Index

J-decomposition, 250
x-rotation, 263
z-rotation, 264
dEQPL, 390
2-colorable underlying graph, 252
Aaronson-Gottesman algorithm, 441
abstract domain, 228
abstract interpretation, 207
abstract semantics, 208
denotational, 229
soundness, 209
abstraction function, 223
adequacy, 217
adjoint functor theorem, 384
Audenaert-Plenio algorithm, 450
auxiliary qubits, 173
axioms of PdEQPL, 394
basis structure, 30
BB84
quantum coin-flipping protocol, 459
quantum key distribution protocol, 415, 416, 461
Bell pair, 237
Bell state, 2, 15–17, 32, 75
Bell’s experiment, 138
Bell’s theorem, 16
bicategory, 33, 35, 45
cartesian bicategory of relations, 46
dagger cartesian bicategory of relations, 46, 47
bipartite normal form, 450, 451
bit flip, 329
Boolean lattice, 361
box, 111
bra-vector, 211
broadcasting, 67
call-by-value reduction, 153
cartesian closed category, 72
categorical
logic, see logic, categorical
quantum mechanics, 1, 6–18, 29
category
*-autonomous, 5, 8, 26, 72
cartesian closed, 2–5, 24
compact, see category, compact closed
compact closed, 9–12, 14, 19, 24, 26, 31, 33, 376
dagger, 11, 247
dagger compact, 11, 12, 20, 26, 33
dagger symmetric monoidal, 11, 12, 31
indexed, 29, 61
inverse, 370
Kleisli, 29, 51–53, 57
monoidal, 6, 7, 18
monoidal closed, 376
of circuits, 94
of commutative monoids, 99
of finite-dimensional vector spaces, 9
generalized proof-nets, 122
of matrices, 100
of relations, 7, 9
symmetric monoidal, 7–9, 11–13, 18, 21, 31
total, 29, 61
traced monoidal, 87
Cauchy sequence, 315
causal flow, 283
circuit model, 236
classical interface, 30, 56, 60
classical structure, 30, 33–41, 45, 46, 48, 50, 53, 57
Clifford group, 419, 444
normal form, 450
operator, 419
Clifford group, 238
cloning, 154
axiomatization, 18
uniform, 19, 25, 26
cloning collapse theorem, 19, 25
CNOT, 265
combinatory logic, 376
communicating quantum processes, see CQP
comonad, 165
compact closed category, 84
compact closure, 9
compact structure, 32
compact symmetric polycategory, 72, 91
comparison formulae, 391
complete lattice, 335
computation as patterns, 238
computational depth complexity, 260
coname, 10, 14, 17, 86
partial, 86
correction commands, 240
counit, 9, 12, 14, 85
determinism, 247
Deutsch’s algorithm, 189
Deutsch’s problem, xi
Deutsch-Jozsa algorithm, 137, 145
diagrammatic morphism, 7, 19, 20, 24, 25
dimension, 33, 89
Dirac notation, 13
direct decomposition, 280
directed complete partial order (DCPO), 214
domain of signal, 240
domain theory, 213
dualizing object, 5
nenrichment over commutative monoids, 99
entangled functions, 135
entanglement, 2, 15, 21, 25, 226, 236
quantum information theory, 227
entanglement analysis, 225
entanglement commands, 240
EPR paradox, 225
EPR state, 15
EQPL (exogenous quantum propositional logic)
complexity of model checking, 450
extensions, 455
semantics, 435
syntax, 435
verification algorithms, 447
error states, 150
exogenous logic, 390
exponential, 141
finite-dimensional Hilbert space, 73
flow
causal, 291
generalized, 286
graphical interpretation, 286
maximally delayed, 289
optimal, 289
formal methods, 389
formal specification
quantum coin-flipping, see quantum coin-flipping protocol, model checking
quantum error correction, see quantum error-correction protocol, model checking
quantum key distribution, see quantum key distribution protocol, model checking
quantum teleportation, see quantum teleportation protocol, model checking
formal verification
quantum coin-flipping, see quantum coin-flipping protocol, model checking
quantum error correction, see quantum error-correction protocol, model checking
