

PUBLICATIONS

Robert J. McEliece

(last revision March 25, 2006)

1. “Codes with Bounded Synchronization Delay” (with S. Golomb), *JPL Space Programs Summary 37-23*, vol. IV (1963), pp. 146–149.
2. “Optimal Communication Nets,” *JPL Space Programs Summary 37-29*, vol. IV (1964), pp. 221–227.
3. “Lattice Structure of Codes over Binary Asymmetric Channels,” *JPL Space Programs Summary 37-29*, vol. IV (1964), pp. 308–310.
4. “Weights of Cyclic Codes” (with G. Solomon), *J. Comb. Theory 1* (1966), pp. 459–475.
5. “A Combinatorial Identity in Order Statistics,” *JPL Space Programs Summary 37-39*, vol. IV (1966), pp. 230–231.
6. “Efficient Solutions of Equations for Decoding,” *JPL Space Programs Summary 37-40*, vol. IV (1966), pp. 216–218.
7. “A Class of Two-Weight Codes,” *JPL Space Programs Summary 37-41*, vol. IV (1966), pp. 264–266.
8. “A Generalization of Difference Sets,” *Can. J. Math.* 19 (1967), pp. 206–211.
9. **Linear Recurring Sequences Over Finite Fields**, Ph.D. Thesis, Caltech, March 1967.
10. “On the Number of Information Bits in Certain Cyclic Codes,” *JPL Space Programs Summary 37-44*, vol. IV (1967), pp. 291–293.
11. “Weights of Cyclic Codes,” *Proc. First Hawaii International Conference on System Sciences*, (1968), pp. 162–165.
12. “A Note on Reed-Solomon Codes,” *JPL Space Programs Summary 37-49*, vol. III (1968), pp. 310–311.
13. “Capabilities of Convolutional Codes” (with Howard Rumsey Jr.), *JPL Space Programs Summary 37-50*, vol. III (1968), pp. 248–251.
14. “Cross-Correlation of Reverse Maximal-Length Shift Register Sequences” (with T. Dowling), *JPL Space Programs Summary 37-53*, vol. III (1968), pp. 192–193.

15. "Sphere-Packing in the Hamming Metric" (with Howard Rumsey Jr.), *Bull. American Math. Soc.*, 75 (1969), pp. 32–34.
16. "Factorization of Polynomials Over Finite Fields," *Math. Comp.* 23 (1969), pp. 861–868.
17. "Cyclic Codes and Exponential Sums," *Proc. Second Hawaii International Conference on System Sciences*, (1969), pp. 223–225.
18. "The Synchronization of Reed-Solomon Codes," *JPL Space Programs Summary 37-55*, vol. III (1969), pp. 38–41.
19. "Quadratic Forms Over Finite Fields and Second-Order Reed-Muller Codes," *JPL Space Programs Summary 37-58*, vol. III (1969), pp. 28–33.
20. "On the Symmetry of Good Nonlinear Codes," *IEEE Trans. Inform. Theory* IT-16 (1970), pp. 609–611.
21. "Error-Correcting Prefixes for Establishing Word Synchronization," *JPL Space Programs Summary 37-61*, vol. III (1970), pp. 48–50.
22. "Some Results on the Capacity of Graphs" (with R. P. Stanley and H. Taylor), *JPL Space Programs Summary 37-61*, vol. III (1970), pp. 51–54.
23. "An Upper Bound on the Free Distance of a Tree Code" (with J. Layland), *JPL Space Programs Summary 37-62*, vol. III (1970), pp. 63–64.
24. "On Periodic Sequences from $GF(q)$," *J. Comb. Theory Series A*, 10 (1971), pp. 80–91.
25. "Ramsey Bounds for Graph Products" (with Paul Erdős and Herbert Taylor), *Pac. J. Math.* 37 (1971), pp. 45–46.
26. "Hide and Seek, Data Storage, and Entropy" (with Edward C. Posner), *Ann. Math. Stat.* 42 (1971), pp. 1706–1716.
27. "Theorem 6.2.2" in J. H. van Lint, **Coding Theory**, Springer Lecture Notes in Mathematics no. 201 (1971), pp. 123–125.
28. "A Combinatorial Packing Problem" (with L. D. Baumert et. al.), **Computers in Algebra and Number Theory** (SIAM-AMS Proceedings vol. IV, 1971), pp. 97–108.
29. "The Limits of Minimum-Distance Decoding," *JPL Deep Space Network Progress Report 42- 2* (1971), pp. 29–61.
30. "Symmetrically Decodable Codes" (with J. Savage), *JPL Deep Space Network Progress Report 42- 2* (1971), pp. 62–64.

