

## References

- [1] S.M. Aji and R.J. McEliece, "A general algorithm for distributing information on a graph," *Proc. 1997 IEEE Int. Symp. on Inform. Theory*, Ulm, Germany, July 1997.
- [2] S.M. Aji, G.B. Horn and R.J. McEliece, "Iterative decoding on graphs with a single cycle," *Proc. 1998 IEEE Int. Symp. on Inform. Theory*, Boston, USA, August 1998.
- [3] M. Ajtai, J. Komlos and E. Szemerédi, "Deterministic simulation in logspace," *Proc. 19th Annual ACM Symp. on Theory of Computing*, pp. 132-139, 1987.
- [4] A. Albanese, J. Blömer, J. Edmonds, M. Luby and M. Sudan, "Priority Encoding Transmission," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1737-1744, Nov. 1996.
- [5] N. Alon, "Eigenvalues and expanders," *Combinatorica*, vol. 6, no. 2, pp. 83-96, 1986.
- [6] N. Alon and F.R.K. Chung, "Explicit construction of linear sized tolerant networks," *Discr. Math.*, vol. 72, pp. 15-19, 1988.
- [7] N. Alon, J. Bruck, J. Naor, M. Naor and R. Roth, "Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs," *IEEE Trans. Inform. Theory*, vol. 38, pp. 509-516, 1992.
- [8] N. Alon, J. Edmonds, and M. Luby, "Linear Time Erasure Codes with Nearly Optimal Recovery," *Proc. 36th Annual Symp. on Foundations of Computer Science*, pp. 512-519, 1995.
- [9] N. Alon and M. Luby, "A Linear Time Erasure-Resilient Code with Nearly Optimal Recovery," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1732-1736, Nov. 1996.
- [10] N. Alon and J.H. Spenser, *The Probabilistic Method*. New York: Wiley, 2000.
- [11] L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Inform. Theory*, vol. 20, pp. 284-287, Mar. 1974.

- [12] A. Barg, "Complexity Issues in Coding Theory," *Handbook on Coding Theory*, editors V. Pless and W.C. Huffman. Amsterdam, Elsevier Publishing, 1998.
- [13] A. Barg and G. Zémor, "Error exponents of expander codes," *IEEE Trans. Inform. Theory*, vol.48, pp. 1725-1729, 2002.
- [14] A. Barg and G. Zémor, "Error exponents of expander codes under linear-complexity decoding," manuscript, 2001.
- [15] S. Benedetto and G. Montorsi, "Unveiling Turbo Codes: Some Results on Parallel Concatenated Coding Schemes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 409-428, Mar. 1996.
- [16] S. Benedetto and G. Montorsi, "Design of Parallel Concatenated Convolutional Codes," *IEEE Trans. Commun.*, vol. 44, no. 5, pp. 591-600, May 1996.
- [17] S. Benedetto, D. Divsalar, G. Montorsi and F. Pollara, "Serial Concatenation of Interleaved Codes: Performance Analysis, Design, and Iterative Decoding," *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 909-926, May 1998.
- [18] E.R. Berlekamp, H. Van Tilborg and R.J. McEliece, "On the inherent intractibility of certain coding problems," *IEEE Trans. Inform. Theory*, vol. 24, pp. 384-386, 1978.
- [19] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes(1)," *Proc. IEEE Int. Conf. on Communications*, Geneva, Switzerland, May 1993.
- [20] C. Berrou and A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo-Codes," *IEEE Trans. Commun.*, vol. 44, no. 10, pp. 1261-1271, Oct. 1996.
- [21] R. C. Bose and D. K. Ray-Chaudhuri, "On a Class of Error Correcting Binary Group Codes," *Information and Control*, Volume 3, pp. 68 - 79, March 1960.
- [22] R. C. Bose and D. K. Ray-Chaudhuri, "Further Results on Error Correcting Binary Group Codes," *Information and Control*, Volume 3, pp. 279 - 290, September 1960.
- [23] D. Burshtein and G. Miller, "Expander Graph Arguments for Message-Passing Algorithms," *IEEE Trans. Inform. Theory*, vol. 47, pp. 782-790, Feb. 2001.
- [24] J.-F. Cheng and R.J. McEliece, "Some High-Rate Near Capacity Codecs for the Gaussian Channel," *Proc. 34th Allerton Conference on Communications, Control and Computing*, 1996.
- [25] S-Y Chung, G.D. Forney Jr., T. Richardson and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Commun. Lett.*, vol. 5, pp. 58-60, Feb. 2001.
- [26] S-Y Chung, T. Richardson and R. Urbanke, "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation," *IEEE Trans. Inform. Theory*, vol. 47, pp. 657-670, Feb. 2001.

- [27] G.F. Cooper, "The Computational Complexity of Probabilistic Inference Using Bayesian Belief Networks," *Artificial Intelligence*, vol. 42, pp. 393-405, 1990.
- [28] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Inc., 1991.
- [29] P. Dagum and M. Luby, "Approximating probabilistic inference in Bayesian belief networks is NP-hard," *Artificial Intelligence*, vol. 60, pp. 141-153, 1993.
- [30] M.C. Davey and D.J.C. MacKay, "Low-Density Parity-Check Codes over  $GF(q)$ ," *IEEE Commun. Letters*, vol. 2., no. 6, June 1998.
- [31] D. Divsalar and F. Pollara, "Multiple Turbo Codes for Deep-Space Communications," *TDA Progress Report 42-121*, pp. 66-77, May 15, 1995.
- [32] D. Divsalar and F. Pollara, "Turbo Codes for PCS Applications," *Proc. IEEE Int. Conf. on Communications*, Seattle, Washington, June 1995.
- [33] D. Divsalar and R.J. McEliece, "On the Design of Generalized Concatenated Coding Systems with Interleavers," manuscript, 1998.
- [34] S. Dolinar and D. Divsalar, "Weight Distributions for Turbo Codes Using Random and Nonrandom Permutations," *TDA Progress Report 42-122*, pp. 56-65, August 15, 1995.
- [35] H. El Gamal and A.R. Hammons, Jr, "Analyzing the turbo decoder using the Gaussian approximation," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 671-686, Feb. 2001.
- [36] P. Elias, "Coding for Noisy Channels," *IRE Conv. Record*, Part 4, pp. 37 - 47, 1955.
- [37] G. D. Forney, Jr.. *Concatenated Codes*, Cambridge: MIT Press, 1966.
- [38] G.D. Forney, Jr., "The forward-backward algorithm," *Proc. 34th Allerton Conference on Communications, Control and Computing*, 1996.
- [39] B.J. Frey, *Graphical Models for Machine Learning and Digital Communication*. The M.I.T. Press, Cambridge, MA, 1998.
- [40] R.G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. 8, pp. 21-28, Jan. 1962.
- [41] R.G. Gallager, *Low-Density Parity-Check Codes*. The M.I.T. Press, Cambridge, MA, 1963.
- [42] E.N. Gilbert, "A Comparison of Signaling Alphabets," *Bell Sys. Tech. J.*, vol. 31, pp. 504-522, 1952.
- [43] D. Gorenstein and N. Zierler, "A Class of Error Correcting Codes in  $p^m$  Symbols," *Journal of the Society of Industrial and Applied Mathematics*, Volume 9, pp. 207 - 214, June 1961.

- [44] W.C. Gore, "Transmitting Binary Symbols with Reed-Solomon Codes," *Proceedings of the Princeton Conference on Information Science and Systems*, Princeton, New Jersey, pp. 495 - 497, 1973.
- [45] V. Guruswami and P. Indyk, "Linear-time Codes to Correct a Maximum Possible Fraction of Errors," *Proc. 39th Allerton Conference on Communications, Control and Computing*, 2001.
- [46] V. Guruswami and P. Indyk, "Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets," preprint, 2002.
- [47] J. Hagenauer, E. Offer and L. Papke, "Iterative decoding of binary block and convolutional codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 2, pp. 429-445, Mar. 1996.
- [48] C. Heegard and S.B. Wicker, *Turbo Coding*. Kluwer Academic Press, 1998.
- [49] S. Hirasawa, M. Kasahara, Y. Sugiyama and T. Namekawa, "Modified Product Codes," *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 299-306, Mar. 1984.
- [50] A. Hocquenghem, "Codes Correcteurs d'Erreurs," *Chiffres*, Volume 2, pp. 147 - 156, 1959.
- [51] T. W. Hungerford, *Algebra*, New York: Springer-Verlag, 1974.
- [52] K. A. S. Imminck, "RS Codes and the Compact Disc," in *Reed Solomon Codes and Their Applications*, (Stephen Wicker and Vijay Bhargava, ed.) , IEEE Press, 1994.
- [53] F.V. Jensen, S.L. Lauritzen and K.G. Olesen, "Bayesian updating in recursive graphical models by local computation," *Computational Statistical Quarterly*, vol. 4, pp. 269-282, 1990.
- [54] H. Jin, A. Khandekar and R. McEliece, "Irregular Repeat-Accumulate Codes," *Proc. 2nd. International Conf. Turbo Codes*, Brest, France, pp. 1-8, Sept. 2000.
- [55] N. Kahale, "Expander Graphs," Ph.D. dissertation, M.I.T., 1993.
- [56] E.M. Kasahara, Y. Sugiyama, S. Hirasawa and T. Namekawa, "New classes of binary codes constructed on the basis of concatenated codes and product codes," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 462-468, July 1976.
- [57] S. Kim, "Probabilistic Reasoning, Parameter Estimation, and Issues in Turbo Decoding," Ph.D. dissertation, Cornell University, 1998.
- [58] S. Kim and S.B. Wicker, "Thoughts on Expander Codes: Codes via Irregular Bipartite Graphs," *Annual Conf. on Information Sciences and Systems '00*, Princeton, USA, 2000.
- [59] S. Kim and S.B. Wicker, "Linear-Time Encodable and Decodable Irregular Graph Codes," *Proc. 2000 IEEE Int. Symp. on Inform. Theory*, Italy, 2000.
- [60] F.R. Kschischang and B.J. Frey, "Iterative Decoding of Compound Codes by Probability Propagation in Graphical Models," *IEEE Journal on Selected Areas in Commun.*, vol. 16, pp. 219-230, Feb. 1998.

