Musa Al-hassy and Wolfram Kahl

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 $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$, and it is symmetric and has identity true.

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

	Modus Ponens		
Shunting $p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$	$p \wedge (p \Rightarrow q)$	$\equiv$	$p \wedge q$
Contrapositive $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$	$p \wedge (q \Rightarrow p)$	$\equiv$	p
Leibniz $e = f \Rightarrow E[z := e] = E[z := f]$	$p \wedge (p \Rightarrow q)$	$\Rightarrow$	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": $p \Rightarrow (q \equiv r) \equiv p \wedge q \equiv p \wedge r$ —we *have* the context p in each side of the equivalence— and $p \Rightarrow (q \Rightarrow r) \equiv p \wedge q \Rightarrow p \wedge r$. 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 $p \wedge (q \equiv r \equiv s) \equiv p \wedge q \equiv p \wedge r \equiv p \wedge s$, 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)	**Indirect Inclusion (from above)**
$x = y \equiv (\forall z \bullet x \sqsubseteq z \equiv y \sqsubseteq z)$	$x \sqsubseteq y \equiv (\forall z \bullet y \sqsubseteq z \Rightarrow x \sqsubseteq z)$
Indirect Equality (from below)	**Indirect Inclusion (from below)**
$x = y \equiv (\forall z \bullet z \sqsubseteq x \equiv z \sqsubseteq y)$	$x \sqsubseteq y \equiv (\forall z \bullet z \sqsubseteq x \Rightarrow z \sqsubseteq y)$

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**	$\sqcap$-**Characterisation**
$a \sqsubseteq c \wedge b \sqsubseteq c \equiv a \sqcup b \sqsubseteq c$	$c \sqsubseteq a \wedge c \sqsubseteq b \equiv c \sqsubseteq a \sqcap b$

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 $\square$ be one of $\sqcap$ or $\sqcup$, then:

Symmetry of $\square$	**Associativity of** $\square$	**Idempotency of** $\square$
$a \square b = b \square a$	$(a \square b) \square c = a \square (b \square c)$	$a \square a = a$

Zero of $\square$	**Identity of** $\square$	**Absorption**	**Self-Distributivity of** $\square$
$a \sqcup \top = \top$	$a \sqcup \bot = a$	$a \sqcap (b \sqcup a) = a$	$a \square (b \sqcup c) = (a \square b) \square (a \square c)$
$a \sqcap \bot = \bot$	$a \sqcap \top = a$	$a \sqcup (b \sqcap a) = a$	

Weakening / Strengthening	**Induced Defs. of Inclusion**			**Golden Rule**		
$a \sqsubseteq a \sqcup b$	$a \sqsubseteq b \equiv a \sqcup b$	$=$	b	$a \sqcap b = a$	$\equiv$	$b = a \sqcup b$
$a \sqcap b \sqsubseteq a$	$a \sqsubseteq b \equiv a \sqcap b$	$=$	a	$a \sqcap b = a \sqcup b$	$\equiv$	$a = b$
$a \sqcap b \sqsubseteq a \sqcup b$	**Monotonicity of** $\square$			$a \sqcup b \sqsubseteq a \sqcap b$	$\equiv$	$a = b$
	$a \sqsubseteq b \wedge c \sqsubseteq d \Rightarrow a \square c \sqsubseteq b \square d$					

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 $\cdots$".

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

Note that the "$\equiv$" and "$\not\equiv$" rules can be parsed in multiple ways since '$\equiv$' is associative, and '$\equiv$' mutually associates with '$\not\equiv$'.

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

if swap	if b then x else y fi $=$ if $\neg b$ then y else x fi
if idempotency	if b then x else x fi $= x$
if guard strengthening	if b then x else y fi $=$ if $b \wedge x \neq y$ then x else y fi
if Context	if b then E else F fi $=$ if b then $E[b := \text{true}]$ else $F[b := \text{false}]$ fi
if Distributivity	$P[z := \text{if } b \text{ then } x \text{ else } y \text{ fi}] =$ if b then $P[z := x]$ else $P[z := y]$ fi
if junctivity	$\big(\text{if } b \text{ then } x \text{ else } y \text{ fi}\big) \oplus \big(\text{if } b \text{ then } x' \text{ else } y' \text{ fi}\big)$ $= \text{if } b \text{ then } (x \oplus x') \text{ else } (y \oplus y') \text{ fi}$

Converse

Axioms,

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

Theorems,

Connection	$a^{\smile} \sqsubseteq b \equiv a \sqsubseteq b^{\smile}$
Elimination	$x^{\smile} = y^{\smile} \equiv x = y$

Named Properties

univalent	x	$\equiv$	$x^{\smile} \,\fatsemi\, x \sqsubseteq \mathsf{Id}$	injective	x	$\equiv$	$x \,\fatsemi\, x^{\smile} \sqsubseteq \mathsf{Id}$
total	x	$\equiv$	$\mathsf{Id} \sqsubseteq x \,\fatsemi\, x^{\smile}$	surjective	x	$\equiv$	$\mathsf{Id} \sqsubseteq x^{\smile} \,\fatsemi\, x$
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 $x \Rightarrow x \,\fatsemi\, x^{\smile} = \mathsf{Id}$

iso $x \equiv x \,\fatsemi\, x^{\smile} = \mathsf{Id} \wedge x^{\smile} \,\fatsemi\, x = \mathsf{Id}$

iso $x \Rightarrow (\exists g \bullet x \,\fatsemi\, g = \mathsf{Id} = g \,\fatsemi\, x)$

Division

Characterisation of $/$: $\quad a \,\fatsemi\, b \sqsubseteq c \quad \equiv \quad a \sqsubseteq c/b$

Characterisation of $\backslash$: $\quad a \,\fatsemi\, b \sqsubseteq c \quad \equiv \quad b \sqsubseteq a \backslash c$

Exact division:

$(\exists z \bullet y = x \,\fatsemi\, z)$	$\equiv$	$x \,\fatsemi\, (x \backslash y) = y$
$(\exists z \bullet y = x \backslash z)$	$\equiv$	$x \backslash (x \,\fatsemi\, y) = y$

Shunting laws:

univalent f	$\Rightarrow$	$(x \,\fatsemi\, f \sqsubseteq y \Leftarrow x \sqsubseteq y \,\fatsemi\, f^{\smile})$
total f	$\Rightarrow$	$(x \,\fatsemi\, f \sqsubseteq y \Rightarrow x \sqsubseteq y \,\fatsemi\, f^{\smile})$
mapping f	$\Rightarrow$	$(x \,\fatsemi\, f \sqsubseteq y \equiv x \sqsubseteq y \,\fatsemi\, f^{\smile})$