ON POLYNOMIALS IN $\mathbb{F}_q[X]$ WITH ABELIAN LIFTS AND THEIR FACTORIZATION

PREDA MIHĂILESCU

ABSTRACT. We give a new frame for factorization of polynomials $F(X) \in \mathbb{F}_q[X]$ with $\mathbb{F}_q$ a finite field of characteristic p, which have equal degree factorization. Under some additional condition, the dominant term in the complexity of the factorization then depends on the number of factors and not on the degree of $F(X)$.

A general class of polynomials satisfying our conditions are the polynomials *with abelian lift* - i.e. polynomials which arise as reduction of polynomials defining relative abelian extensions of number fields, modulo some prime ideal of the base field. We give details for the special cases of cyclotomic polynomials and cyclic factors of division polynomials. Even in the case of cyclotomic polynomials, which is one of the best understood problems in computational algebra, the gains are noteworthy.

1. INTRODUCTION

Let $\Phi_r = \frac{x^r-1}{x-1}$, the $r-$th cyclotomic polynomial and $\mathbb{F}_q$ a finite field of characteristic p; if $f = \text{ord}_r(q)$, the polynomial $\Phi_r(X)$ splits over the field $\mathbb{F}_q$ in $d = \frac{r-1}{f}$ irreducible factors of degree f. In order to compute these factors one uses improved [Sh] variants of the Berlekamp algorithm, requiring

$$O\left(r\log(r)^2\log\log(r) + r\log(r)\log\log(r)\times\log(q)\right) \tag{1}$$

operations. The second term dominates when $q > r$. The value of d is in general quite small compared to q. Since a random element $x \in \mathbb{F}_r^\times$ has the order f with probability $\varphi(f)/(q-1)$. the expected values of f and d are

$$\begin{aligned} E(d) &= E\left(\sum_{f|(r-1)} \frac{r-1}{f}\cdot\frac{\varphi(f)}{r-1}\right) = E\left(\sum_{f|(r-1)}\frac{\varphi(f)}{f}\right) = E\left(\prod_{\substack{p|r-1\\ p \text{ prime}}}\left(2-\frac{1}{p}\right)\right) \\ &\approx E\left(C^{\omega(r-1)}\right) = O(\log(r-1)), \quad \text{for some constant } 3/2 < C < 2. \end{aligned}$$

The function $\varphi(f)/f$ is multiplicative and this explains the last equality in the first line. Since $3/2 \le 2-1/p < 2$ for all primes $p|(r-1)$, the final estimate follows, using the expected value of the number of factors $E(\omega(r-1)) = \log\log(n)$. The very scarce totally splitting polynomials have the same contribution to the above expected value as the frequent inert ones. It is therefore more enlightening to consider the median

$$\mu(d) = \min_{d|(r-1)}\left\{\sum_{e|(r-1), e\le d}\varphi\left(\frac{r-1}{e}\right) > \frac{r-1}{2}\right\} = O\left(\log\log(r-1)\right).$$

Note that the same estimates hold in general for every cyclic polynomial of degree $r-1$. It is therefore a tempting question, whether factoring of $\Phi_r(X)$ can be performed *in dependence of the number of factors, rather than of their degree* . The answer is essentially yes and will

Date: Version 1.0 October 6, 2006.

made precise in the fourth section. The algorithm described there was first presented in [Mi] and similar ideas were developed for the case $d = 2$ be Stein [St1], while subsequent papers of the same author were specifically interested in *deterministic algorithms*. The algorithms we present here are only conditionally deterministic, depending upon the truth of the extended Riemann hypotheses.

We write the complexity of algorithms in dependence of the cost of an $\mathbb{F}_q$ - multiplication, which is a unit denoted by $\mathsf{M}(q)$. When there is more than one variable which may vary in a run - time estimate, the notation $O^\sim$ refers to all of these variables. For instance we may write $O\left(\log(n) \cdot (\log\log(n))^2 + r^2 \log(r)\right) = O^\sim\left(\log(n) + r^2\right)$, when $n, r \to \infty$.

The running time of our algorithm for factoring cyclotomic polynomials is *essentially* $O^\sim\left((r + d \cdot \log(q))\, \mathsf{M}(q)\right)$, where the word essentially refers to the fact that the dependence on d can be improved to one on the prime power factors of d. Observe that the factor $\log(q)$ is multiplied here by $O^\sim(d)$ compared to $O^\sim(r)$ in (1).

The basic idea which was successful in improving the performance for factoring cyclotomic polynomials is more general, while cyclotomy offers some additional useful features, like the simple explicite formulae for Gauss and Jacobi sums. Led by this idea, we develop in Lemma 1 a general frame for factoring polynomials with equal degree factorization over finite fields. It turns out that this frame is closely related to a special case treated by Kaltofen and Shoup in [KaSh], [Sh1]. This general frame, in its common points with [Sh], uses *splitting elements* - elements of the Berlekamp algebra in the terms of [GG] - in a more efficient way than in the Berlekamp null space approach. In [Sh], the splitting elements are obtained as traces of the Frobenius - thus the algorithm requires the computation of the Frobenius map modulo the polynomial to factor.

However, the improvements obtained for factoring cyclotomic polynomials are related also to the possibility of avoiding such Frobenius evaluations and requiring exponentiation only in smaller extensions. This improvements can be obtained for a larger class of polynomials *with abelian lift*. It is on this class that our algorithm focuses and we give an additional application for factoring eigenfactors of division polynomials of elliptic curves over finite fields.

We now give the formal definition of *polynomials with abelian lifts*, which are instances of polynomials to which our method applies.

