

Index

- ' (prime), 53, 56–58
- $\mapsto$ (function constructor), 30, 269
- $\models$, 16, 55, 267
- $\setminus$ (set difference), 129, 268
- $\neg$ (negation), 18, 266
- $\rightarrow$ (in cardinal sequence), 32, 59, 270
- $\rightarrow$ (set of functions), 46, 269
- $\rightarrow$ (step), 56
- $\triangleright$ (temporal operator), 262
- $\leadsto$, *see* leads to
- $\dots^+$ (action operator), 59, 113
- $\dots^+$ (suffix operator), 62
- $\dots^\uparrow$ (finite-behavior completion), 81
- $\dots^R$ (reduced version of program), 221
- $[\dots]^+_{\{\dots\}}$, 113, 230
- $\perp$, 259
- F_{+v} , 258–259
- $\times$ (Cartesian product), 31, 270
- $=_y$, 167
- $\simeq_y$, 167
- $\sim_y$, 168
- $\sim_y$, 202
- $\#$ (cardinality), 46, 267, 271
- $\Rightarrow$ (implication), 18, 266
- $\equiv$ (equivalence), 18, 266
- $\triangleq$ (equals by definition), 19
- $\dots$ (integer interval), 22, 267
- $\cdot$, *see* action composition
- $*$ (multiplication), 14
- $\circ$ (sequence concatenation), 128, 270
- $\oplus$, 129
- $\square$ (always), 59, 62–64
 - formula, 96
- $\square\diamond$ (infinitely often), 66–67
- $\diamond$ (eventually), 64–66
- $\diamond\square$ (eventually always), 66
- $\subseteq$ (is a subset of), 22, 267
- $[]_v$ (action operator), 73
- $\llbracket \rrbracket$ (meaning), 14, 15, 22, 55, 60
- $\langle \rangle_v$ (action operator), 77
- $\langle \rangle$ (tuple notation), 31, 269
- $\lfloor \rfloor$, 132
- $\wedge$, *see* conjunction
- $\cap$ (set intersection), 188, 267
- $\vee$, *see* disjunction
- $\cup$ (set union), 188, 267
- $!$ (factorial), 70, 270
- $\%$ (mod), 37, 266
- $\natural$, 75
- $\natural_y$, 168
- $\forall$ (universal quantification), 25, 267
- $\exists$, *see* existential quantification
- $\exists$ (temporal existential quantification),
 - 83, 165–169
 - definition, 167
- $\exists$ (temporal existential quantification)
 - reasoning about, 166–167
- $\exists_{\text{RTLA}}$, 167
- $\in$ (is an element of), 21, 267
- $\notin$ (is not an element of), 99
- $:\in$, 118
- Abadi, Martín, xiv, 115

INDEX

311

- abstract program, 3
- abstraction, 136
- accuracy, 112, 161
- action, 55, 56
 - commuting, 225
- action composition, 58, 277
 - weirdness, 160
- Add* program, 128
- AddS* program, 129
- AddSeq* program, 132
- algebra, 14
- algorithm
 - concurrent, 1
 - distributed, 1, 136
 - Euclid's, *see* Euclid's algorithm
 - Fischer's, 117–121
 - Paxos, 138–144
 - Paxos voting, 139–142
 - random, 47
- Alpern, Bowen, 81
- always, 59
 - possible, 112
- always eventually, 66
 - possible, 113
- and, 18
- Append*, 129, 270
- Apt, Krzysztof, xiv
- arguments of mapping, 32
- arithmetic, 13–14, 266
 - Boolean, 18–21
- array, 46
- array variable, 90
- associative, 20
- ASSUME/PROVE, 79–80, 272
 - with SUFFICES, 147
- assumption (of proof), 272
- atomic operation, 45
- atomicity, grain of, 45, 58
- await** statement, 90
- AWITH, 155
- axiom, 16
- Batson, Brannon, xiv
- beauty, 131
- behavior, 59, 60
 - halting, 39
 - predicate, 76
 - reduced, 224–226
 - Zeno, 121–123
- behavioral property, 5
- Bhagavad Gita, 89
- Boolean, 14
- Boolean arithmetic, 18–21
- bound constant, 57, 60
- bound variable, 22, 26–28
- bounded quantifier, 25
- Broy, Manfred, xiv
- Burns, James E., 98
- $\mathcal{C}$, 84–85
 - operator on metric space, 280
- cardinal sequence, 31, 270
- CASE proof step, 175, 273
- Chandy, K. Mani, xiv
- CHOOSE, 268–269
- circular definition, 29
- clock, hour-minute, 71
- closed set, 280
- coding language, 4
- Cohen, Ernie, xiv
- commutative, 20
- commuting actions, 225
 - left-, 233
 - right-, 233
- completion of a finite behavior, 81
- component, 251
 - composing, 261–265
- composition, 251, 261–265
 - action, *see* action composition
 - theorem, 263

- concatenation of sequences, 128, 270
- concrete program, 5
- concurrent algorithm, 1
- conjunction, 18, 266
 - list, 32–33, 267
- consensus, 136–138
- constant, 55
 - bound, 57, 60
 - prophecy, 217–219
- constant expression, 57
- context, 17, 272
 - of an expression, 27
- correctness, 5
- countable set, 80, 268
- critical section, 88
 - making atomic, 244–247
- current goal (of proof), 147
- data refinement, 126
- datum, 208
- deadlock, 91
 - freedom, 97
- decomposing program, 251, 253–261
- decomposing proof, 255–261
- decomposition theorem, 260
- DEFINE, 273
- define** statement, 132
- definition, 28
 - circular, 29
 - in an expression, 116
 - in proof, 273
 - of TLA, 76–77
 - recursive, 70–71, 187–188, 270–271
- dense set, 281
- Dijkstra, Edsger, xiv, 2, 88
- discrete time, 123–125
- disjunction, 18, 266
 - list, 32–33, 267
- distance function, 279
- distributed algorithm, 1, 136
 - distributes over, 20
- Doligez, Damien, xiv
- DOMAIN, 30, 269
- domain of a function, 30, 269
- Dwork, Cynthia, 136
- $\mathbb{E}$, 87, 155–161
 - computing it, 156–158
 - weirdness, 160
- element, 21
- empty set, 22
- enabled, 87
- enabling condition, 50
- Engberg, Urban, xiv
- engineer, 2
- equivalence, 18
- Euclid's algorithm, 6–9
 - decomposed, 253
 - termination, 69
 - two-process version, 9
 - type correctness, 23
- eventually, 64–66
- eventually always, 66
- EXCEPT, 47, 91, 269
- execution as a state sequence, 7
- existential quantification, 25, 267
 - $\exists$ Elimination, 164, 267
 - $\exists$ Introduction, 163, 267
 - reasoning about, 163
- expression, 14
 - constant, 57
 - context of, 27
 - definition in, 116
 - meaningless, 23–24
 - state, 56
 - step, 55, 56
- F_{12} , 82
- factorial, 70, 270
- failure, 47, 136

INDEX

313

- fairness, 87
 - for history variable, 173
 - semantic definition, 109–110
 - strong, 106
 - weak, 94
- FALSE, 14, 266
- FGSqs* program, 44–46
- FIFO queue, 203–217
- Fischer’s algorithm, 117–121
- Fischer, Michael, 115, 138
- Floyd, Robert, 42
- FLP theorem, 138
- for all, 25
- formula, 14
 - $\Box$, 96
 - state, 56
 - temporal, 60
- Fraenkel, Abraham, 21
- free variable, 27
- function, 30–31, 269
 - of multiple arguments, 32, 269
- GCD, 7
- Gilkerson, Ellen, ii
- goal (of proof), 272
 - current, 147
- Gonthier, Georges, xiv
- grain of atomicity, 45, 58
- Gray, Jim, xiv
- greatest common divisor (GCD), 7
- Greek letters, 15
- Grønning, Peter, xiv
- halting behavior, 39
- Head*, 128, 270
- Herlihy, Maurice, 204
- Hesselink, Wim, 219
- hidden variable, 165
- hierarchically structured proofs, 146–147
- higher-order mapping, 271
- Hilbert, David, 268
- history independence, 35
- history variable, 169–175
- Hoare logic, 58, 161, 276–279
- Hoare, Tony, 276
- Hochstein, Lorin, xiv
- hybrid system, 125
- $\mathbb{I}$ (set of integers), 21, 267
 - is countable, 80
- I1 and I2, 43, 57, 61
- if and only if, 18
- IF/THEN/ELSE, 32, 270
- iff (if and only if), 19
- implementation
 - is implication, 73
 - see also* refinement
- implication, 18
- implies, 18, 19
- Increment* program, 48–51, 53, 61
 - invariance proof, 284–287
- inductive invariant, 43
- infinite-stuttering variable, 186
- infinitely often, 66–67
- Init*, 53
- initial predicate, 41
- input, user, 47
- interface variable, 164
- interleaving description, 265
- internal variable, 164
- interpretation, 15, 55
- invariance property, 8
- invariant, 8, 43
 - inductive, 43
 - type, 43
- Kuppe, Markus, xiv
- Kurshan, Robert, xiv
- LA (Logic of Actions), 55

- labels in pseudocode, 41
- Ladkin, Peter, xiv
- language, coding, 4
- Langworthy, David, xiv
- leads to, 68–69
 - proving, 100–104
- leads-to lattice, 100
- left-commute, 233
- Len*, 129, 270
- LET/IN, 116
- linear-time temporal logic, 59
- linearizable, 204
- Lipton, Richard, 221
- Liskov, Barbara, 136
- livelock, 97
- liveness property, 8
 - another view of, 279–283
 - as dense set, 282
 - definition, 81–82
 - refinement proof, 152
 - traditional program, 86
- LM* algorithm, 105
- lock, 104
- logic
 - Hoare, 58, 161, 276–279
 - predicate, 26, 267
 - propositional, 18–21, 266
 - temporal, 3, 59
- logic of actions, 53–59
- Lynch, Nancy, xiv, 136, 138
- machine closed, 93, 193
- mapping, 14, 28–29
 - arguments of, 32
 - higher-order, 271
 - not a set/value, 29, 274–275
 - refinement, *see* refinement mapping
 - set constructor, 116, 268
 - time-translation, 123
- math, ordinary, 2, 12, 266–271
- mathematical induction
 - simple, 37
 - strong, 37
- Mathglisch, 17
- meaningless expression, 23–24
- Melliars-Smith, Michael, xiv
- Merz, Stephan, xiv
- message passing in Paxos, 142
- meta-formula, 16
- metric space, 279–282
 - of behaviors, 282–283
- model checking, 5
 - catches type errors, 24
 - real-time program, 123
- mutual exclusion, 88
- IN** (set of natural numbers), 22, 267
 - > well-founded on, 176
- negation, 18
- NEW declaration, 272
- Next*, 53
- nondeterminism, 6, 47
 - none in math, 269
- not, 18
- number, real, 13
- OB* algorithm, 98–104, 145–155
- Oki, Brian, 136
- One-Bit algorithm, 98–104, 145–155
- or, 18
- ordinal sequence, 31, 269
- ordinary math, 2, 12, 266–271
- Owicki, Susan, xiv
- Palais, Richard, xiv
- paradox, amusing, 275
- parameter, 29
- partial order, 207
- Paterson, Michael, 138
- Paxos algorithm, 138–144
 - implementation, 144–145

INDEX

315

- Paxos voting algorithm, 139–142
- pc*, 44
- pipelining, 247–251
- plane, infinite, 279
- planetary motion, 34–35, 71
- Plotkin, Gordon, 279
- PlusCal, 45
 - label convention, 41
- Pnueli, Amir, 59
- possibility, 111–114
- postcondition, 276
- precedence, 20
- precondition, 276
- predicate, 14
 - behavior, 76
 - initial, 41
 - state, 76
 - step, 41
- predicate logic, 26, 267
 - in TLA, 76
- process, 1
 - starved, 87, 97
- process** statement, 48
- program
 - abstract, 3
 - concrete, 5
 - decomposing, 251, 253–261
 - real-time, 115–125
 - reduced version, 221
 - traditional, 1
 - written as conjunction, 253–255
- program state, 131
- program variable, 13, 53
- proof
 - assumption, 272
 - by contradiction, 52
 - CASE step, 175, 273
 - correctness, 3
 - decomposing, 255–261
 - goal, 272
 - machine-checked, 5
 - of leads to, 100–104
 - of liveness properties, 66
 - paragraph, 13, 52, 80, 146
 - Q.E.D. step, 53, 273
 - step numbering, 146, 274
 - structured, 3, 52, 146–147, 271–274
 - SUFFICES step, 147
 - terminal, 271
- property, 76
 - behavioral, 5
 - invariance, 8
- prophecy constant, 217–219
- prophecy variable, 187–202
- propositional logic, 18–21, 266
 - in TLA, 76
- Q.E.D. (proof step), 53, 273
- quantification, 25–26
 - existential, 25, 267
 - universal, 25, 267
- quantifier, 25
 - bounded, 25
 - scope of, 26
 - unbounded, 25
- queue, FIFO, 203–217
- $\mathbb{R}$** (set of real numbers), 21, 267
 - as metric space, 279
- real number, 13
- real-time program, 115–125
- recursive definition, 70–71, 187–188, 270–271
- reduced behavior, 224–226
- reduced version of program, 221
- reduction, 220–251
- reduction theorem, 235, 243
- redundancy, 44
- redundancy, 44

- refinement, 126
 - data, 126
 - invariance under, 135
 - proof of liveness, 152
 - proof of safety, 149
 - step, 126
- refinement mapping, 130
 - existence of, 202–203
 - two views of, 131
- right-commute, 233
- Rosetta spacecraft, 10
- RTLA, 59–70
- Russell's paradox, 23, 52
- Russell, Bertrand, 23
- safe scoping rule, 28, 272
- safety property, 8
 - another view of, 279–283
 - as closed set, 282
 - definition, 81–82
 - refinement proof, 149
- satisfies, 56
- Schneider, Fred, xiv, 81
- Scholten, Carel, xiv
- scientist, 2
- scope
 - of a quantifier, 26
 - of variable declaration, 27
- scoping, safe, 28, 272
- semantics, 12, 14
 - of ZF, 22
- semaphore, binary, 104
- Seq*, 129, 270
- sequence
 - cardinal, 31, 270
 - concatenation, 128, 270
 - operators on, 128, 269
 - ordinal, 31, 269
- set, 21, 22
 - closed, 280
 - dense, 281
 - difference, 129, 268
 - enumerated, 22, 267
 - mapping constructor, 116, 268
 - subset constructor, 22, 117, 268
- SF, 106
- Shostak, Robert, xiv
- SI, 75
- skip** statement, 88
- Sqrs* program, 40–43
- starvation of process, 87, 97
- state, 62
 - of Euclid's algorithm, 7
 - program, 131
 - reachable, 112–113
- state expression, 56
- state formula, 56
- state number, 39
- state predicate is TLA formula, 76
- step, 39, 56
 - refinement, 126
 - stuttering, 39
- step expression, 55, 56
- step predicate, 41
- Stockmeyer, Larry, 136
- strong fairness, 106
- stuttering insensitive, 74–75
- stuttering step, 39, 72–74
 - adding after action, 178–181
 - adding before action, 182–183
 - of a program, 75
- stuttering variable, 175–186
 - fairness, 183–186
 - infinite, 186
- subaction, 107
- subset, 22
- subset constructor, 22, 117, 268
- substitution, notation for, 127
- substitutive, 69
- SUFFICES proof step, 147

INDEX

317

- symmetry under time translation, 123
- Tail*, 128, 270
- tautology, 26, 63
- temporal logic, 3, 59
- termination, 5, 8, 39
 - of Euclid's algorithm, 69
- testing, 6
- theorem, 16
 - composition, 263
 - decomposition, 260
 - FLP, 138
- there exists, 25
- TLA, 3
 - definition, 76–77
- TLA⁺, 2, 10, 45
- TLC, 115
- topology, 281
- traditional program, 1
 - liveness property, 86
- transitive, 20
- TRUE, 14, 266
- tuple, 31, 269
- Tuttle, Mark, xiv
- type, 23–24
- type invariant, 43
- $\mathcal{U}$ (until operator), 93–94, 108
- unbounded quantifier, 25
- UNCHANGED, 205
- universal quantification, 25, 267
- valid, 16
- value, 21
- Varacca, Daniele, 110
- variable, 55
 - array, 90
 - auxiliary, 163–219
 - bound, 22, 26–28
 - free, 27
 - hidden, 165
 - hiding, 163–169
 - history, 169–175
 - infinite-stuttering, 186
 - infinitely many, 17
 - interface, 164
 - internal, 164
 - mathematical, 13, 53
 - program, 13, 53
 - prophecy, 187–202
 - stuttering, 175–186
- variable capture, 28
- variables** statement, 40
- Venn diagram, 282
- Verhulst, Eric, 10
- Virtuoso, 10
- Vogt, Friedrich H., xiv
- Völzer, Hagen, 110
- weak fairness, 94
- well-founded relation, 176, 187
- WF, 94
- while** statement, 40
- Wing, Jeannette, 204
- WITH (substitution), 127, 270
- x** (list notation), 84
- y** (list notation), 202
- Yu, Yuan, xiv
- Zeno behavior, 121–123
- Zermelo, Ernst, 21
- ZF set theory, 21–23