Mathematical Problems of Computer Science 35, 99–103, 2011.

Irreducibility of Some Composite Polynomials Over Finite Fields *

Sergey Abrahamyan and Edita Harutyunyan

Institue for Informatics and Automation Problems of NAS of RA
e-mail serj.abrahamyan@gmail.com, edita@ipia.sci.am

Abstract

Given the field $\mathcal{F}$ with q elements and of characteristics p and an irreducible polynomial $P(x) = c_n x^n + c_{n-1} x^{n-1+c_1 x^n \cdots c_0}$ over $\mathcal{F}$. We prove that the composite polynomial $(dx^p - dx)^n \, p\left(\frac{ax^p - ax + c}{dx^p - dx}\right)$ is irreducible over $\mathcal{F}$ under certain conditions. Also a recursive construction of sequences of irreducible polynomials of degree $n2^k (k = 1, 2, 3, \cdots)$ over $\mathcal{F}_{2^s}$ is given.

References

[1] S. E. Abrahamyan, "Construction of Irreducible Polynomials over Finite Fields", *Proceedings of 12th International Workshop, CASC 2010, in Lecture Notes in Computer Science*, vol. 6244, Gerdt, pp. 3-4, 2010.

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

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

[4] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over $\mathcal{F}_q$ of odd characteristics", *Finite Fields Appl.*, vol. 9, pp. 39–58, 2003.

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

[6] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over $\mathcal{F}_q$ of odd characteristics II", *Finite Fields, Appl.*, vol. 12, pp. 357–378, 2006.

[7] M. K. Kyuregyan and G. M. Kyuregyan, "Irreducible Compositions of Polynomials over Finite Fields", *Design, Codes and Cryptography*, Available online: ISSN:0925-1022 2010.

[8] 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.

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

*The work was supported by Armenian Target Programm 04.10.31.

Որոշ բաղադրյալ բազմանդամների չբերվելիությունը վերջավոր դաշտերի վրա

Ս. Աբրահամյան և Է. Հարությունյան

Ամփոփում

Աշխատանքը նվիրված է վերջավոր դաշտերի վրա չբերվող բազմանդամների բաղադրություններ կառուցմանը: Տրված է q հզորությամբ, p բնութագրիչով $\mathcal{F}_q$ դաշտը և $\mathcal{F}_q$ դաշտի վրա $P(x) = c_n x^n + c_{n-1}x^{n-1+c_1 x^n \cdots c_0}$ չբերվող բազմանդամը: Ցույց է տրված, որ $(dx^p - dx)^n\, p\left(\frac{ax^p-ax+c}{dx^p-dx}\right)$ բաղադրությունը չբերվող է $\mathcal{F}_q$ դաշտի վրա որոշակի պայմանների դեպքում: Ավելին, տրված է $\mathcal{F}_{2^s}$ դաշտի վրա $n2^k (k = 1, 2, 3, \cdots)$ աստիճանի չբերվող բազմանդամների կառուցման հաջորդական եղանակ: