedge$	$P[z := x])$
if to ≢	$P[z \coloneqq \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi}]$	$\equiv$	b	$\wedge$	$P[z \coloneqq x]$	$\not\equiv$	$\neg b$	$\wedge$	$P[z := x]$
if to ≡	$P[z \coloneqq \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi}]$	$\equiv$	b	$\Rightarrow$	$P[z \coloneqq x]$	$\equiv$	$\neg b$	$\Rightarrow$	$P[z := x]$

Note that the "≡" and "≢" rules can be parsed in multiple ways since '≡' is associative, and '≡' mutually associates with '≢'.

if true	$\textsf{if true then } x \textsf{ else } y \textsf{ fi} = x$
if false	$\textsf{if false then } x \textsf{ else } y \textsf{ fi} = y$
then true	$\textsf{if } R \textsf{ then true else } P \textsf{ fi} = R \vee P$
then false	$\textsf{if } R \textsf{ then false else } P \textsf{ fi} = \neg R \wedge P$
else true	$\textsf{if } R \textsf{ then } P \textsf{ else true fi} = R \Rightarrow P$
else false	$\textsf{if } R \textsf{ then } P \textsf{ else false fi} = R \wedge P$

if swap $\quad \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi} = \textsf{if } \neg b \textsf{ then } y \textsf{ else } x \textsf{ fi}$

if idempotency $\quad \textsf{if } b \textsf{ then } x \textsf{ else } x \textsf{ fi} = x$

if guard strengthening $\quad \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi} = \textsf{if } b \wedge x \neq y \textsf{ then } x \textsf{ else } y \textsf{ fi}$

if Context $\quad \textsf{if } b \textsf{ then } E \textsf{ else } F \textsf{ fi} = \textsf{if } b \textsf{ then } E[b \coloneqq \textsf{true}] \textsf{ else } F[b \coloneqq \textsf{false}] \textsf{ fi}$

if Distributivity $\quad P[z \coloneqq \textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi}] = \textsf{if } b \textsf{ then } P[z \coloneqq x] \textsf{ else } P[z \coloneqq y] \textsf{ fi}$

if junctivity
$$\big(\textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi}\big) \oplus \big(\textsf{if } b \textsf{ then } x' \textsf{ else } y' \textsf{ fi}\big)$$
$$= \textsf{if } b \textsf{ then } (x \oplus x') \textsf{ else } (y \oplus y') \textsf{ fi}$$

Quantification

Let $\_\oplus\_$ be an associative and symmetric operation with identity $\textsf{Id}$.

Abbreviation	$(\oplus x \bullet P) = (\oplus x \mid \textsf{true} \bullet P)$
Empty range	$(\oplus x \mid \textsf{false} \bullet P) = \textsf{Id}$
One-point rule	$(\oplus x \mid x = E \bullet P) = P[x \coloneqq E]$
Distributivity	$(\oplus x \mid R \bullet P \oplus Q) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid R \bullet Q)$
Nesting	$(\oplus x, y \mid X \wedge Y \bullet P) = (\oplus x \mid X \bullet (\oplus y \mid Y \bullet P))$
Dummy renaming	$(\oplus x \mid R \bullet P) = (\oplus y \mid R[x \coloneqq y] \bullet P[x \coloneqq y])$

Disjoint Range split $\quad (\oplus x \mid R \vee S \bullet P) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$
provided $R \wedge S \equiv \textsf{false}$

Range split
$$(\oplus x \mid R \vee S \bullet P) \oplus (\oplus x \mid R \wedge S \bullet P)$$
$$= (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$$

Idempotent Range split $\quad (\oplus x \mid R \vee S \bullet P) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$
provided $\oplus$ is idempotent

Set Theory

The set theoretic symbols $\in$, $=$, $\subseteq$, are defined as follows.

Axiom, Set Membership: $F \in \{x \mid R \bullet E\} \quad \equiv \quad (\exists x \mid R \bullet F = E)$

Axiom, Extensionality: $S = T \quad \equiv \quad (\forall x \bullet x \in S \equiv x \in T)$

Axiom, Subset: $S \subseteq T \quad \equiv \quad (\forall x \bullet x \in S \Rightarrow x \in T)$

As witnessed by the following definitions, it is the $\in$ relation that *translates set theory to propositional logic.*

Universe	$x \in \mathbf{U}$	$\equiv$	$true$
Empty set	$x \in \emptyset$	$\equiv$	$false$
Union	$x \in S \cup T$	$\equiv$	$x \in S \vee x \in T$
Intersection	$x \in S \cap T$	$\equiv$	$x \in S \wedge x \in T$
Complement	$x \in \sim S$	$\equiv$	$x \notin S$
Difference	$x \in S - T$	$\equiv$	$x \in S \wedge x \notin T$
Power set	$S \in \mathbb{P}T$	$\equiv$	$S \subseteq T$

The pairs $\emptyset$/false, $\mathbf{U}$/true, $\cup/\vee$, $\cap/\wedge$, $\subseteq/\Rightarrow$, $\tilde{}/\neg$ are related by $\in$ and so all equational theorems of propositional logic also hold for set theory —indeed, that is because both are Boolean algebras.
→ Set difference is a residual wrt $\cup$, and so satisfies the division properties below.
→ Subset is an order and so satisfies the aforementioned order properties. It is bounded below by $\emptyset$ and above by $\mathbf{U}$.

The relationship between set comprehension and quantifier notation is:

Set comprehension as union $\quad \{x \mid R \bullet P\} \quad = \quad (\cup x \mid R \bullet \{P\})$

Combinatorics

Axiom, Size: $\quad \#S = (\Sigma x \mid x \in S \bullet 1)$
Axiom, Interval: $\quad m..n = \{x : \mathbb{Z} \mid m \leq x \leq n\}$

The following theorems serve to define '#' for the usual set theory operators.

Positive definite	$\#S \subseteq 0 \quad \equiv \quad S = \emptyset$
Power set size	$\#\mathbb{P}S = 2^{\#S}$
Principle of Inclusion-Exclusion	$\#(S \cup T) = \#S + \#T - \#(S \cap T)$
Monotonicity	$S \subseteq T \Rightarrow \#S \leq \#T$
Difference rule	$S \subseteq T \Rightarrow \#(T - S) = \#T - \#S$
Complement size	$\#(\sim S) = \#\mathbf{U} - \#S$
Range size	$(\Sigma x : \mathbf{U} \mid x \notin S \bullet 1) = \#\mathbf{U} - \#S$
Interval size	$\#(m..n) = n - m + 1 \text{ for } m \leq n$
Pigeonhole Principle	$(\Sigma i : 1..n \bullet E)/n \leq (\uparrow i : 1..n \bullet E)$
(*"min ≤ avg ≤ max"*)	$(\downarrow i : 1..n \bullet E) \leq (\Sigma i : 1..n \bullet E)/n$

Rule of sum: $\#(\cup i \mid R\,i \bullet P) = (\Sigma i \mid R\,i \bullet \#P)$
provided the range is pairwise disjoint: $\forall i, j \bullet R\,i \wedge R\,j \equiv i = j$.

Rule of product: $\#(\times i \mid R\,i \bullet P) = (\Pi i \mid R\,i \bullet \#P)$

Residuals, Division

Suppose we have an associative operation $\_ ; \_$ with identity Id and two operations "under \" and "over /" specified as follows.

