UNIVERSITY OF DUBLIN
TRINITY COLLEGE

HANDBOOK OF MATHEMATICS

FOR USE IN THE EXAMINATIONS
OF THE
DEPARTMENT OF COMPUTER SCIENCE.

2005 EDITION

This is the *fifth edition* of the HANDBOOK OF MATHEMATICS for use in the examinations of the Department of Computer Science. It had been especially compiled for the new Moderatorship degree *B.A. (Mod.) Information and Communications Technology* of the University of Dublin, the first year of which was examined in 1998. The editors/compilers have made every effort to ensure that there are no serious errors or omissions and welcome comment on the content. The choice of notation was difficult in some instances and guided by practice in the respective courses and by topic. Since the 2000 edition we have included appendices giving (i) the names of contributors and (ii) the names of sources of specific materials. The HANDBOOK OF MATHEMATICS will be under continuous development to meet the needs of degree courses offered by the Department of Computer Science.

Editors

Dr. Andrew Butterfield

Dr. Mícheál Mac an Airchinnigh

Contents

Part I

Notation & Formulæ

1 Numbers

$\mathbb{B}$	the set of Booleans $\{0, 1\}$.
$\mathbb{N}$	the set of natural numbers $\{0, 1, 2, \ldots\}$.
$\mathbf{k}$	the finite set of natural numbers $\{0, 1, 2, \ldots, k-1\}$, $k \geq 1$.
$\mathbb{Z}$, $\mathbb{Z}_{\geq 0}$	the set of integers, natural numbers.
$\mathbb{Q}$	the set of rationals.
$\mathbb{R}$, $\mathbb{R}_{>0}$	the set of real numbers, strictly positive real numbers.
$\mathbb{R}$	the set of complex numbers.

Constant	approximation	comment
e	2.71828	the base of natural logarithms
π	3.14159	the area of a unit disk
γ	0.577216	Euler's constant
ϕ	1.61803	"golden ratio" $(1+\sqrt{5})/2$
$2^{10} = 1024$	1,000	referred to as 1K
$\log_{10} 2$	0.30103	
$10!$	3,500,000	

Table of powers of 2

n	2^n	n	2^n	n	2^n	n	2^n
0	1	10	1024	20	1048576	30	1073741824
1	2	11	2048	21	2097152	31	2147483648
2	4	12	4096	22	4194304	32	4294967296
3	8	13	8192	23	8388608		
4	16	14	16384	24	16777216		
5	32	15	32768	25	33554432		
6	64	16	65536	26	67108864		
7	128	17	131072	27	134217728		
8	256	18	262144	28	268435456		
9	512	19	524288	29	536870912		

2 Sets

$\emptyset$, $\{\,\}$	the unique null set.
$\mathcal{P}\_$	the (direct) powerset functor.
$\mathcal{P}f$	the iterating of map f over a set.
$\mathcal{P}X$, $\mathcal{P}'X$	the powerset of set X, $\mathcal{P}X$ excluding $\emptyset$.
$S \cup T$, $S \sqcup T$, $S \bigtriangleup T$	union, disjoint union, symmetric difference.
$S \cap T$	intersection.
$\lhd_T S$, $S \backslash T$, $S - T$	set difference.
χ_S, φ_S	characteristic function or subset classifier.
$a \in S$	test for set membership.
$\mid S \mid$, $\#S$, $\texttt{card}S$	the cardinality of a set S.
$\pi_\epsilon S$	a 'projection' that selects a random element of a set S.

———— : ———— : ————

3 Sequences

1, Λ, σ	the unique null sequence.
$\_^*$	the sequence or free monoid functor.
f^*	the iterating of map f over a sequence.
Σ^*, Σ^+	sequences of elements over (alphabet) Σ, non-empty sequences.
$\Sigma^*_\leq$, $\Sigma^*_!$	sorted sequences, unique sequences, respectively.
$\mid \sigma \mid$, $\#\sigma$, $\mathsf{len}\ \sigma$	the length of a sequence σ.
$\sigma \cdot \tau$	concatenation of σ and τ.
$\mathsf{elems}\ \sigma$	the set of elements in a sequence σ.
$\mathsf{items}\ \sigma$	the bag of elements in a sequence σ.
$\pi_j \sigma$	a projection that selects the jth element of a sequence σ.

4 Maps

θ, $[\,]$	the unique null map.
$\_ \to \_$	the map functor.
$f \to g$	the iterating of a pair of maps; f must be 1–1.
$X \to Y$	the space of all partial and total maps from X to Y.
Y^X	the space of total maps from X to Y, map object, exponential.
$\mu \in X \to Y$	an arbitrary partial/total map
$\mu\colon X \to Y$	a total map
$\mu\colon X \rightsquigarrow Y$	a strictly partial map
$\mathcal{I}$	the identity map.
$\emptyset^X$	the constant null (map) in the space $(\mathcal{P}Y)^X \subset (X \to \mathcal{P}Y)$.
$\mathsf{dom}\,\mu$, $\mathsf{cod}\,\mu$, $\mathsf{rng}\,\mu$	the domain, codomain, range of the map μ.
$\mu \sqcup \nu$	the extend, or merge of two disjoint maps defined only if $\mathtt{dom}\,\mu \cap \mathtt{dom}\nu = \emptyset$.
$\mu \dagger \nu$	the override or overwrite of two maps.
$\mu \cup \nu$	the glueing of two maps which agree on $\mathtt{dom}\,\mu \cap \mathtt{dom}\nu$.
$\nu \circ \mu$, $\nu\,\mu$	the composition of two maps $\mu \in X \to Y$ and $\nu \in Y \to Z$; defined over $\mathtt{rng}\,\mu \cap \mathtt{dom}\nu$; a strict version requires $\mathtt{rng}\,\mu = \mathtt{dom}\nu$.
$\mu \bowtie \nu$	the join of two maps $\mu \in X \to Y$ and $\nu \in X \to Z$; defined over $\mathtt{dom}\,\mu \cap \mathtt{dom}\nu$.
$\mu\,{-1}$	the inverse of the map $\mu\,{-1}$, where it exists.
$\sphericalangle_S\,\mu$, $\sphericalangle[S]\,\mu$, $S \sphericalangle\,\mu$	the removal of μ with respect to S; classical mathematics uses $\mu \setminus S$.
$\lhd_S\,\mu$, $\lhd[S]\,\mu$, $S \lhd \mu$	the restriction of μ with respect to S; classical mathematics uses $\mu\,\vert_S$.
$\exists_f\,S, \forall_f\,S$	existential image, universal image of map f with respect to set S
$Y \to \mathcal{P}'X$	the (covering) space of inverse image maps.
$(\mathcal{I} \to \sphericalangle_S)'$	the iterator $(\mathcal{I} \to \sphericalangle_S)$ with removal of $y \mapsto \emptyset$ elements.

5 Structures

Semigroup A set S with an associative binary operator $*\colon S \times S \longrightarrow S$ is said to form a semigroup, denoted $(S, *)$.

$(\Sigma^+, \cdot)$	the free semigroup of words over Σ.

Monoid A semigroup $(M, *)$ for which there is an identity element e is called a monoid, denoted $(M, *, e)$.

$(\mathbb{N}, +, 0)$, $(\mathbb{N}, \times, 1)$	monoids of natural numbers.
$(\mathcal{P}X, \cup, \emptyset)$, $(\mathcal{P}X, \cap, X)$	monoids of sets.
$(\Sigma^*, \cdot, 1)$	the free monoid over Σ.
$(X \to Y, \dagger, \theta)$	the usual monoid of maps.
$(M, \cup, \theta)$	glueable submonoids of maps $M \subset (X \to Y)$.

base monoid	indexed monoid	comment
$(\mathbb{N}_0, +, 0)$	$(X \to \mathbb{N}, \bigoplus, \theta)$	bags
$(\mathcal{P}X, \cup, \emptyset)$	$(X \to \mathcal{P}'X, \text{\textcircled{$\cup$}}, \theta)$	relations
$(A \to B, \dagger, \theta)$	$(X \to (A \to B)', \text{\textcircled{$\dagger$}}, \theta)$	partitioned maps
$(\Sigma^*, \cdot, 1)$	$(X \to \Sigma^+, \bigodot, \theta)$	basis for indexed queues, etc.

Group A monoid $(G, *, e)$ for which each element g has an inverse $\bar{g}$ is called a group.

$(\mathbb{Z}, +)$	additive group of integers.
$(\mathbb{R}, +)$, $(\mathbb{R}^+, \times)$	groups of reals.
$(\mathcal{P}X, \triangle)$	group of sets.
$FG(\Sigma)$	free group over Σ.

Name	order	comment
S_n	n!	symmetric group of permutations of $\mathbb{N}_n$
A_n	$\frac{1}{2}n!$	alternating group of even permutations, $A_n \lhd S_n$.
D_{2n}	$2n$	dihedral group of regular polygon of n sides.
C_n	n	cyclic group with generator x, $C_n = \sigma x$.
$Z(G)$	–	centre of G, $\{z \in G \mid zg = gz \text{ for all } g \in G\}$.
Gx	–	the orbit $Gx = \{y \in X \mid y = g(x) \text{ for some } g \in G\}$.
G_x	–	stabilizer of x, $G_x = G(x \to x)$ where $G(x \to y) = \{g \in G \mid g(x) = y\}$.
$A \times B$	–	direct product of groups A and B.
$A \times_\theta B$	–	semi-direct product of groups A and B.

Semiring A set S which is both a multiplicative monoid $(S, \otimes, 1)$ and an additive monoid $(S, \oplus, 0)$ for which multiplication distributes over addition is called a semi-ring.

$(\mathbb{N}_0, +, \times, 0, 1)$	semi-ring of natural numbers.
$(\mathcal{P}X, \cup, \cap, \emptyset, X)$	semi-ring of sets.

Ring A set S which is both a multiplicative monoid $(S, \otimes, 1)$ and an additive group $(S, \oplus, 0)$ for which multiplication distributes over addition is called a ring.

$(\mathbb{Z}, +, \times, 0, 1)$	the ring of integers.
$(\mathcal{P}X, \triangle, \cap, \emptyset, X)$	ring of sets.
$\mathbb{Z}[x]$	the ring of polynomials with coefficients in $\mathbb{Z}$.

Field A set S which is both a multiplicative group $(S, \otimes, 1)$ and an additive group $(S, \oplus, 0)$ for which multiplication distributes over addition is called a field.

$\mathbb{Z}_p$	the finite field of integers modulo p, p a prime.
$(\mathbb{Q}, +, \times, 0, 1)$	the rationals.
$(\mathbb{R}, +, \times, 0, 1)$	the real numbers.
$(\mathbb{R}, +, \times, 0, 1)$	the complex numbers.

$$\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R} \longrightarrow \mathbb{R}$$

Poset A set S which is furnished with an ordering relation $\leq$ which is reflexive, anti-symmetric, and transitive, is said to form a partially ordered set (poset), denoted $(S, \preceq)$.

$(\mathbb{Z}, \leq)$	totally ordered set of integers.
$(\Sigma^*, \preceq)$	words with prefix ordering.
$(\mathcal{P}X, \subseteq)$	powerset of X with inclusion ordering.
$(\mathbf{div}(n), \mid)$	divisors of n with divides relation.

Lattice A poset S in which any two elements s and t have both a meet, $s \wedge t$, and a join, $s \vee t$, is called a lattice, denoted $(S, \wedge, \vee)$.

$(\mathcal{P}X, \cap, \cup)$	powerset of X.
$(\mathbf{div}(n), \gcd, \mathrm{lcm})$	divisors of n.

—————— : ———— : ——————

6 Algorithms

The Big O notation Let f be a function from $\mathbb{N}$ to $\mathbb{N}$. Then $f(n)$ is $O(g(n))$ if there is a positive constant k such that $f(n) \leq kg(n)$ for all n in $\mathbb{N}$ (with possibly a finite number of exceptions).

Assuming a machine can execute 10^6 operations per second:

$f(n)$	$n = 20$	$n = 40$	$n = 60$
n	0.00002 sec	0.00004 sec	0.00006 sec
n^2	0.0004 sec	0.0016 sec	0.0036 sec
n^3	0.008 sec	0.064 sec	0.216 sec
2^n	1.0 sec	12.7 days	366 centuries

Σ^*-morphisms $(\Sigma^*, \cdot, 1) \xrightarrow{\psi} (M, +, e)$

$$\begin{tikzcd} \Sigma \arrow[r, "i"] \arrow[dr, "F"'] & \Sigma^* \arrow[d, "\psi"'] \\ & M \end{tikzcd} \qquad \begin{tikzcd} \Sigma^* \times \Sigma^* \arrow[r, "\cdot"] \arrow[d, "\psi\times\psi"] & \Sigma^* \arrow[d, "\psi"'] \\ M \times M \arrow[r, "+"'] & M \end{tikzcd}$$

$$i(a) := \sigma a$$
$$\psi i = F$$

naïve recursive form

$$\psi(aw) = F(a) + \psi(w)$$
$$\psi(1) = e$$

naïve closed form

$$\psi(w) = {}^{+}/F^{*} w$$
$$\psi(1) = e$$

tail-recursive form

$$\psi_{aw}(m) = \psi_w(m + F(a))$$
$$\psi_1(m) = m$$
$$\psi(w) = \psi_w(e)$$

tail-recursive closed form

$$\psi_w(m) = m + {}^{+}/F^{*} w$$
$$\psi_1(m) = m$$

7 Counting

Pigeon-hole principle: if m objects are distributed into n boxes and $m > n$, then at least one box contains at least 2 objects.

Generalized pigeon-hole principle: if m objects are distributed into n boxes and $m > nr$, then at least one box contains at least $r + 1$ objects.

Sieve principle (Principle of inclusion/exclusion): If $A_1, A_2, \ldots, A_n$ are finite sets and α_i is the sum of the cardinalities of the intersections of the sets taken i at a time $(1 \leq i \leq n)$ then

$$| A_1 \cup A_2 \cup \cdots \cup A_n | := \alpha_1 - \alpha_2 + \alpha_3 - \cdots + (-1)^{n-1}\alpha_n$$

If $A_1, A_2, \ldots, A_n$ are subsets of a given set X, with $| X | = N$, then

$$\begin{aligned} | X \backslash \{A_1 \cup A_2 \cup \cdots \cup A_n\} | &= | X | - | A_1 \cup A_2 \cup \cdots \cup A_n | \\ &= N - \alpha_1 + \alpha_2 - \alpha_3 + \cdots + (-1)^n \alpha_n \end{aligned}$$

Derangements

$$d_n = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!})$$

Partitions If there are α_i parts of size i, then the partition of n is written

$$[1^{\alpha_1} 2^{\alpha_2} \cdots i^{\alpha_i} \cdots n^{\alpha_n}]$$

The number of partitions of n into k parts is given by

$$p_k(n) = p_k(n-k) + p_{k-1}(n-k) + \cdots + p_1(n-k)$$

Permutations The type of a permutation $\pi \in S_n$ in cycle notation is the partition of n:

$$[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$$

The number of permutations of type $[1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n}]$ is

$$\frac{n!}{1^{\alpha_1} 2^{\alpha_2} \cdots n^{\alpha_n} \alpha_1! \alpha_2! \cdots \alpha_n!}$$

——— : ——— : ———

8 Calculus

fundamental theorem

$$F(x) := \int_a^x f(u)du \quad \Rightarrow \quad F'(x) = f(x)$$

natural logarithm $\log x$, $\ln x$, $\log_e x$

$$\log x := \int_1^x \frac{1}{u}du, \qquad \log(1+x) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{x^n}{n}$$

exponential function $\exp x$, e^x

$$x = \log y \Rightarrow y = e^x$$

$$e^x := \sum_{n=0}^{\infty}\frac{x^n}{n!}$$

$$e^{ix} = \cos x + i\sin x, \quad (i^2 = -1)$$

$$\cos x = (e^{ix} + e^{-ix})/2, \qquad \cosh x = (e^x + e^{-x})/2$$

$$\sin x = (e^{ix} - e^{-ix})/2i, \qquad \sinh x = (e^x - e^{-x})/2$$

Gamma function

$$\Gamma(z) := \int_0^{\infty} e^{-t}t^{z-1}dt, \quad (Re(z) > 0)$$

$$\Gamma(z+1) = z\Gamma(z)$$

$$\Gamma(1) = 1$$

Incomplete Gamma function

$$\gamma(z,x) := \int_0^x e^{-t}t^{z-1}dt, \quad (Re(z) > 0), \qquad \gamma(z,\infty) = \Gamma(z)$$

Error function

$$\mathrm{Erf}(x) := \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt, \qquad \mathrm{Erfc}(x) := \frac{2}{\sqrt{\pi}}\int_x^{\infty} e^{-t^2}dt$$

9 Category Theory

$\{*\}$	the unique one point set in the category of sets
0	initial object in a category $\mathcal{C}$
1	terminal object in a category $\mathcal{C}$

Category	object	remark
set S	element of the set S	identity arrows only
monoid $(M, +, e)$	the anonymous object $*$	arrows are elements of M
group $(G, +, e)$	the anonymous object $*$	arrows are elements of G
poset $(\mathcal{P}S, \subseteq)$	subset of S	arrows are inclusions
poset $(\mathbf{div}(n), \mid)$	divisor of n, $n \in \mathbb{N}$	an arrow denotes 'divides'
$\mathcal{S}$, **Set**	set	category of sets
$\mathcal{S}^{op}$	set	opposite or dual category of sets
$\mathcal{S}^{\downarrow}$	$A \xrightarrow{f} B$	A, B are sets
$\mathcal{S}^{\downarrow\downarrow}$	$X \overset{s}{\underset{t}{\rightrightarrows}} P$	X is set of arrows, P is set of dots
$\mathcal{S}^{\circlearrowleft}$	$A^{\circlearrowleft \alpha}$ or $A \xrightarrow{\alpha} A$	A a set with endomap α
$1/\mathcal{S}$	$1 \xrightarrow{x_0} X$	category of pointed sets
$\mathcal{C}/X$	$A = A_0 \xrightarrow{\alpha} X$	slice category
$\mathcal{P}(X) \subseteq \mathcal{C}/X$	$A_0 \overset{\alpha}{\hookrightarrow} X$	category of parts of X, i.e., a poset
Mon	monoid	arrows are monoid morphisms
Grp	group	arrows are group morphisms
Data	data type	arrows are computable functions

———— : ———— : ————

A map $A \xrightarrow{f} B$ is an **isomorphism** if there is a map $B \xrightarrow{g} A$ for which $gf = 1_A$ and $fg = 1_B$. An endomap $A \xrightarrow{\alpha} A$ which is an isomorphism is called an **automorphism**.

If $A \xrightarrow{f} B$, a **retraction** for f is a map $B \xrightarrow{r} A$ for which $rf = 1_A$; a **section** for f is a map $B \xrightarrow{s} A$ for which $fs = 1_B$.

An endomap $A \xrightarrow{\alpha} A$ is **idempotent** if $\alpha \circ \alpha = \alpha^2 = \alpha$. If $\alpha \circ \alpha = 1_A$ then the endomap α is called an **involution**.

For a general map $X \xrightarrow{g} B$ we say that g gives rise to a **sorting**, **fibering**, ..., of X into B sorts, fibres, ..., or that g is a sorting, fibering, ..., of X by B. The map g produces a structure in the **domain**.

For a general map $A \xrightarrow{f} X$ we say that f is an A-shaped **figure** in X or an A-element of X. We might think of f as a naming or listing of elements of X by A. We also say that f parameterizes part of X by moving A following f. The map f produces a structure in the **codomain**.

In any category $\mathcal{C}$, an object T is a **terminal** object if and only if it has the property that for each object X in $\mathcal{C}$ there is exactly one map from X to T.

A **point** of X is a map $T \longrightarrow X$ where T is terminal.

In any category $\mathcal{C}$, an object S is an **initial** object if for every object X there is exactly one map from S to X.

An object which is both initial and terminal is called a **zero** object.

A category $\mathcal{C}$ is said to satisfy the **distributive law** if the standard maps

$$(A \times B) + (A \times C) \longrightarrow A \times (B + C), \qquad 0 \longrightarrow A \times 0$$

are always isomorphisms in the category.

A **parallel pair of maps**$A \underset{g}{\overset{f}{\rightrightarrows}} B$ which hasa diagram of shape $\bullet \rightrightarrows \bullet$ may be represented by a graph object X in $\mathcal{S}^{\downarrow\downarrow}$ with arrows X_A and dots X_B.

$E \xrightarrow{p} A$ is an **equalizer** of $A \underset{g}{\overset{f}{\rightrightarrows}} B$ if $fp = gp$ and for each $T \xrightarrow{x} X$ for which $fx = gx$, there is exactly one $T \xrightarrow{e} E$ for which $x = pe$. The equalizer p identifies the self-loops of the corresponding graph object X.

In any category $\mathcal{C}$, a map $S \xrightarrow{i} X$ is an **inclusion**, or **monomorphism**, or **monic map**, if for each object T and each pair of maps s_1, s_2 from T to S, $is_1 = is_2$ implies $s_1 = s_2$.

A **part** of X is an S-shaped figure in X, $S \overset{i}{\hookrightarrow} X$ where i is an inclusion. A part is often denoted S, i.

: :

Galois correspondence Let $\mathcal{X} = (X, \leq)$ and $\mathcal{Y} = (Y, \preceq)$ be poset categories. A pair of functors

$$\mathcal{X} \underset{\mathsf{F}}{\overset{\mathsf{G}}{\leftrightarrows}} \mathcal{Y}$$

is said to form a covariant Galois correspondence if $\mathsf{F}x \longrightarrow y \Leftrightarrow x \longrightarrow \mathsf{G}y$.

Product object $B_1 \times B_2$

$$\begin{tikzcd}
 & & B_1 \\
X \arrow[urr, bend left, "f_1"] \arrow[r, "\langle f_1, f_2 \rangle"] \arrow[drr, bend right, "f_2"'] & B_1 \times B_2 \arrow[ur, "p_1"'] \arrow[dr, "p_2"] & \\
 & & B_2
\end{tikzcd}$$

$$\frac{X \longrightarrow B_1 \times B_2}{X \longrightarrow B_1\,,\, X \longrightarrow B_2}$$

binary operation on an object A is a map $A \times A \xrightarrow{\alpha} A$

action of an object A on an object X is a map $A \times X \xrightarrow{\xi} X$

Coproduct (i.e. sum) object $B_1 + B_2$

$$\begin{tikzcd}
B_1 \arrow[dr, "j_1"'] \arrow[drr, bend left, "g_1"] & & \\
 & B_1 + B_2 \arrow[r, "\begin{cases} g_1 \\ g_2 \end{cases}"] & Y \\
B_2 \arrow[ur, "j_2"] \arrow[urr, bend right, "g_2"'] & &
\end{tikzcd}$$

$$\frac{B_1 + B_2 \longrightarrow Y}{B_1 \longrightarrow Y\,,\, B_2 \longrightarrow Y}$$

The function $g = \begin{cases} g_1 \\ g_2 \end{cases}$ is defined by cases:

$$g(s) := \begin{cases} g_1(b_1), & \text{if } s = j_1(b_1), \\ g_2(b_2), & \text{if } s = j_2(b_2). \end{cases}$$

Relation $r = \sigma h, k$

$$\begin{tikzcd}
 & R \arrow[dl, "h"'] \arrow[d, "r"] \arrow[dr, "k"] & \\
A & A \times B \arrow[l, "p_1"] \arrow[r, "p_2"'] & B
\end{tikzcd}$$

Graph $\Gamma_f = \sigma 1_A.f$ of map $A \xrightarrow{f} B$

$$\begin{tikzcd}
 & A \arrow[dl, "1_A"'] \arrow[d, "\Gamma_f"] \arrow[dr, "f"] & \\
A & A \times B \arrow[l, "p_1"] \arrow[r, "p_2"'] & B
\end{tikzcd}$$

Exponential or Map object Y^T

$$
\begin{tikzcd}
T \times X \arrow[r, "1_T \times \ulcorner f \urcorner"] \arrow[dr, "f"'] & T \times Y^T \arrow[d, "e"] \\
& Y
\end{tikzcd}
\qquad\qquad
\frac{X \longrightarrow Y^T}{T \times X \longrightarrow Y}
$$

Cartesian closed category A category with products (and therefore with terminal object) in which every pair of objects has a map object.

Topos A category $\mathcal{C}$ is a topos if and only if

1. $\mathcal{C}$ has 0, 1, $\times$, $+$, and for every object X, $\mathcal{C}/X$ has products.
2. $\mathcal{C}$ has map objects Y^X.
3. $\mathcal{C}$ has a ‘truth-value object’ $1 \longrightarrow \Omega$ (also called a ‘subobject classifier’).

What is truth?

$$
1 \xrightarrow{\quad true \quad} \Omega, \qquad \frac{\textit{parts of } X}{\textit{maps } X \longrightarrow \Omega}, \qquad \frac{S \overset{i_S}{\hookrightarrow} X}{X \underset{\varphi_S}{\longrightarrow} \Omega}
$$

Truth-value object Ω in the category of graphs $\mathcal{S}^{\downarrow\downarrow}$:

for arrows
t: arrow in.
b: arrow out, source in, target in.
f: arrow out, source out, target out.
d: arrow out, source in, target out.
c: arrow out, source out, target in.

for dots
1: dot in.
0: dot out.

Not Define not S to be the largest part of X which is disjoint from S.

Non Define non S to be the smallest part of X such that together with S it makes up X.

Boundary Define the boundary of S, denoted ∂S, to be the subobject common to both S and $\mathsf{non}\ S$. $\partial S = S \wedge \mathsf{non}\ S$.

Core Define the core of S, denoted $\mathsf{core}\ S$ to be $\mathsf{non}\ \mathsf{non}\ S$. $S = \partial S \vee \mathsf{core}\ S$.

Topology A Lawvere-Tierney topology is a map $\Omega \xrightarrow{j} \Omega$ such that

$$
\begin{tikzcd}
1 \arrow[r, "t"] \arrow[dr, "t"'] & \Omega \arrow[d, "j"] \\
& \Omega
\end{tikzcd}
\qquad
\begin{tikzcd}
\Omega \arrow[r, "j"] \arrow[dr, "j"'] & \Omega \arrow[d, "j"] \\
& \Omega
\end{tikzcd}
\qquad
\begin{tikzcd}
\Omega \times \Omega \arrow[r, "\wedge"] \arrow[d, "j \times j"'] & \Omega \arrow[d, "j"] \\
\Omega \times \Omega \arrow[r, "\wedge"'] & \Omega
\end{tikzcd}
$$

10 Number Theory

$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$	unique factorization of n, p_j a prime, $\alpha_j \geq 1$.
$\lfloor x \rfloor$, $[x]$	floor function; greatest integer less than or equal to x
$\lceil x \rceil$	ceiling function; least integer greater than or equal to x.
(m, n)	greatest common divisor (gcd) of m and n

—————: ———— : —————

Euler's totient function

$$\phi(n) := n \prod_{p|n} (1 - \frac{1}{p}) \qquad \phi(p) = p - 1$$

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d} \qquad \phi(mn) = \phi(m)\phi(n), \quad (m, n) = 1.$$

$$n = \sum_{d|n} \phi(d) \qquad \phi(p^\alpha) = p^{\alpha-1}\phi(p)$$

$$x^{\phi(m)} \equiv 1 \pmod{m}, \quad (x, m) = 1.$$

Chinese Remainder Theorem The system

$$x \equiv (a_1, \dots, a_n) \mathtt{mod}\, (m_1, \dots, m_n), \qquad (m_i, m_j) = 1, i \neq j$$

has the unique solution

$$x \equiv a_1 M_1^{\varphi(m_1)} + \dots + a_k M_k^{\varphi(m_k)} + \dots + a_n M_n^{\varphi(m_n)} \pmod{M}$$

where $M = m_1 m_2 \dots m_n$, $M_k = M/m_k$.

Möbius function

$$\mu(n) := \begin{cases} 1, & \text{if } n = 1, \\ (-1)^k, & \alpha_1 = \dots = \alpha_k = 1, \\ 0, & \text{otherwise} \end{cases}$$

$$f(n) = \sum_{d|n} g(d), \quad g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$$

—————: ———— : —————

Identity function

$$I(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise} \end{cases}$$

Radical/conductor

$$\kappa(n) := \prod_{p|n} p$$

Unit function

$$u(n) := 1$$

Power function

$$N^{\alpha}(n) := n^{\alpha}$$

von Mangoldt's function

$$\Lambda(n) := \begin{cases} \log p, & \text{if } n = p^m, m \geq 1, \\ 0, & \text{otherwise} \end{cases}$$

Divisor functions

$$\sigma_{\alpha}(n) := \sum_{d|n} d^{\alpha}$$

Liouville's function

$$\lambda(n) := \begin{cases} 1, & \text{if } n = 1, \\ (-1)^{\alpha_1+\alpha_2+\ldots+\alpha_k}, & \text{otherwise} \end{cases}$$

Riemann ζ-function

$$\zeta(s) := \sum_{1}^{\infty} \frac{1}{n^s}, \quad (s = \sigma + it), \qquad \zeta(s) = \prod_{p} (1 - \frac{1}{p^s})^{-1}$$

$$\frac{1}{\zeta(s)} = \sum_{1}^{\infty} \mu(n) \frac{1}{n^s}, \quad (\sigma > 1), \qquad \frac{\zeta(s-1)}{\zeta(s)} = \sum_{1}^{\infty} \phi(n) \frac{1}{n^s}, \quad (\sigma > 2)$$

——— : ——— : ———

Dirichlet product (or convolution) $h = f^* g$

$$h(n) = (f^* g)(n) := \sum_{d|n} f(d) g(\frac{n}{d}) = \sum_{d|n} f(\frac{n}{d}) g(d)$$

$$\mu^* u = I, \qquad \mu^{-1} = u$$
$$\phi = \mu^* N, \qquad \phi^{-1} = u^* \mu N$$
$$\sigma_{\alpha} = u^* N^{\alpha}$$

Associative law:

$$(f^* g)^* h = f^* (g^* h)$$

Identity:

$$f^* I = f = I^* f$$

Commutative law:

$$f^* g = g^* f$$

Inverse:

$$f^{-1}(1) = \frac{1}{f(1)}$$
$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f(\frac{n}{d}) f^{-1}(d)$$

Derivative of an arithmetical function

$$f'(n) := f(n)\log(n), \quad n \geq 1$$

11 Generating Functions

Generating functions/Formal power series. The generating function $G(z)$ for the sequence of numbers

$$\sigma a_n = a_0, a_1, a_2, \ldots$$

is given by

$$G(z) = \sum_{k=0}^{\infty} a_k z^k = a_0 + a_1 z + a_2 z^2 + \ldots$$

Examples:

$$\sigma a_n = 1, 1, 1, 1, \ldots \qquad G(z) = \frac{1}{1-z} \qquad \text{[models the regular tick of a clock]}$$

$$\sigma b_n = 1, 0, 1, 0, \ldots \qquad H(z) = \frac{1}{1-z^2} \qquad \text{[models on, off, on, off, etc.]}$$

$$\sigma c_n = a, b, a, b, \ldots \qquad J(z) = \frac{a+bz}{1-z^2} \qquad \text{[models } a, b, a, b, \text{ etc.]}$$

Properties:

$$\alpha G_1(z) + \beta G_2(z) = \alpha \sum_{k=0}^{\infty} a_k z^k + \beta \sum_{k=0}^{\infty} b_k z^k = \sum_{k=0}^{\infty} (\alpha a_k + \beta b_k) z^k$$

$$z^n G(z) = z^n \sum_{k=0}^{\infty} a_k z^k = \sum_{k=n}^{\infty} a_{k-n} z^k$$

$$G_1(z) G_2(z) = \sum_{k=0}^{\infty} a_k z^k \sum_{k=0}^{\infty} b_k z^k = \sum_{k=0}^{\infty} c_k z^k$$

where $c_k = \sum_{k=0}^{n} a_{n-k} b_k = \sum_{k=0}^{n} a_k b_{n-k}$.

The Exponential generating functions. The exponential generating function $\hat{G}(z)$ for the sequence of numbers

$$\sigma a_n = a_0, a_1, a_2, \ldots$$

is given by

$$\hat{G}(z) = \sum_{k=0}^{\infty} a_k \frac{z^k}{k!} = a_0 + a_1 z + a_2 \frac{z^2}{2!} + \ldots$$

: :

Factorial numbers

$$n! := \prod_{k=1}^{n} k, \quad n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^{n}$$

Binomial numbers

$$n\pi_{\in}r := \frac{n(n-1)\dots(n-r+1)}{r!}, \quad G(z) := (1+z)^{n}$$

Stirling numbers (of the second kind) $S(n,k)$ denotes the number of partitions of an n-set into k parts.

$$S(n,1) = 1, \quad S(n,n) = 1,$$
$$S(n,k) := S(n-1,k-1) + kS(n-1,k), \quad (2 \le k \le n-1)$$
$$\hat{G}(z) := (e^{z}-1)^{k} = k! \sum_{n=k}^{\infty} S(n,k)\frac{z^{n}}{n!}$$

Fibonacci numbers F_n

$$F_1 = 1, \quad F_2 = 1,$$
$$F_n := F_{n-1} + F_{n-2}, \quad (n > 2)$$
$$G(z) := \frac{1}{1-z-z^{2}}$$

Harmonic numbers H_n

$$H_n := \sum_{k=1}^{n} \frac{1}{k}, \quad H_n = \log n + \gamma + O(\frac{1}{n}), \quad \gamma \approx 0.577216$$

Bernoulli numbers B_n

$$\hat{G}(z) := \frac{z}{e^{z}-1} = \sum_{n=0}^{\infty} B_n \frac{z^{n}}{n!}$$

12 Graph Theory

A graph $G = (V, E)$ is composed of a set of vertices V and a set of edges E. In a *simple* graph there is at most one edge between any pair of vertices. If there is more than one edge between a pair of vertices then the graph is called a *multigraph*. In the case that edges are directed, the graph is called a *directed graph*.

Graph catalogue

K_n	complete graph with n vertices.
$K_{m,n}$	complete bipartite graph with $m+n$ vertices
W_n	wheel graph with $V = \mathbf{n} + \mathbf{1}$

Canonical representation: A simple graph $G = (V, E)$ is canonically represented by its (adjacency list) function $V \xrightarrow{\gamma} \mathsf{P}V$. The degree or valency of each vertex is given by $(\mathcal{I} \to \mathtt{card})\gamma$.

Eulerian walk: exists if G has at most 2 odd vertices.

Chromatic Number $\chi(G)$: the least k for which there is a vertex-colouring using k colours.

Height h of m-ary tree with l leaves: $h \geq \lceil \log_m l \rceil$.

Free category on a directed graph. Given a directed graph G with no relations. The free category on G, denoted $\mathcal{G}$ has the vertices of G as objects and paths of G as arrows. Composition of arrows is given by the concatenation of paths.

: :

13 Queueing Theory

M/G/1
average number in server = ρ
average number in system:

$$\rho + \frac{\lambda^2(V) + \rho^2}{2(1-\rho)}, \quad \text{where } V \text{ is the variance of service time.}$$

M/M/1 with finite queue capacity

$$P_n = \frac{\rho^n(1-\rho)}{1-\rho^{N+1}}, \quad \rho \neq 1$$

$$P_n = \frac{1}{N+1}, \quad \rho = 1$$

average number in system:

$$\frac{\rho_{\mathit{eff}}\big(1-(N+1)\rho_{\mathit{eff}}^N + N\rho_{\mathit{eff}}^{N+1}\big)}{(1-\rho_{\mathit{eff}})(1-\rho_{\mathit{eff}}^{N+1})}, \quad \rho_{\mathit{eff}} \neq 1$$

average number in system:

$$\frac{N}{2}, \quad \rho_{\mathit{eff}} = 1$$

average number in server:

$$\rho_{\mathit{eff}} = \frac{\lambda_{\mathit{eff}}}{\mu}, \quad \lambda_{\mathit{eff}} = \lambda(1-P_n)$$

average rate of balking:

$$\lambda P_n$$

M/M/S with finite queue capacity
average number in server = ρ

$$\frac{1}{P_0} = \frac{\rho^s}{s!}\left(\frac{1}{1-\rho/s}\right) + \sum_{n=0}^{s-1}\frac{\rho^n}{n!}$$

average number in system:

$$\rho + \frac{\rho^s \lambda \mu}{(s-1)!(\mu s - \lambda)^2} P_0$$

average number in server: ρ
average number in queue:

$$\frac{\rho^s \lambda \mu}{(s-1)!(\mu s - \lambda)^2} P_0$$

Machine Repair Man finite source of arrivals*:

$$\frac{1}{P_0} = \sum_{i=0}^{N} \frac{N!}{(N-i)!} \rho^i$$

$$P_n = \frac{\rho^n \big(N!/(N-n)!\big)}{\sum_{i=0}^{N} \big(N!/(N-i)!\big) \rho^i}$$

average number in system:

$$P_0 \sum_{i=1}^{N} \frac{iN! \rho_{eff}^i}{(N-i)!}$$

$$\lambda_{eff} = \lambda(N - \text{Average number in system})$$

M/G/S

$$P_j = \frac{(\lambda \,/\, \mu)^j / j!}{\sum_{j=0}^{s} (\lambda \,/\, \mu)^j / j!}$$

average number in the system:

$$\frac{\lambda}{\mu}(1 - P_s)$$

14 Operations Research

Time Series
exponential smoothing:

$$F(t+1) = F(t) + \alpha\big(\tau(t) - F(t)\big), \quad \text{where } \alpha \text{ is a smoothing constant}$$

linear regression:

$$Y_T = a + bX$$
$$b = \frac{n\sum XY - \sum X \sum Y}{n\sum X^2 - (\sum X)^2}$$
$$a = \frac{\sum Y - b\sum X}{n}$$

PERT

$$t_e = \frac{a + 4m + b}{6}$$
$$\sigma^2 = \frac{(b-a)^2}{36}$$

Inventory Models
EOQ model

$$Q = \sqrt{\frac{2C_0 D}{C_c}}$$

Production model

$$Q = \sqrt{\frac{2C_0 D}{C_c(1 - D/R)}}$$

Assumed shortage

$$Q = \sqrt{\frac{2C_0 D}{C_c}}\sqrt{\frac{C_c + C_s}{C_s}}$$

$$V = \sqrt{\frac{2C_0D}{C_c}}\sqrt{\frac{C_s}{C_c + C_s}}$$

$$S = Q - V$$

Non-instantaneous receipt with shortage

$$Q = \sqrt{\frac{2C_0D}{C_c(1 - D/R)}}\sqrt{\frac{C_c + C_s}{C_s}}$$

$$S = \sqrt{\frac{2C_0D}{C_s}}\sqrt{1 - \frac{D}{R}}\sqrt{\frac{C_s}{C_c + C_s}}$$

$$TC = \sqrt{2C_0C_cD}\sqrt{1 - \frac{D}{R}}\sqrt{\frac{C_s}{C_c + C_s}}$$

Carrying cost as a percentage

$$Q = \sqrt{\frac{2C_0D}{K_cP}}$$

Time as a model variable

$$Q = \sqrt{\frac{2C_0D}{C_cT}}$$

Quantity discount model

$$Q = \sqrt{\frac{2C_0D}{K_0P'}}$$

$$TC = \frac{C_0D}{Q} + K_cP'(Q/2) + P'D$$

Non-linear programming

Method of golden sections

$$m = A_1 + r^2(A_2 - A_1)$$
$$n = A_1 + r(A_2 - A_1)$$

where $r = (\sqrt{5} - 1)/2 \approx 0.618$

Gradient method

$$X_1 = X_0 + r(\frac{dy}{dx})$$

15 Laws of Boolean Algebra

No.	Law	Name	Huntington's Postulates
$B1$	$X + 0 = X$	identity	Postulate 2
$B2$	$X \cdot 1 = X$	identity	Postulate 2
$B3$	$X + 1 = 1$	zero	Theorem 2
$B4$	$X \cdot 0 = 0$	zero	Theorem 2
$B5$	$X + X = X$	idempotency	Theorem 1
$B6$	$X \cdot X = X$	idempotency	Theorem 1
$B7$	$X + \overline{X} = 1$	converse	Postulate 5
$B8$	$X \cdot \overline{X} = 0$	converse	Postulate 5
$B9$	$\overline{\overline{X}} = X$	double negation	Theorem 3 (involution)
$B10$	$X + Y = Y + X$	commutativity	Postulate 3
$B11$	$X \cdot Y = Y \cdot X$	commutativity	Postulate 3
$B12$	$X + (Y + Z) = (X + Y) + Z$	associativity	Theorem 4
$B13$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$	associativity	Theorem 4
$B14$	$X(Y + Z) = XY + XZ$	distributivity	Postulate 4
$B15$	$X + YZ = (X + Y)(X + Z)$	distributivity	Postulate 4
$B16$	$\overline{X + Y} = \overline{X} \cdot \overline{Y}$	DeMorgan's Law	Theorem 5
$B17$	$\overline{X \cdot Y} = \overline{X} + \overline{Y}$	DeMorgan's Law	Theorem 5
	$X + X \cdot Y = X$	absorption	Theorem 6
	$X \cdot (X + Y) = X$	absorption	Theorem 6

16 Propositional Logic (Gries/Dijkstra)

Table of Precedences		
(a)	$[x := e]$	(textual substitution) (highest precedence)
(b)	. (function application)	
(c)	unary prefix operators : $+ \ - \ \neg \ \sharp \ \sim$ P	
(d)	$**$	
(e)	$\cdot$ / div **mod gcd**	
(f)	$+ \ - \ \cup \ \cap \ \times \ \circ \ \bullet$	
(g)	$\uparrow \downarrow$	
(h)	$\sharp$	
(i)	$\lhd \ \rhd$ ˆ	
(j)	$= < > \in \subset \subseteq \supset \supseteq \mid$	(conjunctional)
(k)	$\vee \ \wedge$	
(l)	$\Rightarrow \ \Leftarrow$	
(m)	$\equiv$	(lowest precedence)

All nonassociative binary infix operators associate to the left, except $**$, $\lhd$, and $\Rightarrow$, which associate to the right.

The operators on lines (j), (l), and (m) may have a slash / through them to denote negation –e.g. $b \not\equiv c$ is an abreviation for $\neg(b \equiv c)$.

Theorems of the Propositional Calculus

EQUIVALENCE AND *true*

(3.1) Axiom, Associativity of $\equiv$: $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$
(3.2) Axiom, Symmetry of $\equiv$: $p \equiv q \equiv q \equiv p$
(3.3) Axiom, Identity of $\equiv$: $true \equiv q \equiv q$
(3.4) *true*
(3.5) Reflexivity of $\equiv$: $p \equiv p$

NEGATION, INEQUIVALENCE AND *false*

(3.8) Axiom, Definition of *false* : $false \equiv \neg true$
(3.9) Axiom, Distributivity of $\neg$ over $\equiv$: $\neg(p \equiv q) \equiv \neg p \equiv q$
(3.10) Axiom, Definition of $\not\equiv$: $(p \not\equiv q) \equiv \neg(p \equiv q)$
(3.11) $\neg p \equiv q \equiv p \equiv \neg q$
(3.12) Double negation : $\neg\neg p \equiv p$
(3.13) Negation of *false* : $\neg false \equiv true$
(3.14) $(p \not\equiv q) \equiv \neg p \equiv q$
(3.15) $\neg p \equiv p \equiv false$
(3.16) Symmetry of $\not\equiv$: $(p \not\equiv q) \equiv (q \not\equiv p)$
(3.17) Associativity of $\not\equiv$: $((p \not\equiv q) \not\equiv r) \equiv (p \not\equiv (q \not\equiv r))$
(3.18) Mutual associativity : $((p \not\equiv q) \equiv r) \equiv (p \not\equiv (q \equiv r))$
(3.19) Mutual Interchangeability : $p \not\equiv q \equiv r \;\equiv\; p \equiv q \not\equiv r$

DISJUNCTION

(3.24) Axiom, Symmetry of $\vee$: $p \vee q \equiv q \vee p$
(3.25) Axiom, Associativity of $\vee$: $(p \vee q) \vee r \equiv p \vee (q \vee r)$
(3.26) Axiom, Idempotency of $\vee$: $p \vee p \equiv p$
(3.27) Axiom, Distributivity of $\vee$ over $\equiv$: $p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$
(3.28) Axiom, Excluded Middle : $p \vee \neg p$
(3.29) Zero of $\vee$: $p \vee true \equiv true$
(3.30) Identity of $\vee$: $p \vee false \equiv p$
(3.31) Distributivity of $\vee$ over $\vee$: $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$
(3.32) $p \vee q \equiv p \vee \neg q \equiv p$

CONJUNCTION

(3.35) Axiom, Golden rule : $p \wedge q \equiv p \equiv q \equiv p \vee q$
(3.36) Symmetry of $\wedge$: $p \wedge q \equiv q \wedge p$
(3.37) Associativity of $\wedge$: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
(3.38) Idempotency of $\wedge$: $p \wedge p \equiv p$
(3.39) Identity of $\wedge$: $p \wedge true \equiv p$
(3.40) Zero of $\wedge$: $p \wedge false \equiv false$
(3.41) Distributivity of $\wedge$ over $\wedge$: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$
(3.42) Contradiction : $p \wedge \neg p \equiv false$
(3.43) Absortion: (a) $p \wedge (p \vee q) \equiv p$
(b) $p \vee (p \wedge q) \equiv p$
(3.44) Absortion: (a) $p \wedge (\neg p \vee q) \equiv p \wedge q$
(b) $p \vee (\neg p \wedge q) \equiv p \vee q$
(3.45) Distributivity of $\vee$ over $\wedge$: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
(3.46) Distributivity of $\wedge$ over $\vee$: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(3.47) De Morgan: (a) $\neg(p \wedge q) \equiv \neg p \vee \neg q$
(b) $\neg(p \vee q) \equiv \neg p \wedge \neg q$

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

(3.49) $p \wedge (q \equiv r) \equiv p \wedge q \equiv p \wedge r \equiv p$

(3.50) $p \wedge (q \equiv p) \equiv p \wedge q$

(3.51) Replacement : $(p \equiv q) \wedge (r \equiv p) \equiv (p \equiv q) \wedge (r \wedge q)$

(3.52) Definition of $\equiv$: $p \equiv q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

(3.53) Exclusive or : $p \not\equiv q \equiv (\neg p \wedge q) \vee (p \wedge \neg q)$

(3.55) $(p \wedge q) \wedge r \equiv p \equiv q \equiv r \equiv p \vee q \equiv q \vee r \equiv r \vee p \equiv p \vee q \vee r$

IMPLICATION

(3.57) Axiom, Definition of Implication: $p \Rightarrow q \equiv p \vee q \equiv q$

(3.58) Axiom, Consequence : $p \Leftarrow q \equiv q \Rightarrow p$

(3.59) Definition of implication : $p \Rightarrow q \equiv \neg p \vee q$

(3.60) Definition of implication : $p \Rightarrow q \equiv p \wedge q \equiv p$

(3.61) Contrapositive : $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

(3.62) $p \Rightarrow (q \equiv r) \equiv p \wedge q \equiv p \wedge r$

(3.63) Distributivity of $\Rightarrow$ over $\equiv$: $p \Rightarrow (q \equiv r) \equiv p \Rightarrow q \equiv p \Rightarrow r$

(3.64) $p \Rightarrow (q \equiv r) \equiv (p \Rightarrow q) \Rightarrow (p \Rightarrow r)$

(3.65) Shunting : $p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r)$

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

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

(3.68) $p \vee (p \Rightarrow q) \equiv \mathit{true}$

(3.69) $p \vee (q \Rightarrow p) \equiv q \Rightarrow p$

(3.70) $p \vee q \Rightarrow p \wedge q \equiv p \equiv q$

(3.71) Reflexivity of $\Rightarrow$: $p \Rightarrow p \equiv \mathit{true}$

(3.72) Right zero of $\Rightarrow$: $p \Rightarrow \mathit{true} \equiv \mathit{true}$

(3.73) Left identity of $\Rightarrow$: $\mathit{true} \Rightarrow p \equiv p$

(3.74) $p \Rightarrow \mathit{false} \equiv \neg p$

(3.75) $\mathit{false} \Rightarrow p \equiv \mathit{true}$

(3.76) Weakening/strengthening : (a) $p \Rightarrow p \vee q$
(b) $p \wedge q \Rightarrow p$
(c) $p \wedge q \Rightarrow p \vee q$
(d) $p \vee (q \wedge r) \Rightarrow p \vee q$
(e) $p \wedge q \Rightarrow p \wedge (q \vee r)$

(3.77) Modus ponens : $p \wedge (p \Rightarrow q) \Rightarrow q$

(3.78) $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$

(3.79) $(p \Rightarrow r) \wedge (\neg p \Rightarrow r) \equiv r$

(3.80) Mutual implication : $(p \Rightarrow q) \wedge (q \Rightarrow p) \equiv (p \equiv q)$

(3.81) Antisymmetry : $(p \Rightarrow q) \wedge (q \Rightarrow p) \Rightarrow (p \equiv q)$

(3.82) Transitivity : (a) $(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(b) $(p \equiv q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$
(c) $(p \Rightarrow q) \wedge (q \equiv r) \Rightarrow (p \Rightarrow r)$

17 Predicate Logic (Sparkle)

General Logic Axioms and Hypothesis Manipulation

`Exact Hn`	$\dfrac{}{\Gamma, \texttt{Hn:}A \vdash A}$
`Trivial`	$\dfrac{}{\Gamma \vdash \texttt{TRUE}}$
`ExFalso`	$\dfrac{}{\Gamma, \texttt{FALSE} \vdash B}$
`Absurd Hn Hm`	$\dfrac{}{\Gamma, \texttt{Hn:}A, \texttt{Hm:}\neg A \vdash B}$
`Discard Hn`	$\dfrac{\Gamma \vdash B}{\Gamma, \texttt{Hn:}A \vdash B}$
`Assume A`	$\dfrac{\Gamma, A \vdash B \quad \Gamma \vdash A}{\Gamma \vdash B}$

Equivalence Relations

`Reflexive`	$\dfrac{}{\Gamma \vdash A = A}$	$\dfrac{}{\Gamma \vdash A \equiv A}$
`Symmetric`	$\dfrac{\Gamma \vdash A = B}{\Gamma \vdash B = A}$	$\dfrac{\Gamma \vdash A \equiv B}{\Gamma \vdash B \equiv A}$
`Symmetric Hn`	$\dfrac{\Gamma, A = B \vdash C}{\Gamma, \texttt{Hn:}B = A \vdash C}$	$\dfrac{\Gamma, A \equiv B \vdash C}{\Gamma, \texttt{Hn:}B \equiv A \vdash C}$
`Transitive B`	$\dfrac{\Gamma \vdash A = B \quad \Gamma \vdash B = C}{\Gamma \vdash A = C}$	$\dfrac{\Gamma \vdash A \equiv B \quad \Gamma \vdash B \equiv C}{\Gamma \vdash A \equiv C}$

Equality

`Reduce`	$$\frac{}{\Gamma \vdash (\lambda\, v \cdot e_1) e_2 = e_1[e_2/v]}$$
`Reduce`	$$\frac{}{\Gamma \vdash (\lambda\, v \cdot e\ v) = e}$$
`Extensionality`	$$\frac{\Gamma \vdash \forall x \bullet f_1(x) = f_2(x)}{\Gamma \vdash f_1 = f_2}$$
`Rewrite -> Hn`	$$\frac{\Gamma, e_1 = e_2 \vdash A(e_2)}{\Gamma, \texttt{Hn:} e_1 = e_2 \vdash A(e_1)}$$
`Rewrite <- Hn`	$$\frac{\Gamma, e_1 = e_2 \vdash A(e_1)}{\Gamma, \texttt{Hn:} e_1 = e_2 \vdash A(e_2)}$$
`Rewrite -> Hn`	$$\frac{\Gamma, \forall x \bullet e_1 = e_2 \vdash A(e_2)}{\Gamma, \texttt{Hn:} e_1 = e_2 \vdash A(e_1)}$$
`Rewrite <- Hn`	$$\frac{\Gamma, \forall x \bullet e_1 = e_2 \vdash A(e_1)}{\Gamma, \texttt{Hn:} e_1 = e_2 \vdash A(e_2)}$$
`Rewrite -> Hn in Hm`	$$\frac{\Gamma, e_1 = e_2, A(e_2) \vdash B}{\Gamma, \texttt{Hn:} e_1 = e_2, \texttt{Hm:} A(e_1) \vdash B}$$
`Rewrite <- Hn in Hm`	$$\frac{\Gamma, e_1 = e_2, A(e_1) \vdash B}{\Gamma, \texttt{Hn:} e_1 = e_2, \texttt{Hm:} A(e_2) \vdash B}$$
`Rewrite -> Hn in Hm`	$$\frac{\Gamma, e_1 = e_2, A(e_2) \vdash B}{\Gamma, \texttt{Hn:} \forall x \bullet e_1 = e_2, \texttt{Hm:} A(e_1) \vdash B}$$
`Rewrite <- Hn in Hm`	$$\frac{\Gamma, e_1 = e_2, A(e_1) \vdash B}{\Gamma, \texttt{Hn:} \forall x \bullet e_1 = e_2, \texttt{Hm:} A(e_2) \vdash B}$$

Propositional Connectives

`Contradiction`	$\dfrac{\Gamma, A \vdash \mathsf{FALSE}}{\Gamma \vdash \neg A}$
`Contradiction Hn`	$\dfrac{\Gamma, \neg A \vdash A}{\Gamma, \mathtt{Hn:}\neg A \vdash B}$
`Split Deep Hn`	$\dfrac{\Gamma, A, B \vdash C}{\Gamma, \mathtt{Hn:}A \wedge B \vdash C}$
`Split Deep`	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$
`Case Deep Hn`	$\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, \mathtt{Hn:}A \vee B \vdash C}$
`Left`	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$
`Right`	$\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$
`Introduce Hn`	$\dfrac{\Gamma, \mathtt{Hn:}A \vdash B}{\Gamma \vdash A \Rightarrow B}$
`Cut Hn`	$\dfrac{\Gamma, A \vdash A \Rightarrow B}{\Gamma, \mathtt{Hn:}A \vdash B}$
`Apply Hn`	$\dfrac{\Gamma, A \Rightarrow B \vdash A}{\Gamma, \mathtt{Hn:}A \Rightarrow B \vdash B}$
`Apply Hn to Hm`	$\dfrac{\Gamma, A, B \vdash C}{\Gamma, \mathtt{Hm:}A, \mathtt{Hn:}A \Rightarrow B \vdash C}$
`SplitIff`	$\dfrac{\Gamma \vdash A \Rightarrow B \quad \Gamma \vdash B \Rightarrow A}{\Gamma \vdash A \equiv B}$
`SplitIff Hn`	$\dfrac{\Gamma, A \Rightarrow B, B \Rightarrow A \vdash C}{\Gamma, \mathtt{Hn:}A \equiv B \vdash C}$

Quantification

`Introduce x`	$\dfrac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}$	(x not free in Γ)
`Generalize x`	$\dfrac{\Gamma \vdash \forall x.B}{\Gamma \vdash B}$	(x free in B)
`Specialize Hn with t`	$\dfrac{\Gamma, A[t/x] \vdash B}{\Gamma, \texttt{Hn:} \forall x.A \vdash B}$	
`MoveQuantors In`	$\dfrac{\Gamma \vdash A \Rightarrow \forall x.B}{\Gamma \vdash \forall x.A \Rightarrow B}$	(x not free in A)
`MoveQuantors Out`	$\dfrac{\Gamma \vdash \forall x.A \Rightarrow B}{\Gamma \vdash A \Rightarrow \forall x.B}$	(x not free in A)
`Witness t`	$\dfrac{\Gamma \vdash A[t/x]}{\Gamma \vdash \exists x.A}$	
`Witness for Hn`	$\dfrac{\Gamma, A \vdash B}{\Gamma, \texttt{Hn:} \exists x.A \vdash B}$	(x not free in Γ, B)

Induction

`Induction n`	$\dfrac{\Gamma \vdash P(0) \qquad \Gamma \vdash P(n) \Rightarrow P(n+1)}{\Gamma \vdash \forall n : \mathbb{N} \bullet P(n)}$	
`Induction xs`	$\dfrac{\Gamma \vdash P(\langle\rangle) \qquad \Gamma \vdash P(xs) \Rightarrow P(x : xs)}{\Gamma \vdash \forall xs : A^* \bullet P(xs)}$	(x new)
`Induction S`	$\dfrac{\Gamma \vdash P(\emptyset) \qquad \Gamma \vdash P(S) \Rightarrow P(\{x\} \sqcup S)}{\Gamma \vdash \forall S : \mathcal{P}A \bullet P(S)}$	(x new)
`Induction m`	$\dfrac{\Gamma \vdash P(\theta) \qquad \Gamma \vdash P(\mu) \Rightarrow P(\{a \mapsto b\} \sqcup \mu)}{\Gamma \vdash \forall \mu : A \xrightarrow{m} B \bullet P(\mu)}$	(a, b new)

Note: $\sqcup$ is set-union defined only for disjoint arguments, or map extension, defined only for maps with disjoint domains.

Arithmetic/Prop. Calc

$$\texttt{Arithmetic} \qquad \frac{}{\Gamma \vdash e_1 = e_2}$$

if $e_1 = e_2$ provable using the laws of arithmetic.

$$\texttt{Tautology} \qquad \frac{}{\Gamma \vdash T}$$

if T is a propositional tautology.

Conditionals

$$\texttt{Cond True} \qquad \frac{}{\Gamma, B \vdash \textbf{if } B \textbf{ then } e_1 \textbf{ else } e_2 = e_1}$$

$$\texttt{Cond False} \qquad \frac{}{\Gamma, \neg B \vdash \textbf{if } B \textbf{ then } e_1 \textbf{ else } e_2 = e_2}$$

$$\texttt{Conditional} \qquad \frac{\Gamma, B \vdash P \qquad \Gamma, \neg B \vdash Q}{\Gamma \vdash \textbf{if } B \textbf{ then } P \textbf{ else } Q}$$

$$\texttt{Conditional} \qquad \frac{\Gamma, B \vdash A(e_1) \qquad \Gamma, \neg B \vdash A(e_2)}{\Gamma \vdash A(\textbf{if } B \textbf{ then } e_1 \textbf{ else } e_2)}$$

$$\texttt{Conditional} \qquad \frac{\Gamma, B \vdash e = e_1 \qquad \Gamma, \neg B \vdash e = e_2}{\Gamma \vdash e = \textbf{if } B \textbf{ then } e_1 \textbf{ else } e_2}$$

18 Communicating Sequential Processes

CSP Syntax

$$\begin{array}{rcll}
a, c.v & \in & \Sigma & \text{Events} \\
P \in CSP & ::= & STOP & \text{do nothing} \\
& | & SKIP & \text{terminate} \\
& | & a \rightarrow P & \text{prefix} \\
& | & x : A \rightarrow P(x) & \text{choice prefix} \\
& | & a_1 \rightarrow P_1 \mid a_2 \rightarrow P_2 & \text{prefix alternatives} \\
& | & c!v \rightarrow P & \text{output prefix} \\
& | & c?x : T \rightarrow P(x) & \text{input prefix} \\
& | & P_1 \Box P_2 & \text{external choice} \\
& | & P_1 \sqcap P_2 & \text{internal choice} \\
& | & P_1 \; {}_A\|_B \; P_2 & \text{alphabetised parallel} \\
& | & P_1 \; ||| \; P_2 & \text{interleaving parallel} \\
& | & P_1 \underset{A}{\|} P_2 & \text{interface parallel} \\
N_i & = & P_i & \text{definitions}
\end{array}$$

