Finite Fields

11Txx

[1] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang, *A trace conjecture and flag-transitive affine planes*, J. Combin. Theory Ser. A **95** (2001), no. 1, 158–168. MR MR1840482 (2002c:11166)

[2] Aart Blokhuis, Robert S. Coulter, Marie Henderson, and Christine M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 37–42. MR MR1849077 (2002e:11175)

[3] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *A few more quadratic APN functions*, 2008.

[4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. **14** (2008), no. 3, 703–714. MR MR2435056

[5] Marcus Brinkmann and Gregor Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 273–288. MR MR2438456

[6] Jessica F. Burkhart, Neil J. Calkin, Shuhong Gao, Justine C. Hyde-Volpe, Kevin James, Hiren Maharaj, Shelly Manber, Jared Ruiz, and Ethan Smith, *Finite field elements of high order arising from modular curves*, Des. Codes Cryptogr. **51** (2009), no. 3, 301–314. MR MR2485499 (2010b:11164)

[7] Murat Cenk and Ferruh Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010), no. 2, 172–186.

[8] Mihai Cipu, *Dickson polynomials that are permutations*, Serdica Math. J. **30** (2004), no. 2-3, 177–194. MR MR2098331 (2005g:11244)

[9] Mihai Cipu and Stephen D. Cohen, *Dickson polynomial permutations*, Finite Fields and Applications, Contemporary Mathematics, vol. 461, 2008.

[10] Stephen D. Cohen, *Finite field elements with specified order and traces*, Des. Codes Cryptogr. **36** (2005), no. 3, 331–340. MR MR2163064

[11] _____, *Primitive polynomials with a prescribed coefficient*, Finite Fields Appl. **12** (2006), no. 3, 425–491. MR MR2229326 (2007e:11141)

[12] Robert S. Coulter, George Havas, and Marie Henderson, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's p^s-polynomials*, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput, vol. 9, World Sci. Publ., River Edge, NJ, 2001, pp. 36–45. MR MR1877440 (2002m:11103)

[13] ———, *On decomposition of sub-linearised polynomials*, J. Aust. Math. Soc. **76** (2004), no. 3, 317–328. MR MR2053506 (2005b:13013)

[14] Robert S. Coulter and Marie Henderson, *The compositional inverse of a class of permutation polynomials over a finite field*, Bull. Austral. Math. Soc. **65** (2002), no. 3, 521–526. MR MR1910505 (2003f:11185)

[15] Jean-Marc Couveignes and Reynald Lercier, *Elliptic periods for finite fields*, Finite Fields Appl. **15** (2009), no. 1, 1–22. MR MR2468989 (2009j:12006)

[16] Yves Edel and Alexander Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), no. 1, 59–81. MR MR2476525 (2010c:11154)

[17] Ronald Evans, Henk D. L. Hollmann, Christian Krattenthaler, and Qing Xiang, *Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets*, J. Combin. Theory Ser. A **87** (1999), no. 1, 74–119. MR MR1698269 (2001b:05038)

[18] Reza Rezaeian Farashahi and Ruud Pellikaan, *The quadratic extension extractor for (hyper)elliptic curves in odd characteristic*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 4547, Springer, Berlin, 2007, pp. 219–236. MR MR2387145 (2009a:11252)

[19] Kseniya Garaschuk, *On binary and ternary Kloosterman sums*, Ph D thesis, Simon Fraser University, 2007.

[20] Lenwood S. Heath and Nicholas A. Loehr, *New algorithms for generating Conway polynomials over finite fields*, Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999) (New York), ACM, 1999, pp. 429–437. MR MR1739972 (2000j:11187)

[21] Dae San Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, 2008.

[22] ———, *Codes associated with orthogonal groups and power moments of Kloosterman sums*, 2008.

[23] _____, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums*, 2008.

[24] Douglas A. Leonard, *A weighted module view of integral closures of affine domains of type I*, Adv. Math. Commun. **3** (2009), no. 1, 1–11.

[25] Petr Lisoněk, *On the connection between Kloosterman sums and elliptic curves*, Sequences and Their Applications – SETA 2008: Proceedings (Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, eds.), Lecture Notes in Computer Science, vol. 5203, Springer, Berlin Heidelberg, 2008, pp. 182–187.

[26] Marko Moisio, *Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm*, Acta Arith. **132** (2008), no. 4, 329–350. MR MR2413356 (2009f:11149)

[27] Ferruh Özbudak, *Elements of prescribed order, prescribed traces and systems of rational functions over finite fields*, Des. Codes Cryptogr. **34** (2005), no. 1, 35–54. MR MR2126576 (2005k:11239)

[28] B. V. Petrenko, *On the product of two primitive elements of maximal subfields of a finite field*, J. Pure Appl. Algebra **178** (2003), no. 3, 297–306. MR MR1953735 (2004b:11165)

[29] _____, *On the sum of two primitive elements of maximal subfields of a finite field*, Finite Fields Appl. **9** (2003), no. 1, 102–116. MR MR1954786 (2003m:12004)

[30] Håvard Raddum and Igor Semaev, *Solving multiple right hand sides linear equations*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 147–160. MR MR2438447