COMPUTING DISCRETE LOGARITHMS
IN HIGH-GENUS HYPERELLIPTIC JACOBIANS
IN PROVABLY SUBEXPONENTIAL TIME

ANDREAS ENGE

ABSTRACT. We provide a subexponential algorithm for solving the discrete logarithm problem in Jacobians of high-genus hyperelliptic curves over finite fields. Its expected running time for instances with genus g and underlying finite field $\mathbb{F}_q$ satisfying $g \geq \vartheta \log q$ for a positive constant ϑ is given by

$$O\left(e^{\left(\frac{5}{\sqrt{6}}\left(\sqrt{1+\frac{3}{2\vartheta}}+\sqrt{\frac{3}{2\vartheta}}\right)+o(1)\right)\sqrt{(g\log q)\log(g\log q)}}\right).$$

The algorithm works over any finite field, and its running time does not rely on any unproven assumptions.

1. MOTIVATION AND MAIN RESULT

Jacobians of hyperelliptic curves over finite fields were suggested for use in public key cryptosystems by Koblitz in [17]. As abelian groups, these structures are adequate for Diffie-Hellman type systems, whose security relies on the intractability of the discrete logarithm problem in the underlying group. In principle, hyperelliptic cryptosystems offer the same security as elliptic cryptosystems of the same key length.

However, in 1994 Adleman, DeMarrais and Huang showed that under some reasonable heuristic assumptions there is a subexponential algorithm for discrete logarithms in high-genus hyperelliptic Jacobians [1]. The algorithm was presented for curves over prime fields only. Müller, Stein and Thiel gave a rigorous subexponential algorithm for computing logarithms in the infrastructure of a real-quadratic congruence function field in [24]. Again, only the odd characteristic case was described, and the authors did not take into account the dependence of the running time of the algorithm on the ratio $g/\log q$.

The present paper deals with a randomised subexponential algorithm whose expected running time can be rigorously proven without any heuristic arguments. Its running time depends on the minimal ratio $g/\log q$ for all instances under consideration, and this dependence can be quantified. On the other hand, the running time does not depend on the knowledge of the class number. Finally the algorithm is valid for hyperelliptic curves over any finite field, in particular over fields of characteristic 2.

We postpone the introduction of the relevant notions and notations to Section 2 and present the main result of this article:

Theorem 1.1. *Let*

$$L(\rho) := e^{\rho \sqrt{(g \log q) \log(g \log q)}}$$

denote the subexponential function with respect to $g \log q$, and consider all instances of the hyperelliptic logarithm problem satisfying $g \geq \vartheta \log q$ for a given positive constant ϑ. Then there is an algorithm solving these instances in time

$$O \left(L \left(\frac{5}{\sqrt{6}} \left(\sqrt{1 + \frac{3}{2\vartheta}} + \sqrt{\frac{3}{2\vartheta}} \right) + o(1) \right) \right).$$

The rest of this paper is devoted to the proof of this theorem. After introducing hyperelliptic curves, their Jacobians and the discrete logarithm problem associated with them, we describe the subexponential algorithm solving this problem. We then show how to choose the factor base, an essential ingredient of the algorithm, properly. Finally we compose all partial results to prove the desired subexponential running time.

2. Hyperelliptic Jacobians

In this section we briefly present hyperelliptic curves and their Jacobians, relating all results without proof. An excellent elementary introduction is given in [21]. While we are chiefly interested in curves over finite fields, the results hold in full generality.

Let $K = \mathbb{F}_q$ be the finite field with q elements and $\overline{K}$ its algebraic closure. A hyperelliptic curve over K is a degree 2 cover of the projective line $\mathbb{P}^1(K)$. Restricting our attention to curves with a ramified rational prime divisor, we consider hyperelliptic curves of genus g over K which admit an affine model of the form

$$H : Y^2 + vY = u,$$

where $v \in K[X]$ is of degree at most g and $u \in K[X]$ monic of degree $2g + 1$ (see [26, 11, 12]). We first examine H as a curve over $\overline{K}$. Then it consists of the *finite points* $P = (x, y) \in \overline{K} \times \overline{K}$ whose coordinates satisfy the equation, and an additional *point at infinity*, denoted by $\mathcal{O}$. These are in bijection with the *primes* or *valuations* of the function field $\overline{K}(H) := \overline{K}(X)[Y]/(H)$, which is a quadratic extension of the rational function field $\overline{K}(X)$. The *group of divisors* $\overline{\mathrm{Div}}(H)$ associated to H is the free abelian group over the points on H; the *degree* of a divisor $D = \sum_{P \in H} m_P P$ is the sum of its coefficients, $\deg D = \sum_{P \in H} m_P$. The *degree zero part* of the divisor group consists of all divisors of degree zero and is denoted by $\overline{\mathrm{Div}^0}(H)$. To a rational function in $\overline{K}(H)$ can be associated the divisor of its zeroes and poles, each with the corresponding multiplicities; such a divisor is called *principal*, and all principal divisors form the subgroup $\overline{\mathrm{Prin}}(H) \subseteq \overline{\mathrm{Div}^0}(H)$. Now the *Jacobian* of H is defined as the abelian group $\overline{J}(H) := \overline{\mathrm{Div}^0}(H)/\overline{\mathrm{Prin}}(H)$; its elements are called *divisor classes*.

A divisor consisting of only one point is called *prime*, and a different view of such a divisor is useful: Being given a finite prime of the rational function field $\overline{K}(X)$, i.e., an irreducible polynomial $a = X - x$, the equation

$$Y^2 + vY - u \equiv 0 \pmod{a} \Leftrightarrow Y^2 + v(x)Y - u(x) = 0$$

has a solution $y \in \overline{K} \simeq \overline{K}[X]/(a)$, and its second solution is given by $-y - v(x)$; they correspond to the prime $P = (x, y)$ and its *conjugate* $\overline{P} = (x, -y - v(x))$, respectively. Hence P and $\overline{P}$ are the primes of $\overline{K}(H)$ which lie over a, and we call a, P and $\overline{P}$ *split* if $P \neq \overline{P}$ and *ramified* otherwise. The ramified prime $\mathcal{O}$ extends the infinite valuation given by the negative degree on $\overline{K}(X)$.

Furthermore, the degree zero divisor $P - \mathcal{O}$ can be represented as the gcd of the divisors of $X - x$ and $Y - y$, where

$$\gcd \left(\sum_{P \in H} m_P P, \sum_{P \in H} n_P P \right) = \sum_{P \in H,\, P \neq \mathcal{O}} \min(m_P, n_P) P$$
$$- \left(\sum_{P \in H,\, P \neq \mathcal{O}} \min(m_P, n_P) \right) \mathcal{O};$$

we write $P = \operatorname{div}(X - x, y)$.

A degree zero divisor $D = \sum_{P \in H} m_P P$ is called *reduced* if all $m_P \geq 0$ for $P \neq \mathcal{O}$, at most one of m_P and $m_{\overline{P}}$ is positive for a split prime P, $m_P \in \{0, 1\}$ for a ramified prime $P \neq \mathcal{O}$ and $\sum_{P \neq \mathcal{O}} m_P \leq g$. Any divisor class contains a unique reduced representative, which can be uniquely written as $\operatorname{div}(a, b) := \gcd(\operatorname{div}(a), \operatorname{div}(Y - b))$ for a, $b \in \overline{K}[X]$, a monic, $\deg b < \deg a \leq g$, and $a | b^2 + vb - u$.

In order to compute in Jacobians, we must reduce all notions above to the finite field K itself. Note that the Galois group of $\overline{K}/K$ is topologically generated by the Frobenius automorphism

$$\varphi : \overline{K} \to \overline{K},\ x \mapsto x^q,$$

which acts in the obvious manner on points and divisors by $(x, y) \mapsto (x^q, y^q)$. We call a divisor *rational* over K if it consists of complete orbits under φ, each of these orbits representing a prime of the function field $K(H)$. We denote such a rational prime divisor again by P, and define $\deg P$ by the cardinality of the orbit. Adopting the projective point of view it is easy to see that $\mathcal{O}$ is rational of degree 1. Then we can define $\operatorname{Div}(H)$ as the free abelian group over the rational primes, and the definitions of $\operatorname{Div}^0(H)$, $\operatorname{Prin}(H)$ and the Jacobian $J(H)$ carry over from the algebraically closed case. As we are only interested in degree zero divisors, we make use, without explicitly mentioning it in the following, of the canonical epimorphism $\operatorname{Div} \to \operatorname{Div}^0$, $D \mapsto D - (\deg D)\mathcal{O}$, and identify each prime P with the corresponding degree zero divisor $P - (\deg P)\mathcal{O}$.

A finite prime of $K(X)$ is given by an irreducible polynomial $a \in K[X]$, and three cases can be distinguished:

- $Y^2 + vY - u \equiv 0 \pmod{a}$ has two solutions b and $-b - v$ in $K[X]$. Then there are two primes in $K(H)$ which lie over a, given by $P = \operatorname{div}(a, b)$ and $\overline{P} = \operatorname{div}(a, -b - v)$; their degrees are $\deg a$, and a, P and $\overline{P}$ are called *split*.
- There is one (double) solution b, corresponding to a unique prime $P = \operatorname{div}(a, b)$ over a such that $P = \overline{P}$. The degree of P is $\deg a$, and a and P are called *ramified*.
- There is no solution to the congruence in $K[X]$, and a corresponds to the prime $P = \operatorname{div}(a)$ of $K(H)$. The degree of P is $2 \deg a$, and a and P are called *inert*.

It can be easily seen that a reduced divisor $\operatorname{div}(a, b)$ is rational if and only if a, $b \in K[X]$; so as before, each divisor class of $J(H)$ has a unique representative

$\mathrm{div}(a, b)$ with a, $b \in K[X]$, a monic, $\deg b < \deg a \leq g$ and $a|b^2 + vb - u$. Moreover, in this representation there is a deterministic algorithm for adding divisor classes, using $O(g^2)$ elementary operations in K, described by Cantor in [5] (see also [10]).

So far, we have shown how to construct rational prime divisors with respect to their representations as $\mathrm{div}(a, b)$, and that it is possible to compute reduced expressions for arbitrary sums of these primes. We also need the converse operation, namely to determine the multiplicities of the primes in a reduced degree zero divisor $D = \mathrm{div}(a, b)$. To this purpose we decompose a into a product of distinct irreducible polynomials $a = a_1^{e_1} \cdots a_r^{e_r}$. It follows from the definition of reduced divisors that none of the a_i can be inert. If a_i is ramified, then the unique prime P_i over a_i occurs in D with multiplicity $e_i = 1$. If a_i is split, let $b_i \equiv b \pmod{a_i}$, and the prime $P_i = \mathrm{div}(a_i, b_i)$ occurs with multiplicity e_i in D. (This is nicely explained in [1], Section 3.)

3. Solving the discrete logarithm problem

Suppose that we are given two reduced degree zero divisors $D^{(1)}$ and $D^{(2)}$ such that $D^{(2)}$ is in the same divisor class as $lD^{(1)}$ for an integer l (which we denote by $D^{(2)} \sim lD^{(1)}$). The discrete logarithm problem is to determine l, which is unique up to multiples of the *class number* $h = |J(H)|$ of H. As usual for subexponential discrete logarithm algorithms we proceed in two stages: First, we try to determine the structure of the group under consideration; second, we solve the individual discrete logarithm problems.

3.1. **Finding the group structure.** Let $B = \{P_1, \ldots, P_n\}$, the *factor base*, be a set of rational primes that generates $J(H)$. (The term "factor base" comes from the multiplicative setting in a finite field, but we keep some muliplicative terminology in our additive setting. How B is constructed is the topic of Section 4.) The group homomorphism

$$\mathbb{Z}^n \to J(H), \ (e_1, \ldots, e_n) \mapsto e_1 P_1 + \ldots e_n P_n,$$

is surjective, and if Γ is its kernel, then

$$\mathbb{Z}^n / \Gamma \simeq J(H).$$

As $|J(H)| = h$ is finite, Γ is a full lattice of determinant h, whose elements are called *relations*. During the first stage of the algorithm, we try to determine a basis for Γ. Starting with the empty matrix M, by a randomised procedure described below we alternately create a new relation and add it as a new column to M. In the case where h is known it is then easy to determine whether the columns of M generate Γ. Since we do not wish to make this assumption, we have to generate a rather large number of relations, pretend that they generate Γ and try to solve the discrete logarithm problem. If we do not succeed, we have to repeat the group structure finding step. In the case that the columns of M do generate Γ, the structure of $J(H)$ is closely related to a special transform of M; recall the following definitions (see [6, Section 2.4]):

Definition and Theorem 3.1. Let $A = (a_{ij})$ be an integral $n \times m$-matrix of rank n.

1. A is in *column echelon form* if its first $m - n$ columns are zero and its last n columns form an upper triangular matrix.

2. A is in *Hermite normal form* if it is in column echelon form and moreover $a_{i,i+m-n} > 0$ for $i = 1, \ldots, n$ and $0 \leq a_{i,j+m-n} < a_{i,i+m-n}$ for $i = 1, \ldots, n$, $j = i+1, \ldots, n$. There is a unique matrix $N \in \mathbb{Z}^{n \times m}$ in Hermite normal form such that $N = AT$ for a unimodular matrix $T \in \mathbb{Z}^{m \times m}$. Hence the columns of N and A span the same lattice, and the *essential part* of N, i.e., its nonzero columns, forms a canonical basis for this lattice.

3. Suppose that $N \in \mathbb{Z}^{n \times n}$ is the essential part of the Hermite normal form of A. Then there is a unimodular matrix $S \in \mathbb{Z}^{n \times n}$ such that $\Delta := SN$ is a diagonal matrix with diagonal entries $d_1 | \cdots | d_n$; Δ is called the *Smith normal form* of A. If A is the matrix M above, then $d_1, \ldots, d_n$ are the *group invariants* of $J(H)$.

The principles outlined so far are the same as those underlying the algorithm in [1]. The main difference in our algorithm is the creation of new relations, which follows ideas first presented by McCurley in [20]. Basically we compute random linear combinations of prime divisors, reduce them and try to express the reduced divisors as another linear combination of prime divisors. The probability of success for this procedure is apparently easier to analyse than the approach in [1], where divisors of random polynomial functions are used to build relations.

The following algorithm succeeds with a high probability in finding the group structure:

Algorithm 3.2.

1. *Let M be the empty matrix. Fix a maximal exponent E such that $J(H)$ is generated by at most the $(E-1)$-th multiples of primes in B. (The choice of E is discussed in subsection 3.3.) Construct the factor base $B = \{P_1, \ldots, P_n\}$ explicitly as described in Section 2.*

2. *Find $20n$ relations. To this purpose, repeatedly select a random vector $\mathbf{e} = (e_1, \ldots, e_n) \in \{0, \ldots E-1\}^n$ and compute the reduced representation $\mathrm{div}(a,b) \sim e_1 P_1 + \cdots + e_n P_n$ until it factors over B as $\mathrm{div}(a,b) = r_1 P_1 + \cdots + r_n P_n$, as explained in Section 2. Then $(r_1 - e_1, \ldots r_n - e_n)^T \in \Gamma$; add this column to M.*

3. *Compute the rank of M. If M does not have full rank, then go to Step (2).*

4. *Otherwise construct $40n \, \mathrm{ld} \, E$ new relations by the procedure described under Step (2).*

5. *Compute the Smith normal form of M.*

Notice that we have made no attempt to write down an algorithm suited for implementation, but that our concern is to simplify the analysis. For instance, in practice it should usually suffice to create about $2n$ relations and the relations should not be obtained randomly, but by sieving techniques. For a description of an implementation based on a sieving approach, see [14].

3.2. **Computing individual logarithms.** To relate $D^{(1)}$ and $D^{(2)}$ to the primes in B, we have to find B-*smooth* divisors $\tilde{D}^{(1)} \sim D^{(1)}$ and $\tilde{D}^{(2)} \sim D^{(2)}$, i.e., divisors which can be decomposed into the primes in B. To do so, we again choose random vectors $\mathbf{e} \in \{0, \ldots E-1\}^n$ until $D^{(1)} + \sum_{i=1}^{n} e_i P_i \sim \sum_{i=1}^{n} r_i P_i$, and let $\tilde{D}^{(1)} = \sum_{i=1}^{n} (r_i - e_i) P_i$; an analogous procedure yields $\tilde{D}^{(2)}$.