- [61] F.R. Kschischang, B.J. Prey and H-A Loeliger, "Factor Graphs and the Sum-Product Algorithm," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 498-519, Feb. 2001.
- [62] J. Lafferty and D.N. Rockmore, "Spectral Techniques for Expander Codes," *Proc. 29th Annual ACM Symposium on Theory of Computing*, pp. 160-167, 1997.
- [63] J. Lafferty and D.N. Rockmore, "Codes and Iterative Decoding on Algebraic Expander Graphs," *Int. Symp. Inform. Theory and Appl.*, Nov. 2000.
- [64] S.L. Lauritzen and D.J. Spiegelhalter, "Local Computation with Probabilities on Graphical Structures and Their Application to Expert Systems," *Journal of the Royal Statistical Society, Series B*, vol. 50, pp. 157-224, 1988.
- [65] S. Le Goff, A. Glavieux and C. Berrou, "Turbo-Codes and High Spectral Efficiency Modulation," *Proc. IEEE Int. Conf. on Communications*, New Orleans, USA, May 1994.
- [66] R. Lidl and H. Niederreiter, *Finite Fields*, Reading, Mass.: Addison Wesley, 1983.
- [67] A. Lubotzky, R. Phillips and P. Sarnak, "Ramanujan Graphs," *Combinatorica*, vol. 8, no. 3, pp. 261-277, 1988.
- [68] S. Lin and E.J. Weldon, "Further Results on Cyclic Product Codes," *IEEE Trans. Inform. Theory*, vol. IT-16, no. 4, pp. 452-459, July 1970.
- [69] M. Luby, M. Mitzenmacher, M.A. Shokrollahi, D.A. Spielman and V. Stemann, "Practical Loss-Resilient Codes," *Proc. 29th Annual ACM Symp. on Theory of Computing*, pp. 150-159, 1997.
- [70] M. Luby, M. Mitzenmacher and M.A. Shokrollahi, "Analysis of Random Processes via And-Or Trees," in *Proc. 9th Symp. on Discrete Algorithms*, pp. 364-373, 1998.
- [71] M. Luby, M. Mitzenmacher, M.A. Shokrollahi and D.A. Spielman, "Analysis of Low Density Codes and Improved Designs Using Irregular Graphs," *Proc. 30th Annual ACM Symposium of Theory of Computing*, pp. 249-258, 1998.
- [72] M. Luby, M. Mitzenmacher, M.A. Shokrollahi and D.A. Spielman, "Improved Low-Density Parity-Check Codes Using Irregular Graphs and Belief Propagation," *Proc. 1998 IEEE Int. Symp. on Inform. Theory*, Boston, USA, August 1998.
- [73] D.J.C. MacKay and R.M. Neal, "Good error-correcting codes based on very sparse matrices," *Cryptography and Coding, Lecture Notes in Computer Science no. 1025*, pp. 100-111, Springer-Verlag, 1995.
- [74] D.J.C. MacKay and R.M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, pp. 1645-1646, Aug. 1996; reprinted *Electron. Lett.*, vol. 33, no. 6, pp. 457-458, Mar. 1997.

- [75] D.J.C. MacKay, "Good Error-Correcting Codes based on Very Sparse Matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399-431, Mar. 1999.
- [76] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam: North Holland, 1977.
- [77] G.A. Margulis, "Explicit constructions of concentrators," *Probl. Inform. Transm.*, vol. 9, pp. 325-332, 1973.
- [78] G.A. Margulis, "Explicit constructions of graphs without short cycles and low density codes," *Combinatorica*, vol. 2, pp. 71-78, 1982.
- [79] G.A. Margulis, "Explicit group-theoretical constructions of combinatorial schemes and their applications to the design of expanders and concentrators," *Probl. Inform. Transm.*, vol. 24, pp. 39-46, 1988.
- [80] R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr. and L. R. Welch, "New Upper Bounds on the Rate of a Code using the Delsarte-MacWilliams Inequalities," *IEEE Trans. Inform. Theory*, vol. 23, pp. 157-166, 1977.
- [81] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Boston: Kluwer Academic Publishers, 1987.
- [82] R.J. McEliece, E. Rodemich and J.-F. Cheng, "The Turbo Decision Algorithm," *Proc. 33rd Allerton Conference on Communication, Control and Computing*, 1995.
- [83] R.J. McEliece, D.J.C. MacKay and J.-F. Cheng, "Turbo Decoding as an Instance of Pearl's 'Belief Propagation' Algorithm," *IEEE Journal on Selected Areas in Commun.*, vol. 16, pp. 140-152, Feb. 1998.
- [84] G. Miller and D. Burshtein, "Bounds on the Maximum-Likelihood Decoding Error Probability of Low-Density Parity-Check Codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2696-2710, Nov. 2001.
- [85] R. Motwani and P. Raghavan, *Randomized Algorithms*. Cambridge University Press, 1995.
- [86] P. Oswald and M.A. Shokrollahi, "Capacity-Achieving Sequences for the Erasure Channel," manuscript, 2000.
- [87] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann Publishers, Inc., San Mateo, CA, 1988.
- [88] W. W. Peterson, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes," *IRE Transactions on Information Theory*, Volume IT-6, pp. 459 - 470, September 1960.
- [89] L.C. Perez, J. Seghers and D.J. Costello, Jr., "A distance spectrum interpretation of turbo codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1698-1709, Nov. 1996.
- [90] N. Pippenger, "Superconcentrators," *SIAM Journal of Computing*, vol. 6, pp. 298-304, 1977.

- [91] R. Pyndiah, A. Glavieux, A. Picart and S. Jacq, "Near Optimum Decoding of Product Codes," *Proc. of Globecom 94*, vol. 1, pp. 339-343, Nov. 1994.
- [92] I. S. Reed, "A Class of Multiple-Error-Correcting Codes and a Decoding Scheme," *IEEE Transactions on Information Theory*, Volume 4, pp. 38 – 49, September 1954.
- [93] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Trans. Inform. Theory*, vol. 47, pp. 599-618, Feb. 2001.
- [94] T. Richardson, M.A. Shokrollahi and R. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619-637, Feb. 2001.
- [95] T. Richardson and R. Urbanke, "Efficient Encoding of Low-Density Parity-Check Codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 638-656, Feb. 2001.
- [96] J. Rosenthal and P. Vontobel, "Construction of Low-Density Parity-Check Codes using Ramanujan Graphs and Ideas from Margulis," *Proc. 38th Allerton Conference on Commun. Control and Computing*, Monticello, Illinois, Oct. 2000.
- [97] P. Rusmevichientong and B. Van Roy, "An analysis of belief propagation on the turbo decoding graph with Gaussian densities," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp.745-765, Feb. 2001.
- [98] E. Sakk and S. B. Wicker, "Finite Field Wavelet Packets for Error Control Coding", *Proceedings of the 39th Annual Allerton Conference on Communication, Control and Computing*, Urbana-Champaign, Il, October 2001.
- [99] P. Sarnak, *Some Applications of Modular Forms*. Cambridge University Press, 1990.
- [100] C.E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, vol 27, pp. 379-423 and pp. 623-656, 1948.
- [101] S.E. Shimony, "Finding MAPs for belief networks is NP-hard," *Artificial Intelligence*, vol. 68, pp. 399-410, 1994.
- [102] M.A. Shokrollahi, "New Sequences of Linear Time Erasure Codes approaching the Channel Capacity," *Proc. AAECC-13, Lecture Notes in Computer Science no. 1719*, pp. 65-76, 1999.
- [103] M. Sipser and D.A. Spielman, "Expander Codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1710-1722, Nov. 1996.
- [104] P. Smyth, D. Heckerman and M.I. Jordan, "Probabilistic Independence Networks for Hidden Markov Probability Models," *Neural Computation*, vol. 9, pp. 227-269, 1997.
- [105] D.A. Spielman, "Linear-Time Encodable and Decodable Error-Correcting Codes," *IEEE Trans. Inform. Theory*, vol. 42, no. 6, pp. 1723-1731, Nov. 1996.

- [106] O. Y. Takeshita, O. M. Collins, P. C. Massey and D. J. Costello, Jr., "A note on asymmetric turbo-codes," *IEEE Commun. Letters*, vol. 3, no. 3, pp. 69-71, Mar. 1999.
- [107] R.M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, pp. 533-547, Sept. 1981.
- [108] R.M. Tanner, "Explicit concentrators from generalized  $n$ -gons," *SIAM Journal of Alg. Disc. Meth.*, vol. 5, no. 3, pp. 287-293, Sept. 1984.
- [109] R.M. Tanner, "Minimum Distance Bounds by Graph Analysis," manuscript.
- [110] P. Thitimajshima, "Les codes convolutifs recursifs systematiques et leur application a la concatenation parallele," (in French), Ph.D. no. 284, Universite de Bretagne Occidentale, Brest, France, Dec. 1993.
- [111] A. Tietäväinen, "On the Nonexistence of Perfect Codes over Finite Fields," *SIAM Journal of Applied Mathematics*, Volume 24, pp. 88 - 96, 1973.
- [112] A.J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," *IEEE Trans. Inform. Theory*, vol. 13, pp. 260-269, Apr. 1967.
- [113] Y. Weiss, "Correctness of local probability propagation in graphical models and loops," *Neural Computation*, vol. 12, pp. 1-41, 2000.
- [114] Y. Weiss and W.T. Freeman, "On the Optimality of Solutions of the Max-Product Belief-Propagation Algorithm in Arbitrary Graphs," *IEEE Trans. Inform. Theory*, vol. 47, pp. 736-744, Feb. 2001.
- [115] N. Wiberg, H.-A. Loeliger and R. Kötter, "Codes and iterative decoding on general graphs," *European Trans. on Telecommun.*, vol. 6, pp. 513-525, Sep/Oct. 1995.
- [116] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Englewood Cliffs: Prentice Hall, 1995.
- [117] S. B. Wicker, "Deep Space Applications," *Handbook of Coding Theory*, (Vera Pless and William Cary Huffman, ed.), Amsterdam: Elsevier, 1998.
- [118] J.S. Yedidia, W.T. Freeman and Y. Weiss, "Bethe free energy, Kikuchi approximations and belief propagation algorithms," manuscript, 2001.
- [119] G. Zémor, "On Expander Codes," *Trans. on Inform. Theory*, vol. 47, pp. 835-837, Feb. 2001.
- [120] V.V. Zyablov and M.S. Pinsker, "Estimation of the error correction complexity of Gallager low-density codes," *Probl. Inform. Transm.*, vol. 11, no. 1, pp. 18-28, May 1976.



# Index

- $(\alpha, \beta)$  expander, 83
- $(d_{v_1}, d_{v_2}, \alpha, \beta)$  expander, 83
- $(n, k, d)$  code, 2
- a priori* information, 122, 129
  
- abelian, 14
- abstract algebra, 12
- achievable rate, 2
- additive white Gaussian noise channel, 169
- adjacency matrix, 82, 137, 177
- Aji, S. M., 209
- Ajtai, M., 92, 209
- Albanese, A., 209
- algebraic block codes, 12
- algebraic coding theory, 12
- algorithm
  - BCJR, 94, 112, 113, 115
  - belief propagation, 93, 99, 103, 104, 109, 112
  - Berlekamp's, xv
  - error reducing, 182, 183
  - Euclid's, 18
  - exponential time, 5
  - Gallager, 151–153, 181, 187
  - junction tree propagation, 93, 104, 106, 108, 112, 114, 115
  - loss recovery, 197
  - message-passing, 93, 103, 115–118, 120
  - nondeterministic, 5
  - polynomial time, 5
  - probabilistic reasoning, 93, 99, 100, 104, 106
  - Viterbi, 94, 112, 113
- Alon, N., 87, 174, 209
- ancestor, 97
- ancestor set, 97
- AND-OR tree, 188
- associativity, 14
  
- asymptotic behavior, function, 5
- asymptotically good code, 147, 174
- augmented codes, 42
- Azuma's inequality, 85, 86, 90, 156
  
- Bahl, L. R., xvi, 209
- Barg, A., 147, 150, 174, 210
- basis, 24
- Baum, L., xvi
- Baum-Welch algorithm, xvi
- Bayesian network, 95, 99, 123
  - low-density parity-check code, 164
- BCH bound, 54, 57
- BCH codes, xv, 53
  - design procedure, 56
  - narrow-sense, 55
  - primitive, 55
- BCJR algorithm, 94, 112, 113, 115
- belief propagation, xvii, xviii, 12, 93, 99, 103, 104, 109, 112, 123, 162, 174
- Benedetto, S., 77, 132, 210
- Berger, T., xix
- Berlekamp's algorithm, xv, 13
- Berlekamp, E. R., 210
- Berrou, C., xvii, 61, 70, 71, 121, 122, 109, 99,
- Bethe free energy, 117
- Bhargava, V. K., xv, 212
- binary erasure channel (BEC), 4
- binary symmetric channel (BSC), 4, 169
- bipartite graph, 79, 80, 137, 177
- Blömer, J., 209
- Boolean function, xiv, 46
- boolean net function language, 45
- Bose, R. C., xv, 53, 210
- bound
  - BCH, 54, 57
  - Gilbert, 9
  - Gilbert-Varshamov, 11, 42, 150
  - Hamming, 9

- McEliece-Rodemich-Rumsey-Welch, 11
- Singleton, 11, 57, 150
- sphere packing, 9
- bounded distance decoding, 7
- Bruck, J., 209
- Burshtein, D., 210
- capacity, 61
- cardinality, 13
- cascaded code, 200, 202
  - decoding, 201
  - Spielman's construction, 202
- Cauchy-Schwarz inequality, 89
- Cayley graph, 87, 148, 174
- CCSDS standard for deep space teleme-  
try, 61
- cellular telephony, 61
- channel capacity, 4
- characteristic, 26
- check node, 177
  - confused, 186
  - unhelpful, 186
- Cheng, J.-F., xvii, 207, 210
- child, 97
- Chinese remainder theorem, 58
- chord, 105
- chromatic number, 80, 86
- Chung, F. R. K., 209
- Chung, S. Y., 210
- class NP, 5
- clique, 104
- clique graph, 104
- closure, 14
- Cocke, J., xvi, 209
- code
  - asymptotically good, 11, 147, 174
  - augmented, 42
  - BCH, 53
  - cascaded, 200, 202
    - decoding, 201
    - Spielman's construction, 202
  - component, 123
  - concatenated, 12, 61, 68, 147
  - construction, 6
  - convolutional, 12, 61, 65
  - cyclic, 13, 49
  - decoding, 6
  - dimension, 40
  - encoding, 6
  - error reducing, 181
  - expander, 174
  - expurgated, 42
  - extended, 42
  - Golay, 39, 51
  - Hamming, 44
    - duals, 47
  - high girth, 151
    - inner, 61
    - lengthened, 42
    - low-density generator, 12, 177, 179–  
181, 187
      - irregular, 178
      - regular, 178
    - low-density parity-check, 12, 137,  
177, 187
      - Bayesian network representation,  
164
    - maximum cardinality, 9
    - maximum distance separable (MDS),  
12
    - outer, 61
    - parallel concatenated, 71
    - parity-check, 44
      - perfect, 9, 52
      - product, 58
    - punctured, 42
    - quadratic residue, 51
    - rate, 40
    - Reed-Muller, 39, 45
      - duals, 47
    - Reed-Solomon, 13, 39, 53, 57, 69
    - repeat-accumulate, 12, 196
    - repetition, 43
      - shortened, 42
    - systematic, 180
    - tornado, 193
  - code polynomial, 49
  - codeword, 2
    - finite, 71
    - node, 137
  - Collins, O. M., xvi, 215
  - common divisors, 18
  - commutative, 14
  - complexity, 5
  - component code, 68, 123
  - component encoder, xvii, 70
  - concatenated code, 12, 61, 147
    - serial, 61
  - conditional entropy, 3
  - confused, 186
  - conjugacy class, 29
  - conjugates of field elements, 29
  - connected graph, 96
  - constraint
    - length, 63
    - node, 137
      - degree, 138
      - satisfied, 143
      - unsatisfied, 143
  - Consultative Committee for Space Data  
Systems (CCSDS), 68
  - convolutional code, 12, 61, 65
  - convolutional encoder, 62
    - nonrecursive, 62

- nonsystematic, 63
- systematic, 63
- Cooper, G. F., 210
- coset, 15
  - cyclotomic, 33
- Costello, D. J., Jr., 214
- Cover, Thomas M., 211
- cyclic codes, xv, 13, 49
- cyclic graph, 96
- cyclic product code, 58
- cyclotomic cosets, 33
  