31. “The Problem of Synchronization of Noisy Video,” *JPL Deep Space Network Progress Report 42- 3* (1971), pp. 105–107.
32. “Euler Products, Cyclotomy, and Coding” (with Howard Rumsey Jr.), *J. Number Theory* 4 (1972), pp. 302–311.
33. “Weights of Irreducible Cyclic Codes” (with L. D. Baumert), *Inf. and Control* 20 (1972), pp. 158–175.
34. “Weight Congruences for p-ary Cyclic Codes,” *Discrete Math.* 3 (1972), pp. 177–192.
35. “Weights Modulo 8 in Binary Cyclic Codes,” *JPL Deep Space Network Progress Report 42- 11* (1972), pp. 86–88.
36. “On the Weight Enumerators of Quadratic Residue Codes” (with J. Mykkeltveit and C. Lam), *JPL Deep Space Network Progress Report 42- 12* (1972), pp. 161–165.
37. “A Note on the Griesmer Bound” (with L. D. Baumert), *IEEE Trans. Inform. Theory* IT-19 (1973), pp. 134–135.
38. “Comment on ‘A Class of Codes for Asymmetric Channels and a Problem from the Additive Theory of Numbers,’ ” *IEEE Trans. Inform. Theory* IT-19 (1973), p. 137.
39. “Covering Tori with Squares” (with Herbert Taylor), *J. Comb. Thy.* 14 (1973), pp. 119–124.
40. “Hiding and Covering in a Compact Metric Space” (with Edward C. Posner), *Ann. Stat.* 1 (1973), pp. 729–739.
41. “A Golay-Viterbi Concatenated Coding Scheme for MJS’77” (with L. Baumert), *JPL Deep Space Network Progress Report 42- 18* (1973), pp. 76–84.
42. “A Low-Rate Improvement on the Elias Bound” (with Lloyd R. Welch and Howard Rumsey Jr.), *IEEE Trans. Inform. Theory* IT-20 (1974), pp. 676–678.
43. “ON DSN Antenna Scheduling” (with L. Harper and A. Odlyzko), *JPL Deep Space Network Progress Report 42- 20* (1974), pp. 53–56.
44. “The Ultimate Limits of Binary Coding for a Wideband Gaussian Channel” (with S. Butman), *JPL Deep Space Network Progress Report 42- 22* (1974), pp. 78–80.
45. “Forward Error Correction for the Ground Communications Facility” (with O. Adeyemi), *JPL Deep Space Network Progress Report 42- 22* (1974), pp. 114–117.

