Bibliography

O. Amrani and Y. Be'ery. Efficient bounded–distance decoding of the hexacode and associated decoders for the leech lattice and the golay code. *IEEE Trans. Comm.*, 44(5): 612–629, 1996. ISSN 0090-6778.

I. Anderson and I. Honkala. A short course in combinatorial designs. University of Turku (Finland), 1997. URL `http://www.utu.fi/~honkala/designs.ps`.

E. Artin. *Galois theory*. Dover Publications Inc., Mineola, NY, second edition, 1998. ISBN 0-486-62342-4. Edited and with a supplemental chapter by Arthur N. Milgram.

E. Artin. *Geometric algebra*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1988. ISBN 0-471-60839-4. Reprint of the 1957 original, A Wiley-Interscience Publication.

R. B. Ash. *Information theory*. Dover Publications Inc., New York, 1990. ISBN 0-486-66521-6. Corrected reprint of the 1965 original.

E. F. Assmus, Jr. On the Reed-Muller codes. *Discrete Math.*, 106/107:25–33, 1992. ISSN 0012-365X. A collection of contributions in honour of Jack van Lint.

E. F. Assmus, Jr. The category of linear codes. *IEEE Trans. Inform. Theory*, 44(2):612–629, 1998. ISSN 0018-9448.

E. F. Assmus, Jr. and J. D. Key. Polynomial codes and finite geometries, 1996.

E. F. Assmus, Jr. and J. D. Key. Hadamard matrices and their designs: a coding-theoretic approach. *Trans. Amer. Math. Soc.*, 330(1):269–293, 1992a. ISSN 0002-9947.

E. F. Assmus, Jr. and J. D. Key. *Designs and their codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1992b. ISBN 0-521-41361-3; 0-521-45839-0.

A. Barg. Extremal problems of coding theory. In *Coding theory and cryptology (Singapore, 2001)*, volume 1 of *Lect. Notes Ser. Inst. Math. Sci. Natl. Univ. Singap.*, pages 1–48. World Sci. Publishing, River Edge, NJ, 2002.

L. M. Batten. *Combinatorics of finite geometries*. Cambridge University Press, Cambridge, second edition, 1997. ISBN 0-521-59014-0; 0-521-59993-8.

S. Bellini. Teoria dell'informazione e codici. Politecnico di Milano, 2004. URL `http://www.elet.polimi.it/upload/bellini/tinfcod_c/tinfcod_c.html`.

E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Information Theory*, IT-24(3):384–386, 1978. ISSN 0018-9448.

T. Beth, D. Jungnickel, and H. Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999. ISBN 0-521-44432-2.

A. Beutelspacher and U. Rosenbaum. *Projective geometry: from foundations to applications*. Cambridge University Press, Cambridge, 1998. ISBN 0-521-48277-1; 0-521-48364-6.

J. Bierbrauer. Introduction to codes and their use, February 1999. URL `http://www.math.mtu.edu/~jbierbra/HOMEZEUGS/Codecourse.ps`.

A. R. Calderbank. The art of signaling: fifty years of coding theory. *IEEE Trans. Inform. Theory*, 44(6):2561–2595, 1998. ISSN 0018-9448. Information theory: 1948–1998.

P. Cameron. Polynomial aspects of codes, matroids and permutation groups. University of London, March 2002. URL `http://www.maths.qmw.ac.uk/~pjc/csgnotes/cmpgpoly.pdf`.

R. Chapman. Constructions of the goolay codes: A survey. University of Exeter (UK), 1997.

H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. ISBN 3-540-55640-0.

T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley and sons, New York, 1991. ISBN 0-471-06259-6.

R. Diestel. *Graph Theory*. Springer-Verlag, New York, second edition, 2000. ISBN 0-387-98976-5; 0-387-95014-1. URL `http://www.math.uni-hamburg.de/home/diestel/books/graph.theory/`. Graduate Texts in Mathematics, Vol. 173.

I. Dumer, D. Micciancio, and M. Sudan. Hardness of approximating the minimum distance of a linear code. *IEEE Transactions on Information Theory*, 49(1):22–37, Jan. 2003. Preliminary version in FOCS 1999.

I. Duursma. *Decoding codes from curves and cyclic codes*. PhD thesis, 1993. URL http://www.math.uiuc.edu/~duursma/pub/.

Data interchange on read–only 120 *mm optical data disks (CDROM)*. ECMA, Giugno 1996. ECMA–130.

120 *mm DVD Rewritable Disk (DVD–RAM)*. ECMA, Giugno 1999. ECMA–272.

120 *mm DVD — Read–only disk*. ECMA, Aprile 2001. ECMA–267.

D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. ISBN 0-387-94268-8; 0-387-94269-6. With a view toward algebraic geometry.

P. Elias. Error–free coding. Technical Report 285, Massachusetts Institute of Technology (Boston), 1954. URL http://hdl.handle.net/1721.1/4795.

P. Elias. List decoding for noisy channels. Technical Report 335, Massachusetts Institute of Technology (Boston), 1957. URL http://hdl.handle.net/1721.1/4484.

M. A. Epstein. Algebraic decoding for a binary erasure channel. Technical Report 340, Massachusetts Institute of Technology (Boston), 1958. URL http://hdl.handle.net/1721.1/4480.

G. D. Forney. *Concatenated codes*. PhD thesis, M.I.T. Dept. of Electrical Engineering, 1965. URL http://hdl.handle.net/1721.1/13449.

W. Fulton. *Algebraic curves. An introduction to algebraic geometry*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

R. G. Gallager. Low–density parity–check codes. MIT Press, 1963.

GAP. *GAP – Groups, Algorithms, and Programming, Version 4.4*. The GAP Group, 2004. URL http://www.gap-system.org.

K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992. ISBN 0-7923-9259-0.

O. Goldreich. Introduction to complexity theory – lecture notes. The Weizmann Institute of Science, Israel, 1999. URL http://www.wisdom.weizmann.ac.il/~oded/cc99.html.

V. D. Goppa. *Geometry and codes*, volume 24 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1988. ISBN 90-277-2776-7. Translated from the Russian by N. G. Shartse.

V. D. Goppa. Codes on algebraic curves. *Dokl. Akad. Nauk SSSR*, 259(6):1289–1290, 1981.

R. Graham, D. Knuth, and P. O. *Concrete Mathematics*. Addison Wesley, 1988.

R. D. Gray and L. D. Davisson. *An Introduction to Statistical Signal Processing*. Cambridge University Press, Cambridge, 2004. ISBN 0521838606. URL `http://www-ee.stanford.edu/~gray/sp.html`.

R. M. Gray. *Entropy and information theory*. Springer-Verlag, New York, 1990. ISBN 0-387-97371-0. (`http://www-ee.stanford.edu/~gray/it.html`).

G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. URL `http://www.singular.uni-kl.de`.

V. Guruswami and M. Sudan. Extensions to the johnson bound. Manuscript, February 2001.

V. Guruswami and M. Sudan. Improved decoding of reed-solomon and algebraic-geometric codes. In *IEEE Symposium on Foundations of Computer Science*, pages 28–39, 1998. URL `http://citeseer.ist.psu.edu/article/guruswami98improved.html`.

R. W. Hamming. Error detecting and error correcting codes. *Bell System Tech. J.*, 26: 147–160, 1950.

R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. ISBN 0-387-90244-9. Graduate Texts in Mathematics, No. 52.

J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998. ISBN 0-19-850295-8.

T. Høholdt and R. Pellikaan. On the decoding of algebraic–geometric codes. *IEEE Trans. Inform. Theory*, IT–41:1589–1614, 1995.

D. R. Hughes and F. C. Piper. *Projective planes*. Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

D. Jungnickel and B. Schmidt. Difference sets: An update. URL `http://citeseer.ist.psu.edu/jungnickel97difference.html"`.

D. Knuth. *The art of computer programming*, volume 2 – Seminumerical Algorithms. Addison Wesley Longman, 3 edition, 1998.

R. Koekoek and R. F. Swattouw. The askey–scheme of hypergeometric orthogonal polynomials and its q–analogue. Technical report, Delft University of Technology, 1994, no. 94–05. URL http://aw.twi.tudelft.nl/~koekoek/askey.html.

W. J. LeVeque. *Topics in number theory. Vol. I, II*. Dover Publications Inc., Mineola, NY, 2002. ISBN 0-486-42539-8. Reprint of the 1956 original [Addison-Wesley Publishing Co., Inc., Reading, Mass.], with separate errata list for this edition by the author.