Definition 1. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $F(X) \in \mathbb{F}_q[X]$. Let $\mathbb{L}/\mathbb{K}$ be an abelian extension of number fields, which is not ramified above p, let $\mathbf{B} \supset \mathbf{A}$ be the respective orders of the integers and suppose that there is a monic polynomial $\Phi(X) \in \mathbf{A}[X]$ such that $\mathbb{L} = \mathbb{K}[X]/(\Phi(X))$ as simple algebraic extension; we write $\omega = X \bmod \Phi(X) \in \mathbb{L}$ and assume that the discriminant $(\delta(\omega), p) = 1$. Let $\mathfrak{p} \subset \mathbf{A}$ be a prime above (p).*

We say that $F(X)$ has an abelian lift (which is $\Phi(X)$) if in this situation, the following conditions are fulfilled:

A. $\mathbf{A}/\mathfrak{p} \subseteq \mathbb{F}_q$.
B. $\Phi(X) \bmod \mathfrak{p} = F(X)$.

We give a brief overview of the connection between prime ideal factorization in $\mathbb{L}/\mathbb{K}$ and polynomial factorization over $\mathbb{F}_q$, see also [Ri], [La].

Fact 1. *With the notations introduced in the definition above, let $T \subset Gal\,(\mathbb{L}/\mathbb{K})$ be the decomposition group of $\mathfrak{p}$, generated by the Artin symbol $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$ and let $\mathbb{K}_1 = \mathbb{L}^T$ be the decomposition field, with order of integers $\mathbf{C}$. Let $d = [K_1 : \mathbb{K}]$ and $f = [\mathbb{L} : \mathbb{K}]$, the residual field degree, $n = f \cdot d = [\mathbb{L} : \mathbb{K}]$. If $\mathfrak{P} \subset \mathbf{B}$ is a prime above $\mathfrak{p}$ and $\mathfrak{P}_\circ = \mathfrak{P} \cap \mathbf{C}$, then*

1. *$\mathbf{B}/\mathfrak{P} = \mathbb{F}_{q^f}$ and $\mathbf{C}/\mathfrak{P}_\circ = \mathbb{F}_q$.*
2. *There is an irreducible polynomial $\rho(X) \in \mathbf{C}(X)$ with $\mathbb{L} = \mathbb{K}_1[X]/(\rho(X))$ and such that $f(X) = (\rho(X) \bmod \mathfrak{P}_0) \in \mathbb{F}_q[X]$ is an irreducible factor of $F(X)$.*

3. *If* $S = \ Gal\ (\mathbb{L}/\mathbb{K})/T = \ Gal\ (\mathbb{K}_1/\mathbb{K})$, *then all the irreducible factors of* $F(X)$ *arise as* $\tau(\rho(X)) \bmod \mathfrak{P}_0$, *for* $\tau \in S$.
4. *Let* $\eta \in \mathbf{C}$ *generate* $\mathbb{K}_1$ *as* $\mathbb{K}$ *- extension:* $\mathbb{K}_1 = \mathbb{K}[\eta]$. *Let* $\mu(X) \in \mathbf{A}[X]$ *be the minimal polynomial of* η *and* $m(X) = (\mu(X) \bmod \mathfrak{p}) \in \mathbb{F}_q[X]$, *a polynomial of degree. Let* $\tau \in \ Gal\ (\mathbb{L}/\mathbb{K})$ *and* $\gamma_\tau(X) \in \mathbf{A}[X]$ *be a polynomial such that*

$$\tau(\omega) = \gamma_\tau(\omega) \in \mathbb{L},$$

let $\Gamma(X) = \sum_{\tau \in T} \gamma_\tau(X) \in \mathbf{A}(X)$, *and let the reduction be* $G(X) = \Gamma(X) \bmod \mathfrak{p} \in \mathbb{F}_q[X]$ [1].

The GCD $f(X) = (G(X) - \widehat{\eta}, F(X))$ *is an irreducible factor of* $F(X)$ *and it can be obtained by computing* $\widehat{\eta} = \eta \bmod \mathfrak{P}_0$ *as a zero of* $\mu(X)$.

Proof. See [La], **Ch. I, §8** and [Ri], **Ch. 14** for the general theory of splitting of primes in Galois extensions. We take here, most specifically in 4., advantage of the abelian structure and of the presentation as a simple algebraic extension $\mathbb{L} = \mathbb{K}[\omega]$ of the field considered. The existence of the polynomial γ_τ and the properties of $G(X) = \Gamma(X) \bmod \mathfrak{p}$ follow from these conditions. □

The paper is structured as follows: in the next section we present some auxiliary algorithms, in the third section we present the main algorithm and prove that it applies to polynomials with abelian lifts. In the fourth and fifth sections we develop detailed algorithms for the important cases when $F(X)$ is a cyclotomic or a division polynomial, respectively.

2. Auxiliary algorithms

Let $\mathbb{F}_q$ be a finite field of characteristic p, $F(X) \in \mathbb{F}_q[X]$ with degree $n = f \cdot d$ and equal degree factorization:

$$F(X) = \prod_{j=1}^{d} f_j(X) \quad \text{with irreducible} \quad f_j(X) \in \mathbb{F}_q[X], \quad \deg(f_j) = f, \tag{2}$$

and consider the $\mathbb{F}_q$ - algebra $\mathfrak{R} = \mathbb{F}_q[X]/(F(X))$. We also write

$$\theta = X \bmod F(X) \in \mathfrak{R}, \quad \mathbb{K}_j = \mathbb{F}_q[X]/(f_j(X)), \quad \theta_j = X \bmod f_j(X) \in \mathbb{K}_j.$$

The following problems are solved by Shoup in [Sh] by using linear projectors and linearly defined recursions.

- P1. Find the minimal polynomial of an element $\eta \in \mathfrak{R}$, if $\mathfrak{R}$ is a field, or a generating polynomial for the sequence of the powers of η otherwise.
- P2. Given two elements $\eta, \beta \in \mathfrak{R}$, find a polynomial $\gamma(X) \in \mathbb{F}_q[X]$ for which $\beta = \gamma(\eta)$, if such one exists.

