Mathematical Problems of Computer Science 33, 144--149, 2010.

# Construction of Explicit Irreducible Polynomials over $F_2$ in Cluster Computational Environment

Ofelya Manukyan and Melsik Kyuregyan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: manofa81@yahoo.com, melsik@ipia.sci.am

**Abstract**

This paper describes a method for constructing families of explicit irreducible polynomials over $F_2$. The proposed method allows construction of explicit polynomials of higher degree over $F_2$ from a given sequence of primitive polynomials. A computational algorithm has been developed and implemented on base of this method. The program is realized in the most effective way possible in cluster computational environment. Allocation and distribution of memory resources have been implemented in a careful manner, since data size increases drastically with increasing of the amount of computations required. Program paralleling is performed using data paralleling, i.e. data is distributing among all processors, which ran the same program and each of which builds the subsequent irreducible polynomial, and finally a sequence of all the irreducible polynomials in explicit form is obtained. Moreover, the program also searches for the polynomial with the lowest possible weight among of all the polynomials of the same degree.

## References

[1] M. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over $GF(2^s)$", *Finite Fields and Their Applications 8*, pp. 52-68, 2002.

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

[3] 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.

# $F_2$ վերջավոր դաշտի վրա անվերածելի բազմանդամների բացահայտ տեսքով կառուցման եղանակ կլաստերային հաշվողական համակարգում

Օ. Մանուկյան և Մ. Կյուրեղյան

## Ամփոփում

Աշխատանքում նկարագրված է $F_2$ վերջավոր դաշտի վրա անվերածելի բազմանդամների բացահայտ տեսքով կառուցման մի եղանակ, որը հնարավորինս էֆեկտիվորեն մշակվել և իրականացվել է կլաստերային հաշվողական համակարգում: Հիշողության ռեսուրսների բաշխումը՝ հիշողության հատկացումն ու ազատումը կատարվել են խնայողաբար, քանի որ հաշվարկների ընթացքում տվյալների երկարությունները շատ արագ աճում են: Կլաստերային հաշվողական համակարգում ծրագրի զուգահեռացումը կատարվել է ըստ տվյալների, այսինքն տվյալները բաշխվում են պրոցեսորների միջև, բոլոր պրոցեսորները աշխատում են միևնույն ծրագրով և յուրաքանչյուրը կառուցում է հերթական անվերածելի բազմանդամը: Արդյունքում ստանում ենք անվերածելի բազմանդամների հաջորդականություն և բացի այդ փնտրում ենք միևնույն աստիճանի հնարավորինս փոքր կշիռ ունեցող անվերածելի բազմանդամը: