On Complexity of Expression Binary Operations via Polynomials over Finite Fields

Ph.B. Burtyka (CSC SFEDU, Rostov-on-Don)
E-mail address: fburtyka@sfedu.ru

We present an algorithm to construct polynomial expressions of commutative binary operations via polynomials over Galois field extensions. For instance, this paper presents polynomials expressing operations in $\mathbb{Z}_n$ and bitwise logical operations in rings of a form $\mathbb{Z}_{2^n}$. The paper considers algorithmical complexity of constructing and evaluation of the polynomials.

Our implementation of the algorithm uses library NTL by Victor Shoup.

О сложности выражения бинарных операций с помощью полиномов над расширениями конечных полей

Ф.Б. Буртыка (ЮГИНФО ЮФУ, Ростов-на-Дону)
E-mail address: fburtyka@sfedu.ru

Предлагается алгоритм построения полиномов над расширениями полей Галуа, выражающих коммутативные бинарные операции. Для примера приводится построение таких полиномов для операций в $\mathbb{Z}_n$, а также побитовых логических операций в кольцах вида $\mathbb{Z}_{2^n}$. Рассматривается алгоритмическая сложность построения и вычисления таких полиномов, а также некоторые приложения.

Реализация предлагаемого алгоритма использует библиотеку NTL Виктора Шупа.