

## Index

**Bold page numbers indicate the place where the concept is introduced, explained, or defined. Major theorems are listed together under ‘theorem’, and end-of-chapter problems are listed together under ‘problem’.**

- $\Omega(\cdot)$ , 137
- $\Theta(\cdot)$ , 137
- $\epsilon$ -net, 618
- $\geq$  relation for matrices, 645
- $\hbar$ , 82
- $\leq$  relation for matrices, 645
- $\pi/8$  gate, 174
  - fault-tolerant, 485
  - Toffoli construction, 182
- \* operation, 62
- 0-1 integer programming, 149
- 3SAT, 148
  
- Abelian group, 240, 610
- Abelian stabilizer problem, 241
- Abrams, D. S., 214, 215, [AL97]
- accessible information, 529
- acyclic circuits, 23
- Adami, C., 350, [CAK98]
- additive quantum codes, 453
- adjoint, 62, 69
- Adleman, L. M., 11, 168, 214, 641, 644, [ADH97], [AdI94], [AdI98], [RSA78]
- Aharonov, D., xix, xxi, 276, 424, 498, 499, [ABO97], [ABO99], [ABOIN96], [Aha99a], [Aha99b], [AKN98]
- Alberti, P. M., 424, [Alb83]
- Alde, D. M., 607, [HAD<sup>+</sup>95]
- algorithm
  - Deutsch–Jozsa, 36
  - discrete logarithm, 238
  - period-finding, 236
  - quantum order-finding, 232
  - quantum phase estimation, 225
  - quantum search, 254
  - quantum simulation, 208
  - reduction of factoring to order-finding, 233
- algorithm design, 135
- algorithms, 120, 122
- Allen, L., 350, [AE75]
- alphabet, 141
- Ambainis, A., xxi, 276, 607, [Amb00]
- Amer, N., xxi
- amplitude, 81
- amplitude damping, 380
- analog computation, 5, 163, 287
- ancilla, 94
- ancilla bits, 131
  
- AND, 20
- AND gate, 130
- Ando, T., 527, [And79]
- angle between states, 413
- angular momentum, 314
- anti-commutator, 76
- Araki, H., 526, 527, [AL70]
- Araki-Lieb inequality, 516
- architecture, quantum computer, 340
- Ashikhmin, A., 498, [AL99], [Ash97]
- asymptotic notation, 136
- atom traps, 3
- atypical sequences, 538
- auxiliary system, 517
- Awschalom, D. D., 351, [IAB<sup>+</sup>99]
  
- B92 protocol for QKD, 589
- Bacon, D. A., 498, [BKLW99], [LBW99]
- Balandin, A., 351, [VYW<sup>+</sup>99]
- Balcázar, J. L., 168, [BDG88a], [BDG88b]
- Bardeen, J., 4
- Barenco, A., 214, [BBC<sup>+</sup>95], [DBE95]
- Barnett, S. M., 607, [BP93]
- Barnum, H., xxi, 424, 605, 606, [BCF<sup>+</sup>96], [BFJS96], [BKN98], [BNS98], [BST98], [NCSB98]
- Barton, E., 168, [Bar78]
- basis for a vector space, 63
- Bayes’ rule, 608
- BB84 protocol for QKD, 587
- Beals, R., 246, 276, [BBC<sup>+</sup>98]
- beam splitters, 288, 291
- Beckman, D., xxi, 214, [BCDP96]
- Bell basis, 98
- Bell inequality, 17, 111, 115, 119
- Bell states, 16, 25, 98
- Bell, J. S., 17, 25, 112, 116, 119, [Bel64]
- Ben-Or, M., 498, 499, [ABO97], [ABO99], [ABOIN96]
- Benioff, P., 214, [Ben80]
- Bennett, C. H., xix, 9, 11, 59, 119, 168, 169, 214, 276, 497, 604, 606, 607, [BB84], [BBB<sup>+</sup>92], [BBBV97], [BBCM95], [BBC<sup>+</sup>93], [BBC<sup>+</sup>95], [BBE92], [BBPS96], [BBP<sup>+</sup>96], [BBR88], [BD00], [BDS97], [BDSW96], [Ben73], [Ben82], [Ben87], [Ben89], [Ben92], [BS98], [BW92]
- Bernstein, E., 200, 214, 276, [BBBV97], [BV97]
- Bernstein, H. J., 214, 350, 606, [BBPS96], [RZBB94]
- Bertani, P., 214, 350, [RZBB94]
- beryllium, 310, 315

- Bessette, F., 606, 607, [BBB<sup>+</sup>92]  
 Beth, T., 246, 616, [Bet84], [PRB98], [RB98]  
 Bethune, D. S., 607, [BR00], [BR98]  
 Bhatia, R., 118, [Bha97]  
 big  $\Omega$  notation, 137  
 big  $\Theta$  notation, 137  
 big  $O$  notation, 136  
 Biham, E., 607, [BBB<sup>+</sup>98]  
 billiard ball computer, 155  
 binary entropy, 502  
 binary symmetric channel, 426  
 Birkhoff's theorem, 574  
 bit, 13  
 bit flip, 81  
 bit flip channel, 376  
 bit flip code, 427  
 bit flip operator, 427  
 bit-phase flip channel, 377  
 Bloch sphere, 15, 19, 105, 174  
 Bloch vector, 105, 174, 259  
 Bodenhausen, G., 351, [EBW87]  
 Boghosian, B. M., 214, [BT97]  
 Bohm, D., 119, [Boh51]  
 Bohr magneton, 309  
 Bohr, N., 111, 171  
 Boltzmann's constant, 153  
 Boneh, D., 246, [BL95]  
 Boolean circuit, 133  
 Boolean function, 133  
 Boschi, D., 59, [BBM<sup>+</sup>98]  
 Bose condensate, 346  
 Bouwmeester, D., 59, [BPM<sup>+</sup>97]  
 Boyer, M., 276, 607, [BBB<sup>+</sup>98], [BBHT98]  
 Boykin, P. O., 214, 215, [BMP<sup>+</sup>99]  
**BPP**, 152  
**BQP**, 41, 200  
 bra, 62  
 Braginsky, V. B., 118, [BK92]  
 Branca, S., 59, [BBM<sup>+</sup>98]  
 Brassard, G., 11, 59, 276, 606, 607, [BB84], [BBB<sup>+</sup>92], [BBB<sup>+</sup>98], [BBBV97], [BBCM95], [BBC<sup>+</sup>93], [BBE92], [BBHT98], [BBP<sup>+</sup>96], [BBR88], [BHT98], [Bra93], [BS94]  
 Brattain, W., 4  
 Braunstein, S. L., 59, 351, 352, 605, [BCJ<sup>+</sup>99], [BFG98], [BK98a], [BK99], [Bra98], [FSB<sup>+</sup>98], [LB99]  
 Bravyi, S. B., 499, [BK98b]  
 Brennen, G. K., 351, [BCJD99]  
 Brewer, R. G., 350, [BDK92]  
 Brewster's angle, 310  
 Brune, M., 350, [DMB<sup>+</sup>93], [DRBH87], [DRBH95]  
 Buhrman, H., xxi, 246, 276, [BBC<sup>+</sup>98]  
 Burkard, G., 351, [IAB<sup>+</sup>99]  
 c-numbers, 62  
 Cachin, C., 607, [CM97]  
 Caldeira, A. O., 398, [CL83]  
 Calderbank, A. R., 8, 9, 450, 497, 498, [CRSS97], [CRSS98], [CS96]  
 Calderbank–Shor–Steane codes, 445, 450  
 Campman, K., 351, [HSM<sup>+</sup>98]  
 Campos, R. A., 349, [CST89]  
 canonical form for entropy exchange, 562  
 Capelin, S., xxi  
 Carr–Purcell–Meiboom–Gill technique, 331  
 cat state for fault-tolerant measurement, 490  
 catalyst, 577  
 Cauchy–Schwarz inequality, 68  
 Caves, C. M., xxi, 16, 351, 398, 424, 605, 606, [BCF<sup>+</sup>96], [BCJD99], [BCJ<sup>+</sup>99], [Cav99], [FC94], [NC97], [NCSB98], [SC99]  
 cavity quantum electrodynamics, 277, 297, 343  
 cellular automata, 340  
 centralizer, 465  
 Cerf, N. J., 350, [CAK98]  
 characteristic function, 68  
 Chari, A. N., 214, [BCDP96]  
 Chau, H. F., 215, 607, [CW95], [LC99]  
 Chebyshev's inequality, 609  
 check matrix, 456  
 Chernoff bound, 154, 609  
 Chernoff, P. R., 214, [Che68]  
 chi-matrix representation, 391  
 Chiao, R. Y., 350, [KSC<sup>+</sup>94]  
 Childs, A. M., xxi  
 Chinese remainder theorem, 629  
 Choi, M.-D., 398, [Cho75]  
 Chong, F. T., xxi  
 CHSH inequality, 116, 119  
 Chuang, I. L., 215, 349–351, 398, 498, 499, 605, [CGK98], [CGKL98], [CM00], [CN97], [CVZ<sup>+</sup>98], [CY95], [GC97], [GC99], [KCL98], [LCW98], [LNCY97], [LVZ<sup>+</sup>99], [VYSC99], [ZLC00]  
 Church, A., 4, 122, 125, 167, [Chu36]  
 Church–Turing thesis, 4  
   strong form of, 5, 6, 140  
 Church–Turing thesis, 125, 226  
 Cirac, J. I., 350, 398, 498, [CPZ96], [CZ95], [PCZ97]  
 circuit family, 134  
 circuit model of computation, 129  
 classical information over noisy quantum channels, 546  
 classical noise, 354  
 classical physics, 2  
 Clausen, M., 616, [Cla89]  
 Clauser, J. F., 119, [CHSH69]  
 Cleve, R., xxi, 59, 214, 245, 246, 276, 605, [BBC<sup>+</sup>95], [BBC<sup>+</sup>98], [CD96], [CEMM98], [Cle99]  
 clique, 149  
 closed quantum systems, 353  
 CNF, 148  
 co-prime, 627  
 Cohen–Tannoudji, C., 59, 118, [CTDL77a], [CTDL77b]  
 coherent information, 564, 572, 592, 605  
 collusion entropy, 584  
 communication complexity, 164  
 commutator, 76  
 commuting operators, 76, 597  
 compare-and-swap based sorts, 137  
 complete positivity, 368  
   example of a positive map not completely positive, 368  
 completeness equation, 85, 102  
 completeness of a problem for a complexity class, 145  
 completeness relation, 67, 360  
 complex conjugate, 62, 70  
 complexity class, 142, 150  
 composite systems, 93  
 composition of linear operators, 64  
 computational complexity, 40, 135, 138  
   difficulty of obtaining results in, 140  
 concatenated codes, 480

- concavity, 504  
 conditional entropy  
   classical, 506  
   quantum, 514  
 conditional probability, 608  
 conjunctive normal form, 148  
 coNP, 142  
 conservative property of the Fredkin gate, 156  
 continued fraction expansion, 229, 230, 282, 335, 635  
 continued fractions algorithm, 635  
 controlled operation, 177  
 controlled-NOT gate, 20, 178  
   fault-tolerant, 484  
 convergent, 230, 635  
 Conway, J. H., xxi, 168, 169, [Con72], [Con86]  
 Cook, S. A., 138, 168, [Coo71]  
 Cooper pair, 344  
 Coppersmith, D., 245, [Cop94]  
 Cormen, T. H., 167, 639, [CLR90]  
 correctable errors, 440  
 correctable set of errors, 436  
 Cortese, J., xxi  
 Cory, D. G., 350, 351, [CFH97], [CMP<sup>+</sup>98], [STH<sup>+</sup>99]  
 coset invariance, 237, 243  
 cosets, 586, 612  
 Coulomb blockade, 344  
 counting problem, 216  
 Cover, T. M., xxi, 59, 526, 539, 604, 605, [CT91]  
 Cowan, J. D., 168, 498, [WC67]  
 creation and annihilation operators, 284  
 Crépeau, C., 59, 607, [BBCM95], [BBC<sup>+</sup>93]  
 CROSSOVER gate, 131  
 cryptography, 9, 582, 640  
 CSAT, 145  
 Csiszár, I., 604, [CK81]  
 CSS codes, 445, 450, 593  
 cycle, 143  
 cyclic group, 611  
 cyclic property of trace, 75  
 cyclic subgroup, 611  
  
 data compression, 536  
 data pipelining inequality, 510  
 data processing inequality, 572, 606  
   quantum, 564, 572  
 Davidovich, L., 350, [DMB<sup>+</sup>93], [DRBH87]  
 Davies, E. B., 398, [Dav76]  
 Davis, M. D., 59, 167, 652, [Dav65], 662  
 de Wolf, R., xxi, 246, 276, [BBC<sup>+</sup>98]  
 decision problems, 135, 141  
 decoherence  
   as a stochastic phase kick process, 384  
   estimates of, 278  
 decoherence free subspace, 498  
 degeneracy, 69  
 degenerate codes, 444  
 Demarrais, J., 214, [ADH97]  
 density matrix, 99  
 density operator, 99, 119  
 depolarized, 378  
 depolarizing channel, 378  
 DeShazo, M., xxi  
 deterministic query complexity, 272  
 Deutsch's algorithm, 32  
 Deutsch's problem, 34, 241  
 Deutsch, D., 6, 32, 34, 59, 171, 214, 245, 526, [DBE95], [Deu83], [Deu85], [Deu89], [DJ92]  
 Deutsch, I. H., 351, [BCJD99]  
 Deutsch-Jozsa algorithm, 34, 59, 249  
   optical implementation, 294  
 Devabhaktuni, S., 214, [BCDP96]  
 deviation density matrix, 336  
 DeVoe, R. G., 321, 350, [BDK92]  
 Diaconis, P., 616, [DR90]  
 diagonal representation, 69  
 diagonalizable operator, 69  
 Diaz, J., 168, [BDG88a], [BDG88b]  
 Dieks, D., 604, [Die82]  
 Diffie, W., 11, 59, 644, [DH76], [DL98]  
 dimension of a vector space, 63  
 dipolar coupling, 328  
 Dirac notation, 13, 62  
 discrete logarithm problem, 216, 217, 241  
   quantum algorithm for, 238  
 discrete memoryless channel, 551  
 distance measures, 399  
 distance of a code, 448  
 distillable entanglement, 578  
 distributed computation, 164  
 distributed quantum computation, xvii  
 Diu, B., 59, 118, [CTDL77a], [CTDL77b]  
 DiVincenzo, D. P., xix, xxi, 214, 215, 246, 349–351, 497, 498, 604–606, [BBC<sup>+</sup>95], [BD00], [BDS97], [BDSW96], [CD96], [DiV95a], [DiV95b], [DiV98], [DS96], [DSS98], [IAB<sup>+</sup>99], [LD98], [TD98], [VYW<sup>+</sup>99]  
 divisor, 625  
 DNA computing, 163  
 Domokos, P., 350, [DRBH95]  
 double stochasticity, 511  
 dual linear code, 449  
 dual vector, 65  
 dual-rail representation, 288  
 Duan, L.-M., 119, [DG98]  
 Dürr, C., 276, [DH96]  
 Dyer, P., 607, [HAD<sup>+</sup>95]  
 Dykman, M. I., 351, [PD99]  
 dynamic measures of distance, 399, 401  
 Dyson, F. J., 527  
  
 Earnshaw's theorem, 309  
 Earnshaw, S., 350, [Ear42]  
 Eberhard, P. H., 350, [KSC<sup>+</sup>94]  
 Eberly, J. H., 350, [AE75]  
 edges, 143  
 efficiency of quantum simulations, 206  
 Eibl, M., 59, [BPM<sup>+</sup>97]  
 eigenvalue, 68  
 eigenvector, 68  
 Einstein, A., 2, 17, 25, 60, 80, 119, [EPR35]  
 Einstein-Podolsky-Rosen thought experiment, 17  
 Ekert, A. K., 59, 214, 246, 497, 498, 606, 607, [BBE92], [CEMM98], [DBE95], [EHPP94], [EJ96], [EJ98], [Eke91], [EM96], [ME99]  
 electric dipole selection rules, 300  
 electron spin, 309  
 element of reality, 112  
 ENDOR, 350  
 energy, 83, 153  
 energy eigenstates, 83  
 ensemble of pure states, 99  
 entanglement, 11, 95

- as a physical resource, 571
- catalysis, 577
- dilution, 578
- distillation, 578
  - mixed state, 580
  - of formation, 578
- entanglement fidelity, 420
- entropy, 500
  - classical, 500
  - concavity of, 516
  - of an ensemble, 518
  - quantum, 510
  - rate, 538
  - strict concavity of, 504
- entropy exchange, 561, 605
- entropy Venn diagram, 508
- entscheidungsproblem, 122
- environmental models
  - quantum operations, 365
  - trace-preserving quantum operations, 363
- EPR, 17, 111
- EPR pairs, 16, 25, 98, 591
- EPR protocol for QKD, 591
- EPR states, 25
- EPR thought experiment, 119
- Epstein, H., 527, [Eps73]
- equilibration of quantum systems, 211
- Ernst, R. R., 351, [EBW87]
- error propagation
  - in fault-tolerant circuits, 483
- error syndrome, 428
  - classical, 448
- error-correcting codes, 8, 425
- errors, 436
- Ettinger, M., 246, [EH99], [EHK99]
- Euclid's algorithm, 122, 626
- Euler  $\varphi$  function, 631
- Euler cycle, 143
- Everitt, H., xxi
- evolution matrix, 355
- EXP, 151
- expectation of a random variable, 609
- exponential resources, 139
- exponential time, 151
  
- Fabry–Perot cavity, 298
- factoring, 142
- factoring decision problem, 142
- factoring problem, 232
- factors, 625
- Fagin, R., xxi
- Fahmy, A. F., 350, [CFH97]
- FANIN, 23
- Fannes' inequality, 512
- Fannes, M., 526, [Fan73]
- Fano's inequality, 534, 536, 563, 572, 609
  - quantum, *see* quantum Fano inequality
- FANOUT, 23
- FANOUT gate, 131
- Farhi, E., 276, [FG98]
- Fässler, A., 616, [FS92]
- fault-tolerant computation, 425
- fault-tolerant quantum computation, 474
  - $\pi/8$  gate, 485
  - assumptions, 493
  - definition of operations, 476
  - error propagation, 478
  - measurement, 477, 489
  - quantum logic, 482
  - the threshold theorem, 480, 493
  - Toffoli gate, 488
- feasible computational problems, 139
- Feller, W., 609, [Fel68a], [Fel68b]
- Feynman path integral, 398
- Feynman, R. P., 7, 59, 118, 168, 204, 214, [Fey82], [FLS65a], [FLS65b]
- fidelity, 281
  - classical, 400
  - joint concavity of, 415
  - quantum, 409
- fine structure constant, 301
- finite simple continued fraction, 635
- finite state control, 122
- foosball, xxi
- formal languages, 141
- Fourier transform
  - discrete, 217
  - over a group, 615
  - over groups, 240
  - quantum, 191, 209, 217
  - shift-invariance property, 237
- Fractran, 166
- Fredkin gate, 156
  - optical, 295
- Fredkin, E., 168, [FT82]
- Freedman, M. H., xxi, 499, 624, [FM98]
- Freeman, R., 351, [LKF99]
- Fuchs, C. A., xix, xxi, 59, 352, 399, 424, 605, [BCF<sup>+</sup>96], [BFG98], [BFJS96], [FC94], [FSB<sup>+</sup>98], [Fuc96], [Fuc97], [FvdG99]
- full-adder, 132
- fundamental theorem of arithmetic, 625
- Furusawa, A., 59, 352, [FSB<sup>+</sup>98]
  
- Gabarró, J., 168, [BDG88a], [BDG88b]
- Gagen, M., xxi
- Gardiner, C. W., 118, 349, 398, [Gar91], [ZG97]
- Garey, M. R., 168, [GJ79]
- Gauss, K. F., 232
- generalized amplitude damping, 382
- generalized measurements, 118
- generators, 611
  - for the five qubit code, 469
  - for the Shor code, 468
  - of a group, 455
- Gerlach, W., 43
- Gershenfeld, N., xxi, 350, 351, [CGK98], [CGKL98], [GC97]
- Gibbs state, 211
- Gilbert–Varshamov bound
  - for classical codes, 449
  - for CSS codes, 451, 495, 596
- Gisin, N., 607, [MZG96]
- global phase, 93
- Goldberg, D., 168, [HGP96]
- Gordon, J. P., 605, [Gor64]
- Gossard, A. C., 351, [HSM<sup>+</sup>98]
- Gottesman, D., xix, xxi, 9, 215, 453, 497–499, 605–607, [BFG98], [GC99], [Got96], [Got97], [Got98a], [Got98b], [GP10]
- Gram–Schmidt procedure, 66
- graph, 143
- graph isomorphism problem, 150, 242
- graph theory, 143

- Gray code, 191  
 greatest common divisor, 626  
 Griffiths, R. B., 214, 246, [GN96]  
 Grimmett, G. R., 609, [GS92]  
 ground state, 83  
 group commutator, 620  
 group theory, 610  
 Grover iteration, 250  
 Grover operator, 250  
 Grover's algorithm, 7, 38, 248  
 Grover, L. K., 7, 38, 276, [Gro96], [Gro97]  
 Gruska, J., xix, [Gru99]  
 Guo, G.-C., 119, [DG98]  
 Gutmann, S., 276, [FG98]
- Hadamard gate, 19, 174  
 Hadamard transform, 31  
 half-adder, 132  
 Halmos, P. R., 118, [Hal58]  
 halting problem, 130  
 halting state of a Turing machine, 123  
 Hamiltonian, 82  
 Hamiltonian cycle problem, 143, 264  
 Hamiltonian cycle problem  
   inclusion in NP, 143  
 Hamermesh, M., 616, [Ham89]  
 Hamming code, 449  
 Hamming distance, 399, 448  
 Hamming sphere, 549  
 Hamming weight, 448, 547  
 Hammurabi, 4  
 Hansen, R. H., 351, [JMH98]  
 Hardin, R. H., 498, [RHSS97]  
 Hardy, G. H., 246, 639, [HW60]  
 Hardy, L., 59, [BBM<sup>+</sup>98]  
 Haroche, S., 350, [DMB<sup>+</sup>93], [DRBH87], [DRBH95]  
 Harris, J. S., xxi  
 Hausladen, P., 605, [HJS<sup>+</sup>96]  
 Havel, T. F., 350, 351, [CFH97], [CMP<sup>+</sup>98], [STH<sup>+</sup>99]  
 HC, 143, 264  
 Heisenberg uncertainty principle, 88, 89  
 Heisenberg, W., 44  
 Hellman, M., 11, 644, [DH76]  
 Hellwig, K.-E., 398, [HK69], [HK70]  
 Hennessey, J. L., 168, [HGP96]  
 Hermitian conjugate, 62, 69, 70  
 Hermitian operator, 70  
 hidden linear function problem, 241  
 hidden subgroup problem, 38, 217, 234, 336  
   quantum algorithm for, 240  
 Hilbert space, 66  
 Hilbert's problem, 122  
 Hilbert, D., 122  
 Hilbert-Schmidt inner product, 76  
 Hoffmann, B., 61  
 Hofstadter, D. R., 59, 167, [Hof79]  
 Holevo  $\chi$  quantity, 531  
 Holevo bound, 531, 592  
 Holevo, A. S., xxi, 605, [Hol73], [Hol79], [Hol98]  
 Holt, R. A., 119, [CHSH69]  
 Hood, C. J., 306, 350, 398, [THL<sup>+</sup>95]  
 Horn, R. A., 118, [HJ85], [HJ91]  
 Horne, M. A., 119, [CHSH69]  
 Horodecki, M., 605, 606, [HHH96], [HHH98], [HHH99a], [HHH99b], [HHH99c], [Hor97]
- Horodecki, P., 351, 606, [HHH96], [HHH98], [HHH99a], [HHH99b], [HHH99c], [ZHSL99]  
 Horodecki, R., 606, [HHH96], [HHH98], [HHH99a], [HHH99b], [HHH99c]  
 Høyer, P., 246, 276, [BBHT98], [BHT98], [DH96], [EH99], [EHK99]  
 HSW theorem, 581, 592  
 Huang, M. A., 214, [ADH97]  
 Hubbard model, 206  
 Hughes, R. J., 607, [HAD<sup>+</sup>95]  
 Hughston, L. P., 119, [HJW93]  
 Huijbers, A. G., xxi, 351, [HSM<sup>+</sup>98]  
 Huttner, B., 607, [EHPP94]  
 hyperfine states, 315
- i.i.d. source, 537  
 identity matrix, 65  
 identity operator, 63  
 Igeta, K., 350, [YKI88]  
 Imamoglu, A., 350, 351, [IAB<sup>+</sup>99], [IY94]  
 Impagliazzo, R., 499, [ABOIN96]  
 INADEQUATE, 338  
 independent generators of a group, 456  
 independent random variables, 608  
 infeasible computational problems, 139  
 information gain implies disturbance, 586  
 information reconciliation, 584  
 information source, classical, 399  
 information theory, 7  
   operational motivation for definitions in, 501  
 inner product, 62, 65  
 inner product space, 66  
 integers, 625  
 interference, 32  
 interferometers, 296  
 internal states of a Turing machine, 122  
 intractable computational problems, 139  
 ion trap, 277  
   cooling, 312  
   geometry, 309  
   quantum computer, 309, 343  
   toy model, 317  
 irreversible logic gate, 153  
 Ising model, 206  
 Itano, W. M., 350, [MMK<sup>+</sup>95], [WMI<sup>+</sup>98]
- J-coupling, 328  
 James, D., 350, [Jam98]  
 Jaynes, E. T., 119, [Jay57]  
 Jaynes-Cummings Hamiltonian, 281, 300, 302, 308, 315, 318  
 Jessen, P. S., 351, [BCJD99]  
 Jiang, H. W., 351, [VYW<sup>+</sup>99]  
 Johnson noise, 312  
 Johnson, C. R., 118, [HJ85], [HJ91]  
 Johnson, D. S., 168, [GJ79]  
 joint concavity, 519, 645  
 joint convexity of trace distance, 408  
 joint entropy, 506  
   quantum, 514  
 joint entropy theorem, 513  
 Jonathan, D., 606, [JP99]  
 Jones, J. A., 351, [JM98], [JMH98]  
 Jones, K. R. W., 398, [Jon94]  
 Josephson junction, 344  
 Jozsa, R., 59, 119, 246, 351, 424, 605, [BBC<sup>+</sup>93], [BCF<sup>+</sup>96], [BCJ<sup>+</sup>99], [BFS96], [DJ92], [EJ96],

