

Reference Sheet for Discrete Maths

Propositional Calculus

Order of decreasing binding power: $=, \neg, \wedge, \vee, \Rightarrow, \Leftarrow, \equiv, \neq$.

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) ' \neq ' is symmetric, associative, has identity '**false**', mutually associates with equivales $((p \neq q) \equiv r) \equiv (p \neq (q \equiv r))$, and mutually interchanges with it as well $(p \neq q \equiv r) \equiv (p \equiv q \neq r)$. 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 $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

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

Modus Ponens

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

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": $p \Rightarrow (q \equiv r) \equiv p \wedge q \equiv p \wedge r$ —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 -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

$$p \vee \neg p$$

Contradiction

$$p \wedge \neg p \equiv \text{false}$$

Absorption

$$p \wedge (q \vee \neg p) \equiv p \wedge q$$

$$p \vee (q \vee \neg p) \equiv p \vee q$$

De Morgan

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

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

Max \uparrow and Min \downarrow each distribute over the other, addition distributes over both, subtraction acts like De Morgans, the operators are selective, and non-negative multiplication distributes over both. (*Tropical mathematics* is math with ' $\uparrow, +$ ' instead of ' $+, \times$ '.)

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 *both* the Booleans $(\Rightarrow, \wedge, \vee)$ and numbers $(\leq, \downarrow, \uparrow)$ are lattices.

Orders

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

Reflexivity

$$a \sqsubseteq a$$

Transitivity

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

Mutual Inclusion

$$a \sqsubseteq b \wedge b \sqsubseteq a \equiv a = b$$

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 $\top, \perp : \tau$ being the lower and upper bounds of all other elements:

Top Element

$$a \sqsubseteq \top$$

Bottom Element

$$\perp \sqsubseteq a$$

Top is maximal

$$\top \sqsubseteq a \equiv a = \top$$

Bottom is minimal

$$a \sqsubseteq \perp \equiv a = \perp$$

Lattices

A *lattice* is a pair of operations $\sqcap, \sqcup : \tau \rightarrow \tau \rightarrow \tau$ 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

$$a \square b = b \square a$$

Associativity of \square

$$(a \square b) \square c = a \square (b \square c)$$

Idempotency of \square

$$a \square a = a$$

Zero of \square

$$a \sqcup \perp = \perp$$

$$a \sqcap \top = \top$$

Identity of \square

$$a \sqcup \perp = a$$

$$a \sqcap \top = a$$

Absorption

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

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

Self-Distributivity of \square

$$a \square (b \square c) = (a \square b) \square (a \square c)$$

Weakening

/ Strengthening

$$a \sqsubseteq a \sqcup b$$

$$a \sqcap b \sqsubseteq a$$

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

Induced Defs. of Inclusion

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

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

Monotonicity of \square

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

Golden Rule

$$a \sqcap b = a \equiv b = a \sqcup b$$

$$a \sqcap b = a \sqcup b \equiv a = b$$

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

The following four properties are all equivalent:

$$\sqcap\text{-Selective} :: \forall a, b \bullet a \sqcap b = a \vee a \sqcap b = a \quad \sqcup\text{-Selective} :: \forall a, b \bullet a \sqcup b = a \vee a \sqcup b = a$$

$$\text{Linearity} :: \forall a, b \bullet a \sqsubseteq b \vee b \sqsubseteq a$$

$$\text{Order Complement} :: \neg(a \sqsubseteq b) \equiv b \sqsubset a$$

Duality Principle:

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

Conditionals

“If to \wedge ” may be taken as axiom from which we may prove the remaining ‘alternative definitions’ “if to \dots ”.

