Mathematical Problems of Computer Science 35, 63–69, 2011.

Irreducible Compositions of Polynomials Over Finite Fields of Even Characteristic*

Saeid M. Mehrabi and Melsik K. Kyuregyan

Institue for Informatics and Automation Problems of NAS of RA
e-mail smbatt@ipia.sci.am

Abstract

This note presents some results with the constructive theory of synthesis of irreducible polynomials over a Galois field with even characteristic. We prove a theorem that plays an important role for constructing irreducible polynomials. By this theorem a recurrent method for constructing families of irreducible polynomials of degree $n2^k$ $(k = 1, 2, ...)$ over F_{2^s} is proposed.

References

[1] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[2] I.F. Blake, G.Seroussi and N.P.Smart, Elliptic curves in Cryptography, Cambridge University Press, Cambridge, Reprinted 2000.

[3] B. Chor, R. rivest, "A knapsack-type public key cryptosystem based on arithmetic in finite fields", *IEEE Trans.Inform.Theory*, vol. 34, pp. 901-909, 1988.

[4] J. Calmet, "Algebraic algorithms in GF (q)",*Discrete Math*, vol. 56 pp. 101-109, 1985.

[5] R. Chapman, "Completely normal elements in iterated quadratic extensions Of finite fields",*Finite Fields Appl*, vol. 3, pp. 3-10, 1997.

[6] S. D. Cohen,"On irreducible polynomials of certain types in finite fields", *Proc. Cambridge Philos.* Soc, vol. 66, pp. 335-344, 1969.

[7] S. D. Cohen,"The explicit construction of irreducible polynomials over finite fields", *De. Codes Cryptogr*, vol. 2, pp. 169-173, 1992.

[8] W. Eberly," Very fast parallel matrix and polynomial arithmetic", *25th Annual symposium on Foundations of Computer Science*, pp. 21-30, 1984.

[9] S. Gao, Normal bases over finite fields, Ph.D Thesis, Waterloo, 1993.

[10] M.K. Kyuregyan,"Recurrent Methods for Constructing Irreducible Polynomials over" , *Finite Fields Apple*, vol. 8, pp. 52-68, 2002.

[11] M. K. Kyuregyan,"Iterated constructions of irreducible polynomials over finite fields with linearly independent roots" ,*Finite Fields Apple*, vol. 10, pp. 323-431, 2004.

[12] M. K. Kyuregyan,"Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics", *Finite Fields Appl*, vol. 9, pp. 39-58, 2003.

*2000 Mathematics subject classifications: 47A68, 47A70

[13] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics II", *Finite Fields Appl*, vol. 12, pp. 357-378, 2006.

[14] M.K. Kyuregyan, "Quadratic transformations and synthesis of irreducible polynomials over finite fields", *Dokl, Akad, Nauk Arm, SSR*, vol. 84(2), pp. 67-71, 1987. (in Russian).

[15] N.Koblitz, Algebraic Aspects of Cryptography, Springer, Berlin, 1998.

[16] R. Lidl and H. Niederreiter. Finite Fields. Cambridge University Press, 1987.

[17] A. Menezes, I.F. Blake, X. GAO, R. C. Mullin, S. A. Vanstone, T.Yaghoobian. Applications of Finite Fields, Kluwer Academic Publishers, Boston- Dordrecht- Lancaster, 1993.

[18] F.J.MacWilliams, N.J.A, Sloane. The theory of error-correcting codes, Part, Bell Laboratories Murray Hill, NJ, USA, North-Holland Publishing Company, Amsterdam, New York, Oxford.

[19] G. McNay, Topics in finite fields, Ph.D. Thesis, University of Glasgow, 1995.

[20] H. Meyn," Explicit N-polynomials of 2-power degree over finite fields", *Designs Codes Cryptogr*, vol. 6, pp. 107-116, 1995.

[21] S. Perlis, "Normal bases of cyclic fields of prime-power degree",*Duke Math. J.*, vol. 9, pp. 507-517, 1942.

[22] J.Von zur Gathen, E. Kaltofen,"Factorization of multivariate polynomials over finite fields", *Math.Comput*, vol.45, pp. 251-261, 1985.

[23] R. R. Varshamov," A general method of synthesizing irreducible polynomials over Galois fields", *Soviet Math. Dokl*, vol. 29, pp. 334- 336, 1984.

Զույգ բնութագրիչով չբերվող բազմանդամների բաղադրություններ վերջավոր դաշտերի վրա

Ս. Մեհրաբի և Մ. Կյուրեղյան

Ամփոփում

Այս աշխատանքը ներկայացնում է վերջավոր դաշտերի վրա զույգ բնութագրիչով չբերվող բազմանդամների սինտեզման կոնստրուկտիվ տեսության որոշ արդյունքներ: Մենք ապացուցել ենք թեորեմ, որը մեծ դեր է խաղում չբերվող բազմանդամներ կառուցելուց: Այս թեորեմի օգնությամբ առաջարկվում է $n2^k(k = 1, 2 ...)$ աստիճանի չբերվող բազմանդամ կառուցելու ռեկուռենտ մեթոդ: