Index

Note: Page numbers followed by *f* indicate figures.

A

Abstract interpretation techniques, 334
Adiabatic quantum computation, 328
Algebraic laws
  quantum case statements, 241–244
  quantum choice, 242–243
Annihilation operator, 294–295
Associative law
  quantum case statements, 242
  quantum choice, 243
Average running time, 171, 173
Axiomatic system, 123–130

B

Birkhoff-von Neumann quantum logic, 4–5, 104, 253–254
Bit flip channel, 144
Bloch sphere, 32–33
Bosons, 285
  coherent state, 318
  Fock space, 290
Bottom strongly connected component (BSCC), 179–183
  application, 182–183
  characterizations of, 181–182
  decomposition, 185–188
  quantum Markov chain, 192
Bound function
  Floyd-hoare logic, 137
  of quantum loop, 130–132

C

Categorical semantics, 331–332
Circuits, quantum
  controlled gates, 33–34
  definitions, 29–31, 57
  measurement in, 37–38
  one-qubit gates, 32–33
  principle of deferred measurement, 38
  quantum multiplexor, 34–36
  universality of gates, 36–37
Classical case statement in quantum programming, 6, 212
  quantum generalization, 64
  recursive equation with, 320–321
Classical choice, 236
Classical graph, 176–177, 179
Classical programming theory
  algebraic approach, 241
  case statement in, 212
  Floyd-Hoare logic, 111
  recursive equations, 90–91
  syntactic approximation, 282, 303–304
  weakest precondition, 105–106
Classical recursion in quantum programming, 85–94, 273, 295
Classical states, QuGCL semantics, 227–228
Coin-tossing operator, 172
Commutative law
  quantum case statements, 242
  quantum choice, 243
Completeness
  Floyd-Hoare logic, 114–118
  proof system for qPD, 128
  proof system *qTD*, 136–137
Complete partial order (CPO), 77, 297, 311
Concurrent quantum programming, 333
Control flows, 214, 270
  classical, 64
  in lambda calculus, 7
  quantum, 4, 211
  superposition of, 214
Controlled gates
  properties of, 33
  quantum circuits, 33–34
  quantum multiplexor, 34
Copy rule, 306–307
CPO. *See* Complete partial order (CPO)
Creation operator, 294, 322–324

D

Deferred measurement principle, 38
Denotational semantics
  divergence probabilities, 81–83
  of loop, 78–80
  properties of, 75–76
  quantum domains, 76–78
  as quantum operations, 83–85
  of quantum program, 73–74
  recursive quantum program, 87–90
  termination, 81–83

Density operators, 107, 152
in Hilbert space, 25
partial, 65, 77, 108, 118, 121
quantum mechanics, 25–27
reduced, 26
Deutsch-Jozsa algorithm, 41–43, 42*f*, 331
Directed graph, 175–179
Distributive law
quantum case statements, 242
quantum choice, 244

E

Eigenvalues, 157, 159
Entanglement in quantum programming, 333–334
Expectation of observable at outputs, 169–170

F

Fermions, 285
Fock space, 290
Fixed point semantics, 302–303
Floyd-Hoare logic, 103, 336
correctness formulas, 111–114
Grover algorithm, 123, 137–143, 138*f*
partial correctness, 112–114, 123–130
soundness, 124
total correctness, 112–114, 130–137, 133*f*
weakest preconditions, 114–123
while-language, 111–112, 114–115, 118, 121–122
Fock spaces, 287–290
creation functional, 301–302
definition, 287
domain of operators in, 295–299
evolution in, 293–294
extensive observable in, 292
many-body observables, 291
observables in, 292–293
operators in, 289
principle of symmetrization, 288
symmetrization functional, 311–312
Functional quantum programming, 330–331

G

Generalized quantum program scheme, 303–306
Graph
classical, 176–177, 179
directed, 175–179
quantum walks on, 49
Grover algorithm, 95–97, 96*f*, 123, 137–143, 138*f*
correctness formula for, 139
correctness using axiom, 142
performance analysis, 45
search problems, 43–47, 46*f*
termination of loop, 141
verification of loop body, 140
Grover rotation, 44, 44*f*
Guarded Command Language (GCL)
extensions, 270
qGCL, 270
QuGCL, 215–218

H

Hadamard transformation, 72, 95
Harrow-Hassidim-Lloyd algorithm, 57
Hermitian operator, 4, 20
Hilbert space, 104
operator mapping, 108
quantum predicate, 104–105
spectral decomposition theorem, 97–98
Hilbert spaces, 163
asymptotic average, 184
decomposition, 183–189
density operators in, 25
fixed point state, 184
Hermitian operator, 104
operator-valued functions in, 221–222
quantum mechanics, 12–15
quantum predicate in, 104
quantum systems, 26, 291
state decomposition, 183–189
tensor products of, 22–25
transient subspaces, 183
Hoare triple, 111–112

I

Idempotent law
quantum case statements, 242
quantum choice, 243
Imperative quantum programming, 330

J

Jordan decomposition, 156, 167, 202–203
Jordan normal form theorem, 155–156

K

Knaster-Tarski theorem, 77, 92–94
Kraus operator-sum representation, 106–107, 163, 176, 180, 220–221, 261–269

L

Lattice theory, 76
Linear operators
  matrix representation of, 17
  quantum mechanics, 15–18
Löwner order
  definition, 17, 77
  quantum operations, 77–78, 233

M

Matrix representation, 163
Measurement-based quantum computation, 328–329
Model-checking quantum systems, 334–336
Multiple-particle states
  Pauli's exclusion principle, 286
  permutation operators, 284
  principle of symmetrization, 285
  second quantization, 283–286

N

Nontermination probability, 152, 162

O

One-dimensional quantum walks, 47, 277
One-qubit gates, 32–33
Operational semantics
  recursive quantum program, 86–87
  while-language, 65–73
Operator-valued functions
  coefficients in, 250–253
  definition, 220–221
  guarded composition of, 221–224, 255–256
  in Hilbert space, 221–222
  semi-classical semantic function, 234–236

P

Partial density operator, 118
  domain of, 77
  operator mapping, 108
Pauli matrix, 72
Pauli's exclusion principle, 286
PCTL. *See* Probabilistic computation tree logic (PCTL)
Permutation operators, 284
Phase estimation, 55*f*, 247–249
  performance analysis, 56
  quantum algorithms, 54–57
Phase flip channel, 144
Principal system semantics, 313–314
Principle of symmetrization
  Fock space, 288
  multiple-particle states, 285
Probabilistic choice, 237–238
  definition, 237
  quantum implementation, 238–241
Probabilistic computation tree logic (PCTL), 335
Process algebras, 332
Programming paradigm, 6–7, 238
Projective measurements
  definition, 21
  quantum mechanics, 20, 24
Purely quantum semantics, 252–253, 258, 262
  of block command, 239
  probabilistic choice, 239
  QuGCL, 230–232
Pure states, 68, 69*f*

Q

QCTL. *See* Quantum computation tree logic (QCTL)
QMUX. *See* Quantum multiplexor (QMUX)
QPL, 329–330
Quantm while-loops (with quantum control), 319–324
Quantum algorithms, 57
  Deutsch-Jozsa algorithm, 41–43, 42*f*
  Grover search algorithm, 43–47, 44*f*, 46*f*
  phase estimation, 54–57
  quantum Fourier transform, 52–54
  quantum interference, 40
  quantum parallelism, 39
  quantum walks
    on graph, 49
    one-dimensional, 47
    search algorithm, 50–52
Quantum case statements, 211–212
  algebraic laws, 241–244
  associative law, 242
  from classical to quantum, 212–215
  commutative law, 242
  control flows, 214, 270
  denotational semantics, 215
  distributive law, 242
  guarded by subspaces, 253–255
  guarded compositions
    operator-valued functions, 221–224
    quantum operation, 224–226
    unitary operators, 218–219
  idempotent law, 242
  proofs of lemmas, propositions and theorems, 255–270

Quantum case statements *(Continued)*
quantum choice and, 236–241, 252
QuGCL, 215–218
refinement techniques, 233
semantics of QuGCL, 226–236
shift operator, 213
Quantum choice, 236–241
algebraic laws, 242–243
associative law, 243
commutative law, 243
distributive law, 244
idempotent law, 243
parameterized, 252
probabilistic choice *vs.*, 237–241
Quantum circuits
controlled gates, 33–34
definitions, 29–31, 57
measurement in, 37–38
one-qubit gates, 32–33
principle of deferred measurement, 38
quantum multiplexor, 34–36
universality of gates, 36–37
Quantum computation, 3
adiabatic, 328
cluster state, 328
measurement-based, 328
nonstandard models of, 327
teleportation, 328
topological, 329
Quantum computation tree logic (QCTL), 335
Quantum concurrency, 333
Quantum control flow, 211, 214, 270
Quantum domains, 76–78
complete partial order, 76
partial order, 76
Quantum Fourier transform, 52–54
Quantum gates
controlled gates, 33–34
one-qubit gates, 32–33
and quantum circuits, 30
universality of gates, 36–37
Quantum graph theory
BSCC, 179–183
definitions, 175–179
partial density operator, 175
quantum Markov chains, 174–177
state Hilbert space decomposition, 183–189
Quantum interference, 40, 48, 280–281
Quantum logic, 331
Birkhoff-von Neumann, 253–254
effect, 105
unitary transformations, 19
Quantum Markov chains, 335
BSCC decomposition for, 179–189
definition, 175
graph structures of, 189
persistence probability, 195–197
reachability analysis of, 174
reachability probability, 189–191
reachable space, 177
repeated reachability probability, 191–196
Quantum measurements, 19–22
Quantum mechanics
definition, 11–12, 57
density operators, 25–27
Hilbert spaces, 12–15
linear operators, 15–18
postulate of, 14, 19, 23
projective measurements, 20, 24
quantum measurements, 19–22
quantum operations, 27–29
reduced density operators, 26
tensor products of Hilbert spaces, 22–25
unitary transformations, 18–19
Quantum Model-Checker (QMC), 334
Quantum multiplexor (QMUX), 14, 219
in circuits, 34–36
matrix representation of, 36
Quantum operations, 27–29, 226
coefficients in, 250–253
example, 225
guarded compositions of, 224–226
Löwner order, 233
semantic functions as, 83–85
Quantum parallelism, 3, 39
Quantum phase estimation, 55*f*, 247–249
performance analysis, 56
quantum algorithms, 54–57
Quantum predicates, 124, 128, 133, 136
Birkhoff-von Neumann quantum logic, 104
commutativity problem, 143–148
completeness, 128, 136
definition, 103–104
Floyd-Hoare logic, 103, 111–143
Hermitian operator, 104–105
Hilbert space, 104
logic for, 103
soundness, 124, 133
weakest preconditions, 105–111
Quantum process algebras, 332
Quantum programming languages
applied to physics, 335–336

categorical semantics of, 331–332
classical recursion in, 85–94
compilation techniques, 330
definition, 3
design of, 4
entanglement in, 333–334
functional, 330–331
implementation, 329–330
semantics of, 4–5
superposition-of-data paradigm
classical control, 6–7
quantum control, 7
superposition-of-programs paradigm, 238
and Turing machines, 327
verification and analysis, 5
Quantum Random Access Machine (QRAM) model, 3
Quantum recursive programs, 85, 273
denotational semantics, 87–90
fixed point characterization, 90–94
Fock spaces, 287–290
copy rule, 306–307
creation functional, 301–302
definition, 287
domain of operators in, 295–299
evolution in, 293–294
fixed point semantics, 302–303
many-body observables, 291
observables in, 292–293
operators in, 289
principle of symmetrization, 288
semantic functionals of program schemes, 299–302
symmetrization functional, 311–312
syntactic approximation, 303–310
lambda calculus, 324
operational semantics, 86–87
principal system semantics, 313–314
program schemes, 274–275
quantum while-loops, 319–324
recursive quantum walks, 274
bidirectionally, 278
examples, 315–319
solve recursive quantum equations, 282–283
specification of, 277–281
variant of bidirectionally, 278, 281
second quantization, 273
creation and annihilation of particles, 294–295
Fock spaces, 287–290, 293–294
multiple-particle states, 283–286
observables in Fock spaces, 291–293
symmetry and antisymmetry, 310–313
syntax, 85–86, 273–277
transition rule for, 87*f*
Quantum register, 29–30
Quantum systems
continuous-time dynamics, 18
dynamic logic formalism, 5
of fixed number, 287
Hilbert spaces, 26, 291
in mixed states, 25–26
model-checking, 334–336
open, 27–28
Quantum Turing machines, 327
Quantum variables
block command, 84, 239
change and access of, 80
partial density operator, 81–82
in while-loops, 111–112
Quantum walks
example, 244–247
on graph, 49
one-dimensional, 47
recursive, 274
bidirectionally, 278, 316
examples, 315–319
solve recursive quantum equations, 282–283
specification of, 277–281
unidirectionally, 315
variant of bidirectionally, 278, 281
search algorithm, 50–52
shift operator, 213, 215
Quantum while-language, 319–324
almost sure termination, 165
classical control flow, 64
control flow, 211
example, 172–173
Floyd-Hoare logic for, 123, 143
general, 159–172
nondeterminism, 73
operational semantics, 65–73
programs, 115
quantum configuration, 66
for quantum loop, 122
quantum variables in, 111–112
syntax, 62–65
termination, 141
transition rules for, 67*f*, 68

