References

1. Erik Agrell, Alexander Vardy, and Kenneth Zeger. Upper bounds for constant-weight codes. *IEEE Transactions on Information Theory*, 46:2373–2395, 2000.
2. Rudolf Ahlswede. Channel capacities for list codes. *Journal of Applied Probability*, 10:824–836, 1973.
3. Andres Albanese, Johannes Blomer, Jeff Edmonds, Michael Luby, and Madhu Sudan. Priority encoding transmission. *IEEE Transactions on Information Theory*, 42(6):1737–1744, November 1996.
4. Michael Alekhnovich. Linear diophantine equations over polynomials and soft decoding of reed-solomon codes. In *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 439–448, November 2002.
5. Noga Alon, October 1999. Personal Communication.
6. Noga Alon, Jehoshua Bruck, Joseph Naor, Moni Naor, and Ronny Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Transactions on Information Theory*, 38:509–516, 1992.
7. Noga Alon, Jeff Edmonds, and Michael Luby. Linear time erasure codes with nearly optimal recovery. In *Proceedings of the IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 512–519, 1995.
8. Noga Alon, Oded Goldreich, Johan Håstad, and Réne Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures and Algorithms*, 3:289–304, 1992.
9. Noga Alon, Venkatesan Guruswami, Tali Kaufman, and Madhu Sudan. Guessing secrets efficiently via list decoding. In *Proceedings of the 13th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 254–262, January 2002.
10. Noga Alon and Joel Spencer. *The Probabilistic Method*. John Wiley and Sons, Inc., 1992.
11. Sigal Ar, Richard Lipton, Ronitt Rubinfeld, and Madhu Sudan. Reconstructing algebraic functions from mixed data. *SIAM Journal on Computing*, 28(2):488–511, 1999.
12. Sanjeev Arora and Madhu Sudan. Improved low-degree testing and its applications. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 485–495, 1997.
13. Emil Artin. *Collected Papers*. ed. S. Lang and J. T. Tate, Springer-Verlag, 1965. pp. viii-ix.
14. Michael Artin. *Algebra*. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1991.
15. Alexei Ashikhmin, Alexander Barg, and Simon Litsyn. New upper bounds on generalized weights. *IEEE Transactions on Information Theory*, 45(4):1258–1263, 1999.

16. Alexei Ashikhmin, Alexander Barg, and Simon Litsyn. A new upper bound on codes decodable into size-2 lists. In Ingo Althofer *et al.*, editor, *Numbers, Information and Complexity*, pages 239–244. Boston: Kluwer Publishers, 2000.
17. C. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 29:208–210, March 1983.
18. Daniel Augot and Lancelot Pecquet. A Hensel lifting to replace factorization in list decoding of algebraic-geometric and Reed-Solomon codes. *IEEE Transactions on Information Theory*, 46:2605–2613, November 2000.
19. László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3(4):307–318, 1993.
20. Alexander Barg and Gillés Zémor. Error exponents of expander codes. *IEEE Transactions on Information Theory*, 48(6):1725–1729, 2002.
21. Richard Beigel. NP-hard sets are p-superterse unless R = NP. *Technical Report TR 4, Department of Computer Science, Johns Hopkins University*, 1988.
22. Mihir Bellare, Oded Goldreich, and Madhu Sudan. Free bits, PCP's and non-approximability — towards tight results. *SIAM Journal on Computing*, 27(3):804–915, 1998.
23. Elwyn Berlekamp. *Algebraic Coding Theory*. McGraw Hill, New York, 1968.
24. Elwyn Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computations*, 24:713–735, 1970.
25. Elwyn Berlekamp. Bounded distance +1 soft-decision Reed-Solomon decoding. *IEEE Transactions on Information Theory*, 42(3):704–720, 1996.
26. Richard E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, Reading, Massachusetts, 1983.
27. Volodia M. Blinovsky. Bounds for codes in the case of list decoding of finite volume. *Problems of Information Transmission*, 22(1):7–19, 1986.
28. Volodia M. Blinovsky. *Asymptotic Combinatorial Coding Theory*. Kluwer Academic Publishers, Boston, 1997.
29. Volodia M. Blinovsky. Lower bound for the linear multiple packing of the binary hamming space. *Journal of Combinatorial Theory, Series A*, 92(1):95–101, 2000.
30. Bela Bollobás. *Combinatorics*. Cambridge University Press, Cambridge, U.K, 1986.
31. Dan Boneh. Finding smooth integers in short intervals using CRT decoding. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 265–272, 2000.
32. Dan Boneh and Matthew Franklin. An efficient public-key traitor tracing scheme. In *Proc. Advances in Cryptography – Crypto '99*, pages 338–353. Lecture Notes in Computer Science 1666, Springer-Verlag, 1999.
33. R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.
34. Andries E. Brouwer. *Bounds on the size of linear codes*. Chapter 4 in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman (eds), Elsevier, pp. 295-461, 1998.
35. K. A. Bush. Orthogonal arrays of index unity. *Ann. Math. Stat.*, 23:426–434, 1952.

36. Jin-Yi Cai, A. Pavan, and D. Sivakumar. On the hardness of the permanent. In *Proceedings of the 16th International Symposium on Theoretical Aspects of Computer Science*, March 1999.
37. Benny Chor, Amos Fiat, and Moni Naor. Tracing traitors. In *Proc. Advances in Cryptography – Crypto '94*, pages 257–270. Lecture Notes in Computer Science 839, Springer-Verlag, 1994.
38. Fan Chung, Ron Graham, and Tom Leighton. Guessing secrets. *The Electronic Journal of Combinatorics*, 8(1):R13, 2001.
39. Gérard Cohen, Simon Litsyn, and Gillés Zémor. Upper bounds on generalized distances. *IEEE Transactions on Information Theory*, 40:2090–2092, 1994.
40. Gérard D. Cohen, Sylvia B. Encheva, and Hans G. Schaathun. On separating codes. *Technical report, Ecole Nationale Supérieure des Télécommunications, Paris*, 2001.
41. Henri Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics **138**, Springer Verlag, Berlin, 1993.
42. D. E. R. Denning. *Cryptography and Data Security*. Reading, MA: Addison-Wesley, 1983.
43. V. G. Drinfeld and Serge G. Vlădut. Number of points of an algebraic curve. *Func. Anal.*, 17:53–54, 1983.
44. Ilya Dumer, Daniele Micciancio, and Madhu Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Transactions on Information Theory*, 49(1):22–37, January 2003.
45. Ilya I. Dumer. Two algorithms for the decoding of linear codes. *Problems of Information Transmission*, 25(1):24–32, 1989.
46. Ilya I. Dumer. Concatenated codes and their multilevel generalizations. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, volume 2, pages 1911–1988. North Holland, 1998.
47. Peter Elias. Coding for two noisy channels. *Information Theory, Third London Symposium*, pages 61–76, September 1955.
48. Peter Elias. List decoding for noisy channels. *Technical Report 335, Research Laboratory of Electronics, MIT*, 1957.
49. Peter Elias. Zero error capacity under list decoding. *IEEE Transactions on Information Theory*, 34(5):1070–1074, September 1988. Originally appeared as *Quarterly Progress Report*, vol. 48, pp. 88-90, Research Laboratory of Electronics, MIT, January 1958.
50. Peter Elias. Error-correcting codes for list decoding. *IEEE Transactions on Information Theory*, 37:5–12, 1991.
51. Noam D. Elkies. Explicit modular towers. In *Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing*, pages 23–32, 1997.
52. Noam D. Elkies. Excellent non-linear codes from Modular curves. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 200–208, July 2001.
53. Thomas Ericson and Victor Zinoviev. Spherical codes generated by binary partitions of symmetric pointsets. *IEEE Transactions on Information Theory*, 41:107–129, 1995.
54. Uriel Feige, Michael Langberg, and Kobbi Nissim. On the hardness of approximating NP witnesses. In *Proceedings of the 3rd International Workshop on Approximation Algorithms for Combinatorial Optimization (APPROX)*, pages 120–131, September 2000.

55. Uriel Feige and Carsten Lund. On the hardness of computing the permanent of random matrices. In *Proceedings of the 24th ACM Symposium on Theory of Computing*, pages 643–654, 1992.
56. Joan Feigenbaum. The use of coding theory in computational complexity. In R. Calderbank, editor, *Proceedings of Symposia in Applied Mathematics*, pages 203–229. American Mathematics Society, Providence, 1995.
57. G. L. Feng. Two fast algorithms in the Sudan decoding procedure. In *Proceedings of the 37th Annual Allerton Conference on Communication, Control and Computing*, pages 545–554, 1999.
58. Gui-Liang Feng and Thammavarapu R. N. Rao. Decoding algebraic geometric codes up to the designed minimum distance. *IEEE Transactions on Information Theory*, 39(1):37–45, 1993.
59. G. David Forney. *Concatenated Codes*. MIT Press, Cambridge, MA, 1966.
60. G. David Forney. Generalized Minimum Distance decoding. *IEEE Transactions on Information Theory*, 12:125–131, 1966.
61. G. David Forney. Exponential error bounds for erasure, list, and decision feedback schemes. *IEEE Transactions on Information Theory*, 14(2):206–220, March 1968.
62. Anna Gál, Shai Halevi, Richard J. Lipton, and Erez Petrank. Computing from partial solutions. In *Proceedings of the 14th Annual IEEE Conference on Computation Complexity*, pages 34–45, 1999.
63. Shuhong Gao and M. Amin Shokrollahi. Computing roots of polynomials over function fields of curves. *Coding Theory and Cryptography: From Enigma and Geheimschreiber to Quantum Theory (D. Joyner, Ed.), Springer*, pages 214–228, 2000.
64. Arnaldo Garcia and Henning Stichtenoth. Algebraic function fields over finite fields with many rational places. *IEEE Transactions on Information Theory*, 41:1548–1563, 1995.
65. Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlădut bound. *Inventiones Mathematicae*, 121:211–222, 1995.
66. Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behavior of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, December 1996.
67. Peter Gemmell and Madhu Sudan. Highly resilient correctors for multivariate polynomials. *Information Processing Letters*, 43(4):169–174, 1992.
68. Oded Goldreich. *Modern Cryptography, Probabilistic Proofs, and Pseudorandomness*. Number 17 in Algorithms and Combinatorics. Springer-Verlag, 1999.
69. Oded Goldreich and Leonid Levin. A hard-core predicate for all one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 25–32, May 1989.
70. Oded Goldreich, Noam Nisan, and Avi Wigderson. On Yao's XOR Lemma. *Technical Report TR95-050, Electronic Colloquium on Computational Complexity*, March 1995. `http://www.eccc.uni-trier.de/eccc`.
71. Oded Goldreich, Dana Ron, and Madhu Sudan. Chinese remaindering with errors. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 225–234, 1999.
72. Oded Goldreich, Dana Ron, and Madhu Sudan. Chinese remaindering with errors. *IEEE Transactions on Information Theory*, 46(5):1330–1338, July 2000.

73. Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan. Learning polynomials with queries: The highly noisy case. *SIAM Journal on Discrete Mathematics*, 13(4):535–570, November 2000.
74. V. D. Goppa. Codes on algebraic curves. *Soviet Math. Doklady*, 24:170–172, 1981.
75. Dima Grigoriev. Factorization of polynomials over a finite field and the solution of systems of algebraic equations. *Translated from Zapiski Nauchnykh Seminarov Lenningradskogo Otdeleniya Matematicheskogo Instituta im. V. A. Steklova AN SSSR*, 137:20–79, 1984.
76. Venkatesan Guruswami. Limits to list decodability of linear codes. In *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC)*, pages 802–811, 2002.
77. Venkatesan Guruswami. Constructions of codes from number fields. *IEEE Transactions on Information Theory*, 49(3):594–603, March 2003.
78. Venkatesan Guruswami. List decoding from erasures: Bounds and code constructions. *IEEE Transactions on Information Theory*, 49(11):2826–2833, November 2003.
79. Venkatesan Guruswami. Better Extractors for Better Codes? In *Proceedings of 36th Annual ACM Symposium on Theory of Computing (STOC)*, June 2004.
80. Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48(5):1021–1035, 2002.
81. Venkatesan Guruswami and Piotr Indyk. Expander-based constructions of efficiently decodable codes. In *Proceesings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 658–667, 2001.
82. Venkatesan Guruswami and Piotr Indyk. Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets. In *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC)*, pages 812–821, 2002.
83. Venkatesan Guruswami and Piotr Indyk. Linear-time encodable and list decodable codes. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC)*, pages 126–135, June 2003.
84. Venkatesan Guruswami and Piotr Indyk. Efficiently decodable codes meeting gilbert-varshamov bound for low rates. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 756–757, 2004.
85. Venkatesan Guruswami and Piotr Indyk. Linear time encodable/decodable codes with near-optimal rate. *IEEE Transactions on Information Theory*, 2004. To appear.