- D transform, 63
- D-Separation, 98
- Dagum, P., 211
- Davey, M. C., xviii, 174, 211
- decoding, 2, 6
  - belief propagation, 162
    - low-density parity-check code, 164
  - bounded distance, 7
  - Gallager
    - performance, 157
  - hard decision, 7
  - low-density parity-check code, 143, 151
  - maximum likelihood, 8, 112, 113, 115
  - maximum *a posteriori* (MAP), 8
  - nearest-codeword, 7
  - soft decision, 8
  - symbol-by-symbol MAP, 8
  - turbo, 125
  - Viterbi, 69
- deep space telecommunications, xvi, 39
- degree
  - constraint node, 138
  - variable node, 138
  - vertex, 80
- degree sequence, 174, 188
  - irregular code
    - good, 170
  - node, 138
  - right regular, 195
- depth
  - logical circuit, 6
- descendent, 97
- designed distance, 55
- digital audio, 39
- dimension
  - code, 40
    - vector space, 24
- dimension theorem, 26
- directed acyclic graph (DAG), 97
- directed graph, 80, 95
- disconnected graph, 80
- discrete channel, 1
  - discrete memoryless channel, 1
  - distributive law, 16
  - Divsalar, D., 77, 210
  - Dolinar, S., 211
  - double cover, 81, 88
  - dual space, 25
  
  - edge exposure martingale, 84
  - edge-vertex incidence graph, 79, 81, 92, 148
  - Edmonds, J., 209
  - effective free distance, 77
  - eigenvalue, 79, 82, 83, 86, 88
    - graph, 139
  - El Gamal, H., 211
  - Eldridge, N., xiii
  - Elias, P., xv, 61, 211
  - encoders
    - component, 70
    - convolutional, 62
    - parallel concatenated, 70
    - recursive convolutional, 63
    - recursive systematic, 66, 71
  - encoding, 6
  - entropy, 3
    - conditional, 3
    - joint, 3
  - equivalent tree, 115
  - error reducing algorithm, 182, 183
  - error reducing code, 181
  - Euclid's algorithm, 18
    - extended form, 20
  - Euclidean domain, 17
  - Euler  $\phi$  function, 22
  - European Space Agency (ESA), 70
  - evidence, 100
  - expander code, 174
  - expander graph, 79, 83, 175
  - expansion, 79, 139, 142, 143, 184, 187
    - bound, 83
  - Expectation-Maximization (EM) algorithms, xvii
  - explaining away, 98
  - exponential time complexity, 5
  - expurgated codes, 42
  - extended codes, 42
  - extended form of Euclid's algorithm, 20
  - extended Hamming codes, 44
  - extended Reed-Solomon codes, 57
  - extrinsic information, 122, 129
  
  - factoring  $x^n - 1$ , 33
  - Fano, xv
  - field, 20
    - Galois, 21
      - order  $p$ , 21
      - order  $p^m$ , 26
  - Fine, T., xix

- finite codewords, 71  
 Forney, G. D., Jr., xvi, 61, 115, 147, 210, 211  
 fraction of errors, 144  
 fractional rate loss, 62  
 Freeman, W. T., 216  
 Frey, B., xvii, 134, 211  
 function  
   Euler  $\phi$ , 22  
   incidence, 178  
  
 Galileo, 70  
 Gallager, R. G., xviii, 12, 137, 151, 173, 174, 211  
   decoding algorithms, 151–153, 181, 187  
   performance, 157  
 Galois field, 13, 21  
   Fourier transform, 34  
   transform pair, 34  
   multiplicative structure, 22  
   order  $p$ , 21  
   order  $p^m$ , 26  
   primitive element, 23  
 Galois, Evariste, 21  
 gaussian approximation, 174  
 generator matrix, 40  
   convolutional code, 64  
 generator polynomial, 50  
 generator sequence, 63  
 Gilbert bound, 9  
 Gilbert, E. N., 211  
 Gilbert-Varshamov bound, 11, 42, 150  
 Giotto, 70  
 Glavieux, A., xvii, 61, 70, 71, 121, 122, 210  
 Golay codes, xiv, 51  
   extended, 52  
   ternary, 52  
 Golay, M., xiv  
 Gore, W. C., 212  
 Gorenstein, D., 53, 211  
 Gould, S. J., xiii  
 graph  
   adjacency matrix, 82, 177  
   bipartite, 79, 80, 137, 177  
   Cayley, 87, 148, 174  
   chromatic number, 80, 86  
   clique, 104  
   connected, 96  
   directed, 80  
   directed acyclic (DAG), 97  
   disconnected, 80  
   edge-vertex incidence, 79, 81, 92, 148  
   eigenvalue, 79, 82, 83, 86, 88, 139  
   expander, 79, 83, 175  
   expansion, 139, 142, 143, 184, 187  
   high girth, 173  
   irregular, 80  
   junction tree, 104  
   loopy, 115  
   moral, 95  
   multiply-connected, 97  
   path- $l$ -vertex incidence, 92  
   polytree, 97  
   Ramanujan, 87, 88, 148–150, 175, 206  
   random, 84  
   regular, 79, 80  
   singly-connected, 97  
   tree, 97  
     equivalent, 115  
     triangulated, 105  
     unconnected, 96  
     undirected, 80  
   graph theory, xviii, 12, 79  
   greatest common divisors, 18  
   ground field, 23  
   Guruswami, V., 205, 208, 212  
  
 Hagenauer, J., 212  
 Hamming  
   bound, xiv, 9  
   codes, xiv, 44  
   codes, extended, 44  
   distance, 2  
 Hamming, R. W., xiv, 39  
 Hammons, A. R., Jr., 211  
 hard decision decoding, 7  
 head-to-head, 98  
 Heckerman, D., 215  
 Heegard, C., xvii, 212  
 high girth code, 151  
 high girth graph, 173  
 Hirasawa, S., 212  
 Hocquenghem, A., xv, 53, 212  
 Horn, G. B., 209  
 Huffman, W. C., xvi, 216  
 Hungerford, T. W., 212  
  
 ideals, 13, 37  
   principle, 37  
 identity, 14  
 Immink, Kees A. S., 212  
 incidence function, 178  
 Indyk, P., 205, 208, 212  
 inequality  
   Azuma's, 156  
 information  
   *a priori*, 122, 129  
   extrinsic, 122, 129  
   systematic, 122, 129  
 information node, 177  
 inner code, 61, 68

- input-output weight enumerating function (IOWEF), 67
- input-redundancy weight enumerating function (IRWEF), 65
- Intelsat, 54
- interleaver  
uniform, 72
- inverses, 14
- irreducible polynomials, 28
- irregular graph, 80
- iterative decoding, xvii
- Jacq, S., 214
- Jelinek, F., xvi, 209
- Jensen, F. V., 212
- Jin, H., 208, 212
- joint entropy, 3
- Jordan, M. I., 215
- junction tree, 104
- junction tree propagation algorithm, 93, 104, 106, 108, 112, 114, 115
- Kötter, R., 216
- Kahale, N., 92, 212
- Kasahara, E. M., 212
- Khandekar, A., 212
- Kim, S., 208, 212
- Komlos, J., 209
- Kschischang, F. R., xvii, 134, 212
- Lafferty, J., 174, 213
- Lagrange's theorem, 16
- Lagrange, Joseph Louis, 16
- language recognition problem, 5
- Lauritzen, S. L., 212
- Le Goff, S., 213
- left coset, 15
- lengthened codes, 42
- Lidl, R., 13
- Lin, Shu, 213
- linear code, 40
- linear independence, 24
- linear programming, 161, 174
- Lipschitz condition, 85, 86
- locator polynomial, 55
- Loeliger, H. -A., 213
- logarithmic cost model, 6
- logical circuit  
depth, 6  
model, 6  
size, 6
- loop, 97
- loopy graph, 115
- loss recovery algorithm, 197
- low-density generator code, 12, 177, 179–181, 187  
irregular, 178  
regular, 178
- low-density parity-check code, 12, 137, 177, 187  
Bayesian network representation, 164  
decoding, 143, 151  
belief propagation, 162, 164  
regular, 137
- Lubotzky, A., 87, 148, 213
- Luby, M., xviii, 174, 193, 200, 208, 209
- MacKay, D. J. C., xvii, xviii, 174, 211
- MacWilliams, F. J., 214
- Margulis, G. A., 87, 148, 173, 214
- Markov random field, 95, 99
- martingale, 79, 83, 155, 188  
edge exposure, 84  
sequence, 84, 85, 90  
vertex exposure, 85, 86
- Mason's gain rule, 73
- Massey, P. C., 215
- Mattson-Solomon polynomial, 34
- maximum cardinality of a code, 9
- maximum distance separable (MDS), 12
- maximum likelihood decoding, 8, 112, 113, 115
- maximum likelihood sequence decoding, xv
- maximum *a posteriori* (MAP) decoding, 8
- McEliece, R. J., xvii, 13, 77, 134, 196, 207, 209, 214
- McEliece-Rodemich-Rumsey-Welch bound, 11
- memory vector, 63
- memoryless channel, 1
- message, 102
- message-passing algorithm, 93, 103, 115–118, 120
- Miller, G., 210
- minimal polynomial, 13, 28  
roots, 30
- minimum distance, 2  
linear block code, 40
- minimum relative distance, 10
- Minty, G. J., xvi
- Mitzenmacher, M., xviii, 213
- Montorsi, G., 77, 132, 210
- moral graph, 95
- Motwani, R., 214
- Muller, D., xiv, 45
- multiply-connected graph, 97
- mutual information, 3
- Namekawa, T., 212
- Naor, J., 209
- Naor, M., 209
- narrow-sense BCH codes, 55

- National Aeronautics and Space Agency (NASA), 70
- Neal, R. M., 213
- nearest-codeword decoding, 7
- Niederreiter, H., 13
- node degree sequence, 138
- Noisy Channel Coding Theorem, xiii, 3, 4
- nondeterministic algorithm, 5
- nonsystematic convolutional encoders, 63
- NP-complete, 6
- NP-hard, 6, 172
- Offer, E., 212
- Olesen, K. G., 212
- order
  - $q$  modulo  $n$ , 33
  - Galois field element, 21
  - group element, 15
- Oswald, P., 208, 214
- outer code, 61, 68
- Papke, L., 212
- parallel concatenated code, 70, 71, 123
  - encoding, xvii, 61, 70
- parent, 97
- parity check matrix, 41
- parity relations, xiv
- parity-check codes, 44
- path- $l$ -vertex incidence graph, 92
- Pearl, J., 100, 214
- Perez, L. C., 132, 214
- perfect codes, 9, 52
- Peterson, W. W., 53, 214
- $\text{PGL}(2, \mathbf{Z}/q\mathbf{Z})$ , 87
- Phillips, R., 87, 148, 213
- Picart, A., 214
- Pinsker, M. S., 173, 216
- Pippenger, N., 214
- planetary standard, 69
- Pless, V., xvi, 216
- Pollara, F., 210
- polynomial
  - code, 49
  - generator, 50
  - irreducible, 28
  - locator, 55
  - matrix, 64
  - Mattson-Solomon, 34
  - minimal, 28
  - primitive, 28
  - spectrum, 36
- polynomial time complexity, 5
- polytree, 97
- Prange, G., xv
- primitive
  - element, 23
  - polynomial, 28
  - roots, 32
  - primitive BCH codes, 55
  - principle ideal, 37
  - probabilistic independence network, 95
  - probabilistic reasoning, 93, 94, 99, 100, 104, 106
  - probability model, 94
  - product codes, 58
    - cyclic, 58
  - projective general linear group, 87
  - punctuated equilibrium model, xiii
  - punctured codes, 42
  - Pyndiah, R., 214
- quadratic residue, 50
  - codes, 51
- Raghavan, P., 214
- Ramanujan graph, 87, 88, 148–150, 175, 206
- Ramanujan, Srinivasa Aiyangar, 87
- random access machine (RAM), 6
- random graph, 84
- rate
  - achievable, 2
  - code, 40
- Raviv, J., xvi, 209
- Ray-Chaudhuri, D. K., xv, 53, 210
- recursive
  - constructions, 40
  - convolutional encoders, 63
  - systematic convolutional encoders, 66
  - systematic encoders, 71
- redundancy, 2
- Reed, I. S., xiv, 45, 54, 215
- Reed-Muller codes, xiv, 45
- Reed-Solomon codes, xv, 13, 53, 57, 69
  - extended, 57
  - minimum distance, 57
- regular graph, 79, 80
- regular low-density parity-check code, 137
- repeat-accumulate code, 12, 196
- repetition codes, 43
- Richardson, T., xviii, 174, 210
- right coset, 15
- right regular degree sequence, 195
- ring, 16
- Rockmore, D. N., 174, 213
- Rodemich, E. R., 11, 214
- roots
  - minimal polynomial, 30
  - primitive polynomial, 32
- Rosenthal, J., 215
- Roth, R., 209
- Rumsey, H. C., Jr., 11, 214
- Rusmevichientong, P., 215