Assume that the algorithm of subsection 3.1 has yielded a basis for Γ and that $N \in \mathbb{Z}^{n \times n}$ is the essential part of its Hermite normal form and $\Delta = SN$ its Smith normal form with diagonal entries $d_1 | \cdots | d_n$. Denote by $\mathbf{c}^{(j)}$ the coefficient vector of

$\tilde{D}^{(j)}$ with respect to $P_1, \ldots, P_n$. Then since $\tilde{D}^{(2)} - l\tilde{D}^{(1)} \sim 0$ and the columns of N generate Γ, we know that $\mathbf{c}^{(2)} - l\mathbf{c}^{(1)} \in \operatorname{Im} N$, or equivalently $S\mathbf{c}^{(2)} - lS\mathbf{c}^{(1)} \in \operatorname{Im} \Delta$. Letting $S\mathbf{c}^{(j)} = \mathbf{a}^{(j)} = \left(a_1^{(j)}, \ldots, a_n^{(j)} \right)^T$, this is equivalent to

$$a_i^{(2)} \equiv la_i^{(1)} \pmod{d_i} \quad \text{for } i = 1, \ldots, n,$$

from which l can be determined modulo $h = d_1 \cdots d_n$.

If the algorithm of subsection 3.1 did not succeed in finding a basis of Γ, but only of a sublattice, then the above congruences may or may not have a solution. In the first case the solution is the correct discrete logarithm; otherwise we declare failure and start the whole group structure determination again.

3.3. **Estimating the class number.** It would be helpful in two ways to know the class number h. First, Fermat's Little Theorem implies that $hD \sim 0$ for any degree zero divisor D, so that $E = h$ is a suitable parameter in Step (1) of Algorithm 3.2. Second, the columns of M generate Γ if and only if the determinant of the Smith normal form of M equals h. While, on correct input, our algorithm is guaranteed to output the discrete logarithm, without knowledge of h it will run forever if no discrete logarithm exists.

Unfortunately, to date there is no polynomial time algorithm computing h; notice that Pila's deterministic algorithm [25], often referred to as "polynomial", is so only for fixed g. The same is true for the algorithm described by Huang and Ierardi in [16]. However, an approximation Θ of the class number such that $h \leq \Theta < 2h$ would be a sufficient criterion when enough relations have been collected, since we could stop as soon as the determinant of the Smith normal form no longer exceeds Θ. Such an approximation can probably be obtained using methods analogous to those in [27].

Concerning the maximal exponent E, so far it is only necessary that it be at least the exponent of $J(H)$, which is a divisor of h. We recall a bound on h due to Artin (see [3, §24, Formula (8)]):

Theorem 3.3.

$$h \leq (2g + 1)q^g.$$

In order to ease the analysis of subsection 4.2, we set

$$E = 5(2g + 1)q^g + g > 5h.$$

4. A suitable factor base

To keep our intended time bound for the algorithm, we have to secure two points: First of all, B should be large enough to generate the Jacobian and to achieve a reasonable probability of divisors being B-smooth, i.e., of obtaining new relations. This will be the topic of subsections 4.1 and 4.2. On the other hand, B must be small so as to be easily computable and to keep down the expected number of relations needed. We show in subsection 4.3 that this implies an extra condition on g, namely that it be at least of the order of $\log q$.

4.1. **Generating the Jacobian.** In [24], Müller, Stein and Thiel showed that the ideal class group of a real quadratic congruence function field with finite constant field of odd characteristic is generated by prime ideals of small degree. Their proof is based on the extended Riemann hypothesis, which is true in function fields, and

directly carries over to hyperelliptic Jacobians over any finite field. We cite from [24], Corollary 1, slightly reformulated:

Theorem 4.1. *Let χ be a character of finite order of $\mathrm{Div}(H)$, which is not principal when restricted to $\mathrm{Div}^0(H)$. Then there is a prime divisor P of degree at most $\left\lceil \frac{2\log(4g-2)}{\log q} \right\rceil$ such that $\chi(P) \neq 1$.*

Corollary 4.2. *$J(H)$ is generated by the split and ramified prime divisors of degree at most*

$$\left\lceil 2\log_q(4g-2) \right\rceil.$$

Proof of the corollary. Let U be the subgroup of $J(H)$ generated by the split and ramified prime divisors that match the given degree bound. To show that $U = J(H)$ we have to verify that any nonprincipal character χ of $J(H)$ remains nonprincipal when restricted to U. From $J(H) = \mathrm{Div}^0(H)/\mathrm{Prin}(H)$ we can interpret χ as a nonprincipal character of $\mathrm{Div}^0(H)$, and extending trivially to $\mathrm{Div}(H) \simeq \mathrm{Div}^0(H) \times \mathbb{Z}$ yields a character of finite order of $\mathrm{Div}(H)$. Now by the previous theorem, there is a prime divisor P of degree at most $\left\lceil 2\log_q(4g-2) \right\rceil$ such that $\chi(P) \neq 1$. As the restriction of χ to $\mathrm{Prin}(H)$ is principal and any inert prime divisor lies in $\mathrm{Prin}(H)$, we have $P \in U$, and χ is not principal on U. $\qquad\square$

Hence we fix $B = \{P_1, \ldots, P_n\}$ as the set of split and ramified prime divisors of degree at most C, where $C \geq \left\lceil 2\log_q(4g-2) \right\rceil$ will be determined later. Then since each such prime is of the form $\mathrm{div}(a,b)$ with $\deg a \leq C$, a monic, and to each a correspond at most two values of b, we see that $n \leq 2q^C$.

4.2. **Smooth divisors.** In this section we show that a suitable choice of parameters assures a "reasonable" probability of finding new relations. Denote by N_B the number of B-smooth reduced degree zero divisors. If the randomly generated linear combinations of primes in B were uniformly distributed over all divisor classes, the probability of finding a relation would be $\frac{N_B}{h} \approx \frac{N_B}{q^g}$ (cf. Theorem 3.3; this heuristic will be made rigorous in subsection 5.1). This implies that for a subexponential running time we require $\frac{q^g}{N_B}$ to be subexponential, and to this purpose we must raise B to subexponential size. Precisely, we set

$$C = \left\lceil \log_q L(\rho) \right\rceil$$

for a positive constant ρ to be determined later. Then the following theorem, which is proved in [13], provides the desired result:

Theorem 4.3. *Let $C = \left\lceil \log_q L(\rho) \right\rceil$ for a positive constant ρ, and let B consist of the split and ramified rational prime divisors of degree at most C. Then there is a function $\beta(g)$ in $o(1)$ for $g \to \infty$ such that*

$$N_B \geq L\left(-\frac{1}{2\rho} - \beta(g)\right) q^g.$$

We must check that, with this choice for C, the set B is indeed a factor base, i.e., generates the Jacobian. With respect to Corollary 4.2 it is sufficient to verify if

$$\log_q L(\rho) \geq 2\log_q(4g-2),$$

or equivalently

$$\rho\sqrt{(g\log q)\log(g\log q)} \geq 2\log(4g-2)$$

holds. Taking into account that ρ is a constant and that $q \geq 2$, the equation holds asymptotically for $g \to \infty$.

4.3. **A necessary condition for subexponentiality.** We have claimed that our algorithm is of subexponential running time in the input size $O(g\log q)$. Since B contains $O(q^C)$ elements, a first necessary condition is that q^C be subexponential in $g\log q$. The problem is that we have to round up the value assigned to C for Theorem 4.3 to hold, so that q^C can be (almost) as big as $q^{\log_q L(\rho)+1} = qL(\rho)$. Hence we must assume that q is subexponential in $g\log q$, which can only happen for large g. More precisely, we fix a constant ϑ and consider only the problem instances for which $g \geq \vartheta\log q$. Then we have the following result:

Theorem 4.4. *If* $g \geq \vartheta\log q$, *then* $q \leq L\left(\frac{1}{\sqrt{\vartheta}}\right)$, *and*

$$q^C \leq L\left(\rho + \frac{1}{\sqrt{\vartheta}}\right).$$

Proof.

$$q = e^{\log q} = e^{\frac{1}{\sqrt{\vartheta}}\sqrt{\vartheta(\log q)^2}} \leq e^{\frac{1}{\sqrt{\vartheta}}\sqrt{g\log q}} \leq L\left(\frac{1}{\sqrt{\vartheta}}\right).$$

$\square$

We remark that the authors of [24] treat the case $\vartheta = 1$, but do not take into account that C has to be rounded up. Their assumption that $q^C \in L(\rho + o(1))$ and consequently their running time analysis are, however, asymptotically correct for $g\log q \to \infty$ *and* $\vartheta = g/\log q \to \infty$.

5. The running time of the algorithm

According to Section 4, we make the following conventions: $C = \lceil\log_q L(\rho)\rceil$ for a constant ρ to be determined later in this section and B consists of the split and ramified rational prime divisors of degree at most C. We consider all instances satisfying $g \geq \vartheta\log q$ for a given constant $\vartheta > 0$. Notice that we are interested in asymptotic bounds on the running time of our algorithm for the input size $g\log q$ tending to infinity, and that under the restriction imposed on g this is equivalent to $g \to \infty$.

We first analyse different parts of the algorithm separately before collecting the partial results to determine an overall time bound and to optimise the constant ρ.

5.1. **Finding a relation.** The crucial part of Algorithm 3.2 is the creation of relations in Steps (2) and (4). We argued in subsection 4.2 that the probability of finding a relation is heuristically $\frac{N_B}{h}$, a claim we make precise in this section, using techniques inspired by those in [4] and [27]. In a first step we determine how many exponent vectors $\mathbf{e}$ yield a fixed relation $\mathbf{c}$:

Lemma 5.1. *Let* $\mathbf{c} \in \Gamma$. *Then the number of vectors* $\mathbf{e} \in \{0,\ldots,E-1\}^n$ *which yield the relation* $\mathbf{c}$ *equals the number of B-smooth reduced degree zero divisors* $\sum_{i=1}^r r_iP_i$ *such that* $\mathbf{r} - \mathbf{c} \in \{0,\ldots,E-1\}^n$.

Proof. It follows from the description of the relation generating process in Step (2) of Algorithm 3.2 that $\mathbf{e}$ creates the relation $\mathbf{c}$ if and only if $\mathbf{e} + \mathbf{c}$ is the coefficient vector of a B-smooth reduced degree zero divisor. $\qquad\square$

Since the coefficients of a reduced degree zero divisor are elements of the set $\{0, \ldots, g\}$, the lemma allows us to make a more precise assertion for relations contained in the cubes $W^- = \{g + 1 - E, \ldots, 0\}^n$ and $W^+ = \{1 - E, \ldots, g\}^n$:

Corollary 5.2.
1. *Let $\mathbf{c} \in \Gamma \cap W^-$. Then there are exactly N_B choices for $\mathbf{e} \in \{0, \ldots, E - 1\}^n$ which yield the relation $\mathbf{c}$.*
2. *Let $\mathbf{c} \in \Gamma \cap W^+$. Then there are at most N_B exponent vectors $\mathbf{e} \in \{0, \ldots, E - 1\}^n$ which yield the relation $\mathbf{c}$.*
3. *Let $\mathbf{c} \in \Gamma \backslash W^+$. Then there is no exponent vector $\mathbf{e} \in \{0, \ldots, E - 1\}^n$ which yields the relation $\mathbf{c}$.*

This implies that a uniform choice of $\mathbf{e} \in \{0, \ldots, E - 1\}^n$ yields a relation with probability between

$$\frac{|\Gamma \cap W^-| N_B}{E^n} \quad \text{and} \quad \frac{|\Gamma \cap W^+| N_B}{E^n},$$

and we have to estimate the cardinalities of intersections between a lattice and a cube. This can be done using a theorem due to Lenstra ([19, Lemma 4.1]), which we cite in a slightly different phrasing:

Theorem 5.3. *Let $\Gamma' \subseteq \mathbb{Z}^n$ be a full lattice of determinant h' and W' an axes parallel cube with integral vertices and side length $S - 1$. Then*

$$\frac{1}{h'} \left(1 - \frac{h' - 1}{S}\right) S^n \leq |\Gamma' \cap W'| \leq \frac{1}{h'} \left(1 + \frac{h' - 1}{S}\right) S^n.$$

Applying the theorem to our situation we find that

$$
\begin{aligned}
\frac{|\Gamma \cap W^-|}{E^n} &\geq \frac{\frac{1}{h}\left(1 - \frac{h-1}{E-g}\right)(E - g)^n}{E^n} \\
&= \frac{1}{h}\left(1 - \frac{h-1}{E-g}\right)\left(1 - \frac{g}{E}\right)^n \\
&\geq \frac{1}{h}\left(1 - \frac{1}{5}\right)\left(1 - \frac{g}{10gq^g}\right)^{10q^g \cdot \frac{1}{40}} \\
&\qquad \text{for } E = 5(2g + 1)q^g + g \text{ and } n \leq \frac{1}{4}q^g \\
&\geq \frac{4}{5\sqrt[40]{e}h} \quad \text{where } e \text{ is Euler's constant;}
\end{aligned}
$$

and similarly

$$\frac{|\Gamma \cap W^+|}{E^n} \leq \frac{6\sqrt[40]{e}}{5h}.$$

Thus we have shown the following result:

Theorem 5.4. *If $E = 5(2g + 1)q^g + g$, $\mathbf{e}$ is chosen uniformly from $\{0, \ldots, E - 1\}^n$ and g is large enough, then the probability of finding a relation lies between*

$$\frac{4}{5\sqrt[40]{e}h} N_B \quad \text{and} \quad \frac{6\sqrt[40]{e}}{5h} N_B;$$

it is bounded below by a function in

$$\frac{4}{5\,\sqrt[40]{e}(2g+1)}L\left(-\frac{1}{4\rho}-o(1)\right).$$

Proof. The first assertion has been proved above; notice that the condition $n \le \frac{1}{4}q^g$ is asymptotically fulfilled for $g \to \infty$. For the second assertion substitute the results of Theorems 3.3 and 4.3 into the lower bound. $\square$

5.2. **Linear algebra.** Since we are dealing with matrices of subexponential size, we must make sure that all matrix operations involved take time polynomial in the sizes of the matrices and their entries. Moreover, the exact exponents of the polynomial time bounds for the matrix operations have a direct impact on the constant of the subexponential time bound for the algorithm. Hence a judicious arrangement of the computations is necessary. We need the following results:

Theorem 5.5. *Let* $A = (a_{ij}) \in \mathbb{Z}^{n \times m}$ *with* $m \ge n$ *and*

$$|A| = \max\{|a_{ij}| : i = 1, \dots, n,\ j = 1, \dots, m\}.$$

1. *The rank of* A *can be determined in time* $O(m^2 n^2 \log^2(n|A|))$.
2. *If* A *has rank* n, *then its Hermite normal form can be computed in time* $O(mn^2(n^2 + m) \log^2(n|A|))$.
3. *If* $N \in \mathbb{Z}^{n \times n}$ *is the essential part of the Hermite normal form of* A, *then computing the Smith normal form takes time in* $O(n^3 \log^4(|N|))$.

Proof.   1. See [23, Satz 3.9].
2. It is straightforward to see that the Hermite normal form of A can be computed by unimodular transformations with a polynomial number of arithmetic operations. This naïve approach, however, involves intermediate results of possibly exponential size. To remedy to this problem, Domich, Kannan and Trotter described an algorithm using modular arithmetics [8]. It was analysed in detail by Müller (see [23, Satz 4.12]).
3. See [9, Satz 3.29].

$\square$

5.3. **Expected time for one run.** In this section we determine the expected time needed for one run of the algorithm, assuming that each step is executed only once and no jump back to Step (2) is required.

In the first step, we have to compute the factor base B as described in Section 2. The irreducible polynomials of degree at most C are enumerated by trial divisions of all $O(q^C)$ monic polynomials of degree at most C by the $O(q^{C-1})$ monic polynomials of smaller degree. Compared to this, the cost of solving a quadratic equation modulo each of the resulting irreducible polynomials is negligible. So the bit complexity of the first step is in

$$
\begin{aligned}
O\left((C^2 \log^2 q)q^{2C-1}\right) &\subseteq O\left((C^2 \log^2 q)L\left(2\rho + \frac{1}{\sqrt{\vartheta}}\right)\right) \\
&\subseteq O\left(L\left(2\rho + \frac{1}{\sqrt{\vartheta}} + o(1)\right)\right)
\end{aligned}
$$

by Theorem 4.4. Here $o(1)$ is a function of g and q which tends to zero for $g \log q \to \infty$; it is needed to neutralise the effect of the factor $C^2 \log^2 q$, which is polynomial in $g \log q$.

From Theorem 5.4 we know that the expected number of trials for finding a relation is bounded above by $\frac{5}{4}\sqrt[40]{e}(2g + 1)L\left(\frac{1}{2\rho}\right) \in O\left(L\left(\frac{1}{2\rho} + o(1)\right)\right)$. Each trial amounts to computing a linear combination of prime divisors by $O(n \log E)$ polynomial operations and to factoring a polynomial of degree at most g in expected polynomial time. Since $\log E$ is polynomial in the input size, the expected time bound for Step (2) is $O\left(n^2 L\left(\frac{1}{2\rho} + o(1)\right)\right) \subseteq O\left(L\left(2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + \frac{1}{2\rho} + o(1)\right)\right)$.

By Theorem 5.5 (1) the rank of the relation matrix M can be computed in time $O\left(L\left(4\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + o(1)\right)\right)$. We assume that M has full rank, the probability for this event being evaluated in the next section. The expected time bound for computing the additional relations in Step (4) is again in $O\left(L\left(2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + \frac{1}{2\rho} + o(1)\right)\right)$. The Smith normal form of the new relation matrix can be determined in time $O\left(L\left(5\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + o(1)\right)\right)$ by Theorem 5.5 (2) and (3).

Smoothing the divisors $D^{(j)}$ as described in subsection 3.2 is performed in expected time $O\left(L\left(\rho + \frac{1}{\sqrt{\vartheta}} + \frac{1}{2\rho} + o(1)\right)\right)$; this follows from arguments analogous to those of subsection 5.1. With the notation of subsection 3.2, computing $\mathbf{a}^{(1)}$ and $\mathbf{a}^{(2)}$ and solving the system of equations modulo the d_i takes time in $O\left(L\left(2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + o(1)\right)\right)$.

It follows that the complexity of one complete run of the algorithm is in

$$O\left(L\left(\max\left\{5\left(\rho + \frac{1}{\sqrt{\vartheta}}\right), 2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + \frac{1}{2\rho}\right\} + o(1)\right)\right).$$

5.4. **Probability of success.** While we have seen in subsection 5.1 that there is a positive probability of finding relations, there is no guarantee that a new relation is not already contained in the lattice generated so far. Hence there is a small chance that the $20n$ relations created in Step (2) of Algorithm 3.2 do not generate a full lattice.

Formally, assume that during the algorithm we have generated a sublattice Γ_1 of Γ of dimension less than n, and let $\mathbf{c}$ be a further relation as determined in Step (2). We call $\mathbf{c}$ *useful* if it increases the dimension of Γ_1, and it is our aim to determine the probability that a newly created relation is useful.

Denote by $\Gamma_2 \subsetneq \Gamma$ a full sublattice which contains $\mathbb{Q}\Gamma_1 \cap \Gamma$. Then all relations outside Γ_2 are useful, and the probability of finding a relation within Γ_2 is by Corollary 5.2 bounded above by

$$\frac{|\Gamma_2 \cap W^+|}{E^n}N_B \quad \leq \quad \frac{1}{kh}\left(1 + \frac{kh - 1}{E + g}\right)\left(\frac{E + g}{E}\right)^n N_B$$
$$\text{by Theorem 5.3, where } k \geq 2 \text{ is the index of } \Gamma_2 \text{ in } \Gamma$$
$$\leq \quad \frac{7\sqrt[40]{e}}{10h}N_B$$

by arguments analogous to those used in the proof of Theorem 5.4.

Hence the conditional probability that a newly found relation is useless, which is the probability of finding a useless relation divided by the probability of finding any relation, is bounded above by $\frac{7\sqrt[40]{e}}{10h}/\frac{4}{5\sqrt[40]{e}h} = \frac{7\sqrt[20]{e}}{8} < \frac{18}{19}$ according to Theorem 5.4, and the probability that a newly found relation is useful is at least $1/19$.

We can now prove the following theorem:

Theorem 5.6. *The probability of success for one run of the algorithm is asymptotically 1 for $g \log q \to \infty$, whence it has to be repeated an expected $O(1)$ times.*

Proof. We first compute the probability that the matrix M obtained after Step (2) has full rank, which is equivalent to saying that n of the $20n$ relations computed are useful. Let X denote a Binomial$(20n, 1/19)$-distributed random variable. By the discussion above, the probability that M has full rank is at least

$$
\begin{aligned}
P(X \geq n) &\geq 1 - P\left(\left|X - \frac{20}{19}n\right| \geq \frac{1}{19}n\right) \\
&\geq 1 - \frac{\mathrm{Var}(X)}{\frac{1}{361}n^2}
\end{aligned}
$$

by Tschebyscheff's inequality (see any statistics textbook). Since $\mathrm{Var}(X) = \frac{360}{361}n$, the matrix M has full rank with probability at least $1 - \frac{360}{n}$, which tends to 1 for $g \log q \to \infty$.

A similar reasoning applies to Step (4). Now let the full lattice $\Gamma_2 \subsetneq \Gamma$ be already generated, and call a relation useful if it decreases the index of Γ_2 in Γ. Then the same reasoning as above shows that a new relation is useful with probability at least $1/19$. We now have to estimate the number of useful relations needed to find a generating system of Γ. Let Γ_1 be the lattice obtained in Step (2). Then the number of useful relations needed for Γ is bounded above by

$$
\mathrm{ld}[\Gamma : \Gamma_1] = \mathrm{ld}(\det \Gamma_1) - \mathrm{ld}(\det \Gamma) \leq \mathrm{ld}(\det \Gamma_1).
$$

From the description of the relation collecting phase in Algorithm 3.2 we know that all relations constructed lie in the cube $\{1 - E, \ldots, g\}^n$. Now Hadamard's upper bound shows that $\det \Gamma_1 \leq (\sqrt{n}E)^n \leq E^{2n}$ at least asymptotically since n is subexponential and E exponential in $g \log q$. Hence,

$$
\mathrm{ld}(\det \Gamma_1) \leq 2n \, \mathrm{ld} \, E
$$

for $g \log q$ large enough. Simulating the creation of relations again by a binomially distributed variable shows that the probability of obtaining a generating system is asymptotically 1 for $g \log q \to \infty$. $\qquad\square$

5.5. Optimising the parameter ρ.

The analysis of the previous sections shows that the expected running time of the algorithm is in

$$
O\left(L\left(\max\left\{5\left(\rho + \frac{1}{\sqrt{\vartheta}}\right), 2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + \frac{1}{2\rho}\right\} + o(1)\right)\right).
$$

Hence we have to minimise the function

$$
f : \rho \mapsto \max\left\{5\left(\rho + \frac{1}{\sqrt{\vartheta}}\right), 2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + \frac{1}{2\rho}\right\}
$$

subject to $\rho > 0$. This function is unimodal and thus has a unique global minimum.