R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. ISBN 0-521-39231-4. With a foreword by P. M. Cohn.

R. Lidl and G. Pilz. *Applied abstract algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1998. ISBN 0-387-98290-6.

D. Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

R. Ludwig and J. Taylor. *Voyager Telecommunications*. NASA Jet Propulsion Laboratory, California Institute of Technology, Pasadena, 2002. URL http://descanso.jpl.nasa.gov/DPSummary/Descanso4-Voyager_new.pdf.

D. J. MacKay. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, Cambridge (UK), 2004. URL http://www.inference.phy.cam.ac.uk/mackay/itila/.

D. J. C. MacKay. Good error-correcting codes based on very sparse matrices. *IEEE Trans. Inform. Theory*, 45(2):399–431, 1999. ISSN 0018-9448.

D. J. C. MacKay. Errata for: "Good error-correcting codes based on very sparse matrices" [IEEE Trans. Inform. Theory **45** (1999), no. 2, 399–431; MR1677007 (99j:94077)]. *IEEE Trans. Inform. Theory*, 47(5):2101, 2001. ISSN 0018-9448.

J. L. Massey. Threshold decoding. Technical Report 410, Massachusetts Institute of Technology (Boston), 1963. URL http://hdl.handle.net/1721.1/4415.

J. L. Massey. Applied digital information theory. ETH Zurich, 1998. URL http://www.isi.ee.ethz.ch/education/public/free_docs.en.html.

F. Mazzocca. Appunti di geometria superiore. Caserta, 2004. URL http://www.dimat.unina2.it/mazzocca/Geom_Sup.htm.

R. J. McEliece. The algebraic theory of convolutional codes. California Institute of Technology, May 1996. URL http://ece-classweb.ucsd.edu:16080/winter05/ece259bn/Main/ATCC.pdf.

R. J. McEliece. The guruswami–sudan decoding algorithm for reed–solomon codes. Technical report, JPL Interplanetary Network Progress Report 42–153, May 2003. URL http://ipnpr.jpl.nasa.gov/progress_report/42-153/title.htm.

R. J. McEliece. *The theory of information and coding*, volume 86 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 2002. ISBN 0-521-00095-5.

R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Information Theory*, IT-23(2):157–166, 1977. ISSN 0018-9448.

B. Mishra. *Algorithmic algebra*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993. ISBN 0-387-94090-1.

R. H. Morelos-Zaragoza. *The Art of Error Correcting Coding*. Wiley and sons, New York, 2002. ISBN 0-471-49581-6.

C. Moreno. *Algebraic Curves Over Finite Fields*. Cambridge University Press, Cambridge, 1991.

D. Mudgway. *Uplink–Downlink — A History of the Deep Space Network*. NASA Office of External Relations, Wasington (DC), 2001. URL http://history.nasa.gov/SP-4227/Uplink-Downlink.pdf.

D. Mumford. *Algebraic geometry. I*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. ISBN 3-540-58657-1. Complex projective varieties, Reprint of the 1976 edition.

D. Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, expanded edition, 1999. ISBN 3-540-63293-X. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.

K. H. Powers. *A unified theory of information*. PhD thesis, M.I.T. Dept. of Electrical Engineering, 1956. URL http://hdl.handle.net/1721.1/4771.

O. Pretzel. *Codes and algebraic curves*, volume 8 of *Oxford Lecture Series in Mathematics and its Applications*. The Clarendon Press Oxford University Press, New York, 1998.

I. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, June 1960.

M. Reid. *Undergraduate algebraic geometry*, volume 12 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1988. ISBN 0-521-35559-1; 0-521-35662-8.

B. Reiffen. Sequential encoding and decoding for the discrete memoryless channel. Technical Report 374, Massachusetts Institute of Technology (Boston), 1960. URL `http://hdl.handle.net/1721.1/4448`.

T. Richardson and R. Urbanke. Modern coding theory. EPFL Lausanne, 2004. URL `http://lthcwww.epfl.ch/papers/ics.ps`.

T. J. Richardson and R. L. Urbanke. Efficient encoding of low-density parity-check codes. *IEEE Trans. Inform. Theory*, 47(2):638–656, 2001. ISSN 0018-9448.