86. Venkatesan Guruswami, Amit Sahai, and Madhu Sudan. Soft-decision decoding of Chinese Remainder codes. In *Proceedings of the 41st IEEE Symposium on Foundations of Computer Science*, pages 159–168, 2000.
87. Venkatesan Guruswami and Igor Shparlinski. Unconditional proof of tightness of Johnson Bound. In *Proceedings of the 14th ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 754–755, 2003.
88. Venkatesan Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45:1757–1767, 1999.

89. Venkatesan Guruswami and Madhu Sudan. List decoding algorithms for certain concatenated codes. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 181–190, 2000.
90. Venkatesan Guruswami and Madhu Sudan. Decoding concatenated codes using soft information. In *Proceedings of the 17th IEEE Conference on Computational Complexity*, pages 148–157, 2002.
91. Venkatesan Guruswami and Madhu Sudan. Extensions to the Johnson bound. *Manuscript*, February 2001.
92. Venkatesan Guruswami and Madhu Sudan. On representations of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 47(4):1610–1613, May 2001.
93. Richard W. Hamming. Error Detecting and Error Correcting Codes. *Bell System Technical Journal*, 29:147–160, April 1950.
94. Frank Harary. *Graph Theory*. Addison-Wesley, Reading, MA, 1969.
95. G. H. Hardy, J. E. Littlewood, and G. Pólya. *Inequalities*. Cambridge University Press, 2nd edition, 1952.
96. Hermann J. Helgert. Alternant codes. *Information and Control*, 26:369–380, 1974.
97. T. Helleseth, T. Klørdve, V. I. Levenshtein, and O. Ytrehus. Bounds on minimum support weights. *IEEE Transactions on Information Theory*, 41(2):432–440, 1995.
98. A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffres (Paris)*, 2:147–156, 1959.
99. Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
100. Johan Håstad and Mats Näslund. The security of all RSA and discrete log bits. *Journal of the ACM*, 51(2):187–230, 2004.
101. *I've Got a Secret*. A classic '50's and '60's television gameshow. See `http://www.timvp.com/ivegotse.html`.
102. Y. Ihara. Some remarks in the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo*, 28:721–724, 1981.
103. Russell Impagliazzo. Hard-core distributions from somewhat hard problems. In *Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science*, pages 538–545, October 1995.
104. Russell Impagliazzo and Avi Wigderson. P = BPP if E requires exponential circuits: Derandomizing the XOR Lemma. In *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*, pages 220–229, May 1997.
105. Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 2 edition, 1990.
106. Thomas Jakobsen. Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. In Hugo Krawczyk, editor, *Proc. Advances in Cryptography – Crypto '98*. Lecture Notes in Computer Science 1462, Springer-Verlag, 1998.
107. A. Joffe. On a set of almost deterministic k-independent random variables. *Annals of Probability*, 2(1):161–162, 1974.
108. Selmer M. Johnson. A new upper bound for error-correcting codes. *IEEE Transactions on Information Theory*, 8:203–207, 1962.
109. Selmer M. Johnson. Improved asymptotic bounds for error-correcting codes. *IEEE Transactions on Information Theory*, 9:198–205, 1963.

110. Jørn Justesen. A class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18:652–656, 1972.
111. Jørn Justesen. On the complexity of decoding Reed-Solomon codes (corresp.). *IEEE Transactions on Information Theory*, 22(2):237–238, March 1976.
112. Jørn Justesen. On bounds for list decoding. *Manuscript*, March 2001.
113. Jørn Justesen and Tom Høholdt. Bounds on list decoding of MDS codes. *IEEE Transactions on Information Theory*, 47(4):1604–1609, May 2001.
114. Jørn Justesen, Knud J. Larsen, Helge E. Jensen, Allan Havemose, and Tom Høholdt. Construction and decoding of a class of algebraic geometry codes. *IEEE Transactions on Information Theory*, 35:811–821, July 1989.
115. Jørn Justesen, Knud J. Larsen, Helge E. Jensen, and Tom Høholdt. Fast decoding of codes from algebraic plane curves. *IEEE Transactions on Information Theory*, 38:111–119, 1992.
116. Erich Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM Journal on Computing*, 14(2):469–489, 1985.
117. Erich Kaltofen. Polynomial factorization 1987–1991. In *Proceedings of LATIN '92, I. Simon (Ed.), Springer LNCS*, volume 583, pages 294–313, 1992.
118. Richard Karp and Michael Rabin. Efficient randomized pattern-matching algorithms. *Technical report TR-31-81, Aiken Computation Laboratory, Harvard University*, 1981.
119. G. L. Katsman, Michael A. Tsfasman, and Serge G. Vlădut. Modular curves and codes with a polynomial construction. *IEEE Transactions on Information Theory*, 30:353–355, 1984.
120. Marcos Kiwi. Testing and weight distributions of dual codes. *ECCC Technical Report TR-97-010*, 1997.
121. Ralf Koetter and Alexander Vardy. Algebraic soft-decision decoding of Reed-Solomon codes. *IEEE Transactions on Information Theory*, 49(11):2809–2825, November 2003.
122. H. Krishna, B. Krishna, K. Y. Lin, and J. D. Sun. *Computational Number Theory and Digital Signal Processing: Fast algorithms and error control techniques*. Boca Raton, FL: CRC, 1994.
123. S. Ravi Kumar and D. Sivakumar. Proofs, codes, and polynomial-time reducibilities. In *Proceedings of the 14th Annual IEEE Conference on Computation Complexity*, 1999.
124. Arjen K. Lenstra. Factoring multivariate polynomials over finite fields. *Journal of Computer and System Sciences*, 30(2):235–248, April 1985.
125. Arjen K. Lenstra and Hendrik W. Lenstra. Algorithms in number theory. *Handbook of Theoretical Computer Science (Volume A: Algorithms and Complexity), Chap. 12*, pages 673–715, 1990.
126. Arjen K. Lenstra, Hendrik W. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.
127. Hendrik W. Lenstra. Codes from algebraic number fields. In L.G.L.T. Meertens M. Hazewinkel, J.K. Lenstra, editor, *Mathematics and computer science II, Fundamental contributions in the Netherlands since 1945*, pages 95–104. North-Holland, Amsterdam, 1986.
128. V. I. Levenshtein. Universal bounds for codes and designs. *Chapter 6 in Handbook of Coding Theory, V. S. Pless and W. C. Huffman (Eds.)*, pages 499–648, 1998.

129. Richard Lipton. New directions in testing. In *Distributed Computing and Cryptography*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 191–202. AMS, 1991.
130. B. López. Codes on Drinfeld modular curves. In J. Buchmann *et al*, editor, *Coding Theory, Cryptography and Related Areas*, pages 175–183. Springer, Heidelberg, 1998.
131. Alex Lubotzky, R. Phillips, and Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
132. F. J. MacWilliams and Neil J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier/North-Holland, Amsterdam, 1981.
133. David M. Mandelbaum. On a class of arithmetic codes and a decoding algorithm. *IEEE Transactions on Information Theory*, 21:85–88, 1976.
134. David M. Mandelbaum. Further results on decoding arithmetic residue codes. *IEEE Transactions on Information Theory*, 24:643–644, 1978.
135. Y. I. Manin and Serge G. Vlădut. Linear codes and modular curves. *J. Soviet. Math.*, 30:2611–2643, 1985.
136. G. A. Margulis. Explicit group-theoretical constructions of combinatorial schemes and their applications to the design of expanders and superconcentrators. *Problems of Information Transmission*, 24:39–46, 1988.
137. James L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, 15:122–127, January 1969.
138. R. Matsumoto. On the second step in the Guruswami-Sudan list decoding algorithm for AG-codes. *Technical Report of the Institute of Electronics, Information and Communication Engineers (IEICE)*, pages 65–70, 1999.
139. Robert J. McEliece, Eugene R. Rodemich, Howard Rumsey Jr., and Lloyd R. Welch. New upper bounds on the rate of a code via the Delsarte-Macwilliams inequalities. *IEEE Transactions on Information Theory*, 23:157–166, 1977.
140. Daniele Micciancio. Lecture notes on Lattices in Cryptography and Cryptanalysis, University of California at San Diego. Available at `http://www-cse.ucsd.edu/~daniele/cse291fa99.html`, Fall 1999.
141. Daniele Micciancio and Nathan Segerlind. Using prefixes to efficiently guess two secrets. *Manuscript*, July 2001.
142. Elchanan Mossel and Christopher Umans. On the complexity of approximating the VC dimension. *J. Comput. Syst. Sci.*, 65(4):660–671, 2002.
143. Joseph Naor and Moni Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM Journal on Computing*, 22(4):838–856, 1993.
144. Moni Naor, Leonard Schulman, and Aravind Srinivasan. Splitters and near-optimal derandomization. In *Proceedings of the 36th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 182–191, 1995.
145. Rasmus R. Nielsen. Decoding concatenated codes using Sudan's algorithm. *Manuscript submitted for publication*, May 2000.
146. Rasmus R. Nielsen and Tom Hϕholdt. Decoding Hermitian codes with Sudan's algorithm. In *Proceedings of AAECC-13, LNCS 1719*, pages 260–270, 1999.
147. Rasmus R. Nielsen and Tom Hϕholdt. Decoding Reed-Solomon codes beyond half the minimum distance. *Coding Theory, Cryptography and Related areas, (eds. Buchmann, Hoeholdt, Stichtenoth and H. tapia-Recillas)*, pages 221–236, 1999.
148. Noam Nisan. Extracting Randomness: How and Why – A survey. In *Proceedings of the 11th Annual IEEE Symposium on Computational Complexity*, pages 44–58, 1996.

149. Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, October 1994.
150. Vadim Olshevsky and M. Amin Shokrollahi. A displacement structure approach to efficient list decoding of algebraic geometric codes. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, pages 235–244, 1999.
151. Lancelot Pecquet. List decoding of algebraic-geometric codes. *Manuscript*, May 2001.
152. Ruud Pellikaan. On a decoding algorithm for codes on maximal curves. *IEEE Transactions on Information Theory*, 35:1228–1232, 1989.
153. W. Wesley Peterson. Encoding and error-correction procedures for Bose-Chaudhuri codes. *IEEE Transactions on Information Theory*, 6:459–470, 1960.
154. Irving S. Reed and Gustav Solomon. Polynomial codes over certain finite fields. *J. SIAM*, 8:300–304, 1960.
155. Ronny Roth and Gitit Ruckenstein. Efficient decoding of Reed-Solomon codes beyond half the minimum distance. *IEEE Transactions on Information Theory*, 46(1):246–257, January 2000.
156. Gitit Ruckenstein and Ronny Roth. Bounds on the list-decoding radius of Reed-Solomon codes. *SIAM J. Discrete Math.*, 17:171–195, 2003.
157. Uwe Schoning. A probabilistic algorithm for k-SAT and Constraint Satisfaction Problems. In *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*, pages 410–414, 1999.
158. Yu L. Segalovich. Separating systems. *Problems of Information Transmission*, 30(2):105–123, 1994.
159. Ronen Shaltiel and Christopher Umans. Simple extractors for all min-entropies and a new pseudo-random generator. In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, 2001.
160. Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.
161. Claude E. Shannon. The zero error capacity of a noisy channel. *IEEE Transactions on Information Theory*, 2(3):8–19, 1956.
162. Claude E. Shannon, Robert G. Gallager, and Elwyn R. Berlekamp. Lower bounds to error probability for coding on discrete memoryless channels. *Information and Control*, 10:65–103 (Part I), 522–552 (Part II), 1967.
163. Daniel Sheldon and Neal Young. Hamming approximation of NP witnesses. *Manuscript*, 2003.
164. Ba-Zhong Shen. A Justesen construction of binary concatenated codes that asymptotically meet the Zyablov bound for low rate. *IEEE Transactions on Information Theory*, 39:239–242, 1993.
165. M. Amin Shokrollahi and Hal Wasserman. List decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(2):432–437, 1999.
166. Kenneth Shum. *A Low-Complexity Algorithm for Constructing Algebraic-Geometric Codes Better than the Gilbert-Varshamov Bound*. PhD thesis, University of Southern California, Los Angeles, 2000.
167. Kenneth Shum, Ilia Aleshnikov, P. Vijay Kumar, Henning Stichtenoth, and Vinay Deolalikar. A low-complexity algorithm for the construction of algebraic-geomteric codes better than the Gilbert-Varshamov bound. *IEEE Transactions on Information Theory*, 47:2225–2241, 2001.

168. V. M. Sidelnikov. Decoding Reed-Solomon codes beyond $(d-1)/2$ errors and zeros of multivariate polynomials. *Problems of Information Transmission*, 30(1):44–59, 1994.
169. Alice Silverberg, Jessica Standon, and Judy Walker. Efficient traitor tracing algorithms using list decoding. *Manuscript*, 2000.
170. Michael Sipser. Expanders, randomness, or time versus space. *Journal of Computer and System Sciences*, 36(3):379–383, June 1988.