46. “Irreducible Cyclic Codes and Gauss Sums,” in **Combinatorics: Proceedings of the NATO Advanced Study Institute held at Nijenrode Castle, Breuke-
lin, The Netherlands, 8-20 July 1974** (M. Hall Jr. and J. H. van Lint, eds.),
Mathematical Centre, Amsterdam, 1975, pp. 185–202.
47. “Performance of Some Block Codes on a Gaussian Channel” (with L. Baumert), *Proc. 1975 ITC Conference*, pp. 189–195.
48. “Golay-Viterbi Decoding: Results of the MVM’73 X-Band Telemetry Experiment”
(with L. Baumert), *JPL Deep Space Network Progress Report 42– 25* (1975), pp. 108–
110.
49. “Zeroes of Functions in Finite Abelian Group Algebras” (with P. Delsarte), *Am. J. Math.* 98 (1976), pp. 197–224.
50. “Timesharing without Synchronization” (with A. Rubin), *Proc. 1976 ITC Conference*,
pp. 16–20.
51. “The Analysis of Structured Programs—Part I: Kirchhoff’s Equations,” *JPL Deep
Space Network Progress Report 42– 32* (1976), pp. 178–185.
52. “Decoding with Multipliers” (with L. Baumert and G. Solomon), *JPL Deep Space
Network Progress Report 42– 34* (1976), pp. 43–46.
53. “New Upper Bounds on the Rate of a Code via the Delsarte-MacWilliams Inequalities”
(with E. Rodemich, H. Rumsey, L. Welch), *IEEE Trans. Inform. Theory* IT-23 (1977),
pp. 57–166.
54. “An Improved Upper Bound on the Block Coding Error Exponent for Binary Input
Discrete Memoryless Channels” (with J. Omura), *IEEE Trans. Inform. Theory* IT-23
(1977), pp. 611–612.
55. “There Is No MacWilliams Identity for Convolutional Codes” (with J. Shearer), *IEEE
Trans. Inform. Theory* IT-23 (November 1977), p. 775.
56. “On Detection of Combined Occurrences,” *Comm. ACM* 20 (1977), pp. 678–679.
57. **The Theory of Information and Coding**, Reading, MA: Addison-Wesley, 1977.
58. “Multiple-Access Channels without Synchronization” (with E. C. Posner), *ICC’77
Conference Record*, vol. 2, pp. 246–248.
59. “Synchronization Strategies for RFI Channels” (with H. Van Tilborg and S. Tung),
JPL Deep Space Network Progress Report 42– 38 (1977), pp. 103–106.

60. “An Asymptotic Analysis of a General Class of Signal Detection Algorithms” (with E. Rodemich), *JPL Deep Space Network Progress Report 42– 39* (1977), pp. 30–35.
61. “A Property of Euclid’s Algorithm and an Application to Padé Approximation” (with J. Shearer), *J. SIAM Appl. Math.* 34 (1978), pp. 611–615.
62. “On the Inherent Intractability of Certain Coding Problems” (with E. R. Berlekamp and H. Van Tilborg), *IEEE Trans. Inform. Theory* IT-24 (1978), pp. 384–386.
63. “The Lovász Bound and Some Generalizations” (with E. Rodemich and H. Rumsey), *J. Combinatorics, Information, and System Science*, 3 (1978), pp. 134–152.
64. “Soft Decision Decoding of Block Codes” (with L. D. Baumert), *Proc. 1978 ITC Conference*, pp. 879–882. A preliminary version appeared in *JPL Deep Space Network Progress Report 42– 47* (1978), pp. 60–64.
65. “An Analysis of Alternate Symbol Inversion for Improved Symbol Synchronization in Convolutionally Coded Systems” (with L. Baumert and H. Van Tilborg), *JPL Deep Space Network Progress Report 42– 44* (1978), pp. 90–97.
66. “A Public-Key Cryptosystem Based on Algebraic Coding Theory,” *JPL Deep Space Network Progress Report 42– 44* (1978), pp. 114–116.
67. “Coding for Optical Channels” with L. D. Baumert and H. Rumsey Jr.), *JPL Deep Space Network Progress Report 42– 49* (1978), pp. 70–77.
68. “Symbol Synchronization in Convolutionally Coded Systems” (with L. Baumert and H. van Tilborg), *IEEE Trans. Inform. Theory* IT-25 (1979), pp. 362–365.
69. “The Bounds of Delsarte and Lovasz, and Their Applications to Coding Theory,” in **Algebraic Coding Theory and Applications**, G. Longo, ed., CISM Courses and Lectures No. 258, Springer-Verlag, Vienna, 1979, pp. 107–178.
70. “Coding for the Photon Channel,” *Proc. 1979 National Telecommunications Conference*, pp. 23.3.1–23.3.2.
71. “A Note on Digital Signatures,” *JPL Deep Space Network Progress Report 42– 50* (1979), pp. 95–96.
72. “Coding for Optical Channels with Photon-Counting” (with L. Welch), *JPL Deep Space Network Progress Report 42– 52* (1979), pp. 61–66.
73. “The R_0 -Parameter for Optical Communication Using Photon-Counting,” *JPL Deep Space Network Progress Report 42– 53* (1979), pp. 62–65.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.