if to \wedge	$P[z = \text{if } b \text{ then } x \text{ else } y \text{ fi}] \equiv (b \Rightarrow P[z = x]) \wedge (\neg b \Rightarrow P[z = x])$
if to \vee	$P[z = \text{if } b \text{ then } x \text{ else } y \text{ fi}] \equiv (b \wedge P[z = x]) \vee (\neg b \wedge P[z = x])$
if to \neq	$P[z = \text{if } b \text{ then } x \text{ else } y \text{ fi}] \equiv b \wedge P[z = x] \neq \neg b \wedge P[z = x]$
if to \equiv	$P[z = \text{if } b \text{ then } x \text{ else } y \text{ fi}] \equiv b \Rightarrow P[z = x] \equiv \neg b \Rightarrow P[z = x]$

Note that the “ \equiv ” and “ \neq ” rules can be parsed in multiple ways since ‘ \equiv ’ is associative, and ‘ \equiv ’ mutually associates with ‘ \neq ’.

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

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

Quantification

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

Abbreviation	$(\oplus x \bullet P) = (\oplus x \mid \text{true} \bullet P)$
Empty range	$(\oplus x \mid \text{false} \bullet P) = \text{Id}$
One-point rule	$(\oplus x \mid x = E \bullet P) = P[x = E]$
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	$(\oplus x \mid R \bullet P) = (\oplus y \mid R[x = y] \bullet P[x = y])$
Disjoint Range split	$(\oplus x \mid R \vee S \bullet P) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$ <i>provided $R \wedge S \equiv \text{false}$</i>
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	$(\oplus x \mid R \vee S \bullet P) = (\oplus x \mid R \bullet P) \oplus (\oplus x \mid S \bullet Q)$ <i>provided \oplus is idempotent</i>

Set Theory

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

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

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

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

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

Universe	$x \in \mathbf{U}$	$\equiv \text{true}$
Empty set	$x \in \emptyset$	$\equiv \text{false}$
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	$x \in S \rightarrow T$	$\equiv x \in S \Rightarrow x \in T$
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 $\emptyset \mid \text{false}$, $\mathbf{U} \mid \text{true}$, $\cup \mid \vee$, $\cap \mid \wedge$, $\subseteq \mid \Rightarrow$, $\sim \mid \neg$ 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	$\{x \mid R \bullet P\} = (\cup x \mid R \bullet \{P\})$
Membership as inclusion	$x \in S \equiv \{x\} \subseteq S$
Equality as membership	$x = y \equiv x \in \{y\}$

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	$\#S \leq 0 \equiv S = \emptyset$
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	$(\Sigma i : 1..n \bullet E)/n \leq (\uparrow i : 1..n \bullet E)$ ($\downarrow i : 1..n \bullet E \leq (\Sigma i : 1..n \bullet E)/n$)

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

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

Converse —an over-approximation of inverse (A4)

Co-distributivity $(x \circledast y)^\sim = y^\sim \circledast x$	\sim, Involutive $x^{\sim\sim} = x$	Monotonicity $x \sqsubseteq y \Rightarrow x^\sim \sqsubseteq y^\sim$
Identity $\text{Id}^\sim = \text{Id}$	Isotonicity $x \sqsubseteq y \equiv x^\sim \sqsubseteq y^\sim$	Connection $a^\sim \sqsubseteq b \equiv a \sqsubseteq b^\sim$
	Elimination $x^\sim = y^\sim \equiv x = y$	

Residuals, Division

Suppose we have an associative operation \circledast with identity Id and two operations “under \backslash ” and “over $/$ ” specified as follows.

Characterisation of $/$ $a \circledast b \sqsubseteq c \equiv a \sqsubseteq c/b$	Characterisation of \backslash $a \circledast b \sqsubseteq c \equiv b \sqsubseteq a \backslash c$
---	---

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

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

Monotonicity of \circledast $a \sqsubseteq a' \wedge b \sqsubseteq b' \Rightarrow a \circledast b \sqsubseteq a' \circledast b'$
Subdistributivity of \circledast over \sqcap $a \circledast (b \sqcap c) \sqsubseteq a \circledast b \sqcap a \circledast c$