CSP Operational Semantics

Operational Axioms

$$SKIP \xrightarrow{\checkmark} STOP$$

$$(a \rightarrow P) \xrightarrow{a} P$$

$$(x : A \rightarrow P(x)) \xrightarrow{a} P(a) \qquad [a \in A]$$

$$(c!v \rightarrow P) \xrightarrow{c.v} P$$

$$(c?x : T \rightarrow P(x)) \xrightarrow{c.v} P(v) \qquad [v \in T]$$

$$(P_1 \sqcap P_2) \xrightarrow{\tau} P_1$$

$$(P_1 \sqcap P_2) \xrightarrow{\tau} P_2$$

Operational Inferences

$$\frac{P_1 \xrightarrow{a} P_1'}{\begin{array}{l} P_1 \;\Box\; P_2 \xrightarrow{a} P_1' \\ P_2 \;\Box\; P_1 \xrightarrow{a} P_1' \end{array}} \qquad \frac{P_1 \xrightarrow{\tau} P_1'}{\begin{array}{l} P_1 \;\Box\; P_2 \xrightarrow{\tau} P_1' \;\Box\; P_2 \\ P_2 \;\Box\; P_1 \xrightarrow{\tau} P_2 \;\Box\; P_1' \end{array}}$$

$$\frac{P_1 \xrightarrow{\mu} P_1'}{\begin{array}{l} P_1 \;{}_A\|_B\; P_2 \xrightarrow{\mu} P_1' \;{}_A\|_B\; P_2 \\ P_2 \;{}_A\|_B\; P_1 \xrightarrow{\mu} P_2 \;{}_A\|_B\; P_1' \end{array}} \quad [\ \mu \in (A \cup \{\tau\} \setminus B)\ ]$$

$$\frac{\begin{array}{l} P_1 \xrightarrow{a} P_1' \\ P_2 \xrightarrow{a} P_2' \end{array}}{P_1 \;{}_A\|_B\; P_2 \xrightarrow{a} P_1' \;{}_A\|_B\; P_2'} \quad [\ a \in A^{\checkmark} \cap B^{\checkmark}\ ]$$

$$\frac{P_i \xrightarrow{\mu} P'}{N_i \xrightarrow{\mu} P'} \quad [\ [N_i = P_i]\ ]$$

Traces

$$tr \in TRACES \quad = \quad \{tr \mid \sigma(tr) \subseteq \Sigma^{\checkmark} \wedge \#tr \in \mathbb{N} \wedge \checkmark \notin \sigma(init(tr))\}$$

- $\sigma(tr) \subseteq \Sigma^{\checkmark}$: All elements of a trace belong to $\Sigma^{\checkmark}$.
- $\#tr \in \mathbb{N}$: All traces are finite.
- $\checkmark \notin \sigma(init(tr))$: If $\checkmark$occurs in a trace it occurs exactly once, at the end.

Trace Semantics of CSP

$$
\begin{array}{rcl}
traces(STOP) & = & \{\langle\rangle\} \\
traces(a \rightarrow P) & = & \{\langle\rangle\} \cup \{\langle a\rangle \frown tr \mid tr \in traces(P)\} \\
traces(x : A \rightarrow P(x)) & = & \{\langle\rangle\} \cup \{\langle a\rangle \frown tr \mid a \in A \wedge tr \in traces(P(a))\} \\
traces(c!v \rightarrow P) & = & \{\langle\rangle\} \cup \{\langle c.v\rangle \frown tr \mid tr \in traces(P)\} \\
traces(c?m : T \rightarrow P(m)) & = & \{\langle\rangle\} \cup \{\langle c.v\rangle \frown tr \mid v \in T \wedge tr \in traces(P(v))\} \\
traces(SKIP) & = & \{\langle\rangle, \langle\checkmark\rangle\} \\
traces(P_1 \Box P_2) & = & traces(P_1) \cup traces(P_2) \\
traces(P_1 \sqcap P_2) & = & traces(P_1) \cup traces(P_2) \\
traces(P_1 \; {}_A\|_B \; P_2) & = & \{\, tr \in TRACE \mid \sigma(tr) \subseteq (A \cup B)^{\checkmark} \\
& & \qquad \wedge\, tr \upharpoonright A^{\checkmark} \in traces(P_1) \wedge tr \upharpoonright B^{\checkmark} \in traces(P_2) \,\} \\
traces(P \setminus A) & = & \{tr \setminus A \mid tr \in traces(P)\} \\
traces(f(P)) & = & \{f(tr) \mid tr \in traces(P)\} \\
traces(f^{-1}(P)) & = & \{tr \mid f(tr) \in traces(P)\} \\
traces(P_1 \fatsemi P_2) & = & \{tr \mid tr \in traces(P_1) \wedge \checkmark \notin \sigma(tr)\} \\
& & \cup\, \{\, tr_1 \frown tr_2 \mid tr_1 \frown \langle\checkmark\rangle \in traces(P_1) \wedge tr_2 \in traces(P_2) \,\}
\end{array}
$$

Equivalences valid only in Traces model

$$P =_T Q \quad \textbf{iff} \quad traces(P) = traces(Q)$$

$$
\begin{array}{rcllr}
P \Box RUN & =_T & RUN & & \langle \Box\text{−zero}_T \rangle \\
P_1 \sqcap P_2 & =_T & P_1 \Box P_2 & & \langle \text{choice-equiv}_T \rangle \\
P \; {}_A\|_A \; P & =_T & P & \text{if } \alpha(P) \subseteq A & \langle \|\text{−idem}_T \rangle \\
P \; {}_A\|_\Sigma \; STOP & =_T & STOP & & \langle \|\text{−zero}_T \rangle \\
P \;|||\; RUN_\Sigma & =_T & RUN_\Sigma & & \langle |||\text{−zero}_T \rangle \\
P \fatsemi SKIP & =_T & P & & \langle \fatsemi\text{−unit-r}_T \rangle
\end{array}
$$

Laws of CSP

The following laws hold true in the full Failures-Divergences-Infinities Model (FDI).

Prefixes

$$
\begin{array}{rcll}
x : \{\} \to P(x) & = & STOP & \langle STOP\text{– step}\rangle \\
x : \{b\} \to P(x) & = & b \to P(b) & \langle\text{prefix}\rangle
\end{array}
$$

External Choice

$$
\begin{array}{rcll}
P \,\Box\, DIV & = & DIV & \langle\Box\text{–zero}\rangle \\
P \,\Box\, P & = & P & \langle\Box\text{–idem}\rangle \\
P_1 \,\Box\, (P_2 \,\Box\, P_3) & = & (P_1 \,\Box\, P_2) \,\Box\, P_3 & \langle\Box\text{–assoc}\rangle \\
P_1 \,\Box\, P_2 & = & P_2 \,\Box\, P_1 & \langle\Box\text{–sym}\rangle \\
P \,\Box\, STOP & = & P & \langle\Box\text{–unit}\rangle \\
\multicolumn{3}{l}{x : A \to P_1(x) \,\Box\, y : B \to P_2(y)} & \\
 & = & z : (A \cup B) \to R(z) & \langle\Box\text{–step}\rangle \\
\textbf{where } R(c) & = & P_1(c), \quad \text{if } c \in A \setminus B & \\
 & = & P_2(c), \quad \text{if } c \in B \setminus A & \\
 & = & P_1(c) \sqcap P_2(c), \quad \text{if } c \in A \cap B & \\
 & & & \\
\Box_{i \in \{\}} P_i & = & STOP & \langle\Box\text{–unit}\rangle \\
\Box_{i \in I}(x : A_i \to P_i(x)) & = & x : (\bigcup_{i \in I} A_i) \to \sqcap_{\{i \mid x \in A_i\}} P_i(x) & \langle\Box\text{–step}\rangle
\end{array}
$$

Internal Choice

$$
\begin{array}{rcll}
P \sqcap DIV & = & DIV & \langle\sqcap\text{–zero}\rangle \\
P \sqcap P & = & P & \langle\sqcap\text{–idem}\rangle \\
P_1 \sqcap (P_2 \sqcap P_3) & = & (P_1 \sqcap P_2) \sqcap P_3 & \langle\sqcap\text{–assoc}\rangle \\
P_1 \sqcap P_2 & = & P_2 \sqcap P_1 & \langle\sqcap\text{–sym}\rangle \\
P_1 \sqcap (P_2 \,\Box\, P_3) & = & (P_1 \sqcap P_2) \,\Box\, (P_1 \sqcap P_3) & \langle\sqcap\text{–}\Box\text{–distr}\rangle
\end{array}
$$

Alphabetised Parallel

$$
\begin{array}{rcll}
P \parallel DIV & = & DIV & \langle\parallel\text{-zero}\rangle \\
P_1 \,{}_A\!\parallel_{B\cup C} (P_2 \,{}_B\!\parallel_C P_3) & = & (P_1 \,{}_A\!\parallel_B P_2) \,{}_{A\cup B}\!\parallel_C P_3 & \langle\parallel\text{-assoc}\rangle \\
P_1 \,{}_A\!\parallel_B P_2 & = & P_2 \,{}_B\!\parallel_A P_1 & \langle\parallel\text{-sym}\rangle \\
P \,{}_A\!\parallel_B RUN_{(A\cap B)^\checkmark} & = & P \qquad \text{if } \alpha(P) \subseteq A & \langle\parallel\text{-unit}\rangle
\end{array}
$$

$$
\begin{array}{rcll}
\textbf{if } C \subseteq A \wedge D \subseteq B \textbf{ then}: & & & \\
(x : C \rightarrow P_1(x)) \,{}_A\!\parallel_B (y : D \rightarrow P_2(y)) & & & \\
 & = & z : ((C \setminus B) \cup (D \setminus A) \cup (C \cap D)) \rightarrow R(z) & \langle\parallel\text{-step}\rangle \\
\textbf{where } R(c) & = & P_1(c) \,{}_A\!\parallel_B (y : D \rightarrow P_2(y)), \quad \text{if } c \in C \setminus B & \\
 & = & (x : C \rightarrow P_1(x)) \,{}_A\!\parallel_B P_2(c)), \quad \text{if } c \in D \setminus A & \\
 & = & P_1(c) \,{}_A\!\parallel_B P_2(c), \quad \text{if } c \in C \cap D &
\end{array}
$$

$$
\begin{array}{rcll}
SKIP \,{}_A\!\parallel_B SKIP & = & SKIP & \langle\parallel\text{-term 1}\rangle \\
(x : C \rightarrow P(x)) \,{}_A\!\parallel_B SKIP & = & x : C \cap (A \setminus B) \rightarrow (P(x) \,{}_A\!\parallel_B SKIP) & \langle\parallel\text{-term 2}\rangle \\
P \,{}_\Sigma\!\parallel_\Sigma RUN & = & P & \langle\parallel\text{-unit}\rangle
\end{array}
$$

