Field extensions and index calculus on algebraic curves

Vanessa Vitse

Contemporary Mathematics

Field extensions and index calculus on algebraic curves

Vanessa Vitse

Abstract. Discrete logarithm index calculus algorithms are usually more efficient for non-hyperelliptic curves (Diem's method) than for hyperelliptic curves (Gaudry's method). However when the field of definition is not prime, Nagao's algorithm is even faster asymptotically, but is more efficient for hyperelliptic curves than for non-hyperelliptic ones. A natural question is then whether it is possible to adapt Nagao's method and design an index calculus that takes advantage of both the field extension and the non-hyperellipticity. In this work we explain why this is not possible, and why the asymptotic complexity of Nagao's algorithm is optimal using the known decomposition techniques.

Keywords : discrete logarithm problem, hyperelliptic curve cryptography, index calculus, divisor class group, Jacobian variety.

1. Introduction

Because of its relevance to cryptography, the discrete logarithm problem (DLP) is one of the most studied in the field of algorithmic number theory. We recall briefly that its consists of finding an integer k (the discrete logarithm) such that $h = k.g$, where g and h are two given elements in a group G. Initially only the multiplicative group $\mathbb{F}_q^*$ of a finite field was considered for G [**4**]. But of course, any finite group whose law is efficiently computable while sufficiently not trivial can be used, and for cryptographic applications Koblitz and Miller proposed in the mid-eighties to use the divisor class group (or Jacobian variety) of algebraic curves defined over finite fields [**14, 16**]. However, it turns out that the difficulty of the discrete logarithm problem is quite sensitive to the type of curves considered and their field of definition, for a fixed (prime) group size. Currently, only genus 1 (i.e. elliptic curves) and genus 2 curves, defined over prime fields or degree 2 extensions of prime fields, are considered secure enough for cryptography. Still, because of the existence of transfer attacks [**6**], assessing the concrete difficulty of computing discrete logarithms in the divisor class group of curves is an important problem, both from a theoretical and a practical point of view.

Today, the most successful approach to the discrete logarithm problem is the index calculus method. Originally developed for factoring integers, it has been successfully applied to the multiplicative group of finite fields, and more recently to Jacobian varieties. Basically, it consists of several phases; more details will be given in Section 3. In an initial stage, a small subset $\mathcal{F}$ of G (called the factor

base) is chosen, or progressively constructed; the overall contribution of this step is mostly negligible. Then in the relation search stage, one tries to obtain relations between elements of the factor base, and potentially of the challenge, of the form

$$ag + bh = \sum_i c_i g_i, \quad g_i \in \mathcal{F} \ \forall i.$$

Such a relation (or decomposition) immediately translates into a similar linear equation between the discrete logarithms of the elements of $\mathcal{F}$. The main difficulty is to devise an efficient way to compute such relations, for a small enough factor base. Once sufficiently many relations have been found (i.e. $\approx \#\mathcal{F}$), one proceeds to the linear algebra stage. The goal is to find a non-trivial linear combination of relations for which the right-hand term vanishes, yielding the requested discrete logarithm. This amounts to determining the kernel of the relation matrix, which is huge but extremely sparse. It is a well-known problem, and its resolution has a complexity which is quadratic in the size of the matrix, i.e. quadratic in $\#\mathcal{F}$.

The main parameter in this description is the size of the factor base. In the "large genus" case, i.e. when the genus g of the curve grows faster than the size of its field of definition, the complexity is asymptotically subexponential [**5**]. On the other hand, in the "small genus" case, i.e. when g is fixed and q goes to infinity, then the linear algebra stage becomes the main bottleneck. The best known workaround is the so-called double large prime technique. A second factor base $\mathcal{F}'$, the "small primes" base, is chosen; it is a small subset of $\mathcal{F}$, the "large primes" base. Then during the relation search, the relations that involves more than two elements of $\mathcal{F} \setminus \mathcal{F}'$ are discarded; those that remain are stored in a graph or tree (see [**9**] for details). Once enough relations are found, it is possible to combine them and eliminate the large primes, and then proceed to the linear algebra phase with a smaller matrix, still sparse and of size given by the cardinality of $\mathcal{F}'$.

This approach has first been applied by Gaudry, Thériault, Thomé and Diem following earlier works of Gaudry and Thériault [**7, 9, 19**]. Their method solves the DLP in the Jacobian variety of a genus g hyperelliptic curve defined over $\mathbb{F}_q$ in $\tilde{O}(q^{2-2/g})$, asymptotically as $q \to \infty$ and g fixed. Actually, it works for any algebraic curves of genus $g > 2$, but is less efficient in the non-hyperelliptic case as the hidden constant in the $\tilde{O}$ notation is much worse. At the same time, Diem [**2**] showed that for most genus g curves, but specifically excluding the hyperelliptic curves, it was possible to solve the DLP in complexity $\tilde{O}(q^{2-2/(g-1)})$. In other words, it is possible to take advantage of the non-hyperellipticity to speed up the index calculus method.

A few years later, Nagao [**17**] (following Gaudry [**8**]) investigated the case where the field of definition is an extension field, i.e. of the form $\mathbb{F}_{q^n}$ with $n > 1$. He showed that it is possible to use this fact and proposed an index calculus algorithm solving the DLP in $\tilde{O}(q^{2-2/ng})$ on a hyperelliptic genus g curve defined over $\mathbb{F}_{q^n}$, which is of course asymptotically better than with Gaudry's or Diem's method. Here again, this algorithm designed for hyperelliptic curves can be adapted to arbitrary curves, but with degraded performances.

	hyperelliptic	non-hyperelliptic
$n = 1$	$\tilde{O}(q^{2-2/g})$ (Gaudry)	$\tilde{O}(q^{2-2/(g-1)})$ (Diem)
$n > 1$	$\tilde{O}(q^{2-2/ng})$ (Nagao)	?

The table above summarizes the current situation. A natural question then arises : is it possible to combine both the non-hyperellipticity and the extension ? Or differently : why are non-hyperelliptic curves weaker than hyperelliptic ones when defined over prime fields, but not when defined over extension fields ? The goal of this paper is to answer these questions, and our main result is that Nagao's complexity is optimal for $n > 1$, at least within the currently known relation search techniques. Of course, we will begin by explaining these techniques and fit all existing algorithms in a unified framework. This uses the notion of linear system of divisor as well as Weil restriction, which are recalled in Section 2. The following section recapitulates the known methods, and Section 4 deals with the general case and the proof of our main result.

2. Index calculus and the divisor class group

2.1. Quotient description and decompositions. Index calculus usually relies on *arithmetical formations*. We refer to [**5, 13**] for a complete treatment, but the main idea is that the group G is given as a quotient of a free commutative monoid or group $\mathcal{M}$ over a countable set of *prime* or *irreducible* elements. For instance, if $G = (\mathbb{Z}/p\mathbb{Z})^*$ then $\mathcal{M}$ is the set $\mathbb{N} \setminus p\mathbb{N}$ of integers coprime to p, which is the free commutative monoid (for the multiplication law) generated by the prime numbers different from p. Similarly, if $G = (\mathbb{F}_{p^n})^*$ with p small, then $\mathcal{M}$ is $\mathbb{F}_p[X] \setminus (P(X))$, which is the monoid generated by the irreducible polynomials over $\mathbb{F}_p$ coprime to the degre n irreducible polynomial $P(X)$. Note that in each case, elements of G are always described by a representative in $\mathcal{M}$.

To apply the index calculus method in this setting, we choose for the factor base $\mathcal{F}$ a finite subset of "small" elements of the generating set of $\mathcal{M}$, that we identify with their equivalence classes in G. Then for the relation search, we produce elements of G in some controlled way (for instance known multiples of the challenge elements) and consider representatives in $\mathcal{M}$, for which there is a well-defined notion of factorization. We obtain a relation each time a representative is smooth, i.e. all its irreducible factors belongs to $\mathcal{F}$. One of the main difficulty is thus finding smooth representatives of a given group element. The size of the factor base is clearly an important factor here, since it affects the smoothness probability; if $\mathcal{F}$ is too small, very few elements will be smooth, whereas if it is too large we will need too many relations for the linear algebra step.

Index calculus in the divisor class group (or Jacobian variety) of an algebraic smooth curve $\mathcal{C}$ defined over $\mathbb{F}_{q^n}$ $(n \geq 1)$ fits in this description; the role of $\mathcal{M}$ is played by the set $\mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$ of $\mathbb{F}_{q^n}$-rational divisors, which is a free abelian group over the set of irreducible divisors. We recall briefly that a divisor D is a formal sum of the form

$$D = \sum_{P \in \mathcal{C}(\bar{\mathbb{F}}_q)} n_P(P)$$

where the n_P's are integers and only a finite number of them are non-zero, and $\mathcal{C}(\bar{\mathbb{F}}_q)$ is the set of points of $\mathcal{C}$ in the algebraic closure of $\mathbb{F}_{q^n}$. If $\mathbb{K}$ is an algebraic extension of $\mathbb{F}_{q^n}$, then a divisor D is defined over $\mathbb{K}$ (or $\mathbb{K}$-rational) if it is invariant under the natural action of the Galois group $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{K})$, induced by its action on $\mathcal{C}(\bar{\mathbb{F}}_q)$. The abelian group of $\mathbb{K}$-rational divisors is noted $\mathrm{Div}_{\mathbb{K}}(\mathcal{C})$; note that its elements are usually not formal sums of $\mathbb{K}$-rational points of $\mathcal{C}$.

A divisor D is called effective if $n_P \geq 0 \ \forall P \in \mathcal{C}(\bar{\mathbb{F}}_q)$. More generally, we can define a partial order by setting $\sum_{P\in\mathcal{C}(\bar{\mathbb{F}}_q)} n_P(P) \geq \sum_{P\in\mathcal{C}(\bar{\mathbb{F}}_q)} n'_P(P)$ if $n_P \geq n'_P \ \forall P \in \mathcal{C}(\bar{\mathbb{F}}_q)$; a divisor is thus effective if it is greater than or equal to the zero divisor. The degree of a divisor is $\deg(D) = \sum_P n_p$, and the set of degree zero divisors forms a subgroup of $\mathrm{Div}_{\mathbb{K}}(\mathcal{C})$. A non-zero, effective divisor $D \in \mathrm{Div}_{\mathbb{K}}(\mathcal{C})$ is called irreducible if it cannot be written non-trivially as a sum of $\mathbb{K}$-rational effective divisors. Obviously degree 1 effective divisors are irreducible, and are in one-to-one correspondence with the $\mathbb{K}$-rational points of $\mathcal{C}$; they are the only ones if $\mathbb{K} = \bar{\mathbb{F}}_q$, but not otherwise. In any case $\mathrm{Div}_{\mathbb{K}}(\mathcal{C})$ is easily seen to be the free abelian group generated by the irreducible divisors, with the set of effective divisors as submonoid. Therefore, elements of $\mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$ admit a well-defined decomposition in irreducible elements, and thus a notion of smoothness.

The divisor class group of $\mathcal{C}$ is obtained as the quotient of $\mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$ by the subgroup of principal divisors; we recall that a principal divisor $\mathrm{div}(f)$ is the divisor formed by the zeroes and poles (with multiplicities) of the function $f \in \mathbb{F}_{q^n}(\mathcal{C})$. It is a classical fact that the elements of the degree zero subgroup of the divisor class group are in one-to-one correspondence with the points of the Jacobian variety of $\mathcal{C}$, hence the notation $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ for both. Consequently, elements of $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ can be described either with equivalence classes of divisors, or with coordinates associated to a projective embedding of the variety, typically given by Theta functions. However, this second point of view does not correspond to an arithmetical formation, and has not yet found applications to index calculus. Thus the description of $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_{q^n})$ as the quotient of $\mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$ is the only one available for our purpose, and the main practical way of finding relations; note that it does not depend of the model of the curve. By contrast, the multiplicative group of a finite field can be expressed as a quotient in different ways, for instance by varying the irreducible polynomial $P(X)$ defining $\mathbb{F}_{p^n}$ as $\mathbb{F}_p[X]/(P(X))$. Using two different quotient representations is the basis for the improved performances of the function field sieve (notwithstanding the recent progress of [**1**]) and to a certain extent of the number field sieve.

2.2. Linear systems of divisors. Another difference between divisor class groups and finite fields is that the search space is finite dimensional: for any D in $\mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$, there are finitely many effective divisors linearly equivalent to D. To be precise, the set

$$|D| = \{D' \in \mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C}) \mid D' \sim D,\ D' \geq 0\},$$

which is called a complete linear system on $\mathcal{C}$, has the natural structure of a projective space over $\mathbb{F}_{q^n}$: it is in one-to-one correspondence with the projectivisation of the Riemann-Roch vector space

$$\mathcal{L}(D) = \{f \in \mathbb{F}_{q^n}(\mathcal{C})^* \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

The dimension $\ell(D)$ of this vector space (that is thus one more than the dimension of $|D|$) is related to the degree of D by the Riemann-Roch formula

$$\ell(D) - 1 \geq \deg(D) - g,$$

with equality if $\deg(D) \geq 2g - 1$. More generally, a linear system of divisors $\mathfrak{d}$ is a non-empty projective subspace of a complete linear system $|D|$ for some $D \in \mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$.

Both quantities $\deg(D)$ and $\ell(D)$ are important for our purpose. Indeed, for any $D' \in |D|$ we have $\deg(D') = \deg(D)$, and the smoothness probability of an effective divisor clearly decreases with its degree. More precisely, one can show that the probability for a random effective degree d divisor to be split, that is, to be a sum of degree 1 $\mathbb{F}_{q^n}$-rational divisors, is asymptotically equal to $1/d!$. We would like this estimate to hold for arbitrary divisors in a linear system, but as such it cannot be true because a linear system $\mathfrak{d}$ may not be base-free, i.e. there may exist a non-zero, effective divisor D_b (the base locus) such that $D \geq D_b$ for any $D \in \mathfrak{d}$. We will however make the following heuristic assumption, which is quite accurate in practice:

Assumption.
Divisors in a base-free linear system $\mathfrak{d}$ behave like random effective divisors of the same degree.

Since we are looking for split divisors, it is better if we can manage to work with low degree divisors. On the other hand, when $\ell(D)$ grows, so does the dimension of $|D|$, and we can use the additional degrees of freedom to improve the efficiency of the relation search; this will be made more precise in Section 4.

2.3. Weil restriction. An important tool when dealing with extension fields is the Weil restriction, or restriction of scalars. The idea is quite simple: if $\mathbb{L}/\mathbb{K}$ is a degree n field extension, then any variety V of dimension d defined over $\mathbb{L}$ can be viewed as a variety of dimension nd defined over $\mathbb{K}$, in the exact same way that algebraic curves over $\mathbb{C}$ are viewed as real surfaces. More precisely, we obtain a functor $W_{\mathbb{L}/\mathbb{K}}$, which sends varieties defined over $\mathbb{L}$ to varieties defined over $\mathbb{K}$.

If V is defined over $\mathbb{L}$, then the two sets $V(\mathbb{L})$ and $W_{\mathbb{L}/\mathbb{K}}(V)(\mathbb{K})$ are equal, but their algebraic structures are different and the latter has a finer topology. In particular, the Weil restriction of $\mathcal{C}(\mathbb{F}_{q^n})$ contains many algebraically defined subsets; we will use this fact for the definition of the factor bases. Also, since linear systems of divisors are projective spaces and hence algebraic varieties, we will consider their Weil restriction for the relation search.

3. Known index calculus methods

In what follows, we consider as given the algebraic curve $\mathcal{C}$ defined over $\mathbb{F}_{q^n}$ ($n \geq 1$) as well as two divisors D_0 and D_1 on $\mathcal{C}$ forming a DLP challenge, i.e. our goal is to find the discrete logarithm of $[D_1]$ in base $[D_0]$ in the divisor class group of $\mathcal{C}$.

3.1. Common outline. We focus in this article on the small genus case, i.e. when the genus g of $\mathcal{C}$ is fixed. We also fix the extension degree n; only the cardinality of the base field $\mathbb{F}_q$ grows to infinity. In this case, the factor base $\mathcal{F}$ only contains degree one $\mathbb{F}_{q^n}$-rational effective divisors (or rather their equivalence classes in the divisor class group), which are in one-to-one correspondence with the $\mathbb{F}_{q^n}$-rational points of $\mathcal{C}$.

The known index calculus methods on algebraic curves use different techniques, but they can be all described in a united framework.

(1) Choice of the factor bases:
   - if $n = 1$, the "large prime" factor base is $\mathcal{F} = \{(P) \mid P \in \mathcal{C}(\mathbb{F}_q)\} \subset \mathrm{Div}_{\mathbb{F}_q}(\mathcal{C})$;

- if $n > 1$, we use the Weil restriction structure and set $\mathcal{F} = \{(P) \mid P \in \mathcal{V}(\mathbb{F}_q)\} \subset \mathrm{Div}_{\mathbb{F}_{q^n}}(\mathcal{C})$ where $\mathcal{V}$ is a dimension one subvariety of $W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathcal{C})$.

In both cases, the cardinality of $\mathcal{F}$ is approximately equal to q. In order to apply the double large prime technique, we also define a "small prime" factor base $\mathcal{F}'$, which is an arbitrary subset of $\mathcal{F}$ of size in the order of q^α.

(2) Relation search: until $\approx q$ relations are found,
   (a) we compute a linear system $\mathfrak{d} \in |D|$, where the divisor D depends of the elements of the DLP challenge and of the factor bases, the equation of the curve, and potentially a randomness source;
   (b) we look for divisors $D' \in \mathfrak{d}$ which are sums of elements of $\mathcal{F}'$ and at most two "large primes", i.e. elements of $\mathcal{F}$; this search can be narrowed down using several techniques as discussed below. Each such divisor gives a relation in the divisor class group, of the form $D' \sim D$.

(3) Double large prime stage: the relations obtained in 2. are combined in order to eliminate the large primes and produce more than $\#\mathcal{F}'$ relations involving only small primes, i.e. elements of $\mathcal{F}'$, and the DLP challenge.

(4) Linear algebra stage: using sparse matrix techniques, we compute the kernel of the relation matrix and use this knowledge to solve the DLP challenge.

Of course, this outline is subject to adaptations. For instance, some authors suggest to construct the factor base $\mathcal{F}'$ progressively, during a first part of the relation stage [**15**]. Similarly, the double large prime stage is often merged with the relation search. Also, a descent phase can be needed in order to express the elements of the DLP challenge in terms of elements of the factor base, but it is usually just a variation around the relation search.

3.2. Gaudry's method. Gaudry's pioneering approach to the DLP on algebraic curves [**7**] originally did not use the double large prime technique and was designed for (imaginary) hyperelliptic curves. The double large prime variation, already used for the factorization of integers (hence its name), was later incorporated in the algorithm by Gaudry and Thériault, Thomé and Diem [**9**], still in the context of hyperelliptic curves. However, the generalization to arbitrary curves is not difficult; the only difference is that computations in the divisor class group are more complex but possible thanks to e.g. the works of Hess [**10**]. For simplicity, we will refer to this algorithm as Gaudry's. Since it does not rely on Weil restriction, the field of definition of $\mathcal{C}$ will be simply denoted by $\mathbb{F}_q$ (even though q can be a prime power).

In this method, we consider a particular point $\mathcal{O} \in \mathcal{C}(\mathbb{F}_q)$; if $\mathcal{C}$ is imaginary hyperelliptic then this is the point at infinity. Then for many random values of a and b, we compute the unique divisor D' linearly equivalent to $aD_0 + bD_1$ which is maximally reduced along $\mathcal{O}$ (i.e. we compute $a[D_0]+b[D_1]$ in the divisor class group, using maximally reduced divisors along $\mathcal{O}$ as representatives). This is usually done using a pseudo-random walk, so that only few operations in the divisor class group are needed at each step. We obtain a relation of the form

$$aD_0 + bD_1 \sim (P_1) + \cdots + (P_{r-2}) + (Q_1) + (Q_2) - r(\mathcal{O})$$

if D' (or rather $D' + r(\mathcal{O})$) is split with at most two large primes.

Generically we have $r = g$, so in our framework Gaudry's method corresponds to choosing $\mathfrak{d} = |D|$ with $D = aD_0 + bD_1 + g(O)$. This linear system contains (with overwhelming probability) only one element, namely $D' + g(\mathcal{O})$. Its splitness probability is asymptotically $1/g!$, which does not depend of q; however the probability that all elements of the decomposition but two are in the small prime factor base $\mathcal{F}'$ is asymptotically in $\Theta(q^{(\alpha-1)(g-2)})$ (recall that $\#\mathcal{F}' \approx q^\alpha$). Thus we need to test about $q.q^{(1-\alpha)(g-2)}$ divisors in order to generate enough relations to eliminate the large primes. Since the linear algebra stage requires $\approx q^{2\alpha}$ operations, we obtain that the asymptotically optimal value of α is $1 - 1/g$, equating the cost of the two main stages for an overall complexity in $\tilde{O}(q^{2-2/g})$.

Note that each trial requires some operations in the divisor class group as well as a splitting test and decomposition computation, whose costs are polynomial in $\log(q)$ and thus do not impact the above estimate; nevertheless, they are much faster in the hyperelliptic case than for arbitrary curves. For this reason, even though the asymptotic complexities are the same in both cases, the actual complexities are not.

Recently, a different approach has been proposed by Sarkar and Singh ([**18**], see also [**20**]). The idea (reformulated to fit our framework) is to consider the complete linear system $\mathfrak{d}$ associated to $aD_0 + bD_1 + (g+1)(\mathcal{O})$ (instead of $g(\mathcal{O})$). This corresponds to looking for decompositions of $a[D_0] + b[D_1]$ as sums of $g-1$ small primes and 2 large primes. The probability of obtaining one relation is lower since there are more elements in the decomposition, but it is compensated by the use of a sieving technique in the spirit of [**11**]. This is possible because $\mathfrak{d}$ has (generically) dimension one, so there is one parameter to sieve along.

3.3. Diem's method. Diem's method [**2**] uses the fact that most non-hyperelliptic curves admit small degree plane models — more precisely, plane models of degree at most $g+1$, where g is the genus of the curve. For a target curve $\mathcal{C}$ defined over $\mathbb{F}_q$ and having a plane model given by a degree d homogeneous equation $F(X,Y,Z) = 0$, we consider the divisor D_∞ given by the zeroes of Z (i.e. the points at infinity). The relation search works with the dimension two linear system $\mathfrak{d} \subset |D_\infty|$ consisting of affine lines, or rather of the intersections of affine lines with the plane model. It corresponds to the linear subspace $\mathrm{Span}(1, x, y)$ of the Riemann-Roch space $\mathcal{L}(D_\infty)$, with $x = X/Z$ and $y = Y/Z$.

Instead of sampling the space $\mathfrak{d}$ randomly, we use the fact that we have two degrees of freedom and look for divisors in $\mathfrak{d}$ having specified points in their support. In details, we repeatedly pick two non-singular, affine points P_1 and P_2 in the small factor base $\mathcal{F}'$ and compute the divisor D' given by the intersection of the line passing through these two points with the plane model. If D' is smooth, i.e. if the intersection contains $d-2$ other rational non-singular points, and if at most two of these intersection points are not in the small factor base, then we obtain a relation of the form

$$D_\infty \sim (P_1) + (P_2) + (P_3) + \cdots + (P_{d-2}) + (Q_1) + (Q_2).$$

Since by design (P_1) and (P_2) are already in $\mathcal{F}'$, the probability of having at most two large primes is in $\Theta(q^{(\alpha-1)(d-4)})$. A simple computation then shows that the asymptotically optimal value of α is $1 - 1/(d-2)$, yielding an overall complexity in $\tilde{O}(q^{2-2/(d-2)})$. This is smaller than the complexity of Gaudry's method as soon as the degree d of the plane model satisfies $d \leq g+1$. Finding such plane models

is effectively possible for most algebraic curves, but not for the hyperelliptic ones. For this reason, the DLP in the divisor class group of non-hyperelliptic curves is considered as weaker than for hyperelliptic ones.

3.4. Nagao's method. Nagao's method [**17**] is a generalization for algebraic curves $\mathcal{C}$ defined over an extension field $\mathbb{F}_{q^n}$ of an earlier work of Gaudry [**8**] on the DLP for elliptic curves. The main idea is to use the Weil restriction structure to define the (large) factor base $\mathcal{F}$. Nagao suggests choosing

$$\mathcal{F} = \{(P) \mid P \in \mathcal{C}(\mathbb{F}_{q^n}),\ x(P) \in \mathbb{F}_q\},$$

but more generally, the last condition can be restated as $P \in \mathcal{V}(\mathbb{F}_q)$, where $\mathcal{V}$ is an algebraic dimension one subvariety of the Weil restriction $W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\mathcal{C})$.

As in Gaudry's method, we choose a distinguished point $\mathcal{O}$, typically the point at infinity. During the relation search we consider, for many different values of a and b, the complete linear system $\mathfrak{d} = |D|$ associated to the divisor $D = aD_0 + bD_1 + ng(\mathcal{O})$. We observe that $\deg(D) = ng$ and $\dim_{\mathbb{F}_{q^n}} |D| = (n-1)g$ according to Riemann-Roch theorem, so as a variety over $\mathbb{F}_q$, the Weil restriction of the projective space $|D|$ has dimension $n(n-1)g$. Since $\mathcal{F}$ is defined by algebraic equations, the condition that a divisor $D' \in |D|$ is a sum of ng elements of $\mathcal{F}$ can be expressed as a system of multivariate polynomial equations. We refer to [**17**] (cf also [**11**]) for the details, but informally, asking that a point in the support of D' belongs to $\mathcal{F}$ gives $n-1$ equations over $\mathbb{F}_q$. Since there are ng points in the support, we obtain a system (over $\mathbb{F}_q$) of $(n-1)ng$ equations, which is exactly the dimension of $W_{\mathbb{F}_{q^n}/\mathbb{F}_q}(|D|)$. Indeed, this system has generically dimension 0, i.e. a finite number of solutions. Thus for each value of a and b, we solve this multivariate polynomial system and consider the resulting divisors $D' \in |D|$. By design, they are sums of elements of $\mathcal{F}$, but it remains to test if at least $ng-2$ ot them are in $\mathcal{F}'$; this happens with probability in $\Theta(q^{(\alpha-1)(ng-2)})$.