- [EJ98], [HJS<sup>+</sup>96], [HJW93], [Joz94], [Joz97], [JS94]
- Kahn, D., 59, [Kah96]
- Kallenbach, R., 350, [BDK92]
- Kane, B. E., 351, [Kan98]
- Karp, R. M., 168, [Kar72]
- Kay, A., 80, 120
- Kempe, J., xxi, 498, [BKLW99]
- Kerr effect, optical, 290
- Kerr media, nonlinear, 293, 305
- ket, 62, 62
- Khahili, F. Y., 118, [BK92]
- Kimble, H. J., 59, 306, 350, 352, 398, [BK98a], [BK99], [FSB<sup>+</sup>98], [THL<sup>+</sup>95]
- King, B. E., 350, [MMK<sup>+</sup>95], [WMI<sup>+</sup>98]
- King, C., 605, [KR99]
- Kitaev's algorithm, 243
- Kitaev, A. Y., xix, xxi, 38, 246, 424, 498, 499, 624, [AKN98], [BK98b], [Kit95], [Kit97a], [Kit97b], [Kit97c]
- Kitagawa, M., 350, [KU91], [YKI88]
- Klein's inequality, 526
- Klein, O., 526, [Kle31]
- Knight, P. L., 350, 398, [PK96], [PK98]
- Knight, T., 168, [YK95]
- Knill, E., xxi, 59, 214, 246, 351, 424, 497–499, 606, [BKN98], [CMP<sup>+</sup>98], [EHK99], [KCL98], [KL97], [KL99], [KLV99], [KLZ98a], [KLZ98b], [Kni95], [NKL98]
- Knuth, D. E., 59, 122, 167, 171, 216, 232, 632, [Knu97], [Knu98a], [Knu98b]
- Koblitz, N., 639, 644, [Kob94]
- Kolmogorov distance, 400
- Kong, S., xxi
- Körner, J., 604, [CK81]
- Kraus, K., 118, 398, 526, [HK69], [HK70], [Kra83], [Kra87]
- Kronecker product, 74
- Kubinec, M. G., 351, [CGK98], [CGKL98], [LVZ<sup>+</sup>99]
- Kullback, S., 526, [KL51]
- Kupce, E., 351, [LKF99]
- Kurtsiefer, C., 321
- Kwiat, P. G., 119, 350, [CAK98], [KMSW99], [KSC<sup>+</sup>94], [MWKZ96]
- L, 151**
- $L_1$  distance, 400
- Ladner, R. E., 168, [LLS75]
- Laflamme, R., xxi, 59, 214, 351, 424, 497–499, 606, [CMP<sup>+</sup>98], [KCL98], [KL97], [KL99], [KLV99], [KLZ98a], [KLZ98b], [LMPZ96], [NKL98], [SL97], [STH<sup>+</sup>99], [ZL96]
- Laloë, F., 59, 118, [CTDL77a], [CTDL77b]
- Lamb–Dicke parameter, 312
- Lamb–Dicke criterion, 312
- Landahl, A., xxi
- Landau, L., 119, [Lan27]
- Landau, L. J., 398, [LS93]
- Landau, S., 59, [DL98]
- Landauer's principle, 153, 569
- Maxwell's demon and, 162
- Landauer, R., 1, 168, [Lan61]
- Lanford, O. E., 527, [LR68]
- Lange, W., 306, 350, 398, [THL<sup>+</sup>95]
- Langevin equations, 353
- language, 141
- law of large numbers, 541, 609
- law of total probability, 608
- Lazere, C., 59, [SL98]
- Lecerf, Y., 168, [Lcc63]
- Leff, H. S., 168, [LR90]
- Legere, R., xxi
- Leggett, A. J., 398, [CL83]
- Leibfried, D., 350, [WMI<sup>+</sup>98]
- Leibler, R. A., 526, [KL51]
- Leighton, R. B., 59, 118, 168, [FLS65a], [FLS65b]
- Leiserson, C. E., 167, 639, [CLR90]
- Lenstra, A. K., 246, [LL93]
- Lenstra Jr., H. W., 246, [LL93]
- Leonhardt, U., 398, [Leo97]
- Leung, D. W., xxi, 351, 498, 499, [CGKL98], [CVZ<sup>+</sup>98], [LNCY97], [LVZ<sup>+</sup>99], [ZLC00]
- Levin, L., 138, 168, [Lev73]
- Levitov, L., 351, [MOL<sup>+</sup>99]
- Lewenstein, M., 351, [ZHSL99]
- Li, M., 169, [LTV98], [LV96]
- Lidar, D. A., xxi, 498, [BKLW99], [LBW99], [LCW98]
- Lie formula
- composition of Lie operations, 207
- Lie, S., 215
- Lieb's theorem, 519, 526, 645, 646
- Lieb, E. H., xxi, 527, [AL70], [Lie73], [Lie75], [LR73a], [LR73b]
- Lindblad form, 207, 386, 398
- Lindblad operators, 388
- Lindblad, G., 398, 527, 605, [Lin75], [Lin76], [Lin91]
- Linden, N., 351, [BCJ<sup>+</sup>99], [LKF99], [LP99]
- linear algebra, 61, 118
- linear code, 445
- linear dependence, 63
- linear independence, 63
- linear operators, 63
- linearity of trace, 75
- Lipton, R. J., 168, 246, [BL95], [Lip95]
- literals, 148
- Lloyd, S., 214, 215, 349, 351, 352, 606, [AL97], [CVZ<sup>+</sup>98], [LB99], [Llo93], [Llo94], [Llo95], [Llo96], [Llo97], [LS98], [MOL<sup>+</sup>99]
- Lo, H.-K., xix, 605–607, [BFG98], [LC99], [Lo99], [LP97], [LSP98]
- local realism, 116
- LOCC, 573
- logarithmic space, 151
- logic gate, 129
- logical labeling, 333
- Lomont, J. S., 616, [Lom87]
- Loss, D., 351, [IAB<sup>+</sup>99], [LD98]
- Louisell, W. H., 349, [Lou73]
- Luther, G. G., 607, [HAD<sup>+</sup>95]
- Lynch, N. A., 168, [LLS75]
- Lynn, T., xxi
- Lytsin, S., 498, [AL99]
- Maali, A., 350, [DMB<sup>+</sup>93]
- Maassen, H., 526, [MU88]
- Mabuchi, H., xxi, 306, 350, 398, [THL<sup>+</sup>95]
- Macchiavello, C., 59, 246, 497, 498, [CEMM98], [EM96]
- MacWilliams, F. J., 59, 497, [MS77]
- magnetic resonance, 326
- majorization, 573
- Manin, Y. I., xxi, 204, 214, [Man80], [Man99]

- Marcus, C. M., 351, [HSM<sup>+</sup>98]  
 Marcus, M., 118, [MM92]  
 Margolus, N., 214, [BBC<sup>+</sup>95]  
 Markov chain, 509  
 Markov processes, 354, 355  
 Marshall, A. W., 606, [MO79]  
 Martini, F. D., 59, [BBM<sup>+</sup>98]  
 Mass, W., 351, [CMP<sup>+</sup>98]  
 master equations, 353, 386  
 matrices, 64  
 matrix representation of an operator, 64  
 Mattle, K., 59, 119, [BPM<sup>+</sup>97], [MWKZ96]  
 Maurer, U. M., 607, [BBCM95], [CM97], [Mau93]  
 Maxwell's demon, 161, 162, 569  
 Maxwell, J. C., 162, 168, [Max71]  
 Mayers, D., 607, [May98]  
 measurement, 84, 185, 356  
   fault-tolerant, 489  
   in the Bell basis, 187  
   in the stabilizer formalism, 463  
   of an operator, 188  
 measurement operators, 84, 102  
 Meekhof, D. M., 350, [MMK<sup>+</sup>95], [WMI<sup>+</sup>98]  
 Menezes, A. J., 59, 275, [MvOV96]  
 Merkle, R., 11, 644, [Mer78]  
 metric, 400  
 Meyer, D. A., 499, [FM98]  
 Milburn, G. J., xxi, 59, 350, 606, [Mil89a], [Mil96],  
   [Mil97], [Mil98]  
 Miller, D. A. B., 350, [Mil89b]  
 Miller, G. L., 644, [Mil76]  
 Minc, H., 118, [MM92]  
 Minsky machine, 165  
   program, 165  
 Minsky, M. L., 168, [Min67]  
 Miquel, C., 497, [LMPZ96]  
 mirror, 288  
 Mitchell, J. R., 350, [KMSW99]  
 mixed state, 100  
 Modha, D., 605, [CM00]  
 modular arithmetic, 626  
 modular exponential, 228  
 modular exponentiation, 227  
 monotonicity of the relative entropy, 524  
 Monroe, C., 322, 350, [MMK<sup>+</sup>95], [WMI<sup>+</sup>98]  
 Mooij, J. E., 351, [MOL<sup>+</sup>99]  
 Moore's law, 4  
 Moore, G., 4  
 Mor, T., 214, 215, 351, 605, 607, [BBB<sup>+</sup>98],  
   [BMP<sup>+</sup>99], [Mor98], [VYW<sup>+</sup>99]  
 Morgan, G. L., 607, [HAD<sup>+</sup>95]  
 Mosca, M., xix, xxi, 59, 246, 276, 351, [BBC<sup>+</sup>98],  
   [CEMM98], [JM98], [JMH98], [ME99], [Mos98],  
   [Mos99]  
 Mossbauer effect, 312  
 Motwani, R., 168, [MR95]  
 Muller, A., 607, [MZG96]  
 multiplicative inverse, 627  
 Murphy, E. A., Jr., 546  
 mutual information, classical, 506  
 mutual information, quantum, 514
- Nakamura, Y., 351, [NPT99]  
 NAND, 20  
 NAND gate, 130  
 natural numbers, 625  
 Nielsen, M. A., xix, 59, 119, 351, 398, 424, 498, 527,  
   605, 606, [BKN98], [BNS98], [CN97],  
   [LNCY97], [NC97], [NCSB98], [Nie98],  
   [Nie99a], [Nie99b], [NKL98], [SN96]  
 Nisan, N., 424, 499, [ABOIN96], [AKN98]  
 Niu, C.-S., 214, 246, [GN96]  
 NMR, 324, 343  
 no-cloning theorem, 3, 24, 530, 586  
 noise  
   classical, 354  
   quantum, 353  
 noiseless channel coding theorem, 8, 500  
 noiseless quantum codes, 498  
 noisy channel coding theorem, 8  
 noisy classical channels, 548  
 non-Abelian groups, 242  
 non-trace-preserving quantum operations, 367  
 non-uniform circuit family, 134  
 NOR, 20  
 NOR gate, 130  
 norm, 66  
 norm of a matrix, 645  
 normal operator, 70  
 normalization condition for state vectors, 81  
 normalized vectors, 66  
 normalizer of  $G_n$ , 461  
 normalizer operations, 461  
   fault-tolerant, 482  
 NOT gate, 129  
 NP, 40, 142, 263  
 NPI, 149  
 nuclear spin, 309  
 number field sieve, 216
- $O(\cdot)$ , 136  
 observable, 87  
 Ohya, M., 526, [OP93]  
 Olkin, I., 606, [MO79]  
 one time pad, 583  
 open quantum systems, 353  
 operation elements, 360  
 operator-sum representation, 360  
   freedom in, 370  
 optical computer, classical, 296  
 optical lattice, 346  
 optical pumping, 312  
   xenon, 341  
 OR, 20  
 OR gate, 130  
 oracle, 221  
   for quantum searching, 248  
   models of computation, 129  
 order  
   of  $x$  modulo  $N$ , 226, 633  
   of a group element, 610  
   of a permutation, 241  
 order-finding problem, 216, 226, 241, 633  
 Orlando, T. P., 351, [MOL<sup>+</sup>99]  
 orthogonal complement, 70  
 orthogonality, 66  
 orthonormal decomposition, 69  
 orthonormality, 66  
 outer product notation for operators, 67  
 output of a computation, 123  
 Ozawa, M., 605, [YO93]
- P**, 40, 141  
 Pais, A., 59, 112, [Pai82], [Pai86], [Pai91]

- Palma, G. M., 607, [EHPP94]  
 Pan, J. W., 59, [BPM<sup>+</sup>97]  
 Papadimitriou, C. M., 138, 168, 639, [Pap94]  
 parallel computers, 162  
 parity check matrix, 447  
 partial trace, 105  
 Pashkin, Y. A., 351, [NPT99]  
 Patterson, D. A., 168, [HGP96]  
 Patterson, M., xxi  
 Paturi, R., 276, [Pat92]  
 Pauli gates, *see* quantum logic gate  
 Pauli group, 454, 611  
 Pauli matrices, 65, 174, 427  
 Paz, J.-P., 497, [LMPZ96]  
 Pellizzari, T., 498, [CPZ96]  
 Penrose, R., 59, 167, [Pen89]  
 Peres, A., 59, 112, 118, 119, 607, [BBC<sup>+</sup>93], [EHPP94], [Per88], [Per93], [Per95]  
 period-finding problem, 241  
 period-finding, quantum algorithm for, 236  
 Perlis, S., 118, [Per52]  
 Petroff, M. D., 350, [KSC<sup>+</sup>94]  
 Petz, D., 526, 527, [OP93], [Pet86]  
 phase, 81, 93  
 phase estimation, quantum algorithm for, 221  
 phase flip, 81  
 phase flip channel, 376  
 phase flip operator, 430  
 phase gate, 174  
 phase kicks, as a model of quantum noise, 384  
 phase shifter, 288  
 Phoenix, S. J. D., 607, [BP93]  
 phonon, 311  
 photodetector, 288  
 physical quantum operations, 367  
 Pines, A., xxi  
 Planck's constant, 82  
 Platzman, P. M., 351, [PD99]  
 Plenio, M. B., 350, 398, 606, [JP99], [PK96], [PK98], [VP98]  
 Podolsky, B., 17, 25, 119, [EPR35]  
 Poisson equation, 205  
 polar decomposition, 78  
 polynomial resources, 139  
 polynomial time, 141  
 Polzik, E. S., 59, 352, [FSB<sup>+</sup>98]  
 Popescu, S., xix, 59, 351, 606, [BBM<sup>+</sup>98], [BBPS96], [BBP<sup>+</sup>96], [BCJ<sup>+</sup>99], [LP97], [LP99], [LSP98]  
 Popeye the Sailor, 60  
 Poplavskii, R. P., 204, [Pop75]  
 positive definite operator, 71  
 positive operator, 71  
 Positive Operator-Valued Measures, 90  
 POVM, 90  
 POVM measurements, 90, 118  
   completeness relation for, 92  
   elements for, 90  
 Poyatos, J. F., 398, [PCZ97]  
 Preskill, J., xix, xxi, 214, 499, 606, 607, [BCDP96], [GP10], [Pre97], [Pre98a], [Pre98b], [Pre98c], [SP00]  
 Price, M., 351, [CMP<sup>+</sup>98]  
 primality decision problem, 141  
 prime number, 625  
 prime number theorem, 638  
 principle of deferred measurement, 185  
 principle of implicit measurement, 186  
 privacy amplification, 584  
 private key cryptography, 582, 640  
 problem,  
   Addition by Fourier transforms, 244  
   Alternate characterization of the fidelity, 423  
   Alternate universality construction, 212  
   Analogue of the triangle inequality for conditional entropy, 525  
   Ancilla bits and efficiency of reversible computation, 167  
   Classical capacity of a quantum channel – Research, 603  
   Computable phase shifts, 212  
   Computing with linear optics, 346  
   Conditional forms of strong subadditivity, 526  
   Control via Jaynes–Cummings interactions, 347  
   Database retrieval, 275  
   Efficient temporal labeling, 346  
   Encoding by teleportation, 496  
   Encoding stabilizer codes, 495  
   Feynman–Gates conversation, 58  
   Find a hard-to-compute class of functions (Research), 167  
   Finding the minimum, 274  
   Fractran, 166  
   Functions of the Pauli matrices, 117  
   Generalized Klein's inequality, 525  
   Generalized quantum searching, 274  
   Generalized relative entropy, 525  
   Gilbert–Varshamov bound, 495  
   Hardness of approximation of TSP, 166  
   Ion trap logic with two-level atoms, 348  
   Kitaev's algorithm, 243  
   Lindblad form to quantum operation, 395  
   Linearity forbids cloning, 603  
   Measured quantum Fourier transform, 243  
   Methods for achieving capacity – Research, 603  
   Minimal Toffoli construction, 213  
   Minsky machines, 165  
   Non-Abelian hidden subgroups – Research, 244  
   Non-universality of two bit reversible logic, 166  
   Prime number estimate, 638  
   Properties of the Schmidt number, 117  
   Quantum channel capacity – Research, 603  
   Quantum searching and cryptography, 275  
   Random unitary channels, 396  
   Reversible PSPACE = PSPACE, 167  
   Reversible Turing machines, 166  
   Strong subadditivity – Research, 526  
   Teleportation as a quantum operation, 395  
   Tsirelson's inequality, 118  
   Undecidability of dynamical systems, 166  
   Universality with prior entanglement, 213  
   Vector games, 166  
 process tomography, 308, 389  
 program for a Turing machine, 123  
 projective measurements, 87, 282  
 projectors, 70  
 promise problems, 243  
 pseudocode, 126  
 PSPACE, 150  
 public key cryptography, 582  
 public key cryptosystems, 11, 640  
 Pueschel, M., 246, [PRB98]  
 Pulver, M., 214, 215, [BMP<sup>+</sup>99]  
 pure state, 100  
 purifications, 109, 110, 119



- QKD, 582, 586  
   B92 protocol, 589  
   BB84 protocol, 587, 593  
   EPR protocol, 591  
   security of, 593  
 quantum chromodynamics, 206  
 quantum circuits, 22  
 quantum code, 435  
 quantum corollary to Moore's law, 39  
 quantum cryptography, 10, 582  
 quantum dots, 344  
 quantum efficiency, 288  
 quantum electrodynamics, 2, 206  
 quantum error-correction, 425  
 quantum factoring, 216  
 quantum Fano inequality, 563, 572, 605  
 quantum field theory, 6  
 quantum Fourier transform, 216  
   quantum circuit for, 219  
 quantum gravity, 6  
 quantum Hall effect, 346  
 quantum Hamming bound, 444  
 quantum information theory, 528  
   data processing inequality, 564  
   entanglement, 571  
   entropy exchange, 561  
   Holevo bound, 531  
   quantum cryptography, 582  
   quantum Fano inequality, 561  
   Schumacher's noiseless coding theorem, 542  
   Singleton bound, 568  
   summary of important relations, 572  
 quantum key distribution, 586  
 quantum logic gate  
    $\pi/8$ , 174, 485  
   controlled phase-flip, 319  
   controlled-NOT, 20, 178, 321, 482  
   Hadamard, 174, 483  
   Pauli, 483  
   phase, 174, 483  
   single qubit, 174, 319  
   swap, 320  
   Toffoli, 29, 485  
 quantum money, 56  
 quantum noise, 353  
   estimates of, 278  
 quantum operations, 353, 353  
   chi-matrix representation, 391  
   environmental models for, 363, 365  
   limitations to the formalism, 394  
   non-trace-preserving, 367  
   partial trace map, 374  
   physical, 367  
   trace map, 374  
   trace-preserving, 367  
 quantum process tomography, 389, 398  
 quantum search algorithm, 248, 339  
 quantum searching, 263  
 quantum source, 542  
 quantum state tomography, 389, 398  
 quantum teleportation, *see* teleportation, quantum  
 quantum trajectories, 398  
 quantum Turing machine, 203  
 qubit, 13, 80, 605  
   charge representation, 344  
   harmonic oscillator representation, 283  
   implementation, 277  
   photon representation, 287  
   spin representation, 309, 324, 345  
   square well representation, 280  
   superconductor representation, 344  
 qutrit, 203, 343, 359  
  
 Rabi frequency, 318  
 Rabi oscillations, 303  
 Rabin, M. O., 120, 644, [Rab80]  
 Raghavan, P., 168, [MR95]  
 Rahim, H. Z., 59, [Rah99]  
 Raimond, J. M., 350, [DMB<sup>+</sup>93], [DRBH87], [DRBH95]  
 Rains, E. M., 9, 497, 498, [CRSS97], [CRSS98], [Rai98], [Rai99a], [Rai99b], [Rai99c], [RHSS97]  
 Rajagopalan, S., xxi  
 Ramo, S., 350, [RWvD84]  
 random coding, 549  
 randomized algorithms, 5  
 rank of a Hermitian operator, 117  
 Rasetti, M., 498, [ZR98]  
 read-write tape-head for a Turing machine, 123  
 Reck, M., 214, 350, [RZBB94]  
 reduced density operator, 105  
 reducibility of one language to another, 145  
 reduction, 144  
 reduction of factoring to order-finding, 232, 633  
 refocusing, 331  
 relative entropy, 526  
   classical, 504  
   quantum, 511  
 relative phase, 93  
 remainders, 626  
 Rényi entropy, 584  
 Ressler, A., 168, [Res81]  
 reversible logic gates, 153  
 reversible Turing machine, 155  
 Rex, R., 168, [LR90]  
 Risk, W., xxi  
 Risk, W. P., 607, [BR00], [BR98]  
 Risken, H., 398, [VR89]  
 Rivest, R. L., 11, 167, 639, 644, [CLR90], [RSA78]  
 Robert, J. M., 607, [BBR88]  
 Robinson, D. W., 527, [LR68], [RR67]  
 Rockmore, D., 616, [DR90]  
 Roetteler, M., 246, [PRB98], [RB98]  
 Rosen, N., 17, 25, 119, [EPR35]  
 rotation operators, 174  
 Roychowdhury, V., 214, 215, 351, [BMP<sup>+</sup>99], [VYW<sup>+</sup>99]  
 Royer, A., 398, [Roy96]  
 RSA cryptosystem, 11  
 Ruelle, D., 527, [RR67]  
 Ruskai, M. B., xxi, 424, 527, 605, [KR99], [LR73a], [LR73b], [Rus94]  
  
 Sakurai, J. J., 59, 118, 349, [Sak95]  
 Saleh, B. E. A., 349, [CST89], [ST91]  
 Salvail, L., 606, 607, [BBB<sup>+</sup>92], [BS94]  
 Sands, M., 59, 118, 168, [FLS65a], [FLS65b]  
 Sanpera, A., 351, [ZHSL99]  
 scalar, 62  
 scanning tunneling microscope, 3  
 Schack, R., 351, [BCJ<sup>+</sup>99], [SC99]  
 Schauer, M., 607, [HAD<sup>+</sup>95]  
 Schmidt bases, 110  
 Schmidt co-efficients, 109

