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

$$
\begin{aligned}
p \wedge (p \Rightarrow q) &\quad\equiv\quad p \wedge q \\
p \wedge (q \Rightarrow p) &\quad\equiv\quad p \\
p \wedge (p \Rightarrow q) &\quad\Rightarrow\quad q
\end{aligned}
$$

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 $\square$ 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 $\square$
$a \sqcup \top = \top$	$a \sqcup \bot = a$	$a \sqcap (b \sqcup a) = a$	$a \square (b \square c) \ = \ (a \square b) \square (a \square c)$
$a \sqcap \bot = \bot$	$a \sqcap \top = a$	$a \sqcup (b \sqcap a) = a$	

Weakening / Strengthening

$a \ \sqsubseteq\ a \sqcup b$

$a \sqcap b \ \sqsubseteq\ a$

$a \sqcap b \ \sqsubseteq\ a \sqcup b$

Induced Defs. of Inclusion

$a \sqsubseteq b \ \equiv\ a \sqcup b \ = \ b$

$a \sqsubseteq b \ \equiv\ a \sqcap b \ = \ a$

Monotonicity of $\square$

$a \sqsubseteq b \wedge c \sqsubseteq d \ \Rightarrow\ a \square c \ \sqsubseteq\ b \square d$

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 $\wedge$" may be taken as axiom from which we may prove the remaining 'alternative definitions' "if to $\cdots$".

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

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	$\textsf{if } b \textsf{ then } x \textsf{ else } y \textsf{ fi} \;=\; \textsf{if } \neg b \textsf{ then } y \textsf{ else } x \textsf{ fi}$
if idempotency	$\textsf{if } b \textsf{ then } x \textsf{ else } x \textsf{ fi} \;=\; x$

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

Set Theory

Axiom (11.3) "Set membership":
$F \in \{\, x \mid R \bullet E \,\} \equiv (\exists\, x \mid R \bullet F = E)$

Theorem (11.7) "Simple Membership":
$e \in \{\, x \mid P \,\} \equiv P[x \coloneqq e]$

Theorem (11.6) "Mathematical formulation of set comprehension":
$\{x \mid P \bullet E\,\} = \{\, y \mid (\exists\, x \mid P \bullet y = E)\,\}$

Theorem (11.9) "Simple set comprehension equality":
$\{x \mid Q\} = \{x \mid R\} \equiv (\forall\, x \bullet Q \equiv R)$

Axiom (11.13) "Subset" "Definition of $\subseteq$" "Set inclusion":
$S \subseteq T \equiv (\forall\, e \mid e \in S \bullet e \in T)$

More coming soon!