References

[1] V. Álvarez, J.A. Armario, M.D. Frau, and P. Real. An algorithm for computing cocyclic matrices developed over some semidirect products. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 287–296. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[2] Vladimir B. Balakirsky. On algebraic soft decision decoding of cyclic binary codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 315–322. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[3] A. Baliga and J. Chua. Self-dual codes using image restoration techniques. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 46–56. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[4] Thierry P. Berger and Louis de Maximy. Cyclic projective reed-muller codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 77–81. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[5] Koichi Betsumiya, Masaaki Harada, and Akihiro Munemasa. Type ii codes over if_{2^r}. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra,*

Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001), volume 2227 of *LNCS*, pages 102–111. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[6] François Boulier and Sylvain Neut. Cartan's characters and stairs of characteristic sets. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 363–372. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[7] Eimear Byrne. Lifting decoding schemes over a galois ring. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 323–332. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[8] E. Cadic, J.C. Carlach, G. Olocco, A. Otmani, and J.P. Tillich. Low complexity tail-biting trellises of self-dual codes of length 24, 32 and 40 over $gf(2)$ and z_4 of large minimum distance. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 57–66. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[9] Chris Charnes, Martin Rötteler, and Thomas Beth. On homogeneous bent functions. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 249–259. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[10] Bikash Kumar Dey and B. Sundar Rajan. f_q-linear cyclic codes over f_{q^m}: Dft characterization. In Serdar Boztaş and Igor E. Shparlinski,

editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 67–76. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[11] Sylvia Encheva and Gérard Cohen. Partially identifying codes for copyright protection. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 260–267. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[12] P. Gaudry and É. Schost. On the invariants of the quotients of the jacobian of a curve of genus 2. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 373–386. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[13] Olav Geil and Tom Høholdt. On hyperbolic codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 159–171. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[14] Mark Giesbrecht, Jr. Jacobson, Michael, and Arne Storjohann. Algorithms for large integer matrix problems. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 297–307. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[15] Andrew M. Guidi, Alex J. Grant, and Steven S. Pietrobon. Algebraic constructions for psk space-time coded modulation. In Ser-

dar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 387–396. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[16] T. Aaron Gulliver and Masaaki Harada. Optimal double circulant z_4-codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 122–128. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[17] Manish K. Gupta, David G. Glynn, and T. Aaron Gulliver. On senary simplex codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 112–121. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[18] Venkatesan Guruswami. Constructions of codes from number fields. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 129–140. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[19] Jaime Gutierrez and Domingo Gomez-Perez. Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 192–199. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[20] Iiro Honkala, Mark G. Karpovsky, and Simon Litsyn. On the identification of vertices and edges using cycles. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 308–314. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[21] Hiroshi Horimoto and Keisuke Shiromoto. On generalized hamming weights for codes over finite chain rings. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 141–150. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[22] Tadao Kasami, Hitoshi Tokushige, and Yuichi Kaji. Sufficient conditions on most likely local sub-codewords in recursive maximum likelihood decoding algorithms. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 333–342. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[23] Andrei Kelarev and Olga Sokratova. Information rates and weights of codes in structural matrix rings. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 151–158. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[24] Margreta Kuijper, Marten van Dijk, Henk Hollmann, and Job Oostveen. A unifying system-theoretic framework for errors-and-erasures reed-solomon decoding. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*,

pages 343–352. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[25] Tero Laihonen and Sanna Ranto. Codes identifying sets of vertices. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 82–91. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[26] James L. Massey. The ubiquity of reed-muller codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 1–12. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[27] Matthew G. Parker. Even length binary sequence families with low negaperiodic autocorrelation. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 200–209. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[28] Patrice Parraud. On the non-existence of (almost-)perfect quaternary sequences. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 210–218. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[29] A. Peinado, F. Montoya, J. Muñoz, and A.J. Yuste. Maximal periods of $x^2 + c$ in f_q. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages

219–228. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[30] Vera Pless. Self-dual codes-theme and variations. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 13–21. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[31] M.C. Rodríguez-Palánquex, L.J. García-Villalba, and I. Luengo-Velasco. Computing the genus of a class of curves. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 182–191. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[32] Shojiro Sakata. On fast interpolation method for guruswami-sudan list decoding of one-point algebraic-geometry codes. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 172–181. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[33] Hans Georg Schaathun. Duality and greedy weights of linear codes and projective multisets. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 92–101. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[34] Amin Shokrollahi. Design of differential space-time codes using group theory. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*,

pages 22–35. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[35] Igor E. Shparlinski. On the generalised hidden number problem and bit security of xtr. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 268–277. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[36] Madhu Sudan. Ideal error-correcting codes: Unifying algebraic and number-theoretic algorithms. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 36–45. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[37] P. Udaya and S. Boztaş. On the aperiodic correlation function of galois ring m-sequences. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 229–238. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[38] Vasyl Ustimenko. Cryptim: Graphs as tools for symmetric encryption. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 278–286. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[39] Tadashi Wadayama. An algorithm for computing rejection probability of mld with threshold test over bsc. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes,*

AAECC'2001 (Melbourne, Australia, November 26-30, 2001), volume 2227 of *LNCS*, pages 353–362. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.

[40] Liping Wang. Euclidean modules and multisequence synthesis. In Serdar Boztaş and Igor E. Shparlinski, editors, *Proceedings of the 14th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC'2001 (Melbourne, Australia, November 26-30, 2001)*, volume 2227 of *LNCS*, pages 239–248. Springer-Verlag, Berlin-Heidelberg-New York-Barcelona-Hong Kong-London-Milan-Paris-Tokyo, 2001.