References

[1] Koichi Betsumiya, T. Aaron Gulliver, and Masaaki Harada. Binary optimal linear rate 1/2 codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 462–471. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[2] Mahesh C. Bhandari, Manish K. Gupta, and Arbind K. Lal. On z_4-simplex codes and their gray images. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 170–180. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[3] Ian F. Blake. Curves with many points and their applications. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 55–64. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[4] Uri Blass, Iiro Honkala, and Simon Litsyn. On the size of identifying codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 142–147. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[5] James W. Bond, Stefen Hui, and Hank Schmidt. The euclidean algorithm and primitive polynomials over finite fields. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Alge-*

braic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999), volume 1719 of *LNCS*, pages 482–491. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[6] M. Bossert, H. Grieẞer, J. Maucher, and V.V. Zyablov. Some results on generalized concatenation of block codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 181–190. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[7] Serdar Boztag. New lower bounds on the periodic crosscorrelation of qam codes with arbitrary energy. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 410–419. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[8] Claude Carlet and Philippe Guillot. A new representation of boolean functions. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 94–103. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[9] K.K.P. Chanduka, Mahesh C. Bhandari, and Arbind K. Lal. Lower bounds for group covering designs. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 334–345. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[10] Wende Chen and Torleiv Kløve. On the second greedy weight for binary linear codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 131–141. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[11] Michael Clausen and Meinard Müller. A fast program generator of fast fourier transforms. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 29–42. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[12] Elena Couselo, Santos Gonzalez, Victor Markov, and Alexandr Nechaev. Recursive mds-codes and pseudogeometries. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 211–220. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[13] Sylvia Encheva and Gérard Cohen. On the state complexities of ternary codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 454–461. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[14] Karin Engdahl, Michael Lentmaier, and Kamil Sh. Zigangirov. On the theory of low-density convolutional codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii,*

November 15-19, 1999), volume 1719 of *LNCS*, pages 77–86. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[15] F. Fekri, S.W. McLaughlin, R.M. Mersereau, and R.W. Schafer. Double circulant self-dual codes using finite-field wavelet transforms. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 355–364. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[16] G. David Jr. Forney. Codes on graphs: A survey for algebraists. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 1–9. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[17] Marc P.C. Fossorier, Miodrag J. Mihaljević, and Hideki Imai. Critical noise for convergence of iterative probabilistic decoding with belief propagation in cryptographic applications. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 282–293. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[18] Markus Grassl, Willi Geiselmann, and Thomas Beth. Quantum reed-solomon codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 231–244. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[19] M. Greferath and S.E. Schmidt. Linear codes and rings of matrices. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 160–169. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[20] Frances Griffin, Harald Niederreiter, and Igor E. Shparlinski. On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 87–93. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[21] A. Halbutoğullari and Ç.K. Koç. Mastrovito multiplier for general irreducible polynomials. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 498–507. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[22] T. Høholt and R. Refslund Nielsen. Decoding hermitian codes with sudan's algorithm. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 260–270. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[23] K.J. Horadam. Sequences from cocycles. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 121–130. Springer-

Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[24] Garry Hughes. Characteristic functions of relative difference sets, correlated sequences and hadamard matrices. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 346–354. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[25] Hui Jin and Robert J. McEliece. Ra codes achieve awgn channel capacity. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 10–18. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[26] Marek Karpinski and Igor Shparlinski. On the computational hardness of testing square-freeness of sparse polynomials. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 492–497. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[27] Tadao Kasami. On integer programming problems related to soft-decision iterative decoding algorithms. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 43–54. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[28] V.L. Kurakin, A.S. Kuzmin, V.T. Markov, A.V. Mikhalev, and A.A. Nechaev. Linear codes and polylinear recurrences over finite rings and

modules (a survey). In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 365–391. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[29] Didier Le Ruyet, Hong Sun, and Han Vu Thien. Properties of finite response input sequences of recursive convolutional codes. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 324–333. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[30] Shengli Liu and Yumin Wang. An authentication scheme over non-authentic public channel in information-theoretic secret-key agreement. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 294–301. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[31] Ryutaroh Matsumoto and Shinji Miura. Computing a basis of $\updownarrow(\lceil)$ on an affine algebraic curve with one rational place at infinity. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 271–281. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[32] Ezra Miller and Bernd Sturmfels. Monomial ideals and planar graphs. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages

19–28. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[33] Mehul Motani and Chris Heegard. Computing weight distributions of convolutional codes via shift register synthesis. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 314–323. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[34] B. Mourrain. A new criterion for normal form algorithms. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 430–443. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[35] Jörn Müller-Quade and Thomas Beth. Calculating generators for invariant fields of linear algebraic groups. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 392–403. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[36] Zsigmond Nagy and Kenneth Zeger. Capacity bounds for the 3-dimensional $(0,1)$ runlength limited channel. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 245–251. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[37] Patric R.J. Östergård. On binary-ternary error-correcting codes with minimum distance 4. In Marc Fossorier, Hideki Imai, Shu Lin, and

Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 472–481. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[38] Matthew G. Parker. Conjectures on the size of constellations constructed from direct sums of psk kernerls. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 420–429. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[39] A. Poli, M.C. Gennero, and D. Xin. Discrete fourier transform and gröbner bases. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 444–453. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[40] Markus Püschel, Martin Rötteler, and Thomas Beth. Fast quantum fourier transforms for a class of non-abelian groups. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 148–159. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[41] Shojiro Sakata and Masazumi Kurihara. A systolic array architecture for fast decoding of one-point ag codes and scheduling of parallel processing on it. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages

302–313. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[42] M. Amin Shokrollahi. New sequences of linear time erasure codes approaching the channel capacity. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 65–76. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[43] V. Sidorenko, J. Maucher, and M. Bossert. Rectangular codes and rectangular algebra. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 252–259. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[44] Hidema Tanaka, Kazuyuki Hisamatsu, and Toshinobu Kaneko. Strength of misty1 without fl function for higher order differential attack. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 221–230. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[45] Yuansheng Tang, Tadao Kasami, and Toru Fujiwara. An optmality testing algorithm for a decoded codeword of binary block codes and its computational complexity. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 201–210. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[46] I. Vaughan and L. Clarkson. An algorithm to compute a nearest point in the lattice a_n^*. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli,

editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 104–120. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[47] Joachim von zur Gathen and Igor Shparlinski. Constructing elements of large order in finite fields. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 404–409. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.

[48] Qi Wang, Lei Wei, and Rodney A. Kennedy. Near optimal decoding for tcm using the biva and trellis shaping. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Proceedings of the 13th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'99 (Honolulu, Hawaii, November 15-19, 1999)*, volume 1719 of *LNCS*, pages 191–200. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Singapore-Tokyo, 1999.