Quantum while-loops, 163
QuGCL programs
  alphabet, 215–216
  definition, 216
  design, 217–218
  probabilistic choice, 238–239
  quantum phase estimation, 247–249
  quantum walks, 244–247
  semantics
    classical states, 227–228
    example, 234–236
    notations, 226–227
    purely quantum, 230–232
    semi-classical, 228–230
    weakest precondition, 232–233
  syntax of, 217

R

Ranking function, 130
Recursive quantum program, 85, 89, 92–95, 207
Recursive quantum walks, 274
  bidirectionally, 278, 316
  examples, 315–319
  solve recursive quantum equations, 282–283
  specification of, 277–281
  unidirectionally, 315
  variant of bidirectionally, 278, 281

S

SCC. *See* Strongly connected component (SCC)
Schrödinger equation, 18
Schrödinger-Heisenberg duality, 108, 109*f*
Search algorithm
  Grover search algorithm, 43–47, 44*f*, 46*f*
  quantum walks, 50–52
Second quantization, 273
  creation and annihilation of particles, 294–295
  Fock spaces, 287–290
    definition, 287
    evolution in, 293–294
    many-body observables, 291
    observables in, 291–293
    operators in, 289
    principle of symmetrization, 288
  multiple-particle states, 283–286
Semantic functionals of program schemes, 299–302
Semantics
  fixed point, 302–303
  principal system, 313–314
  quantum case statements, 215
  QuGCL program
    classical states, 227–228
    example, 234–236
    notations, 226–227
    purely quantum semantic, 230–232
    semi-classical semantic, 228–230
    weakest precondition semantic, 232–233
Semi-classical semantics
  of program, 264
  QuGCL, 228–230
Sequential Quantum Random Access Memory machine (SQRAM), 329–330
Shift operator, 173
  case statements, quantum, 213
  quantum walks, 213, 215
  quantum while-loops, 173
Shor algorithm for factoring, 57
Soundness, 124, 133
State Hilbert space
  asymptotic average, 184
  decomposition, 183–189
  fixed point state, 184
  transient subspaces, 183
Strongly connected component (SCC), 180–181
Subspaces
  quantum case statements guarded by, 253–255
  transient subspaces, 183
Superposition of control flows, 214
Superposition-of-programs, 7
  definition, 238
  idea of, 238
  paradigm, 211
Syntactic approximation, 303–310
Syntactic approximation, definition, 306
Syntax
  QuGCL programs, 217
  recursive quantum program, 85–86, 273–277
  while-language, 62–65
System-environment model, 106–108, 147

T

Teleportation quantum computation, 328
Tensor products, of Hilbert spaces, 22–25
Termination problem, 154
Toffoli gate, 34
Topological quantum computation, 329
Total correctness, 137–138
Transition rules
  pure states, 68, 69*f*

Transition rules *(Continued)*
recursive quantum program, 87*f*
while-language, 67*f*
Trojan Horse, 334

U

Unitary operators, guarded compositions of, 218–219, 271
Unitary transformations
in Hilbert space, 28
quantum mechanics, 18–19
quantum recursive programs, 274
Universality of gates, 36–37

W

Weakest preconditions
Floyd-Hoare logic, 114–123
Quantum predicates, 105–111
QuGCL semantics, 232–233