We use the definition of linearly generated sequences and their generating polynomial given by Soup in [Sh], §3. Since the setting is here slightly more general than Shoup's[2], we give an outline of the algorithms and their running times in our specific context. We start by proving

Lemma 1. *Let* $\mathbb{F}_q, F(X), f_j(X), \mathfrak{R}$ *be as above and*

$$\eta = (\eta_1, \eta_2, \ldots, \eta_d) \in \mathfrak{R} \quad \textit{with} \quad \eta_j = \eta \bmod f_j(X)$$

an element of the algebra $\mathfrak{R}$ *together with its representation in the Chinese Remainder Theorem and*

$$E = \{1, \eta, \eta^2, \ldots, \eta^m, \ldots\}$$

[1] Note that $\eta = \Gamma(\omega)$.

[2] Shoup mentions that his ideas easily generalize to the case when the polynomial $F(X)$ is not irreducible, i.e. $\mathfrak{R}$ is not a field. However, he only treats the latter case in the paper.

the sequence of powers of η.

Let $g_j(X) \in \mathbb{F}_q[X]$ be the minimal polynomial of $\eta_j \in \mathbb{F}_q[X]/(f_j(X))$ over $\mathbb{F}_q$. The power sequence is linearly generated and has the minimal polynomial

$$g(X) = \prod_{j=1}^{d} g_j(X).$$

In particular, if $\eta_j \in \mathbb{F}_q$ then $g(X)$ has degree d and splits completely over $\mathbb{F}_q$.

Proof. The algebra $\mathfrak{R}/\mathbb{F}_q$ is a vector space and the power sequence generates a subspace. One verifies in particular that it is linearly generated. Let $g(X)$ be the minimal polynomial; since the product $g^{\sim}(X) = \prod_j g_j(X)$ generates the power sequence modulo $f_j(X)$ for each j, it generates also the power sequence in $\mathfrak{R}$ and is a multiple of $g(X)$. The converse follows from the minimality of $g_j(X)$: if $g^{\sim}(X) \neq g(X)$, there is a j such that $g(X) \bmod f_j(X) \neq g^{\sim}(X) = g_j(X)$; since both $g_j(X)$ and $g(X) \bmod f_j(X)$ generate the $j-$th projection of the power sequence, we obtain a contradiction of the minimality of $g_j(X)$. The case when $\eta_j \in \mathbb{F}_q$ is evident: the minimal polynomials $g_j(X)$ have degree one, and thus $\deg(g(X)) = d$. □

Following [Sh], one defines the projector $P : \mathfrak{R} \to \mathbb{F}_q$ by $P(\omega^i) = \delta_{0,i}$ and the minimal generating polynomial $g(X)$ in the Lemma can be found by the following steps:

1. Compute $2m - 1$ successive elements of the linear generated sequence $P(\eta^i) \in \mathbb{F}_q$, where $m = \deg(g(X)) = \sum_j \deg(g_j(X))$.
2. Compute $g(X)$ either by a GCD computation - [Sh], Fact 3. - or by solving a linear Toeplitz system - as in Theorem 5.

In both cases, the operation count over $\mathbb{F}_q$ is $O^{\sim}\left(m^{(\omega-1)/2}n\right)$ with ω the exponent of matrix multiplication - so, for not too large values of m, the cost is indeed $O^{\sim}(m \cdot n)$. This solves problem P1. As for P2., assume that $\eta \in \mathfrak{R}$ as above and $\beta \in \mathbb{F}_q[\eta] \subset \mathfrak{R}$ are given and one seeks a polynomial with $\beta = h(\eta)$.

One may also consider the more restricted question of interest, when one knows explicitely that

$$\beta = \tau(\eta) = (\eta_2, \eta_3, \ldots, \eta_d, \eta_1),$$

yet without knowing the factors and thus the actual values of η_j. In general, one proceeds as follows:

3. Compute the $2m - 1$ successive elements $P(\eta^i) : i = 0, 1, \ldots, 2m - 2$ and find the generating polynomial $g(X)$ of the sequence.
4. Compute the m projections $P(\beta), P(\beta\eta), \ldots, P(\beta\eta^{m-1})$.
5. Compute $h(X)$ by solving a linear Toeplitz system - as in [Sh], Theorem 5.

Again, the number of $\mathbb{F}_q$ - operations is $O^{\sim}(nm)$. This solves the general case of our problem P2 and allows us to formulate an algorithm for factoring polynomials over finite fields, by using relations between the roots.

3. Factoring of a special class of polynomials over finite fields

We use the same notations as in the previous section and consider the problem of factoring the polynomial $F(X)$ under the additional assumption that there is a polynomial $\phi(X) \in \mathbb{F}_q[X]$ such that

$$\eta_j = \phi(\theta_j) \in \mathbb{F}_q \cap \mathbb{K}_j, \quad j = 1, 2, \ldots, d, \quad \text{and} \tag{3}$$

$$\exists\, i_0 : \ \eta_{i_0} \neq \eta_j \quad \text{for } j \neq i_0. \tag{4}$$

If η satisfies the conditions (3) and (4), we say that η is a **splitting** element for $F(X)$.

Algorithm 1: Factoring Polynomials over Finite Fields, which satisfy (3)

Input: A finite field $\mathbb{F}_q$, a polynomial $F(X) \in \mathbb{F}_q[X]$ with equal degree factorization (2) and a polynomial $\phi(X) \in \mathbb{F}_q[X]$ satisfying the assumption (3) with respect to the irreducible factors of $F(X)$.
Output: An irreducible factor $f(X)|F(X)$.

A. Compute $G(T) \in \mathbb{F}_q[T]$, a generating polynomial for the linearly generated sequence $1,\ \phi(\omega),\ \phi(\omega)^2, \ldots \in \mathbb{K}$.
B. Let $G_1(T)$ be the square free part of $G(T)$, if necessary, and find $\eta \in \mathbb{F}_q$, a zero of $G_1(T)$.
C. Let $f(X) = (G(X) - \eta, F(X))$ and output $f(X)$.

