Mathematical Problems of Computer Science 35, 26–32, 2011.

Constructing Methods for Irreducible Polynomials

Mahmood Alizadeh

Islamic Azad University- Ahvaz Branch
E-mail: Alizadeh@iauahvaz.ac.ir

Abstract

In this paper we study the irreducibility of some composite polynomials, constructed with a polynomial composition method over finite fields. Furthermore, a recurrent method for constructing families of irreducible polynomials of higher degree from given irreducible polynomials over finite fields is given.

References

[1] E.R. Berlekamp, Algebraic coding theory, Mc Graw-Hill, New York, 1968.

[2] I.F. Blake, G.Seroussi, N.P.Smart, *Elliptic curves in cryptography*, Cambridge University Press, Cambridge , reprinted 2000.

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

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

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

[6] S.D.Cohen, "The explicit construction of irreducible polynomial over finite fields",*Des. Codes cryptogr.*, vol. 2, pp. 169-174, 1992.

[7] N.Koblitz, *Algebraic aspects of cryptography*, Springer, Berlin 1998.

[8] R. Lidl, H.Niederreiter, *Finite fields*, Cambridge University, Press Cambridge 1987.

[9] M. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over $GF(2^s)$", *Finite fields and their applications*, vol. 8, pp. 52-68, 2002.

[10] M.K. Kyuregyan, "Iterated constructions of irreducible polynomials over finite fields with linearly independent roots", *Finite fields and their applications*, vol. 10, pp. 323-341, 2004.

[11] A.J. Menezes, I. F. Blake , X.Gao, R.C.Mullin, S.A.Vanstone, T.Yaghoobian, *Applications of finite fields*, Kluwer Academic publishers, Boston, 1993.

Չբերվող բազմանդամների կառուցման եղանակ

Մ. Ալիզադեհ

Ամփոփում

Այս աշխատանքում մենք ուսումնասիրում ենք որոշ կոմպոզիցիոն բազմանդամների չբերվելիությունը, որոնք կառուցված են բազմաքնդամային կոմպոզիցիոն մեթոդով, վերջավոր դաշտերի վրա: Ավելին տրվել է ռեկուրենտ մեթոդ, վերջավոր դաշտերի վրա տրված չբերվող բազմանդամից բարձր աստիճանի չբերվող բազմանդամ կառուցելու համար: