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

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 'false $\Rightarrow$ true'; whence "from false, follows anything": 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
$p \vee \neg p$	$p \wedge \neg p \equiv$ 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 $S[(\sqsubseteq, \sqcap, \sqcup, \top, \bot) \coloneqq (\sqsupseteq, \sqcup, \sqcap, \bot, \top)]$.

Conditionals

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

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

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

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

Quantification

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

Abbreviation	$(\oplus x \bullet P) = (\oplus x \mid \mathsf{true} \bullet P)$
Empty range	$(\oplus x \mid \mathsf{false} \bullet P) = \mathsf{Id}$
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	$(\oplus x \mid R \vee S \bullet P) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$ *provided* $R \wedge S \equiv \mathsf{false}$
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	$(\oplus x \mid R \vee S \bullet P) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$ *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	$x \in \emptyset$	$\equiv$	$false$
Complement	$x \in {\sim}S$	$\equiv$	$x \notin S$
Union	$x \in S \cup T$	$\equiv$	$x \in S \vee x \in T$
Intersection	$x \in S \cap T$	$\equiv$	$x \in S \wedge x \in T$
PseudoComplement	$x \in S \to T$	$\equiv$	$x \in S \Rightarrow x \in T$
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, $\cup|\vee$, $\cap|\wedge$, $\subseteq|\Rightarrow$, ${\sim}|\neg$ 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.
$\rightarrow$ Set difference is a residual wrt $\cup$, and so satisfies the division properties below.
$\rightarrow$ 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	$\{x \mid R \bullet P\} \quad = \quad (\cup x \mid R \bullet \{P\})$
Membership as inclusion	$x \in S \quad \equiv \quad \{x\} \subseteq S$
Equality as membership	$x = y \quad \equiv \quad x \in \{y\}$

Combinatorics

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

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	$\#(m..n) = n - m + 1$ 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 $\_ \fatsemi \_$ with identity Id and two operations "under \" and "over /" specified as follows.

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

When $\fatsemi$ is symmetric, as in the special cases $\fatsemi = \sqcap$, the divisions coincide: $x/y \;=\; y\backslash x$.

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

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

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:

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

Division for the special case $\fatsemi = \sqcap$ is known *the relative pseudo-complement*: Denoted $x \rightarrow y$ ("*x implies y*"), it is *the largest piece 'outside' of x that is still included in y*. The relative pseudocomplement *internalises inclusion*, $z \sqsubseteq (x \rightarrow y) \;\Rightarrow\; (z \sqsubseteq x \Rightarrow z \sqsubseteq y)$; more generally: $x \sqsubseteq y \;\equiv\; \mathsf{Id} \sqsubseteq x\backslash y$.

Pseudo-complement	Semi-complement
$x \sqcap a \sqsubseteq b \;\equiv\; x \sqsubseteq a \rightarrow b$	$a - b \sqsubseteq x \;\equiv\; a \sqsubseteq b \sqcup x$

Strong modus ponens	Absorption
$a \sqcap (a \rightarrow b) \;=\; a \sqcap b$	$(x \sqcup b) - b \;=\; x - b$
$a \rightarrow (x \sqcap a) \;=\; a \rightarrow x$	$(a - b) \sqcup b \;=\; a \sqcup b$

Division for the special case $\fatsemi = \sqcup$ in the *dual order* ($\sqsupseteq$) is known as *the difference* or *relative semi-complement*: Denoted $x - y$ ("*x without y*"), it is *the smallest piece that along with y 'covers' x*; i.e., it is the least value that 'complements' ("fill up together") y to include x. (Possibly for this reason, set difference is sometimes denoted $S\backslash T$ in other books!)

Converse —an over-approximation of inverse (A4)

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

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

Named Properties

reflexive	x	$\equiv$	$\mathsf{Id} \sqsubseteq x$	symmetric	x	$\equiv$	$x^\smile = x$
irreflexive	x	$\equiv$	$\mathsf{Id} \sqcap x = \bot$	antisymmetric	x	$\equiv$	$x \sqcap x^\smile \sqsubseteq \mathsf{Id}$
transitive	x	$\equiv$	$x \fatsemi x \sqsubseteq x$	asymmetric	x	$\equiv$	$x \sqcap x^\smile = \bot$
idempotent	x	$\equiv$	$x \fatsemi x = x$				

The above properties are preserved by converse: Let P be any of the above properties, then $P\,x \;\equiv\; P(x^\smile)$.

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			**Invertiblility theorems**
univalent $(x^\smile)$	$\equiv$	injective x	total $x \wedge$ injective $x \Rightarrow x \fatsemi x^\smile = \mathsf{Id}$
total $(x^\smile)$	$\equiv$	surjective x	iso $x \;\equiv\; x \fatsemi x^\smile = \mathsf{Id} \;\wedge\; x^\smile \fatsemi x = \mathsf{Id}$
mapping $(x^\smile)$	$\equiv$	bijective x	iso $x \;\Rightarrow\; (\exists g \bullet x \fatsemi g = \mathsf{Id} = g \fatsemi x)$
iso $(x^\smile)$	$\equiv$	iso x	

Shunting laws:

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

Relations

Relations are sets of pairs ...

Tortoise	$x \,(\, R \,)\, y$	$\equiv$	$\langle x, y\rangle \in R$
Extensionality	$R = S$	$\equiv$	$(\forall\, x, y \;\bullet\; x \,(\, R \,)\, y \equiv x \,(\, S \,)\, y)$
Inclusion	$R \subseteq S$	$\equiv$	$(\forall\, x, y \;\bullet\; x \,(\, R \,)\, y \Rightarrow x \,(\, S \,)\, y)$
Empty	$u \,(\, \emptyset \,)\, v$	$\equiv$	false
Universe	$u \,(\, A \times B \,)\, v$	$\equiv$	$u \in A \;\wedge\; v \in B$
Complement	$u \,(\, \sim S \,)\, v$	$\equiv$	$\neg(u \,(\, S \,)\, v)$
Union	$u \,(\, S \cup T \,)\, v$	$\equiv$	$u \,(\, S \,)\, v \;\vee\; u \,(\, T \,)\, v$
Intersection	$u \,(\, S \cap T \,)\, v$	$\equiv$	$u \,(\, S \,)\, v \;\wedge\; u \,(\, T \,)\, v$
Difference	$u \,(\, S - T \,)\, v$	$\equiv$	$u \,(\, S \,)\, v \;\wedge\; \neg(u \,(\, T \,)\, v)$
PseudoComplement	$u \,(\, S \rightarrow T \,)\, v$	$\equiv$	$u \,(\, S \,)\, v \;\Rightarrow\; u \,(\, T \,)\, v$
An Identity	$u \,(\, \mathbb{I}\, A \,)\, v$	$\equiv$	$u = v \in A$
The Identity	$u \,(\, \mathsf{Id} \,)\, v$	$\equiv$	$u = v$
Converse	$u \,(\, R^\smile \,)\, v$	$\equiv$	$v \,(\, R \,)\, u$
Composition	$u \,(\, R \fatsemi S \,)\, v$	$\equiv$	$(\exists\, x \;\bullet\; u \,(\, R \,)\, x \;\wedge\; x \,(\, S \,)\, v)$
Over Division	$u \,(\, S/R \,)\, v$	$\equiv$	$(\forall\, x \;\bullet\; v \,(\, R \,)\, x \;\Rightarrow\; u \,(\, S \,)\, x)$
Under Division	$u \,(\, R\backslash S \,)\, v$	$\equiv$	$(\forall\, x \;\bullet\; x \,(\, R \,)\, u \;\Rightarrow\; x \,(\, S \,)\, v)$

"Residuals arise from negating compositions": By comparing symbol-by-symbol in the RHS of '$\fatsemi$' and '/', it is not difficult to see that $S/R \;=\; \sim(R \fatsemi \sim S^\smile)^\smile \;=\; \sim(\sim S \fatsemi R^\smile)$ —note $(\sim T)^\smile \;=\; \sim(T^\smile)$.

Example: Define $x \,(\, \mathsf{E} \,)\, X \;\equiv\; x \in X$, then $A \,(\, \mathsf{E}\backslash\mathsf{E} \,)\, B \;\equiv\; A \subseteq B$.

Interpreting Named Properties

We will interpret the named properties using

- Relations: Formulae on sets of pairs; “ $\forall x \bullet \ldots$ ”
- Graphs: Dots and lines on a page
- Matrices: 1s and 0s on a grid
- Programs: Transformations of inputs to outputs

Properties of a relationship flavour

reflexive $R \equiv (\forall\, b \bullet b \llparenthesis R \rrparenthesis b)$
Every node in a graph has a ‘loop’, a line to itself
(Thus, paths can always be increased in length: $R \subseteq R \fatsemi R$)
The diagonal of a matrix is all 1s

irreflexive $R \equiv (\forall\, b \bullet \neg(b \llparenthesis R \rrparenthesis b))$
No node in a graph has a loop
The diagonal of a matrix is all 0s

symmetric $R \equiv (\forall\, b, c \bullet b \llparenthesis R \rrparenthesis c \equiv c \llparenthesis R \rrparenthesis b)$
The graph is undirected; we have a symmetric matrix

antisymmetric $R \equiv (\forall\, b, c \bullet b \llparenthesis R \rrparenthesis c \land c \llparenthesis R \rrparenthesis b \Rightarrow b = c)$
Mutually related nodes are necessarily self-loops
“Mutually related items are necessarily indistinguishable”

asymmetric $R \equiv (\forall\, b, c \bullet b \llparenthesis R \rrparenthesis c \Rightarrow \neg(c \llparenthesis R \rrparenthesis b))$
At most 1 edge (regardless of direction) relating any 2 nodes

transitive $R \equiv (\forall b, c, d \bullet b \llparenthesis R \rrparenthesis c \llparenthesis R \rrparenthesis d \Rightarrow b \llparenthesis R \rrparenthesis d)$
Paths can always be shortened (but nonempty)

idempotent $R \equiv$ Lengths of paths can be changed arbitrarily (nonzero)

Intuitively, by considering the interpretations only, we find

$$\mathsf{reflexive}\, R \land \mathsf{transitive}\, R \Rightarrow \mathsf{idempotent}\, R$$

Super cool stuff!

“Relations are simple graphs”

Relations directly represent *simple graphs*: Dots (*nodes*) and at most 1 line (*edge*) between any two. E.g., cities and highways (ignoring multiple highways).

Treating R as a graph:

R	A bunch of dots on a page and an arrow from x to y when $x \llparenthesis R \rrparenthesis y$
$R^{\smile}$	Flip the arrows in the graph
$\mathsf{Dom}\, R$	The nodes that have an outgoing edge
$\mathsf{Ran}\, R$	The nodes that have an incoming edge
$x \llparenthesis R \rrparenthesis y$	A path of length 1 (an edge) from x to y
$x \llparenthesis R \fatsemi R \rrparenthesis y$	A path of length 2 from x to y
$R \cup R^{\smile}$	The associated undirected graph (“symmetric closure”)

Properties of an operational flavour

univalent $R \equiv (\forall b, c, c' \bullet b \llparenthesis R \rrparenthesis c \land b \llparenthesis R \rrparenthesis c' \Rightarrow c = c')$ —aka “partial function”
Graph: Every node has at most one outgoing edge
Matrix: Every row has at most one 1
Prog: The program is deterministic, same-input yields same-output

injective $R \equiv (\forall b, b', c \bullet b \llparenthesis R \rrparenthesis c \land b' \llparenthesis R \rrparenthesis c \Rightarrow b = b')$
Graph: Every node has at most one incoming edge
Matrix: Every column has at most one 1
Prog: The program preserves distinctness (by contraposition)

total $R \equiv (\forall b \bullet \exists c \bullet b \llparenthesis R \rrparenthesis c)$
Graph: Every node has at least one outgoing edge
Matrix: Every row has at least one 1
Prog: The program terminates; has at least one output for each input

surjective $R \equiv (\forall c \bullet \exists b \bullet b \llparenthesis R \rrparenthesis c)$
Graph: Every node has at least one incoming edge
Matrix: Every column has at least one 1
Prog: All possible outputs arise from some input

mapping $R \equiv \mathsf{total}\, R \land \mathsf{univalent}\, R$ —also known as a “(total) function”
Graph: Every node has exactly one outgoing edge
Matrix: Every row has exactly one 1
Prog: The program always terminates with a unique output

bijective $R \equiv \mathsf{surjective}\, R \land \mathsf{injective}\, R$
Graph: Every node has exactly one incoming edge
Matrix: Every column has exactly one 1
Prog: Every output arises from a unique input

iso $R \equiv \mathsf{mapping}\, R \land \mathsf{bijective}\, R$
Graph: It’s a bunch of ‘circles’
Matrix: It’s a permutation; a re-arrangement of the identity matrix
Prog: A non-lossy protocol associating inputs to outputs