Interleaving

$$
\begin{array}{rcll}
P \interleave DIV & = & DIV & \langle\interleave\text{-zero}\rangle \\
P_1 \interleave (P_2 \interleave P_3) & = & (P_1 \interleave P_2) \interleave P_3 & \langle\interleave\text{-assoc}\rangle \\
P_1 \interleave P_2 & = & P_2 \interleave P_1 & \langle\interleave\text{-sym}\rangle \\
P \interleave RUN_{(A\cap B)^\checkmark} & = & P \qquad \text{if } \alpha(P) \subseteq A & \langle\interleave\text{-unit}\rangle
\end{array}
$$

$$
\begin{array}{rcll}
(x : C \rightarrow P_1(x)) \interleave (y : D \rightarrow P_2(y)) & = & z : (C \cup D) \rightarrow R(z) & \langle\interleave\text{-step}\rangle \\
\textbf{where } R(c) & = & P_1(c) \interleave (y : D \rightarrow P_2(y)), \quad \text{if } c \in C \setminus D & \\
 & = & (x : C \rightarrow P_1(x)) \interleave P_2(c)), \quad \text{if } c \in D \setminus C & \\
 & = & P_1(c) \interleave (y : D \rightarrow P_2(y)) & \\
 & & \sqcap & \\
 & & (x : C \rightarrow P_1(x)) \interleave P_2(c)), & \\
 & & \quad \text{if } c \in C \cap D &
\end{array}
$$

$$
\begin{array}{rcll}
SKIP \interleave SKIP & = & SKIP & \langle\interleave\text{-term 1}\rangle \\
(x : C \rightarrow P(x)) \interleave SKIP & = & x : C \rightarrow (P(x) \interleave SKIP) & \langle\interleave\text{-term 2}\rangle \\
P \interleave SKIP & = & P & \langle\interleave\text{-unit}\rangle
\end{array}
$$

Hiding

$DIV \setminus A$	$=$	DIV	$\langle$hide-zero$\rangle$
$(P \setminus A) \setminus B$	$=$	$P \setminus (A \cup B)$	$\langle$hide-combine$\rangle$
$(a \rightarrow P) \setminus A$	$=$	$\begin{cases} a \rightarrow (P \setminus A), & a \notin A \\ P \setminus A, & a \in A \end{cases}$	$\langle$hide-step 1$\rangle$
$(\sqcap_{i \in I} P_i) \setminus A$	$=$	$\sqcap_{i \in I}(P_i \setminus A)$	$\langle\sqcap$–dist$\rangle$
$STOP \setminus A$	$=$	$STOP$	$\langle$hide-$STOP\rangle$
$(x : C \rightarrow P(x)) \setminus A$	$=$	$x : C \rightarrow (P(x) \setminus A) \quad \text{if } A \cap C = \{\}$	$\langle$hide-step 2$\rangle$
$(x : C \rightarrow P(x)) \setminus A$	$=$	$\sqcap_{x \in C}(P(x) \setminus A) \quad \text{if } C \subseteq A$	$\langle$hide-step 3$\rangle$
$SKIP \setminus A$	$=$	$SKIP$	$\langle$hide-term$\rangle$

Renaming

$f(DIV)$	$=$	DIV	$\langle f(.)$– zero$\rangle$
$f(x : C \rightarrow P(x))$	$=$	$y : f(C) \rightarrow f(P(f^{-1}(y))) \quad \text{if } f \text{ is 1–1}$	$\langle f(.)$– step 1$\rangle$
$f(x : C \rightarrow P(x))$	$=$	$y : f(C) \rightarrow \sqcap_{\{x \mid f(x)=y\}} f(P(x))$	$\langle f(.)$– step 2$\rangle$
$f(SKIP)$	$=$	$SKIP$	$\langle f(.)$– term$\rangle$
$f^{-1}(x : C \rightarrow P(x))$	$=$	$y : f^{-1}(C) \rightarrow f^{-1}(P(f(y)))$	$\langle f^{-1}(.)$– step$\rangle$
$f^{-1}(SKIP)$	$=$	$SKIP$	$\langle f^{-1}(.)$– term$\rangle$

Sequential Composition

$DIV \fatsemi P$	$=$	DIV	$\langle\fatsemi$–zero-l$\rangle$
$P_1 \fatsemi (P_2 \fatsemi P_3)$	$=$	$(P_1 \fatsemi P_2) \fatsemi P_3$	$\langle\fatsemi$–assoc$\rangle$
$(x : C \rightarrow P(x)) \fatsemi P_1$	$=$	$x : C \rightarrow (P(x) \fatsemi P_1)$	$\langle\fatsemi$–step$\rangle$
$SKIP \fatsemi P$	$=$	P	$\langle\fatsemi$–unit-l$\rangle$
$P \fatsemi SKIP$	$=$	P	$\langle\fatsemi$–unit-r$\rangle$

Distributivity over internal choice

$$\begin{array}{rcll}
a \rightarrow (P_1 \sqcap P_2) & = & (a \rightarrow P_1) \sqcap (a \rightarrow P_2) & \langle\text{prefix-dist}\rangle \\
a \rightarrow \bigsqcap_{i \in J} P_i & = & \bigsqcap_{i \in J} (a \rightarrow P_i) & \langle\text{prefix-Dist}\rangle
\end{array}$$

for $\sharp \in \{\Box, {}_A\|_B, |||, \underset{A}{\|}\}$:

$$\begin{array}{rcll}
P_1 \sharp (P_2 \sqcap P_3) & = & (P_1 \sharp P_2) \sqcap (P_1 \sharp P_3) & \langle\sharp\text{– dist}\rangle \\
P_1 \sharp \bigsqcap_{i \in J} P_i & = & \bigsqcap_{i \in J} (P_1 \sharp P_i) & \langle\sharp\text{– Dist}\rangle
\end{array}$$

$$\begin{array}{rcll}
(P_1 \sqcap P_2) \setminus A & = & (P_1 \setminus A) \sqcap (P_2 \setminus A) & \langle\text{hide-dist}\rangle \\
(\bigsqcap_{i \in J} P_i) \setminus A & = & \bigsqcap_{i \in J} (P_i \setminus A) & \langle\text{hide-Dist}\rangle
\end{array}$$

$$\begin{array}{rcll}
f(P_1 \sqcap P_2) & = & f(P_1) \sqcap f(P_2) & \langle f(.)\text{– dist}\rangle \\
f(\bigsqcap_{i \in J} P_i) & = & \bigsqcap_{i \in J} f(P_i) & \langle f(.)\text{– Dist}\rangle
\end{array}$$

$$\begin{array}{rcll}
f^{-1}(P_1 \sqcap P_2) & = & f^{-1}(P_1) \sqcap f^{-1}(P_2) & \langle f^{-1}(.)\text{– dist}\rangle \\
f^{-1}(\bigsqcap_{i \in J} P_i) & = & \bigsqcap_{i \in J} f^{-1}(P_i) & \langle f^{-1}(.)\text{– Dist}\rangle
\end{array}$$

$$\begin{array}{rcll}
(P_1 \sqcap P_2) \fatsemi P_3 & = & (P_1 \fatsemi P_3) \sqcap (P_2 \fatsemi P_3) & \langle \fatsemi\text{–dist-l}\rangle \\
P_1 \fatsemi (P_2 \sqcap P_3) & = & (P_1 \fatsemi P_2) \sqcap (P_1 \fatsemi P_3) & \langle \fatsemi\text{–dist-r}\rangle \\
(\bigsqcap_{i \in J} P_i) \fatsemi P_1 & = & \bigsqcap_{i \in J} (P_i \fatsemi P_1) & \langle \fatsemi\text{–Dist-l}\rangle \\
P_1 \fatsemi (\bigsqcap_{i \in J} P_i) & = & \bigsqcap_{i \in J} (P_1 \fatsemi P_i) & \langle \fatsemi\text{–Dist-r}\rangle
\end{array}$$

Useful Definitions

Manipulating Set Comprehensions

$$\begin{array}{rcll}
\{f(x) \mid x \in \{a\}\} & = & \{f(a)\} & \langle\text{comp-single}\rangle \\
\{f(x) \mid x \in A \cup B\} & = & \{f(x) \mid x \in A\} \cup \{f(x) \mid x \in B\} & \langle\text{comp-split}\rangle \\
\{f(x) \mid x \in \{g(y) \mid y \in A\}\} & = & \{f(g(y)) \mid y \in A\} & \langle\text{comp-nest}\rangle
\end{array}$$

Sequence Notation

A^*	– Sequences of elements of A
$\langle\rangle$	– Empty Sequence
$\langle a, b, c\rangle$	– Sequence of a then b then c
$s_1 \frown s_2$	– Concatenation of s_1 with s_2
s^n	– s concatenated n times ($s^0 = \langle\rangle$)
$head(s)$	– First element of s (undefined if $s = \langle\rangle$)
$tail(s)$	– All but the first element of s (undefined if $s = \langle\rangle$)
$foot(s)$	– Last element of s (undefined if $s = \langle\rangle$)
$init(s)$	– All but the last element of s (undefined if $s = \langle\rangle$)
$\#s$	– Sequence Length

a **in**s	– Assert that a occurs in s
$\sigma(s)$	– Set of all elements in s
$s_1 \leqslant s_2$	– s_1 is a prefix of s_2
$s_1 < s_2$	– $s_1 \leqslant s_2$, but $s_1 \neq s_2$.
$s_1 \leqslant_n s_2$	– s_1 is a prefix of s_2, whose lengths differ by no more than n
$s_1 \preccurlyeq s_2$	– s_1 is a subsequence of s_2 (not necessarily contiguous).
$s \upharpoonright A$	– Sequence s restricted to those elements in A
$s \upharpoonright a$	– Abbreviation for $s \upharpoonright \{a\}$
$s \setminus A$	– Sequence s with elements in A removed
$s \setminus a$	– Abbreviation for $s \setminus \{a\}$
$f(s)$	– Apply function f to every element of s.

A Contributors

Butterfield, Andrew	§ 15 Laws of Boolean Algebra
	§ 17 Predicate Logic
	§ 18 Communicating Sequential Processes
Hägele, Klemens	§ 16 Propositional Logic
Mac an Airchinnigh, Mícheál	§ 1–13
	concept, design, and layout
Sharpe, Mary	§ 13 Queueing Theory
	§ 14 Operations Research

B Sources

§ 10 Category Theory	F. William Lawvere and Stephen H. Schanuel *Conceptual Mathematics, A first introduction to categories* Cambridge University Press, 1997
§ 16 Propositional Logic	David Gries and Fred B. Schneider *A Logical Approach To Discrete Math* Springer-Verlag, 1993
§ 17 Predicate Logic	Malcolm Dowse and Maartens de Mol private communication, 2004
§ 18 Laws of CSP	Steve Schneider *Concurrent and Real-time Systems – The CSP Approach* Wiley, 2000