CORR 2000-31

Efficient Algorithm for Polynomial Reduction

Huapeng Wu

Abstract In this paper, we consider the problem of efficient computation of polynomial modular reduction: $A(x) \bmod f(x)$, where $f(x)$ is a monic polynomial of degree n and $A(x)$ is a polynomial of degree not greater than $n+t-1,\ t \geq 1$, the coefficients of both $f(x)$ and $A(x)$ are defined over a commutative ring R with identity. For given $f(x)$ and the degree $n+t-1$ of $A(x)$, we present an algorithm to compute this problem in $t(w-1)$ addition operations in R and the same number of multiplication operations in R, where w is the Hamming weight of $f(x)$. Applications of the proposed algorithm to finite field arithmetic are also discussed.

Keywords Polynomial arithmetic, modular operation, finite field arithmetic, complexity