Given that the degree of $G(T)$ is known a priori to be d, the first step requires [Sh] $\mathcal{O}^{\sim}(n \cdot d\mathsf{M}(q))$ while the second is the only one which needs an exponentiation and thus takes $\mathcal{O}^{\sim}(d\log(q)\mathsf{M}(q))$ and finally, the GCD computation in step 3. takes $\mathcal{O}^{\sim}(n \cdot \mathsf{M}(q))$. The complexity adds thus up to:

$$\mathcal{O}^{\sim}\left(d \cdot (n + \log(q)) \cdot \mathsf{M}(q)\right)$$

operations.

3.1. **Applications.** Let $F(X)$ be a polynomial with abelian lift $\Phi(X)$. Using the notation in the previous sections, there is a map:

$$\iota : \mathbf{B} \to \mathbf{B}/\left(\mathfrak{p} \cdot \mathbf{B}\right) \cong \mathfrak{R}.$$

With the polynomial $G(X) = \Gamma(X) \bmod \mathfrak{p}$ one verifies that

$$\eta = G(\theta) \in \mathfrak{R}$$

is a splitting element for $F(X)$ in the sense of Algorithm 1, which can be applied in this case. Methods for fast evaluation of traces of the Frobenius in algebras over finite fields are known [GS], [Sh1]. Using the abelian lift, the same idea may be used for speeding the computation of traces even without evaluation of the Frobenius - which we consider in our context as a time - consuming operation, to perform is extensions as small as possible. Rather than the Frobenius, one shall use the polynomials $g_a(X) = (\gamma_a(X) \bmod \mathfrak{p}) \in \mathbb{F}_q[X]$.

It interesting to observe that there is a degree of freedom in the choice of the extension $\mathbb{F}_q$ which can be useful for instance when the precise factoring type of $F(X)$ is not known.

The notion of splitting element arises from a quite different context; it is a fact that the set of splitting elements build and $\mathbb{F}_q$ - algebra, which is the *Berlekamp* - algebra [GG]. In the algorithm with the same name, one considers the linear map $\sigma : \mathfrak{R} \to \mathfrak{R}$ given by $a \mapsto a^q - a$; its kernel is the Berlekamp algebra and is used for factoring the polynomial $F(X)$.

In fact one can use the Algorithm 1, after having found at least one element in $\mathbb{B} = \mathbf{Ker}\ (\sigma)$. This fact, also shown in [KaSh], [Sh1], reduces the computations in the probabilistic step of that algorithm, and also the amount of randomness required: basically one only needs the random bits for finding a $d-$th root of unity. The important additional gain from the use of abelian lifts consists in the possibility of computing splitting elements without evaluation of the Frobenius modulo the polynomial to split.

4. Factoring cyclotomic polynomials

Let $\mathbb{F}_q$ be a finite field of characteristic p and $m > 2$ an integer, $(p, m) = 1$, $\Phi_m(X)$ the $m-$th cyclotomic polynomial and $F_m(X) = \Phi_m(X) \bmod p$. Since $\mathbb{Q}(\zeta_m) = \mathbb{Q}[X]/(\Phi_m(X))$

is an abelian field, $F_m(X)$ has an abelian lift and we may apply Algorithm 1. In fact the polynomial $G(X)$ in this case the simple shape

$$G(X) = \sum_{i=0}^{n-1} X^{q^i} \bmod F_m(X),$$

and the corresponding splitting element is

$$\eta = \sum_{i=0}^{n-1} \zeta_m^{q^i} \bmod p\mathbb{Z}[\zeta_m].$$

Indeed, in this case we have plainly $\mathfrak{R} = \mathbb{Z}[\zeta_m]/(p \cdot \mathbb{Z}[\zeta_m])$.

One can do even better in this case by using Gauss and Jacobi sums, which allow simpler computations of η.

4.1. **Gauss Periods and Jacobi Sums.** The approach to factoring cyclotomic polynomials presented in this section has been solved completely over finite fields and certain galois rings in [Mi]. Stein presented independently some related ideas and particular solutions, [St1], [St2].

We consider further a finite field $\mathbb{F}_q$ but restrict our attention to the $r-$th cyclotomic polynomial, with r some prime. We let $f = \mathrm{ord}_r(q)$ and $n = r - 1 = f \cdot d$. Furthermore, $F(X) = (\Phi_r(X) \bmod p) \in \mathbb{F}_p[X] \subset \mathbb{F}_q[X]$, $\zeta = \zeta_r$ is a complex $r-$th root of unity and $\mathbb{K} = \mathbb{Q}(\zeta)$ the $r-$th cyclotomic extension of $\mathbb{Q}$. The automorphisms of $\mathrm{Gal}\,(\mathbb{K}/\mathbb{Q})$ are denoted by $\sigma_a : \zeta \mapsto \zeta^a$. If $H =< q \bmod r > \subset \mathrm{Gal}\,(\mathbb{K}/\mathbb{Q})$, let the fixed field be $\mathbb{L} = \mathbb{K}^H$, a field of degree d.

We let $g \in (\mathbb{Z}/r \cdot \mathbb{Z})^*$ be a generator; then

$$\begin{aligned} \Phi_r(X) &= \frac{X^r - 1}{X - 1} = \prod_{i=1}^{r-1} \left(X - \zeta^i\right) = \prod_{j=1}^{d} \Psi_j(X), \quad \text{where} \\ \Psi_j(X) &= \prod_{i=1}^{f} \left(X - \sigma_{g^j}(\zeta^{q^i})\right) \in \mathcal{O}(\mathbb{L})[X]. \end{aligned} \tag{5}$$

The factors of $\Phi_r(X)$ over $\mathbb{F}_q$ are $\widehat{\Psi}_j(X) = \Psi_j(X) \bmod \mathfrak{P}$, with $\mathfrak{P} \subset \mathcal{O}(\mathbb{L})$, a prime above p; by construction, the prime will have the right residue field degree, so that $\mathcal{O}(\mathbb{L})/\mathfrak{P} = F_q$.

Let $\alpha_{i,j} = \sigma_{g^j}(\zeta^{p^i})$ be the roots of $\Psi_j(X)$. The corresponding power sums are

$$S_k(j) = \sum_{i=1}^{f} \alpha_{i,j}^k = \sigma_{kg^j}(\eta) \quad \text{with} \quad \eta = \mathbf{Tr}_{\mathbb{K}/\mathbb{L}}(\zeta) = \sum_{i=1}^{f} \zeta^{q^i}. \tag{6}$$

The central remark for this algorithm are the following two facts:

A. The polynomial $\Psi_j(X)$ is retrieved from its power sums and this can be done with fast algorithms, in $O(f \cdot \mathsf{M}(q))$ operations [BMSS].
B. There are exactly d distinct conjugates of η in $\mathbb{L}$.

It follows from B. that the knowledge of the d conjugates of η yields the factors of Φ_r in time $O(f \cdot \mathsf{M}(q))$. The conjugates of η are determined by their Lagrange resolvents, the Gauss sums.

Let χ be a primitive character of conductor r and order d, with $\chi(q) = 0$ and $\tau(\chi) = \sum_{x \in (\mathbb{Z}/q \cdot \mathbb{Z})^*} \chi(x)\zeta^x$ the Gauss sum. If ρ is a $d-$th root of unity which generates the image $\chi((\mathbb{Z}/q \cdot \mathbb{Z})^*)$ and such that $\chi(g) = \rho$, the Gauss sum is related to η by:

$$\tau(\chi) = \sum_{j=1}^{d} \rho^j \sigma_{g^j}(\eta). \tag{7}$$

We also need the Jacobi sums, which are defined, for $\chi^a, \chi^{a+1} \neq 1$ by

$$j(\chi, \chi^a) = \frac{\tau(\chi)\tau(\chi^a)}{\tau(\chi^{a+1})} = \sum_{x=1}^{q} \chi(x)\chi(1-x) \in \mathbb{Z}[\rho], \tag{8}$$

and yield the *multiple Jacobi sums*

$$J_a(\chi) = \frac{\tau^a(\chi)}{\tau(\chi^a)} = \tau(\chi)^{a-\nu_a} = \prod_{i=1}^{a-1} j(\chi, \chi^i), \tag{9}$$

where $\nu_a : \rho \mapsto \rho^a$. We have in particular

$$\tau(\chi)^d = \chi(-1) \cdot q \cdot J_{d-1}(\chi) \in \mathbb{Z}[\rho]. \tag{10}$$

Since Gauss sums are Lagrange resolvents, the conjugates of η can be computed from the values of $\tau(\chi^a)$ by formulae of the type:

$$d \cdot \sigma_b(\eta) = -1 + \sum_{a=1}^{d-1} \rho^{-ab} \cdot \tau(\chi^a). \tag{11}$$

This already suggests an algorithm for computing the traces $\sigma(\eta)$:

G1. Compute $P = \tau(\chi)^d \in \mathbb{Z}[\rho]$ and retrieve $T = \tau(\chi) = P^{1/d}$ by a root computation.

G2. Determine $\tau(\chi^a) = \frac{\tau(\chi)\tau(\chi^{a-1})}{j(\chi,\chi^a)} \in \mathbb{Z}[\rho, T]$ by induction on a. Here divisions may be replaced by multiplications using the identities

$$\begin{aligned} \tau(\chi) \cdot \tau(\chi^{-1}) &= \chi(-1) \cdot r, \quad \text{and thus} \\ j(\chi, \chi^a) \cdot j(\chi^{-1}, \chi^{-a}) &= r, \\ \frac{r}{j(\chi, \chi^a)} &= j(\chi^{-1}, \chi^{-a}). \end{aligned}$$

G3. Determine $\eta \in \mathbb{Z}[T]$ by means of (11).

All the steps may be thought of in $\mathbb{K}$ but reduced to some extension of $\mathbb{F}_q$ containing the appropriate roots of unity. This essentially bypasses the step A of Algorithm 1. and leads directly to the analog of the root computation in step B. Since the computations in G1. may be transported with an homomorphism to some ring or field $\mathbf{R} \supset \mathbb{F}_q$ which contains a $d-$th root of unity, and since such a ring may have smaller degree over $\mathbb{F}_q$ than the algebra $\mathbb{F}_q[X]/(g(X))$ in step B. of algorithm 1., this reveals a further advantage of direct computation with Jacobi sums.

The above procedure may be reduced to the case of Gauss sums of prime power order. Indeed, assume that $d = \prod_i s_i$ with s_i being prime powers and $\mathbf{R} \supset \mathbb{F}_q$ is a ring containing primitive s_i-th roots of unity, i.e. $\rho_i \in \mathbf{R}$ such that $\Phi_{s_i}(\rho_i) = 0$. Furthermore, we assume that for each i, we computed $P_i = \tau(\chi_i)^{s_i} \in \mathbf{R}$ for characters of conductor r and order s_i and an s_i-th root of P_i is $T_i \in \mathbf{R}$. This requires an exponentiation in an extension of degree $n_i = \mathrm{ord}_{s_i}(q)$ for each i. From these values, all Gauss sums of conductor r and order dividing d can be computed. Indeed, we have shown how this is done for each s_i. Suppose that all Gauss sums of orders $m, m' | d$ with $(m, m') = 1$ are computed. If χ is a character of order $M = m \cdot m'$ it can be split in a product of characters of orders m and m', say $\chi = \chi' \cdot \chi''$. Then

$$\tau(\chi) = \frac{\tau(\chi') \cdot \tau(\chi'')}{j(\chi' \cdot \chi'')},$$

and by induction, the Gauss sums on the right hand side have been computed. Note that the coefficients of Jacobi sums of conductor r as algebraic integers $j(\chi, \chi') \in \mathbb{Z}[\rho]$ are bounded by

$O^\sim(\sqrt{r})$. This is useful especially for large values of q. There are methods for fast evaluation of Jacobi sums using lattice reduction, [BK], [Wa].

Algorithm 2: Factoring cyclotomic polynomials over finite fields

Input: A finite field $\mathbb{F}_q$ of characteristic p and an odd prime r with $f = \text{ord}_r(q), n = r-1 = d \cdot f$ and $d = \prod_{i=1}^{c} s_i$, with s_i being prime powers; a Galois extension ring $\mathbf{R} \supset \mathbb{F}_q$ which contains roots of unity $\rho_i \in \mathbf{R}$ with $\Phi_{s_i}(\rho_i) = 0$. Let $\mathbf{R}_i = \mathbb{F}_q[\rho_i]$ have degree $n_i = [\mathbf{R}_i : \mathbb{F}_q]$.
Output: $\widehat{\Psi}_j(X), j = 1, 2, \ldots, d$, the factorization of $\Phi_q(X)$ over $\mathbb{F}_p$.

1. For $i = 1, 2, \ldots, c$ compute the Gauss sum powers $t_i = \tau(\chi_i)^{s_i} \in \mathbf{R}_i$, with χ_i characters of order s_i
2. Compute $T_i \in \mathbf{R}_i$ with $T_i^{s_i} = t_i$.
3. Compute recursively the images of $\tau(\chi)\mathbf{R}$, for all the characters of conductor r and order d.
4. Compute using additions in $\mathbf{R}$ the d traces
$$\widehat{\eta}_j = \sigma_{g^j}\left(\mathbf{Tr}_{\mathbb{K}/\mathbb{L}}(\zeta) \bmod \mathfrak{P}\right), \quad \text{for} \quad j = 1, 2, \ldots, d.$$
5. Retrieve the d factors $\widehat{\Psi}_j(X) | \Phi_q(X)$ using algorithms in [BMSS] or [Bo] for inversion of the Newton formulae. Alternately one can use the GCD computation in Algorithm 1.

Let $S = \sum_i s_i^2$ and $\mathsf{M}(q)$ the number of operations for a $\mathbb{F}_q$ multiplication. The first step requires $O(s_i)$ multiplications in extensions of degree $O(s_i)$ for a total of $O^\sim(S_2 \cdot \mathsf{M}(q))$ operations. The root taking in step 2 requires exponentiations in the same extensions and with exponents in the order of q^{s_i}, which leads to $O^\sim(S_2 \log(q)\mathsf{M}(q))$ operations. Step 3 takes $O^\sim(d\mathsf{M}(q))$ operations, the 4. step consisting of additions may be neglected and the 5. step requires $O^\sim(f\mathsf{M}(q))$ operations per factor found, using either of the two methods proposed; if all factors are required, this amounts to $O^\sim(r \cdot \mathsf{M}(q))$. The total run time of the algorithm is herewith
$$O^\sim\left((S_2 \log(q) + r)\,\mathsf{M}(q)\right)$$
operations. Note that the reduction to prime power factors of d is a variant which also applies to the first algorithm. However in that case traces may be more cumbersome to evaluate and the trade off has to be decided on a case by case base.

5. Eigenfactors of Division Polynomials

Let $\mathbb{F}_q$ and p be as before and ℓ be an odd prime. Consider the elliptic curve:
$$\mathcal{E}_q : Y^2 = f(X) \quad \text{with} \quad f(X) = X^3 + AX + B, \quad A, B \in \mathbb{F}_q,$$
defined over $\mathbb{F}_q$. We assume that $\mathcal{E}$ is not supersingular and let $\Delta = t^2 - 4q$ be the (unknown) discriminant of the Frobenius of the curve over the algebraic closure of $\overline{\mathbb{F}_q}$. We assume that $\left(\frac{\Delta}{\ell}\right) = 1$ [3] and that an eigenpolynomial corresponding to some eigenpoint P of the representation of Φ_q in the ℓ - torsion was found. Let this polynomial be
$$F(X) = F_P(X) = \prod_{a=1}^{(\ell-1)/2} (X - ([a]P)_x) \in \mathbb{F}_p[X]. \tag{12}$$

The reader may consult [BMSS] for a comprehensive overview of currently known methods for computing such eigenpolynomials.

[3] so, using a denomination which is common in the context of point counting on curves over finite fields, ℓ *is an Elkies prime for* q.

For counting the number of points $|\mathcal{E}(A,B)|$, one needs to solve the discrete logarithm problem:

$$[\lambda]P = \Phi_q(P) = (P_x^q, P_y^q); \tag{13}$$

in the SEA algorithm this is done via an exponentiation $\bmod F(X)$ which yields $\Phi_q(P)$. The factorization of $F(X)$ can thus be a useful preprocessing step of this algorithm, provided it can be performed in time which is affordable compared to the state of the art approach to this discrete logarithm step.

We set $\mathfrak{R} = \mathbb{F}_q[X]/(F(X))$ and $\mathfrak{R}' = \mathbf{R}[Y]/\left(Y^2 - (X^3 + AX + B)\right)$ and show that the polynomial $F(X)$ has an abelian lift. Indeed, since the curve $\mathcal{E}(A,B)$ is not singular and not supersingular, it has a Deuring lift. There is a field $\mathbb{K} = \mathbb{Q}[A', B']$, a prime ideal $\mathfrak{p} \subset \mathcal{O}(\mathbb{K})$ with $\mathcal{O}(\mathbb{K})/\mathfrak{p} \subseteq \mathbb{F}_q$ and $A' \bmod \mathfrak{p} = A$, $B' \bmod \mathfrak{p} = B$ and such that the elliptic curve $\mathcal{E}'(A,B')$ has CM and $\mathcal{E}'$ good reduction at $\mathfrak{p}$. We let $\mathbb{K}_\ell$ be the ℓ - torsion extension, i.e. the smallest field which contains all the coordinates of ℓ - torsion points of $\mathcal{E}'$, let $\Psi'_\ell[A,B'](X)$ be the $\ell-$th division polynomial of $\mathcal{E}'$, an irreducible polynomial over $\mathbb{K}$ (see e.g. [CCR]); by definition of the reduction, we have $\Psi_\ell[A,B](X) = \Psi'_\ell[A,B'] \bmod \mathfrak{p}$. Thus, the algebraic extension $\mathbb{K}_1 = \mathbb{K}[X]/(\Psi'_\ell(X))$ maps to $\mathbb{F}_q[X]/(\Psi_\ell)$. We choose an embedding of $\mathbb{K}_1 \subset \mathbb{K}_\ell$ and so there is a point $\mathbf{P} \in \mathcal{E}'[\ell]$ such that $\mathbb{K}_1 = \mathbb{K}[\theta]$ with $\theta = \mathbf{P}_x$.

The division polynomials $\Psi'_a(X), a \in \mathbb{N}_{>1}$ are pairwise coprime for coprime values of a and the x coordinates of the multiples of *any* point $([a]Q)_x$, $Q \in \mathcal{E}'/\mathbb{C}$ are expressed by a rational function $R_a(X)$ depending on the curve $\mathcal{E}'$ and with denominator $\Psi_a^2(X)$[4]. This holds in particular for ℓ - torsion points. It follows from the coprimality of the division polynomials for $a < \ell$ that $\Psi_a(Q_x) \in \mathbb{K}_\ell^\times$ for all $Q \in \mathcal{E}'[\ell]$ and there is a polynomial $\gamma_a(X) \in \mathcal{O}(\mathbb{K})[X]$ such that

$$\gamma_a(Q_x) = ([a]Q)_x.$$

For $Q = \mathbf{P} \in \mathbb{K}_1$ we have $\gamma_a(\mathbf{P}_x) = ([a]\mathbf{P})_x \in \mathbb{K}_1$ and it follows that the x - coordinates of all the multiples of $\mathbf{P}$ are in $\mathbb{K}_1$. There is thus a group of automorphisms of $\mathbb{K}_1/\mathbb{K}$ with $\rho_a : \mathbf{P}_x \to ([a]\mathbf{P})_x$, $1 \le a \le \frac{\ell-1}{2}$; let H be this group and $\mathbb{K}_2 = \mathbb{K}_1^H$ be its fixed field.

Then the extension $\mathbb{K}_1/\mathbb{K}_2$ is abelian and if $\mathbf{T} = \mathbf{Tr}_{\mathbb{K}_1/\mathbb{K}_2}\ \mathbf{P}_x = \sum_{a=1}^{(\ell-1)/2} ([a]\mathbf{P})_x \in \mathbb{K}_2$, then $\mathbb{K}_2 = \mathbb{K}[\mathbf{T}]$. We want to show that this extension gives raise to an abelian lift of $F(X)$.

Let $\iota : \mathcal{O}(\mathbb{K}) \to \mathbb{F}_q$ be the reduction $\bmod \mathfrak{p}$; we have seen that this induces a map of curve equations $\mathcal{E}' \to \mathcal{E}$ and of divsion polynomials $\Psi'_a[A',B'](X) \to \Psi_a[A,B](X)$. In particular, it extends ι to map $\mathcal{O}(\mathbb{K}_1) \to \mathbf{R} = \mathbb{F}_q[X]/(\Psi_\ell(X))$ defined by $\theta \mapsto X \bmod \Psi_\ell(X) \in \mathbf{R}$. Since $F_P(x) | \Psi_\ell(X)$, there is a further map $\mathbf{R} \to \mathfrak{R}$ and we let the composition be

$$\kappa : \mathcal{O}(\mathbb{K}_1) \to \mathfrak{R} \quad \text{where} \quad \theta \mapsto X \bmod F_P(X) \in \mathfrak{R}.$$

Let $\Phi(X)\mathcal{O}(\mathbb{K}_2)$ be the minimal polynomial of θ over $\mathbb{K}_2$, a polynomial of degree $(\ell-1)/2 = [\mathbb{K}_1 : \mathbb{K}_2]$. Then

$$\kappa(\Phi(X)) = F_P(X).$$

Since the extension $\mathbb{K}_1/K_2$ is abelian, so is the polynomial $\Phi(X)$ and this completes the proof that $F(X) = F_P(X)$ has an abelian lift and allows the application of Algorithm 1. for the factorization of the division eigenpolynomial $F(X)$.

Let $g_a(X) = \gamma_a(X) \bmod \mathfrak{P} \in \mathbb{F}_q[X]$. By definition, we have $g_a(P_x) = ([a]P)_x$. Let $\lambda \in \mathbb{F}_\ell$ be the eigenvalue of P, so $\phi_q(P) = [\lambda]P$ and let f be the order of λ in the group $\mathbb{F}_\ell^\times/\{-1,1\}$. Let c be a generator for the group $\mathbb{F}_\ell^\times/\{-1,1\}$ and consider the polynomial

$$G(X) = \sum_{i=1}^{f} (g_{c^{di}}(X)) \bmod F(X).$$

[4]It is useful to recall that the division polynomials can be defined in the ring in $\mathbb{Z}[A,B]$ of two formal parameters.