Numerator monotonicity	$b \sqsubseteq b' \Rightarrow a \backslash b \sqsubseteq a \backslash b'$	$b \sqsubseteq b' \Rightarrow b/a \sqsubseteq b'/a$
Denominator antitonicity	$a' \sqsubseteq a \Rightarrow a \backslash b \sqsubseteq a' \backslash b$	$a' \sqsubseteq a \Rightarrow b/a \sqsubseteq b/a'$
Exact division	$(\exists z \bullet y = x \circledast z) \equiv$	$x \circledast (x \backslash y) = y$
Exact division	$(\exists z \bullet y = x \backslash z) \equiv$	$x \backslash (x \circledast y) = y$

Modal and Dedekind rules: (‘ \sqsubseteq ’ instead of ‘ $=$ ’ since ‘ \circledast ’ may not be cancellable)

(Axioms)	(Theorems)
$a \circledast b \sqcap c \sqsubseteq a \circledast (b \sqcap a^\sim \circledast c)$	$a \backslash b \sqcap c \sqsubseteq a \backslash (b \sqcap a \circledast c)$
$a \circledast b \sqcap c \sqsubseteq (a \sqcap c \circledast b^\sim) \circledast b$	$a \backslash b \sqcap c \sqsubseteq (a \sqcap c \backslash b) \backslash b$
$a \circledast b \sqcap c \sqsubseteq (a \sqcap c \circledast b^\sim) \circledast (b \sqcap a^\sim \circledast c)$	$a \backslash b \sqcap c \sqsubseteq (a \sqcap c \backslash b) \backslash (b \sqcap a \circledast c)$

Division for the special case $\circledast = \sqcap$ 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: $x \sqsubseteq y \equiv \text{Id} \sqsubseteq x \backslash y$.

Pseudo-complement $x \sqcap a \sqsubseteq b \equiv x \sqsubseteq a \rightarrow b$	Semi-complement $a - b \sqsubseteq x \equiv a \sqsubseteq b \sqcup x$
Strong modus ponens $a \sqcap (a \rightarrow b) = a \sqcap b$ $a \rightarrow (x \sqcap a) = a \rightarrow x$	Absorption $(x \sqcup b) - b = x - b$ $(a - b) \sqcup b = a \sqcup b$

Division for the special case $\circledast = \sqcup$ 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!)

Named Properties

reflexive	$x \equiv \text{Id} \sqsubseteq x$	symmetric	$x \equiv x^\sim = x$
irreflexive	$x \equiv \text{Id} \sqcap x = \perp$	antisymmetric	$x \equiv x \sqcap x^\sim \sqsubseteq \text{Id}$
transitive	$x \equiv x \circledast x \sqsubseteq x$	asymmetric	$x \equiv x \sqcap x^\sim = \perp$
idempotent	$x \equiv x \circledast x = x$		

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

univalent	$x \equiv x^\sim \circledast x \sqsubseteq \text{Id}$	injective	$x \equiv x \circledast x^\sim \sqsubseteq \text{Id}$
total	$x \equiv \text{Id} \sqsubseteq x \circledast x^\sim$	surjective	$x \equiv \text{Id} \sqsubseteq x^\sim \circledast x$
mapping	$x \equiv \text{total } x \wedge \text{univalent } x$	bijjective	$x \equiv \text{surjective } x \wedge \text{injective } x$
iso	$x \equiv \text{mapping } x \wedge \text{bijjective } x$		

Duality theorems

univalent (x^\sim)	\equiv	injective x
total (x^\sim)	\equiv	surjective x
mapping (x^\sim)	\equiv	bijjective x
iso (x^\sim)	\equiv	iso x

Invertibility theorems

total $x \wedge \text{injective } x$	\Rightarrow	$x \circledast x^\sim = \text{Id}$
iso $x \equiv x \circledast x^\sim = \text{Id} \wedge x^\sim \circledast x = \text{Id}$		
iso $x \Rightarrow (\exists g \bullet x \circledast g = \text{Id} = g \circledast x)$		

Shunting laws:

univalent f	\Rightarrow	$(x \circledast f \sqsubseteq y \Leftarrow x \sqsubseteq y \circledast f^\sim)$
total f	\Rightarrow	$(x \circledast f \sqsubseteq y \Rightarrow x \sqsubseteq y \circledast f^\sim)$
mapping f	\Rightarrow	$(x \circledast f \sqsubseteq y \equiv x \sqsubseteq y \circledast f^\sim)$

Relations

Relations are sets of pairs ...