quantum key distribution, see quantum key distribution protocol, model checking
quantum teleportation, see quantum teleportation protocol, model checking
free category, 72
free compact closed category, 89
Frobenius algebra, 34, 49
commutative, 34, 51
special, 34
special commutative, 33, 34
special dagger, 30
condition, 34, 35
dagger structure, 25
functor
monoidal, 18
generalized flow
algorithm, 291
generalized proof-nets, 108
geometry of interaction, 378
GHZ, 266
Gottesman-Knill theorem, 419
graphical calculus, 16, 20, 31, 33, 35
Grothendieck construction, 29, 61
Hadamard operator, 242, 249
Hadamard transformation, 184
Haskell, 135, 173
Hermitian operators
quantum predicates, 324
hierarchy of quantum semantics, 224
Hilbert space, 315, 361
lattice of projectors, 363
subspace, 337
incompatible observables, 36
induction rules, 357
influencing walks, 297
Pauli, 299
interval analysis, 209
inverse category, 369
involution, 90
Joyal’s lemma, 4, 5, 24
Jozsa conjecture, 297
ket-vector, 211
Kleisli adjunction, 52
Kleisli category, see category, Kleisli, 164
Knaster-Tarski fixed point theorem, 349
Kraus decomposition, 246
Kraus representation theorem, 221
Kripke structure, 398
Löwner partial order, 316
lambda calculus, 71, 135
linear, 72
quantum, 139
lazy evaluation, 175
limits of quantum computation, 236
Lindenbaum-Tarski algebras, 361
linear exponential comonad, 165
linear logic, 141, 151
LISP, 135
logic
categorical, 2
category-theoretic, 375
classical, 4
epistemic, 417
exogenous, 390
exogenous quantum propositional, see EQPL
intuitionistic, 3–5, 71
intuitionistic multiplicative linear, 72
linear, 71, 379
multiplicative linear, 5, 9
quantum computation tree, see QCTL
temporal, 397, 414
loop, 90, 103
majorization, 50
MBQC
denotational semantics, 245
operational semantics, 244
semantics, 243
syntax, 240
universality, 249
versus circuit, 296
measurement, 236
measurement-based quantum computation, see MBQC
measurement calculus, 253
confluence, 257
extended, 292
termination, 255
measurement pattern, 240, 241
mixed state, 38, 77
mixing, 54
mixture, 54
ML, 135
model checking, 411, 414–416
modularity, 214
monoidal tensor, 376
monads, 178
monoidal category, 82, 161
<table>
<thead>
<tr>
<th>Index</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>monoidal comonad (symmetric), 165</td>
<td>476</td>
</tr>
<tr>
<td>monoids, 178</td>
<td></td>
</tr>
<tr>
<td>monotonic, 214</td>
<td></td>
</tr>
<tr>
<td>morphism</td>
<td></td>
</tr>
<tr>
<td>classical, 37</td>
<td></td>
</tr>
<tr>
<td>completely positive, 38</td>
<td></td>
</tr>
<tr>
<td>decoherent, 40</td>
<td></td>
</tr>
<tr>
<td>doubly stochastic, 50</td>
<td></td>
</tr>
<tr>
<td>positive, 37</td>
<td></td>
</tr>
<tr>
<td>real, 41</td>
<td></td>
</tr>
<tr>
<td>stochastic, 50</td>
<td></td>
</tr>
<tr>
<td>name, 10, 14, 17, 86</td>
<td></td>
</tr>
<tr>
<td>partial, 86</td>
<td></td>
</tr>
<tr>
<td>natural deduction, 71</td>
<td></td>
</tr>
<tr>
<td>natural transformation</td>
<td></td>
</tr>
<tr>
<td>monoidal, 18, 19, 26</td>
<td></td>
</tr>
<tr>
<td>Newman’s lemma, 260</td>
<td></td>
</tr>
<tr>
<td>no-broadcasting theorem, 1</td>
<td></td>
</tr>
<tr>
<td>no-cloning theorem, 1, 19, 34</td>
<td></td>
</tr>
<tr>
<td>no-cloning theorem, 141</td>
<td></td>
</tr>
<tr>
<td>no-deleting theorem, 1, 26, 34</td>
<td></td>
</tr>
<tr>
<td>no-go theorem, 2, 25</td>
<td></td>
</tr>
<tr>
<td>NP-completeness, 449, 468</td>
<td></td>
</tr>
<tr>
<td>one-way model, 237</td>
<td></td>
</tr>
<tr>
<td>open graph</td>
<td></td>
</tr>
<tr>
<td>extended, 293</td>
<td></td>
</tr>
<tr>
<td>labelled, 276</td>
