DAVID THOMSON, Carleton University, Ottawa, ON

Efficient p-th root computations in finite fields of characteristic p

We present a method for computing p-th roots using a polynomial basis over finite fields $\mathbb{F}_q$ of odd characteristic p, $p \geq 5$, by taking advantage of a binomial reduction polynomial. For a finite field extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ our method requires $p-1$ scalar multiplications of elements in $\mathbb{F}_{q^m}$ by elements in $\mathbb{F}_q$. In addition, our method requires at most $(p-1)\lceil m/p \rceil$ additions in the extension field. In certain cases, these additions are not required. If z is a root of the irreducible reduction polynomial, then the number of terms in the polynomial basis expansion of $z^{1/p}$, defined as the Hamming weight of $z^{1/p}$ or $\mathrm{wt}(z^{1/p})$, is directly related to the computational cost of the p-th root computation. We find that $\mathrm{wt}(z^{1/p}) = 1$ in all cases using binomials. We also give conditions on which degrees m admit an irreducible binomial over $\mathbb{F}_q$.