Mathematical Problems of Computer Science 36, 57–62, 2012.

Computation of the Complexity of some Recursive Constructed Normal Polynomials

Mahmood Alizadeh

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

Abstract

In this paper we give some algorithms for computing the complexity of some normal polynomials constructed by some recurrent methods. Finally some results of our algorithms are given in a table.

Keywords: Complexity, Irreducible Polynomial, Normal Polynomial.

References

[1] S. Abrahamyan, "Some construction of N-polynomials over finite fields", *National Academy of Sciences of Armenia Reports*, vol. 111, no. 3, 232-239, 2011.

[2] M. Alizadeh, "Some algorithms for normality testing irreducible polynomials and computing complexity of the normal polynomials over finite fields, *Applied Mathematical Sciences*, vol. 6, no. 40, 1997 - 2003, 2012.

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

[4] M. K. Kyuregyan, "Iterated construction of irreducible polynomials over finite fields with linearly independent roots",*Finite Fields Appl.* , vol. 10, pp. 323-341, 2004.

[5] M. K. Kyuregyan,"Recursive constructions of N-polynomials over $GF(2^s)$", *Discrete Applied Mathematics*, vol. 156, pp. 1554-1559, 2008.

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

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

[8] H. Meyn, "Explicit N-polynomial of 2-power degree over finite fields", *Designs, Codes and Cryptography*, vol. 6, pp. 147-158, 1995.

[9] R. Mullin, I. Onyszchuk, S. Vanstone and R. Wilson,"Optimal normal basesin $GF(p^n)^n$",*Discreate Applied math.*,vol. 22, ,149-161, 1988/1989.

[10] J. Omura and J. Massey, "Computational method and apparatus for finite field arithmatic",U.S. patent 4,586,627, 1986.

[11] I. Onyszchuk, R. Mullin, and S. Vanstone, "Computational method and apparatus for multiplication",U.S patent 4,745,568, 1988.

Ռեկուրսիվ կառուցված որոշ նորմալ բազմանդամների բարդության հաշվումը

Մ. Ահլիզադեհ

Ամփոփում

Այս աշխատանքում մենք առաջարկում ենք որոշակի ալգորիթմ հաշվելու համար որոշ նորմալ բազմանդամների բարդությունը, որոնք կառուցվել են ռեկուրենտ եղանակներով: Բերված է աղյուսակ, որում նշված է որոշ արդյունքներ:

Вычисление сложности некоторых рекурсивно построенных полиномов

М. Ализаде

Аннотация

В этой статье мы предлагаем алгоритмы вычисления сложности нормальных полиномов, построенных определенными рекуррентными методами.

В заключении приведена таблица, которая содержит некоторые результаты.