D. Salomon. *Data Compression — The complete reference*. Springer–Verlag, 3 edition, 2004.

A. Samorodnitsky. On the optimum of Delsarte's linear program. *J. Combin. Theory Ser. A*, 96(2):261–287, 2001. ISSN 0097-3165.

C. B. Schleger and L. C. Pérez. *Trellis and Turbo Coding*. Wiley and sons, New York, 2004. ISBN 0-471-22755-2.

A. Seidenberg. *Elements of the theory of algebraic curves*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1968.

J. G. Semple and L. Roth. *Introduction to algebraic geometry*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1985.

J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423, 623–656, 1948.

J. Singer. A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.*, 43(3):377–385, 1938. ISSN 0002-9947.

M. Sipser and D. A. Spielman. Expander codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1710–1722, 1996. ISSN 0018-9448. Codes and complexity.

A. N. Skorobogatov and S. G. Vlăduț. On the decoding of algebraic–geometric codes. *IEEE Trans. Inf. theor.*, 36:1051–1060, 1990.

S. A. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum Publishers, New York, 1999.

W. R. Stevens. *TCP/IP Illustrated — The protocols*, volume 1. Addison–Wesley, New York, 1993a.

W. R. Stevens. *TCP/IP Illustrated — The implementation*, volume 2. Addison–Wesley, New York, 1993b.

H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, Berlin, 1993. ISBN 3-540-56489-6.

M. Sudan. Algorithmic introduction to coding theory. Massachusetts Institute of Technology (Boston), 2002. URL `http://theory.lcs.mit.edu/~madhu/FT01/`.

Y. Suhov. Lecture notes on algebraic coding theory. University of Cambridge, January 2003. URL `http://www.statslab.cam.ac.uk/~yms/`.

R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, 27(5):533–547, 1981. ISSN 0018-9448.

M. A. Tsfasman and S. G. Vlăduţ. *Algebraic–geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991. ISBN 0-7923-0727-5. Translated from the Russian by the authors.

M. A. Tsfasman, S. G. Vlăduţ, and T. Zink. Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

J. H. van Lint. *Introduction to coding theory*, volume 86 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 1992. ISBN 3-540-54894-7.

A. Vardy. Algorithmic complexity in coding theory and the minimum distance problem. In *STOC '97 (El Paso, TX)*, pages 92–109 (electronic). ACM, New York, 1999.

A. J. Viterbi. Convolutional codes and their performace in communication systems. *IEEE Trans. Comm.*, COM-19(5):751–772, 1971. ISSN 0090-6778.

P. V.S., W. Huffman, and B. R.A., editors. *Handbook of Coding Theory*. Elsevier, 1998.

J. L. Walker. *Codes and curves*, volume 7 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2000. URL `http://www.math.unl.edu/~jwalker/`. IAS/Park City Mathematical Subseries.

R. J. Walker. *Algebraic curves*. Springer-Verlag, New York, 1978.

H. N. Ward and J. A. Wood. Characters and the equivalence of codes. *J. Combin. Theory Ser. A*, 73(2):348–352, 1996. ISSN 0097-3165.

D. Welsh. *Codes and cryptography*. Oxford Science Publications. The Clarendon Press Oxford University Press, New York, 1988. ISBN 0-19-853288-1; 0-19-853287-3.

S. G. Wilson. *Digital Modulation and Coding*. Prentice Hall, 1995. ISBN 0-132-10071-1.

P. Wocjan. The brill–noether algorithm: Construction of geometric goppa codes and absolute factorization. Master's thesis, University of Kalsruhe, 1999. URL http://www.cs.caltech.edu/~wocjan/.

J. A. Wood. Extension theorems for linear codes over finite rings. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, volume 1255 of *Lecture Notes in Comput. Sci.*, pages 329–340. Springer, Berlin, 1997.

J. R. Wozencraft. Sequential decoding for reliable communication. Technical Report 325, Massachusetts Institute of Technology (Boston), 1957. URL http://hdl.handle.net/1721.1/4758.

K. S. Zigangirov. *Theory of Code Division Multiple Access Communication*. Wiley and sons, New York, 2004. ISBN 0-471-45712-4.