Letting $\omega = X \bmod F(X) \in \mathfrak{R}$ and $\eta = G(\omega)$ it follows that η is a splitting element. We have thus proved:

Theorem 1. *Let $\mathcal{E} : Y^2 = X^3 + AX + B$ be a non-supersingular elliptic curve over a finite field $\mathbb{F}_q$ with discriminant of the Frobenius $\Delta = t^2 - 4q$ and let ℓ be an odd prime different from the characteristic and such that $\left(\frac{\Delta}{\ell}\right) = 1$. Suppose that $P \in \overline{\mathbb{F}_q}$ is an eigenpoint of the representation of the Frobenius in the ℓ - torsion of $\mathcal{E}$ and the polynomial*

$$F(X) = \prod_{a=1}^{(\ell-1)/2} (X - ([a]P)_x) \in \mathbb{F}_q[X]$$

is given together with the order f of the corresponding eigenvalue $\lambda \in \mathbb{F}_\ell^\times / \{-1, 1\}$. Let $\ell - 1 = 2 \cdot f \cdot d$. Then there is an algorithm which is deterministic under the ERH and computes the irreducible factors of $F(X)$ in time

$$\mathcal{O}^\sim \left((d \cdot (\log(q) + \ell) + f\ell)\mathsf{M}(q) \right)$$

operations.

In general one does not know the value of λ or f. However, the Lemma 1 and the steps 3.-5. of the related algorithms of Shoup for linear generated sequences yield

Theorem 2. *Let $\mathbb{F}_q, \mathcal{E}, \ell, F(X), P, g_a(X), \mathfrak{R}, \omega$ be like above, let $c \in \mathbb{F}_\ell^\times$ be a generator and $d \cdot f = (\ell - 1)$. If $H = \{c^{di} : i = 1, 2, \ldots, f\}$ and*

$$\eta = \sum_{a \in H} g_a(\omega), \quad \eta_1 = \sum_{a \in H} g_{ac}(\omega) \in \mathfrak{R}.$$

Then there is an algorithm which computes the minimal generating polynomial $g(X)$ of the power sequence of η together with a polynomial $h(X)$ such that $h(\eta) = \eta_1$ in time

$$\mathcal{O}^\sim \left(d \cdot \ell \cdot \mathsf{M}(q) \right).$$

This result is of particular use in the context of a new algorithm [Mi1] for computing the discrete logarithm in the SEA algorithm for counting points on elliptic curves.

6. Conclusions

We have proposed a new frame for factoring polynomials $F(X) \in \mathbb{F}_q[X]$ with $\mathbb{F}_q$ a finite field, which is particularly efficient for polynomials with *abelian lift* . The resulting algorithms depend on the number of factors of $F(X)$ rather than on their degree and are interesting whenever the former figure is sensibly smaller than the latter.

We have shown that this frame is applicable to interesting cases of polynomials, such as the cyclotomic polynomials and eigenfactors of division polynomials of elliptic curves. Future research might reveal larger classes of polynomials than the ones with abelian lifts and to which the presented frame applies.

Acknowledgment: I thank V. Vuletescu for interesting discussions and careful proof - reading and A. Bostan for his observations and literature pointers during the development of this text.

References

[BK] J. Buhler and N. Koblitz: *Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems*, Bull. Austral. Math. Soc. **58** (1998), no. 1, 147–154.

[Bo] A. Bostan: *Algorithmique efficace pour des opérations de base en Calcul formel*, thése présentée à l'École Polytechnique Palaiseau (2003).

[BMSS] A. Bostan, F. Morain, B. Salvy and R. Schost: *Fast algorithms for computing isogenies between elliptic curves*, preprint, http://algo.inria.fr/bostan/

[CCR] L.S. Charlap, R. Coley and D. Robbins: *Enumeration of Rational Points on Elliptic Curves over Finite Fields*, unpublished manuscript (1992).

[GG] J. von zur Gathen, J. Gerhard: *Modern Computer Algebra* , 2-nd Edition, Cambridge University Press (2000).

[GS] J. von zur Gathen and V. Shoup: *Computing Frobenius maps and factoring polynomials*, Computational Complexity, **2** (1992), 187-224.

[KaSh] E. Kaltoffen and V. Shoup: *Subquadratic time factoring of polynomials over finite fields*, Math. Comp. **67, Nr. 223** (1998), p. 1179-1197.

[La] S. Lang: *Algebraic Number Theory*, Springer **GTM**, **110**, (1986)

[Mi] P. Mihăilescu : *Cyclotomy of Rings & Primality Testing*, dissertation 12278, ETH Zürich, 1997.

[Mi1] P. Mihăilescu: *Elliptic Curve Gauss Sums and Counting Points* , submitted.

[Ri] P. Ribenboim: *Classical Theory of Algebraic Numbers*, Springer **UTX**, (2001)

[Sch] R. Schoof: *Elliptic Curves over Finite Fields and the Computation of Square Roots mod p*, Mathematics of Computation, Vol. 44, Vol. 44 (1985), pp. 483-494.

[Sch1] R. Schoof: *Counting points on elliptic points over finite fields* J. Th. Nombr. Bordeaux, **7** (1995), pp. 363-397.

[Sh] V. Shoup: *Fast Construction of Irreducible Polynomials over Finite Fields*, J. Symb. Comp. **17**, (1994), pp. 371-391.

[Sh1] V. Shoup: *A New Polynomial Factorization Algorithm and its Implementation*, J. Symb. Comp., **20** (1995), pp. 363-397.

[Si] J. Silverman: *The Arithmetic of Elliptic Curves*, Springer Graduate Texts in Mathematics **106**.

[St1] G. Stein: *Factoring cyclotomic polynomials over large finite fields*, Finite fields and applications (Glasgow, 1995), pp. 349 – 354, London Math. Soc. Lecture Note Ser., **233**, Cambridge Univ. Press, Cambridge, 1996.

[St2] G. Stein: *Using the theory of cyclotomy to factor cyclotomic polynomials over finite fields*, Math.Comp. **70** (2001), no.235, pp. 1237 – 1251.

[Wa] P. van Wamelen: *Jacobi sums over finite fields*, Acta Arithmetica **102** (2002), pp. 1-20.

(P. Mihăilescu) Mathematisches Institut der Universität Göttingen
E-mail address, P. Mihăilescu: preda@uni-math.gwdg.de