<td></td>
</tr>
<tr>
<td>operational semantics, 146</td>
<td></td>
</tr>
<tr>
<td>QMCLang, see QMCLang, semantics</td>
<td></td>
</tr>
<tr>
<td>orthomodular lattice, 361, 363</td>
<td></td>
</tr>
<tr>
<td>orthomodular lattices, 335</td>
<td></td>
</tr>
<tr>
<td>orthomodular law, 335</td>
<td></td>
</tr>
<tr>
<td>orthonormal basis, 270</td>
<td></td>
</tr>
<tr>
<td>parity analysis, 208</td>
<td></td>
</tr>
<tr>
<td>partial isometry, 362, 365</td>
<td></td>
</tr>
<tr>
<td>category, 369</td>
<td></td>
</tr>
<tr>
<td>physical, 366</td>
<td></td>
</tr>
<tr>
<td>partial order, 366</td>
<td></td>
</tr>
<tr>
<td>path</td>
<td></td>
</tr>
<tr>
<td>extreme, 252</td>
<td></td>
</tr>
<tr>
<td>pattern</td>
<td></td>
</tr>
<tr>
<td>circuits, 300</td>
<td></td>
</tr>
<tr>
<td>computation space, 242</td>
<td></td>
</tr>
<tr>
<td>stepwise deterministic, 248</td>
<td></td>
</tr>
<tr>
<td>synthesis, 281</td>
<td></td>
</tr>
<tr>
<td>tensor, 243</td>
<td></td>
</tr>
<tr>
<td>type, 242</td>
<td></td>
</tr>
<tr>
<td>patterns, see measurement patterns</td>
<td></td>
</tr>
<tr>
<td>Pauli</td>
<td></td>
</tr>
<tr>
<td>group, 418, 443</td>
<td></td>
</tr>
<tr>
<td>measurements, 295</td>
<td></td>
</tr>
<tr>
<td>model, 268</td>
<td></td>
</tr>
<tr>
<td>operator, 78, 238, 418, 441, 443</td>
<td></td>
</tr>
<tr>
<td>spin matrices, 249</td>
<td></td>
</tr>
<tr>
<td>permutation, 49</td>
<td></td>
</tr>
<tr>
<td>phase flip, 329</td>
<td></td>
</tr>
<tr>
<td>phase map decomposition, 239</td>
<td></td>
</tr>
<tr>
<td>phase model, 267</td>
<td></td>
</tr>
<tr>
<td>picture calculus, see graphical calculus</td>
<td></td>
</tr>
<tr>
<td>point, 86</td>
<td></td>
</tr>
<tr>
<td>polycategorical, 247</td>
<td></td>
</tr>
<tr>
<td>polycategory, 72</td>
<td></td>
</tr>
<tr>
<td>polymorphic functions, 175</td>
<td></td>
</tr>
<tr>
<td>predicate transformers</td>
<td></td>
</tr>
<tr>
<td>projective, 337</td>
<td></td>
</tr>
<tr>
<td>preorder, 213</td>
<td></td>
</tr>
<tr>
<td>PRISM model checker, 416</td>
<td></td>
</tr>
<tr>
<td>projection-based quantum computing, 275</td>
<td></td>
</tr>
<tr>
<td>projective weakest preconditions, 341</td>
<td></td>
</tr>
<tr>
<td>proof-net, 77</td>
<td></td>
</tr>
<tr>
<td>proof-nets</td>
<td></td>
</tr>
<tr>
<td>local confluence, 118</td>
<td></td>
</tr>
<tr>
<td>subject reduction, 117</td>
<td></td>
</tr>
<tr>
<td>termination of reduction, 118</td>
<td></td>
</tr>
<tr>
<td>proof-slice, 109</td>
<td></td>
</tr>
<tr>
<td>pure quantum evolution, 55</td>
<td></td>
</tr>
<tr>
<td>pure quantum measurement, 56</td>
<td></td>
</tr>
<tr>
<td>pure quantum state, 55, 77</td>
<td></td>
</tr>
<tr>
<td>purely functional approach, 174</td>
<td></td>
</tr>
<tr>
<td>QCTL (quantum computation tree logic), 397</td>
<td></td>
</tr>
<tr>
<td>complexity of model checking, 455</td>
<td></td>
</tr>
<tr>
<td>interpretation over QMC models, 438</td>
<td></td>
</tr>
<tr>
<td>semantics, 437</td>
<td></td>
</tr>
<tr>
<td>syntax, 437</td>
<td></td>
</tr>
<tr>
<td>verification algorithms, 452</td>
<td></td>
</tr>
<tr>
<td>QIL, 212</td>
<td></td>
</tr>
<tr>
<td>program, 212</td>
<td></td>
</tr>
<tr>
<td>QIO monad, 183</td>
<td></td>
</tr>
<tr>
<td>QMC (quantum model checker), 416, 439</td>
<td></td>
</tr>
<tr>
<td>case studies, 456–466</td>
<td></td>
</tr>
<tr>
<td>complexity, 445</td>
<td></td>
</tr>
<tr>
<td>graphical user interface, 439</td>
<td></td>
</tr>
<tr>
<td>interpreter, 441</td>
<td></td>
</tr>
<tr>
<td>model-checking algorithms, 446</td>
<td></td>
</tr>
<tr>
<td>modeling language, see QMCLang</td>
<td></td>
</tr>
<tr>
<td>parser, 440</td>
<td></td>
