Selecting polynomials for the Function Field Sieve

Razvan Barbulescu

The Function Field Sieve (FFS) algorithm is dedicated to computing discrete logarithms in a finite field $\mathbb{F}_{q^n}$, where q is a prime power, small compared to q^n. Introduced by Adleman in [Adl94] and inspired by the Number Field Sieve (NFS), the algorithm collects pairs of polynomials $(a, b) \in \mathbb{F}_q[t]$ such that the norms of $a - bx$ in two function fields are both smooth (the sieving stage), i.e having only irreducible divisors of small degree. It then solves a sparse linear system (the linear algebra stage), whose solutions, called virtual logarithms, allow to compute the discrete algorithm of any element during a final stage (individual logarithm stage).

The choice of the defining polynomials f and g for the two function fields can be seen as a preliminary stage of the algorithm. It takes a small amount of time but it can greatly influence the sieving stage by slightly changing the probabilities of smoothness. In order to solve the discrete logarithm in $\mathbb{F}_{q^n}$, the main required property of $f, g \in \mathbb{F}_q[t][x]$ is that their resultant $\mathrm{Res}_x(f, g)$ has an irreducible factor $\varphi(t)$ of degree n.

Various methods have been proposed to build such polynomials, but the best results in practice correspond to the method of Joux and Lercier [JL02]. Its particularity is that one of the two polynomials, say g, is linear. Moreover, for any polynomial f in $\mathbb{F}_q[t][x]$ and any input $\mathbb{F}_{q^n}$, one can associate a linear polynomial g satisfying the requirements of the FFS. This allows us to precompute some polynomials f which have good properties for the sieving stage.

For this, we define and measure the size property and the so-called root and cancellation properties. In short, the cancellation property is measured by a function σ related to the size of the coefficients of f as well as to the cardinality of the set of pairs (a, b) to be sieved. The root property is measured by α, which is inspired by the function used for the factorization algorithms. It is related to the number of roots of f when reduced modulo small irreducible polynomials of $\mathbb{F}_q[t]$. Finally, α_∞ measures the cancellation property, by evaluating the average loss of degree due to the cancellation of the terms of $f(r)$ when r is a random rational fraction of $\mathbb{F}_q[t]$. We present a sieving procedure which computes α, the most costly to evaluate of the three functions.

We next combine the different criteria in order to compare arbitrary polynomials. In particular we show experimental evidence that ϵ, defined as $\sigma + \alpha + \alpha_\infty$, predicts the efficiency of any polynomial.

Our methods were used in two records of discrete logarithm in $\mathbb{F}_{2^n}$ with prime values of n. In the last couple of weeks, new algorithms were proposed, which are particularly well adapted for the fields $\mathbb{F}_{2^n}$ for composite values of n. In the case when n is prime, the crossing point is to be computed, this latter being determined by the practical improvement of the FFS. See [Bar13] for a broader presentation of our work.

References

[Adl94] L. Adleman. The function field sieve. In *Algorithmic number theory-ANTS I*, volume 877 of *Lecture Notes in Computer Science*, pages 108–121. Springer, 1994.

[Bar13] R. Barbulescu. Selecting polynomials for the Function Field Sieve. 2013. arXiv preprint arXiv:1303.1998.

[JL02] A. Joux and R. Lercier. The function field sieve is quite special. In *Algorithmic Number Theory-ANTS V*, volume 2369 of *Lecture Notes in Computer Science*, pages 431–445. Springer, 2002.