- Schmidt decomposition, 109, 119  
 Schmidt number, 110  
 Schmidt, E., 119, [Sch06]  
 Schneider, S., xxi  
 Schneier, B., 59, 275, [Sch96a]  
 Schrader, R., xxi  
 Schrödinger equation, 82, 205, 280, 284, 301  
   quantum simulation of, 209  
 Schrödinger's cat, 387  
 Schrödinger, E., 119, [Sch36]  
 Schulman, L. J., 351, [SV99]  
 Schumacher compression, 547  
 Schumacher's quantum noiseless coding theorem, 542  
 Schumacher, B. W., xxi, 8, 398, 424, 605–607,  
   [BBS96], [BBP<sup>+</sup>96], [BCF<sup>+</sup>96], [BFJS96],  
   [BNS98], [HJS<sup>+</sup>96], [JS94], [NCSB98], [Sch95],  
   [Sch96b], [SN96], [SW97], [SW98], [SWW96],  
   [WS98]  
 Schwindt, P. D. D., 350, [KMSW99]  
 security of quantum key distribution, 593  
 selection rules, electric dipole, 300  
 self-adjoint operator, 70  
 Selman, A. L., 168, [LLS75]  
 Shamir, A., 11, 641, 644, [RSA78]  
 Shannon entropy, 500, 526  
 Shannon's noiseless coding theorem, 500, 537  
 Shannon, C. E., 8, 59, 526, 604, 605, [Sha48], [SW49]  
 Shasha, D., 59, [SL98]  
 Sherwin, M., 351, [IAB<sup>+</sup>99]  
 Sherwood, M. H., 351, [LVZ<sup>+</sup>99], [VYSC99]  
 shift-invariance property of the Fourier transform, 237  
 Shimony, A., 119, [CHSH69]  
 Shockley, W., 4  
 Shor code, 432  
 Shor's algorithm, 7  
 Shor, J., 216  
 Shor, P. W., xix, xxi, 6, 8, 9, 214, 216, 245, 246, 265,  
   432, 450, 497–499, 604, 606, 607, [BBC<sup>+</sup>95],  
   [BS98], [CRSS97], [CRSS98], [CS96], [DS96],  
   [DSS98], [RHSS97], [Sho94], [Sho95], [Sho96],  
   [Sho97], [SL97], [SP00], [SS96]  
 similarity transformation, 75  
 Simon's problem, 241  
 Simon, B., 527, [Sim79]  
 Simon, D. R., 246, [Sim94], [Sim97]  
 simple cycle, 143  
 simple harmonic oscillator, 277, 283  
 simulation of one computational model by another, 126  
 simulations, quantum and classical, 204  
 single photons, 287, 296, 343  
 Singleton bound, 445  
   quantum, 568  
 singular value decomposition, 78  
 singular values, 79  
 Sleator, T., 214, [BBC<sup>+</sup>95]  
 Slepian, D., 59, [Sle74]  
 Slichter, C. P., 351, [Sli96]  
 Sloane, N. J. A., 59, 497, 498, [CRSS97], [CRSS98],  
   [MS77], [RHSS97], [SW93]  
 Slotine, J. E., 352, [LS98]  
 Small, A., 351, [IAB<sup>+</sup>99]  
 Smolin, J. A., 214, 497, 606, 607, [BBB<sup>+</sup>92],  
   [BBC<sup>+</sup>95], [BBP<sup>+</sup>96], [BDS97], [BDSW96],  
   [BST98], [DSS98], [SS96]  
 Solovay, R., 5, 624, 644, [SS76]  
 Solovay–Kitaev theorem, 197, 617  
 Somaroo, S. S., 351, [CMP<sup>+</sup>98], [STH<sup>+</sup>99]  
 Sørensen, J. L., 59, 352, [FSB<sup>+</sup>98]  
 Sornborger, A. T., 214, 215, [SS99]  
 sorting, 137  
 source–channel coding, 553  
 space hierarchy theorem, 151  
 space-bounded computation, 150  
 span of a set of vectors, 63  
 spanning set, 62  
 spatial labeling, 333  
 spectral decomposition, 70, 72  
 Spiller, T., xix, [LSP98]  
 spin, 310  
 spin orbit interaction, 301  
 spin singlet, 113  
 spin valve, 345  
 spin–lattice relaxation, 280, 330  
 spin–spin relaxation, 280, 330  
 spontaneous emission, 315, 380  
 spur, 559  
 square well, 280  
 stabilizer codes, 453, 465  
 stabilizer formalism, 453  
 stabilizer of a vector space, 454  
 standard deviation of a random variable, 609  
 standard form  
   for a stabilizer code, 470  
   for parity check matrix, 447  
 starting state of a Turing machine, 123  
 state space, 80, 102  
 state tomography, 389  
   with NMR, 336  
 state vector, 80  
 static measures of distance, 399  
 stationary states, 83  
 Steane code, 453  
 Steane, A. M., 8, 350, 450, 497, 499, [Ste96a],  
   [Ste96b], [Ste97], [Ste99]  
 Steinberg, A. M., 350, [KSC<sup>+</sup>94]  
 Stern, O., 43  
 Stern–Gerlach experiment, 43  
 Stewart, E. D., 214, 215, [SS99]  
 Stiefel, E., 616, [FS92]  
 Stirzaker, D. R., 609, [GS92]  
 stochastic differential equations, 353  
 stochastic processes, 355  
 Stoll, S., xxi  
 Strang, G., 118, [Str76]  
 Strassen, V., xxi, 5, 216, 644, [SS76]  
 Streater, R. F., 398, [LS93]  
 strict concavity, 504  
 strictly self-dual linear codes, 449  
 string theory, 6  
 strong concavity of the fidelity, 414  
 strong convexity of trace distance, 408  
 strong subadditivity  
   classical, 506  
   proof of, 519  
   quantum, 519  
 structural complexity, 168  
 subadditivity  
   classical, 506  
   quantum, 516  
 subgroup, 610  
 subset–sum, 149  
 superconductor, 344  
 superdense coding, 17, 97, 119, 275, 352  
 superposition principle, 94

- superpositions, 81  
 support of a Hermitian operator, 105  
 swap operation in Fourier transform, 219  
 Switkes, M., 351, [HSM<sup>+</sup>98]  
 Szilard, L., 168, [Szi29]
- $T_1$ , 280, 330  
 $T_2$ , 280, 330  
 tape for a Turing machine, 123  
 Tapp, A., 59, 276, [BBHT98], [BHT98]  
 Tarjan, R., 217  
 Taylor, W., 214, [BT97]  
 Teich, M. C., 349, [ST91]  
 teleportation, quantum, 17, 26, 352  
 temporal labeling, 333  
 tensor product, 62, 71, 72  
 Terhal, B. M., 215, 606, [BST98], [TD98]  
 Thapliyal, A., 119  
 theorem  
    $Z$ - $Y$  decomposition for a single qubit, 175  
   Basic properties of Shannon entropy, 506  
   Basic properties of von Neumann entropy, 513  
   Birkhoff's theorem, 574  
   Chaining rule for conditional entropies, 508  
   Characterization of density operators, 101  
   Chinese remainder theorem, 629  
   Concavity of the quantum conditional entropy, 520  
   Convexity of the relative entropy, 520  
   Cook–Levin, 146  
   Data processing inequality, 509  
   Error-correction conditions for stabilizer codes, 466  
   Euler's theorem, 144  
   Fannes' inequality, 512  
   Fermat's little theorem, 630  
   Fundamental theorem, 613  
   Fundamental theorem of arithmetic, 625  
   Gottesman–Knill theorem, 464  
   High fidelity implies low entropy, 594  
   Holevo–Schumacher–Westmoreland (HSW) theorem, 555  
   Information gain implies disturbance, 586  
   Klein's inequality, 511  
   Lagrange's theorem, 610  
   Law of large numbers, 541  
   Lieb's theorem, 520, 646  
   Monotonicity of the fidelity, 414  
   Monotonicity of the relative entropy, 524  
   Non-negativity of the relative entropy, 505  
   Polar decomposition, 78  
   Projective measurements increase entropy, 515  
   Quantum data processing inequality, 564  
   Quantum error-correction conditions, 436  
   Quantum Fano inequality, 563  
   Representation theorem for the gcd, 626  
   Schmidt decomposition, 109  
   Schumacher's noiseless channel coding theorem, 544  
   Schur's lemma, 613  
   Shannon's noiseless channel coding theorem, 540  
   Shannon's noisy channel coding theorem, 553  
   Simultaneous diagonalization theorem, 77  
   Singular value decomposition, 79  
   Solovay–Kitaev theorem, 618  
   Spectral decomposition, 72  
   Strong concavity of the fidelity, 414  
   Strong convexity of the trace distance, 407  
   Strong subadditivity, 521  
   Subadditivity of the conditional entropy, 523  
   The Chernoff bound, 154  
   The Holevo bound, 531  
   Theorem of typical sequences, 539  
   Trace-preserving quantum operations are contractive, 406  
   Trotter formula, 207  
   Typical subspace theorem, 543  
   Uhlmann's theorem, 410  
   Unitary freedom in the ensemble for density matrices, 103  
   Unitary freedom in the operator-sum representation, 372  
   thermal equilibrium, 328  
   Thomas, J. A., 59, 526, 539, 604, 605, [CT91]  
   threshold condition, 480, 493  
   threshold for quantum computation, 493  
   threshold theorem, 425  
   Tian, L., 351, [MOL<sup>+</sup>99]  
   Tiech, M. C., 349, [CST89]  
   time hierarchy theorem, 151  
   TIME $f(n)$ , 141  
   TOCSY, 339  
   Toffoli gate, 29, 155, 159  
     control bits, 159  
     fault-tolerant, 488  
     target bit, 159  
   Toffoli, T., 168, [FT82]  
   tomography, 389  
   trace distance, 618  
     classical, 400  
     operational meaning for, 400  
     quantum, 403  
   trace inner product, 76  
   trace of a matrix, 75  
   trace-preserving quantum operations, 360, 367  
   tractable computational problems, 139  
   transistor, 4  
   transpose, 62, 70  
   transpose operation, 368  
   transversal property of fault-tolerant operations, 483  
   triangle inequality, 516  
   Tromp, J., 169, [LTV98]  
   Trotter formula, 207  
   Trotter, H. F., 214, [Tro59]  
   Tsai, J. S., 351, [NPT99]  
   Tseng, C. H., 351, [STH<sup>+</sup>99]  
   Tsirelson's inequality, 118, 119  
   Tsirelson, B. S., 119, [Tsi80]  
   Turchette, Q. A., 306, 307, 350, 398, [THL<sup>+</sup>95], [Tur97]  
   Turing machine, 4, 120, 122  
     quantum, 203  
   Turing number, 125  
   Turing, A. M., 4, 59, 122, 125, 167, [Tur36]  
   two-level atom, 298, 327  
     resonance, 326  
   two-level unitary matrices, 189  
   typical sequences, 538
- Ueda, M., 350, [KU91]  
 Uffink, J. H. B., 526, [MU88]  
 Uhlmann's formula, 411  
 Uhlmann's theorem, 410  
 Uhlmann, A., xxi, 119, 424, 527, 606, [Uhl70], [Uhl71], [Uhl72], [Uhl73], [Uhl76], [Uhl77]  
 Umegaki, H., 526, [Ume62]  
 uncomputation, 158

- uniform circuit family, 134  
 unit vector, 66  
 unitary evolution, 356  
 unitary operators, 70  
   approximation, 194  
   efficient decompositions, 191, 198  
 Universal Turing Machine, 4, 128  
 universality, 281  
   discrete set of universal operations, 194  
   family of quantum gates, 188, 281  
   of the Fredkin gate, 157  
   proof of, 132  
   single qubit gates and CNOT, 191  
   two-level unitary operators, 189
- Vaidman, L., 352, [Vai94]  
 van Dam, W., 276, [van98a]  
 van de Graaf, J., 424  
 van de Graaf, J., 424, 607, [BBB<sup>+</sup>98], [FvdG99]  
 van der Waal, C. H., 351, [MOL<sup>+</sup>99]  
 van Duzer, T., 350, [RWvD84]  
 van Enk, S. J., xxi, 605, [van98b]  
 van Oorschot, P. C., 59, 275, [MvOV96]  
 Vandersypen, L. M. K., xxi, 215, 351, [CVZ<sup>+</sup>98], [LVZ<sup>+</sup>99], [VYSC99]  
 Vanstone, S. A., 59, 275, [MvOV96]  
 variance of a random variable, 609  
 Vatan, F., 214, 215, [BMP<sup>+</sup>99]  
 Vazirani, U., xxi, 200, 214, 276, 351, [BBBV97], [BV97], [SV99]  
 vector game, 166  
 vector spaces, 61  
 vector subspace, 62  
 vectors, 61  
 Vedral, V., 606, [Ved99], [VP98]  
 Verhulst, A., xxi  
 Vernam cipher, 583  
 vertex cover, 149  
 vertices, 143  
 Vidal, G., 351, 606, [Vid98], [Vid99]  
 Viola, L., 498, [KLV99]  
 Vitanyi, P., 169, [LTV98], [LV96]  
 Vogel, K., 398, [VR89]  
 von Neumann entropy, 54, 510, 526  
 von Neumann, J., 4, 119, 164, 168, 498, [von27], [von56], [von66]  
 Vrijen, R., 351, [VYW<sup>+</sup>99]
- Wallach, D., xxi  
 Walsh–Hadamard transform, 31  
 Wang, K., 351, [VYW<sup>+</sup>99]  
 Warren, W., 351, [War97]  
 Watanabe, K., 350, [WY90]  
 Watrous, J., 214, [Wat99]  
 weakly self-dual linear codes, 449  
 Weaver, W., 59, 604, 605, [SW49]  
 Wehrl, A., 526, 527, [Weh78]  
 Weinfurter, H., 59, 119, 214, [BBC<sup>+</sup>95], [BPM<sup>+</sup>97], [MWKZ96]  
 Welsh, D. J. A., 497, [Wel88]  
 Westmoreland, M. D., xxi, 605, 607, [HJS<sup>+</sup>96], [SW97], [SW98], [SWW96], [WS98]  
 Whaley, K. B., 498, [BKLV99], [LBW99], [LCW98]  
 Whinnery, J. R., 350, [RWvD84]  
 White, A. G., 350, [KMSW99]  
 Wiesner, S. J., 9, 10, 119, 214, 215, 606, [BW92], 663, [Wie83], [Wie96], [Wie]
- Wigner, E. P., 527, [WY63]  
 Wilczek, F., 215, [CW95]  
 Williams, D., 609, [Wi91]  
 Wilson, E. O., 1  
 Wineland, D. J., xxi, 323, 350, [MMK<sup>+</sup>95], [WMI<sup>+</sup>98]  
 Winfree, E., 168, [Win98]  
 Winograd, S., 168, 498, [WC67]  
 Wiseman, H., xxi  
 witness, 142  
 Wokaun, A., 351, [EBW87]  
 Wootters, W. K., 59, 119, 497, 604–606, [BBC<sup>+</sup>93], [BBP<sup>+</sup>96], [BDSW96], [HJS<sup>+</sup>96], [HJW93], [SWW96], [WZ82]  
 word of length  $l$  from  $\mathcal{C}$ , 618  
 work bits, 131  
 Wright, E. M., 246, 639, [HW60]  
 Wyner, A. D., 59, [SW93]
- XOR, 20  
 XOR gate, 130
- Yablonoitch, E., 351, [VYW<sup>+</sup>99]  
 Yamaguchi, F., 351, [YY99]  
 Yamamoto, Y., xxi, 349–351, 498, [CY95], [IY94], [LNCY97], [WY90], [YKI88], [YY99]  
 Yanase, M. M., 527, [WY63]  
 Yannoni, C. S., 351, [LVZ<sup>+</sup>99], [VYSC99]  
 Yao, A. C., 214, [Yao93]  
 Yard, J., xxi  
 Younis, S., 168, [YK95]  
 Yuen, H. P., 605, [YO93]  
 Yurke, B., xxi, 349
- Z* gate, 19  
 Zalka, C., 214, 215, 276, [Zal98], [Zal99]  
 Zanardi, P., 498, [Zan99], [ZR98]  
 Zbinden, H., 607, [MZG96]  
 Zeilinger, A., 59, 119, 214, 350, [BPM<sup>+</sup>97], [MWKZ96], [RZBB94]  
 zero operator, 63  
 zero vector, 62  
 Zhou, X. L., xxi, 246, 351, 499, [CVZ<sup>+</sup>98], [LVZ<sup>+</sup>99], [ZLC00]  
 Zoller, P., 350, 398, 498, [CPZ96], [CZ95], [PCZ97], [ZG97]  
 Zurek, W. H., xxi, 351, 398, 497–499, 604, 606, [CMP<sup>+</sup>98], [KLZ98a], [KLZ98b], [LMPZ96], [WZ82], [ZL96], [Zur89], [Zur91]  
 Zyczkowski, K., 351, [ZHSL99]