- Sakk, Eric, 215  
 Sarnak, P., 87, 148, 213  
 satisfied constraint, 143  
 scalar field, 23  
 scalar multiplication, 23  
 Seghers, J., 214  
 semigroups, 13  
 semiring, 17  
 separation theorem, 99  
 sequential decoding, xv  
 set, 13  
 Shannon limit, xvii, 39, 71, 79, 175  
 Shannon, C. E., 1, 61, 121, 215  
 Sharp concentration theorem, 155, 157–159, 163, 169  
 Shimony, S. E., 215  
 Shokrollahi, M. A., xviii, 191, 194, 195, 208, 213  
 shortened codes, 42  
 simple tree, 97  
 Singleton bound, 57, 150  
 Singleton upper bound, 11  
 singly-connected graph, 97  
 Sipser, M., xviii, 143, 148, 174, 215  
 Sloane, Neil J. A., 214  
 Smyth, P., 215  
 soft decision decoding, 8  
 Solomon, G., xv, 54  
 spanning set, 24  
 spectral method, 83  
 spectrum, 54  
     polynomial, 36  
 Spenser, J. H., 209  
 sphere packing upper bound, 9  
 Spiegelhalter, D. J., 213  
 Spielman, D. A., xviii, 143, 148, 174, 183, 202, 207, 213  
 state complexity, 63  
 Stemmann, V., 213  
 Stirling's formula, 9, 10  
 subgroup, 15  
 Sudan, M., 209  
 Sugiyama, Y., 212  
 symbol-by-symbol MAP decoding, 8, 121, 122  
 systematic, 41  
     code, 180  
     convolutional encoder, 63  
     information, 122, 129  
 Szemerédi, E., 209  
  
 Takeshita, O. Y., 215  
 Tanner, R. M., xviii, 87, 173, 216  
 theorem  
     Chinese remainder, 58  
     dimension, 26  
     GFFT convolution, 35  
     Lagrange's, 16  
     Noisy Channel Coding, 3, 4  
     separation, 99  
     Sharp Concentration, 155, 157–159  
     Sharp concentration, 163, 169  
 Thitimajshima, P., xvii, 61, 66, 70, 71, 121, 122, 210, 216  
 Thomas, J. A., 211  
 Thomes, R. J., xix  
 Thorp, J. S., xix  
 Tietäväinen, A., xiv, 53, 216  
 tornado code, 193  
 tornado sequence, 193  
 total encoder memory, 63  
 transform  
     D, 63  
     Galois field Fourier, 34  
 transform pair, Galois field Fourier transform, 34  
 tree, 97  
     AND-OR, 188  
 tree-like neighborhood, 155, 189  
 triangulated graph, 105  
 truth table, 46  
 turbo coding, xvii  
 turbo decoding, 12, 121, 125  
     extended parallel mode, 130  
     multiple counting of evidence, 126  
     parallel mode, 126, 130  
  
 U-Separation, 98  
 unconnected graph, 96  
 undirected graph, 80, 95  
 unhelpful, 186  
 uniform cost model, 6  
 uniform interleaver, 72  
 unsatisfied constraint, 143  
 Urbanke, R., xviii, 174, 210  
  
 Van Roy, B., 215  
 Van Tilborg, H., 210  
 Vandermonde matrices, 54  
 variable node  
     degree, 138  
 vector addition, 23  
 vector space, 23  
 vertex exposure martingale, 85, 86  
 video storage technologies, 39  
 Viterbi algorithm, 94, 112, 113  
 Viterbi decoder, xv, 69, 70  
 Viterbi, A. J., 216  
 Vontobel, P., 215  
 Voyager, 70  
  
 wavelets, 215  
 weight, 7  
 weight enumerating function (WEF), 65  
 Weiss, Y., 117, 216

Welch, L. R., xvi, 11, 214

Weldon, E. J., 213

Wiberg, N., 115, 134, 216

Wicker, S. B., xv–xvii, 208, 212, 215, 216

Yedidia, J. S., 117, 216

Zémor, G., 147, 150, 174, 210

Zierler, N., 53, 211

Zyablov, V. V., 173, 216