The main difficulty in Nagao's method is the resolution of the polynomial system. Even for relatively small values of n and g, this resolution quickly exhausts the resources of a personal computer. In the hyperelliptic case, the $n(n-1)g$ equations in $n(n-1)g$ variables are quadratic, and have been solved only for $n \leq 3$ and $g \leq 4$. But for non-hyperelliptic curves (hence $g \geq 3$), the equations have bigger degrees and the resolution is infeasible in practice, except by exhaustive search for small q. Nevertheless, since the number of equations / variables and their degrees do not depend of q, asymptotically for n and g fixed the complexity of the resolution is polynomial in $\log(q)$ as $q \to \infty$. Then the asymptotically optimal value of α is $1 - 1/ng$, yielding an overall complexity in $\tilde{O}(q^{2-2/ng})$. This is much lower than the complexity of Gaudry's or Diem's method, which run in $\tilde{O}(q^{n(2-2/g)})$ or $\tilde{O}(q^{n(2-2/(d-2))})$, since the definition field is $\mathbb{F}_{q^n}$ instead of $\mathbb{F}_q$; but we emphasize that except for hyperelliptic curves and small values of n and g (see e.g. [**11**]), Nagao's method is impractical because of the intractability of the polynomial system resolution in the relation search.

4. The general case

4.1. Relation search techniques and their impact on complexity. In the above examples, we have seen that the different relation search techniques amount to looking for divisors D' in a particular linear system $\mathfrak{d} \subset |D|$ such that D' is not only split, but also a sum of small primes and at most two large primes.

Let $d = \deg(D)$ be the degree of the elements of $\mathfrak{d}$. Since $\#\mathcal{C}(\mathbb{F}_{q^n}) \approx q^n$, $\#\mathcal{F} \approx q$, and $\#\mathcal{F}' \approx q^\alpha$, with our heuristic assumption we see that a random $D' \in \mathfrak{d}$ yields a relation with probability in

$$\Theta(q^{d(1-n)}.q^{(\alpha-1)(d-2)}) = \Theta(q^{2(1-n)+(d-2)(\alpha-n)}).$$

But obviously, we will not sample $\mathfrak{d}$ or $|D|$ at random. We recall that the dimension of $|D|$ is $\ell(D)-1$ as a projective space over $\mathbb{F}_{q^n}$, or $n(\ell(D)-1)$ as a variety over $\mathbb{F}_q$; we will denote by r the dimension of $\mathfrak{d}$ over $\mathbb{F}_{q^n}$.

(1) We can consider divisors having a number a of specified "small primes" points in their support, as in Diem's method (where $a = 2$). In effect, it replaces d by $d-a$ in the above probability, i.e. it improves the decomposition probability by a factor $q^{a(n-\alpha)}$. Of course, a must be smaller than or equal to d (the number of points in the support). Looking for such divisors gives a $\mathbb{F}_{q^n}$-linear constraints, or na $\mathbb{F}_q$-linear constraints, on $\mathfrak{d}$.

(2) If $n > 1$, we can require that b points in the support of D' belong to $\mathcal{F}$ and express this condition algebraically, as in Nagao's method (where $b = ng$). Since $\mathcal{F}$ has codimension $(n-1)$ in (the Weil restriction of) $\mathcal{C}$, this gives $b(n-1)$ non-linear equations or constraints. It still remains to check that enough points in the support of D' are actually small primes, so it improves the decomposition probability by a factor $(\frac{q^n/q^\alpha}{q/q^\alpha})^b = q^{b(n-1)}$.

(3) Finally, we can sieve on c parameters, in the spirit of Joux-Vitse or Sarkar-Singh [**11, 18, 20**] (where $c = 1$). The idea is to find coordinates on $\mathfrak{d}$ such that c of them directly relate to the choice of $\mathcal{F}'$ as a subset of $\mathcal{F}$. Then we iterate through $\mathfrak{d}$, but it only requires q^α instead of q iterations for each of the sieved parameters. This process does not improve the decomposition probability, but provides a speed-up by a factor $q^{c(1-\alpha)}$.

Of course, these three techniques can be combined[1]. However, we have the two following inequalities:

$$\begin{cases} a + b \leq d \\ an + b(n-1) + c \leq nr \leq n(\ell(D)-1) \end{cases}$$

The first one simply expresses that we cannot have more conditions on the points of the support of the divisor than the number of points in this support. The second one states that we cannot have more constraints on $\mathfrak{d}$ than its dimension, otherwise there will be generically no divisor satisfying these constraints in the linear system[2].

If these inequalities are satisfied, and remembering that we need $\approx q$ relations to eliminate the large primes, we see that the complexity of the relation search is in

$$\tilde{O}(q.q^{2(n-1)+(d-2)(n-\alpha)}.q^{a(\alpha-n)}.q^{b(1-n)}.q^{c(\alpha-1)}) = \tilde{O}(q^{2\alpha+\alpha(a+c-d)+nd-1-(an+b(n-1)+c)}).$$

[1]It is not clear if every such combinations can be implemented, but they still provide interesting complexity bounds.

[2]In practice (i.e. not from the asymptotic complexity point of view), it is sometimes interesting to work with overdetermined systems, see [**12**].

The asymptotically optimal value of α is the one for which this is equal to the complexity of the linear algebra stage, in $\tilde{O}(q^{2\alpha})$, and a quick computation leads to

$$\alpha = \frac{nd - 1 - (an + b(n-1) + c)}{d - (a + c)}.$$

We will now look for the "best" index calculus choices, i.e. divisors D and values of a, b and c yielding the smallest α. Our main result is the following:

Theorem. *Using the above-mentioned techniques, the asymptotically optimal complexity of the discrete logarithm index calculus method on $\mathcal{C}$ is*

- $\tilde{O}(q^{2-2/g})$ *if $\mathcal{C}$ is an hyperelliptic curve defined over $\mathbb{F}_q$;*
- $\tilde{O}(q^{2-2/ng})$ *if $\mathcal{C}$ is defined over $\mathbb{F}_{q^n}$ with $n > 1$.*

4.2. The $n = 1$ case. If $n = 1$, i.e. if q is prime or more generally if we do not take into account the field extension, then b is irrelevant and the optimal choice is $a + c = r$. A basic result in Riemann-Roch theory is that $r \leq d$, so the first inequality is satisfied as well, and we obtain

$$\alpha = \frac{d - r - 1}{d - r} = 1 - \frac{1}{d - r}.$$

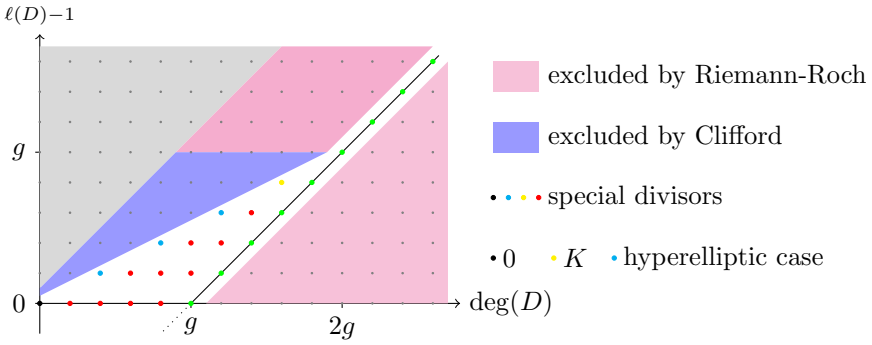
Thus we are led to look for linear systems such that $d - r$ is as small as possible. This means that r should be equal $\ell(D) - 1$ (i.e. $\mathfrak{d} = |D|$) and $\deg(D) - \ell(D) + 1$ should be as small as possible, or equivalently the index of speciality $i(D) = g + r - d$ is as large as possible. However, special divisors (i.e. effective divisors such that $\ell(D) - 1 > \max(0, \deg(D) - g)$) in the hyperelliptic case are uninteresting for index calculus. Indeed, such divisors are always of the form $D = E + (P) + (\imath(P))$ with E effective and $\imath$ the hyperelliptic involution. Therefore relations involving D give as much information as relations only involving E, and this prevents achieving a better asymptotic complexity than Gaudry's method.

In the non-hyperelliptic case, Diem's method provides a special divisor by constructing a small degree plane model, and the smaller the degree the better. More recently, Diem and Kochinke have proposed a way to work with more special divisors, using singularities of plane models. A limitation then arises from Brill-Noether theory, which bounds the number of special divisors according to their specialty index, see [**3**] for details. Anyhow, this further increases the discrepancy between the difficulty of the DLP on hyperelliptic and non-hyperelliptic curves.

4.3. The extension case. If $n > 1$, i.e. if we work with a non-prime base field and decide to use this property, then we are still interested by special divisors. However, Clifford's theorem bounds the possible index of specialty.

Theorem (Clifford). *Let $D \in Div(\mathcal{C})$ be a divisor such that $\ell(D) - 1 > \deg(D) - g$. Then $\ell(D) - 1 \leq \deg(D)/2$, with equality only if $D = 0$, or D is canonical, or $\mathcal{C}$ is hyperelliptic.*

The following picture sums up the possible values of $\deg(D)$ and $\ell(D)$.



In order to prove our main results, we have to consider different cases according to the values of the degree $d = \deg(D)$ of D and the dimension r of $\mathfrak{d}$. Note that since the expression of α does not involve r, we can assume without loss of generality that $r = \ell(D) - 1$, i.e. $\mathfrak{d}$ is the complete linear system $|D|$.

- If $g \leq d \leq ng$ and $d = r + g$ (this second condition is always satisfied as soon as $d > 2g - 2$ thanks to Riemann-Roch theorem), then $\frac{nr}{n-1} = \frac{nd-ng}{n-1} \leq \frac{nd-d}{n-1} = d$, so we can take $b = \frac{nr}{n-1}$ and $a = c = 0$. This is optimal for fixed d, provided $\frac{nr}{n-1}$ is an integer. Then $\alpha = \frac{nd-1-nr}{d} = \frac{ng-1}{d}$, which is smallest when $d = ng$. We recover the value $\frac{ng-1}{ng} = 1-1/ng$ of Nagao's approach.
- If $d > ng$, then $\frac{nr}{n-1} > d$, so the best we can do is choose b between ng and d, $a = d - b$, and $c = nr - an - b(n-1) = n(r-d) + b = b - ng$. Then $\alpha = \frac{nd-1-nr}{d-(d-ng)} = \frac{ng-1}{ng}$, which is not better than for $d = ng$.
- If $d < r + g$ (and so necessarily $d \leq 2g - 2$), then D is special. But Clifford's theorem on special divisors asserts that $r \leq d/2$. More precisely, the equality $2r = d$ occurs only in three cases: $D = 0$, which does not happen here; D is a canonical divisor; or $\mathcal{C}$ hyperelliptic (see the above figure). The hyperelliptic case can be ruled out, as we have seen that their special divisors do not yield more non-trivial relations. The case where D is canonical is interesting when $n = 2$; however, it gives only one complete linear system and can provide only a small number of relations, so it does not impact the overall complexity.
  Otherwise $2r \leq d - 1$. The best choice is again to take $a = c = 0$ and (assuming it is an integer) $b = \frac{nr}{n-1} \leq \frac{n(d-1)}{2(n-1)} \leq d$. In particular, $\alpha \geq \frac{nd-1-c(n-1)}{d} \geq \frac{nd-1-n(d-1)/2}{d} = \frac{n}{2} + \frac{n-2}{2d}$. Since $d \geq 1$ and $n \geq 2$, this is greater than or equal to 1 and thus uninteresting.

Finally, we obtain that the optimal complexity is for $\alpha = 1 - 1/ng$, which can be reached for $d \geq ng$. In particular, it is not possible to improve asymptotically on the complexity of Nagao's method.

5. Conclusion

While it is possible to combine the three techniques (sieving, specifying points directly or via Weil restriction) in different ways, we have seen that Nagao's method is optimal in this respect. Our main result can be restated informally as follows :

index calculus in $\mathrm{Div}^0_{\mathbb{F}_{q^n}}(\mathcal{C})$ requires divisors of degree $\approx ng$. If $n = 1$, this gives plenty of special divisors to choose from, but since special divisors are uninteresting on hyperelliptic curves, this explains why non-hyperelliptic curves are easier DLP targets. If $n = 2$, this leaves available only the canonical divisor, which is interesting but does not impact the overall complexity. Finally, if $n > 2$ there is no available special divisor, and index calculus is not faster on non-hyperelliptic curves.

Besides this result, we have shown that all known index calculus methods on algebraic curves follow a similar framework, with the same limitations. It seems reasonable to claim that no essential progress will be made on the DLP on algebraic curves if one remains within this framework, and it is only by going beyond and finding new decomposition methods that real advances will be made.

References

[1] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé, *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic.*, Advances in cryptology – EUROCRYPT 2014, Lecture Notes in Comput. Sci., vol. 8441, Springer, Berlin, 2014, pp. 1–16.

[2] Claus Diem, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory – ANTS-IX, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557.

[3] Claus Diem and Sebastian Kochinke, *Computing discrete logarithms with special linear systems*, Preprint, 2013.

[4] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654.

[5] Andreas Enge and Pierrick Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arith. **102** (2002), no. 1, 83–103.

[6] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46.

[7] Pierrick Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in cryptology—EUROCRYPT 2000, Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34.

[8] ———, *Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem*, J. Symbolic Comput. **44** (2008), no. 12, 1690–1702.

[9] Pierrick Gaudry, Emmanuel Thomé, Nicolas Thériault, and Claus Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76** (2007), 475–492.

[10] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445.

[11] Antoine Joux and Vanessa Vitse, *Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a seemingly secure curve over* $\mathbb{F}_{p^6}$, Advances in cryptology—EUROCRYPT 2012, Lecture Notes in Comput. Sci., vol. 7237, Springer, 2012, pp. 9–26.

[12] Antoine Joux and Vanessa Vitse, *Elliptic curve discrete logarithm problem over small degree extension fields*, J. Cryptology **26** (2013), no. 1, 119–143.

[13] John Knopfmacher, *Abstract analytic number theory (2nd edition).*, Dover Book on Advanced Mathematics, Dover Publications, New York, 1990 (English).

[14] Neal Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209.

[15] Kim Laine and Kristin Lauter, *Time-memory trade-offs for index calculus in genus 3*, J. Math. Cryptol. **9** (2015), no. 2, 95–114.

[16] Victor S. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology – CRYPTO 1985, Lecture Notes in Comput. Sci., vol. 218, Springer, Berlin, 1986, pp. 417–426.

[17] Koh-ichi Nagao, *Decomposition attack for the Jacobian of a hyperelliptic curve over an extension field*, Algorithmic Number Theory – ANTS-IX, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 285–300.

[18] Palash Sarkar and Shashank Singh, *A new method for decomposition in the Jacobian of small genus hyperelliptic curves*, to appear in Des. Codes Cryptogr.

[19] Nicolas Thériault, *Index calculus attack for hyperelliptic curves of small genus*, Advances in Cryptology – ASIACRYPT 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, 2003, pp. 75–92.
[20] Vanessa Vitse and Alexandre Wallet, *Improved sieving on algebraic curves*, Progress in Cryptology – LATINCRYPT 2015, Lecture Notes in Comput. Sci., vol. 9230, Springer, 2015, pp. 295–307.

Université Grenoble Alpes, Institut Fourier, CS 40700, 38058 Grenoble cedex 9, France
E-mail address: vanessa.vitse@ujf-grenoble.fr