</tr>
<tr>
<td>scheduler, 441</td>
<td></td>
</tr>
<tr>
<td>simulation algorithm, 441</td>
<td></td>
</tr>
<tr>
<td>QMCLang</td>
<td></td>
</tr>
<tr>
<td>semantics, 423</td>
<td></td>
</tr>
<tr>
<td>syntax, 423</td>
<td></td>
</tr>
<tr>
<td>type system, 432</td>
<td></td>
</tr>
<tr>
<td>quantum categorical semantics, 31</td>
<td></td>
</tr>
<tr>
<td>quantum cellular automata, 236</td>
<td></td>
</tr>
</tbody>
</table>
quantum closure, 147  
quantum coin-flipping protocol  
model checking, 459  
quantum commands, 348  
quantum error-correction  
model checking, 464  
quantum Fourier transform, 157, 196  
quantum imperative language, see QIL  
quantum information flow, 15–17  
quantum information processing, 206  
quantum IO monad, 173  
quantum key distribution protocol  
model checking, 461  
quantum Kripke structure, 399  
quantum lambda calculus, 139  
quantum logic, 70, 361  
quantum measurements, 320  
quantum mechanics, xi  
quantum parallelism, 185  
quantum programming language, xii, 212  
quantum programming languages, 311  
quantum state  
entangled, 75  
quantum state transformers, 314  
quantum states, 314  
quantum system (in categorical quantum mechanics), 33, 75  
quantum teleportation, 190  
quantum teleportation protocol, 77  
description, 16, 420  
in categorical quantum mechanics, 17, 57, 58  
model checking, 456  
quantum Turing machines, 236  
quantum walk, 393  
quantum weakest preconditions, 324, 325  
commutativity, 328  
reachability relation, 151  
relation, 43  
reversible arithmetic, 192  
reversible let, 173  
rotation  
general, 265  
Sasaki hook, 364  
SAT problem, 395  
scalar, 7, 13, 88  
scheme, 135  
semantics  
abstract, 228  
admissible, 221, 223  
constructive, 173  
hierarchy, 213  
observable, 218  
predicate transformer, 312  
probabilistic, 214  
pure, 216  
semantics of dEQPL, 392  
semiadditive category, 100  
semiadditive functor, 100  
shift operator, 367  
Shor’s algorithm, 194  
signal shifting, 245, 259  
specification  
formal, see formal specification  
spectral decomposition, 317  
spider, 35  
stabilizer  
formalism, 416, 417, 468  
Aaronson-Gottesman simulation algorithm, 441  
complexity, 445  
efficient simulation, 419  
entanglement, 450  
group, 418  
standardization, 238, 255  
state transfer, 273  
state-transfer approach, 238  
stochastic state, 54  
strength (of endofunctor), 51  
strict compact closed category, 85  
strict monoidal category, 84  
strictness, 214  
strong normalization of proof-nets, 82  
subject reduction, 152  
substitution, 151  
subtype, 142  
subtyping relation, 142  
superoperators, 320  
symmetric monoidal category, 83  
syntax of dEQPL, 391  
teleportation, 206, 263, 269  
abstract semantics, 230  
teleportation algorithm, 145  
teleportation procedure, 137  
teleportation protocol, 237  
teleportation technique, 238  
temporal logic, 397  
tensor  
product of Hilbert spaces, 15  
structure in a category, 6, 7  
tenor sum logic, 103  
syntax, 103  
tenor-sum proof-nets, 108  
topological space, 214
Index

trace
  in a compact closed category, 87
  in a symmetric monoidal category, 12
  of a linear map, 12
transpose endofunctor, 33
Turing machine, 135
type inference, 155
type isomorphism, 154
type safety, 152
type theory, 173
type classes, 175
typing context, 143
typing judgment, 143

uncurrying, 86
uniformity of data, 153
unit, 6, 7, 9, 12, 14, 85
unitary embedding, 247
unitary transformations, 319
universal quantum computing, 237
universality, 251
  approximate, 251

verification
  formal, see formal verification

zero object, 95