171. Michael Sipser and Daniel Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996.
172. D. Sivakumar. On membership comparable sets. *Journal of Computer and System Sciences*, 59(2):270–280, October 1999.
173. Alexei N. Skorobogatov and Serge G. Vlădut. On decoding of algebraic geometric codes. *IEEE Transactions on Information Theory*, 36:1051–1060, 1990.
174. M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and F. J. Taylor. *Residue Number System Arithmetic: Modern Applications in Digital Signal Processing*. New York: IEEE Press, 1986.
175. Daniel Spielman. *Computationally Efficient Error-Correcting Codes and Holographic Proofs*. PhD thesis, Massachusetts Institute of Technology, June 1995.
176. Daniel Spielman. Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory*, 42(6):1723–1732, 1996.
177. Henning Stichtenoth. *Algebraic Function Fields and Codes*. Universitext, Springer-Verlag, Berlin, 1993.
178. Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.
179. Madhu Sudan. Decoding of Reed-Solomon codes beyond the error-correction diameter. In *Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing*, 1997.
180. Madhu Sudan. *A Crash Course in Coding Theory*, Lecture no. 5. Slides available from `http://theory.lcs.mit.edu/~madhu`, November 2000.
181. Madhu Sudan. List decoding: Algorithms and applications. *SIGACT News*, 31:16–27, 2000.
182. Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. *J. Comput. Syst. Sci.*, 62(2):236–266, 2001.
183. Yasuo Sugiyama, Masao Kasahara, Shigeichi Hirasawa, and Toshihiko Namekawa. A method for solving key equation for decoding Goppa codes. *Information and Control*, 27:87–99, 1975.
184. Amnon Ta-Shma and David Zuckerman. Extractor Codes. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 193–199, July 2001.
185. Amnon Ta-Shma, David Zuckerman, and Shmuel Safra. Extractors from Reed-Muller codes. In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pages 638–647, 2001.
186. S. Toda. On polynomial-time truth-table reducibility of intractable sets to p-selective sets. *Math. Systems Theory*, 24:69–82, 1991.
187. Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.
188. Luca Trevisan. List-decoding using the XOR Lemma. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 126–135, 2003.

189. M. A. Tsfasman and S. G. Vlădut. Geometric approach to higher weights. *IEEE Transactions on Information Theory*, 41:1564–1588, 1995.
190. Michael A. Tsfasman, Serge G. Vlădut, and Thomas Zink. Modular curves, Shimura curves, and codes better than the Varshamov-Gilbert bound. *Math. Nachrichten*, 109:21–28, 1982.
191. Leslie Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, April 1979.
192. Leslie Valiant and Vijay Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.
193. J. H. van Lint. *Introduction to Coding Theory*. Graduate Texts in Mathematics **86**, (Third Edition) Springer-Verlag, Berlin, 1999.
194. V. Wei. Generalized Hamming weights for linear codes. *IEEE Transactions on Information Theory*, 37(5):1412–1418, 1991.
195. Victor K. Wei and Gui-Liang Feng. Improved lower bounds on the sizes of error-correcting codes for list decoding. *IEEE Transactions on Information Theory*, 40(2):559–563, 1994.
196. Lloyd R. Welch and Elwyn R. Berlekamp. Error correction of algebraic block codes. *US Patent Number 4,633,470*, December 1986.
197. Edward J. Weldon, Jr. Justesen's construction — the low-rate case. *IEEE Transactions on Information Theory*, 19:711–713, 1973.
198. Stephen B. Wicker and Vijay K. Bhargava, editors. *Reed-Solomon Codes and Their Applications*. John Wiley and Sons, Inc., September 1999.
199. John M. Wozencraft. List Decoding. *Quarterly Progress Report, Research Laboratory of Electronics, MIT*, 48:90–95, 1958.
200. Xin-Wen Wu and Paul H. Siegel. Efficient list decoding of algebraic geometric codes beyond the error correction bound. In *Proceedings of the International Symposium on Information Theory*, June 2000.
201. Gillés Zémor. On expander codes. *IEEE Transactions on Information Theory*, 47(2):835–837, 2001.
202. Victor V. Zyablov. An estimate of the complexity of constructing binary linear cascaded codes. *Problemy Peridachi Informatsii*, 15(2):58–70, 1971.
203. Victor V. Zyablov and Mark S. Pinsker. List cascade decoding. *Problems of Information Transmission*, 17(4):29–34, 1981 (in Russian); pp. 236-240 (in English), 1982.

Index