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

Division generalises extensional subset inclusion and indirect reasoning for orders.

- u is related by ‘ R **over** S ’ to v precisely when “anything is R -over u if it is S -over v .”

- u is related by ‘ S **under** R ’ to v precisely when “everything S -under u is also R -under v .”

Example: Define E via $x \langle E \rangle X \equiv x \in X$, then $A \langle E \rangle B \equiv A \subseteq B$.

Example (Indirect inclusion): Define L via $x \langle L \rangle y \equiv x \sqsubseteq y$, then $L \backslash L = L / L = L$.

Interpreting Named Properties

We will interpret the named properties using

- ◇ Relations: Formulae on sets of pairs; “ $\forall x \bullet \dots$ ”
- ◇ 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

The following properties are what one may ascribe to a *comparative relationship*, such as equality or inclusion.

reflexive	$R \equiv (\forall b \bullet b(R)b)$	Every node in a graph has a ‘loop’, a line to itself (Thus, paths can always be increased in length: $R \subseteq R \circ R$) The diagonal of a matrix is all 1s
irreflexive	$R \equiv (\forall b \bullet \neg(b(R)b))$	No node in a graph has a loop The diagonal of a matrix is all 0s
symmetric	$R \equiv (\forall b, c \bullet b(R)c \equiv c(R)b)$	The graph is undirected; we have a symmetric matrix
antisymmetric	$R \equiv (\forall b, c \bullet b(R)c \wedge c(R)b \Rightarrow b = c)$	Mutually related nodes are necessarily self-loops “Mutually related items are necessarily indistinguishable”
asymmetric	$R \equiv (\forall b, c \bullet b(R)c \Rightarrow \neg(c(R)b))$	At most 1 edge (regardless of direction) relating any 2 nodes
transitive	$R \equiv (\forall b, c, d \bullet b(R)c \wedge c(R)d \Rightarrow b(R)d)$	Paths can always be shortened (but nonempty)
idempotent	$R \equiv$	Lengths of paths can be changed arbitrarily (nonzero) Prog: Outputs fed back into the program don’t change. Ex: Pressing ‘send’ on an email only sends it once.

Intuitively, by considering the interpretations only, we find

$$\text{reflexive } R \wedge \text{transitive } R \Rightarrow \text{idempotent } R$$

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 $x(R)y$
R^\sim	Flip the arrows in the graph
$\text{Dom } R$	The nodes that have an outgoing edge
$\text{Ran } R$	The nodes that have an incoming edge
$x(R)y$	A path of length 1 (an edge) from x to y
$x(R \circ R)y$	A path of length 2 from x to y
$R \cup R^\sim$	The associated undirected graph (“symmetric closure”)

Properties of an operational flavour

The following properties are what one may ascribe to a *process* or an *operation*.

univalent	$R \equiv (\forall b, c, c' \bullet b(R)c \wedge b(R)c' \Rightarrow c = c')$	—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	$R \equiv (\forall b, b', c \bullet b(R)c \wedge b'(R)c \Rightarrow b = b')$	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	$R \equiv (\forall b \bullet \exists c \bullet b(R)c)$	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	$R \equiv (\forall c \bullet \exists b \bullet b(R)c)$	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	$R \equiv \text{total } R \wedge \text{univalent } R$	—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
bijjective	$R \equiv \text{surjective } R \wedge \text{injective } R$	Graph: Every node has exactly one incoming edge Matrix: Every column has exactly one 1 Prog: Every output arises from a unique input
iso	$R \equiv \text{mapping } R \wedge \text{bijjective } R$	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