Characterisation of /	**Characterisation of **
$a ; b \sqsubseteq c \quad\equiv\quad a \sqsubseteq c/b$	$a ; b \sqsubseteq c \quad\equiv\quad b \sqsubseteq a\backslash c$

Cancellation	$(a/b) ; b \sqsubseteq a$	$a ; (a\backslash b) \sqsubseteq b$
Dividing a division	$(a/b)/c \;=\; a/(c ; b)$	$a\backslash(b\backslash c) \;=\; (b ; a)\backslash c$
Division of multiples	$a \sqsubseteq (a ; b)/b$	$b \sqsubseteq a\backslash(a ; b)$

Monotonicity of ; $\quad a \sqsubseteq a' \wedge b \sqsubseteq b' \Rightarrow a ; b \sqsubseteq a' ; b'$

Numerator monotonicity	$b \sqsubseteq b' \Rightarrow a\backslash b \sqsubseteq a\backslash b'$	$b \sqsubseteq b' \Rightarrow b/a \sqsubseteq b'/a$
Denominator antitonicity	$a' \sqsubseteq a \Rightarrow a\backslash b \sqsubseteq a'\backslash b$	$a' \sqsubseteq a \Rightarrow b/a \sqsubseteq b/a'$
Self-reflexivity	$\mathsf{Id} \sqsubseteq a\backslash a$	$\mathsf{Id} \sqsubseteq a/a$
Denominator Identity	$\mathsf{Id}\backslash a = a$	$a/\mathsf{Id} = a$
Numerator Zero	$a\backslash \top = \top$	$\top/a = \top$
Wraparound rule	$\bot\backslash a = \top$	$a/\bot = \top$

Exact division:

$$(\exists z \bullet y = x ; z) \quad\equiv\quad x ; (x\backslash y) = y$$
$$(\exists z \bullet y = x\backslash z) \quad\equiv\quad x\backslash(x ; y) = y$$

Converse

Axioms,

Co-distributivity	**$\smile\smile$, Involutive**	**Monotonicity**
$(x ; y)^\smile = y^\smile ; x$	$x^{\smile\smile} = x$	$x \sqsubseteq y \Rightarrow x^\smile \sqsubseteq y^\smile$

Theorems,

Identity	**Connection**	**Elimination**
$\mathsf{Id}^\smile = \mathsf{Id}$	$a^\smile \sqsubseteq b \;\equiv\; a \sqsubseteq b^\smile$	$x^\smile = y^\smile \;\equiv\; x = y$

Named Properties

univalent	x	$\equiv$	$x^\smile ; x \sqsubseteq \mathsf{Id}$	injective	x	$\equiv$	$x ; x^\smile \sqsubseteq \mathsf{Id}$
total	x	$\equiv$	$\mathsf{Id} \sqsubseteq x ; x^\smile$	surjective	x	$\equiv$	$\mathsf{Id} \sqsubseteq x^\smile ; x$
mapping	x	$\equiv$	total x $\wedge$ univalent x	bijective	x	$\equiv$	surjective x $\wedge$ injective x
iso	x	$\equiv$	mapping x $\wedge$ bijective x				

Duality theorems

univalent	$(x^\smile)$	$\equiv$	injective x
total	$(x^\smile)$	$\equiv$	surjective x
mapping	$(x^\smile)$	$\equiv$	bijective x
iso	$(x^\smile)$	$\equiv$	iso x

Invertiblility theorems

total x $\wedge$ injective $x \Rightarrow x ; x^\smile = \mathsf{Id}$

iso $x \quad\equiv\quad x ; x^\smile = \mathsf{Id} \;\wedge\; x^\smile ; x = \mathsf{Id}$

iso $x \quad\Rightarrow\quad (\exists g \bullet x ; g = \mathsf{Id} = g ; x)$

Shunting laws:

univalent f	$\Rightarrow$	$(x ; f \sqsubseteq y \;\Leftarrow\; x \sqsubseteq y ; f^\smile)$
total f	$\Rightarrow$	$(x ; f \sqsubseteq y \;\Rightarrow\; x \sqsubseteq y ; f^\smile)$
mapping f	$\Rightarrow$	$(x ; f \sqsubseteq y \;\equiv\; x \sqsubseteq y ; f^\smile)$