The strictly convex function $\rho \mapsto 2\left(\rho + \frac{1}{\sqrt{\vartheta}}\right) + \frac{1}{2\rho}$ admits its unique global minimum at

$$
\overline{\rho} = \frac{1}{2}.
$$

Both functions have the same value for

$$
\rho^*(\vartheta) = \frac{1}{\sqrt{6}}\left(\sqrt{1 + \frac{3}{2\vartheta}} - \sqrt{\frac{3}{2\vartheta}}\right).
$$

Hence f admits its unique minimum at $\min\{\overline{\rho}, \rho^*(\vartheta)\}$. (This can easily be veri-
fied by drawing two generic pictures corresponding to $\overline{\rho} < \rho^*(\vartheta)$ and $\overline{\rho} \geq \rho^*(\vartheta)$,
respectively.) Since $\overline{\rho} > \rho^*(\vartheta)$ for all positive values of ϑ, this proves Theorem 1.1.

Acknowledgments

References

[1] Leonard M. Adleman, Jonathan DeMarrais, and Ming-Deh Huang, *A subexponential algo-
rithm for discrete logarithms over the rational subgroup of the Jacobians of large genus
hyperelliptic curves over finite fields*, Lecture Notes in Comput. Sci., 877, Springer, Berlin,
1994, pp. 28–40. MR **96b:**11078

[2] Leonard M. Adleman and Ming-Deh Huang (eds.), *Algorithmic number theory*, Lecture Notes
in Comput. Sci., 877, Springer-Verlag, Berlin, 1994. MR **95j:**11119

[3] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen II*, Math. Z. **19** (1924),
207–246.

[4] Johannes Buchmann, *A subexponential algorithm for the determination of class groups and
regulators of algebraic number fields*, Progr. Math. 91, Birkhäuser, Boston, 1990, pp. 27–41.
MR **92g:**11125

[5] David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987),
no. 177, 95–101. MR **88f:**11118

[6] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math.,
Springer-Verlag, Berlin, 1993. MR **94i:**11105

[7] Henri Cohen (ed.), *Algorithmic number theory — Ants-II*, Lecture Notes in Comput. Sci.,
vol. 1122, Springer-Verlag, Berlin, 1996. MR **97k:**11001

[8] P. D. Domich, R. Kannan, and L. E. Trotter Jr., *Hermite normal form computation using
modulo determinant arithmetic*, Math. Oper. Res. **12** (1987), no. 1, 50–59. MR **88e:**65047

[9] Stephan Düllmann, *Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter
binärer quadratischer Formen*, Dissertation, Universität des Saarlandes, Saarbrücken, 1991.

[10] Andreas Enge, *The extended Euclidian algorithm on polynomials, and the computational ef-
ficiency of hyperelliptic cryptosystems*, Des. Codes Cryptogr., 23 (2001), 53–74. CMP 2001:11

[11] ———, *Hyperelliptic cryptosystems: Efficiency and subexponential attacks*, Dissertation,
Universität Augsburg, 2000, ISBN 3-8311-1868-X.

[12] ———, *How to distinguish hyperelliptic curves in even characteristic*, to appear in *Pro-
ceedings of the Conference on Public Key Cryptography and Computational Number Theory*,
Warszawa 2000.

[13] Andreas Enge and Andreas Stein, *Smooth ideals in hyperelliptic function fields*, Math. Comp.,
posted on October 4, 2001, PII S0025-5718(01)01352-7 (to appear in print).

[14] Ralf Flassenberg and Sachar Paulus, *Sieving in function fields*, Experiment. Math. **8** (1999),
no. 4, 339–349. MR **2000j:**11179

[15] Catherine Goldstein (ed.), *Séminaire de théorie des nombres, Paris 1988–1989*, Progress in
Mathematics, Birkhäuser, Boston, 1990. MR **91k:**11004

[16] Ming-Deh Huang and Doug Ierardi, *Counting points on curves over finite fields*, J. Symbolic
Comput. **25** (1998), 1–21. MR **98i:**11040

[17] Neal Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150. MR **90k:**11165

[18] ———, *Algebraic aspects of cryptography*, Algorithms Comput. Math., vol. 3, Springer-
Verlag, Berlin, 1998. MR **2000a:**94012

[19] A. K. Lenstra, *Fast and rigorous factorization under the generalized Riemann hypothesis*,
Nederl. Akad. Wetensch. Indag. Math. **50** (1988), 443–454. MR **90a:**11152

[20] Kevin S. McCurley, *Cryptographic key distribution and computation in class groups*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 459–479. MR **92e:**11149

[21] Alfred J. Menezes, Yi-Hong Wu, and Robert J. Zuccherato, *An elementary introduction to hyperelliptic curves*, Springer-Verlag, 1998, pp. 155–178. MR **2000a:**94012

[22] Richard A. Mollin (ed.), *Number theory and applications*, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 265, Kluwer Acad. Publ., Dordrecht, 1989. MR **92c:**11002

[23] Achim Müller, *Effiziente Algorithmen für Probleme der linearen Algebra über $\mathbb{Z}$*, Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1994.

[24] Volker Müller, Andreas Stein, and Christoph Thiel, *Computing discrete logarithms in real quadratic congruence function fields of large genus*, Math. Comp. **68** (1999), no. 226, 807–822. MR **99i:**11119

[25] J. Pila, *Frobenius maps of Abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), no. 192, 745–763. MR **91a:**11071

[26] Bjorn Poonen, *Computational aspects of curves of genus at least* 2, Lecture Notes in Comput. Sci., 1122, Springer, Berlin, 1996, pp. 283–306. MR **98c:**11059

[27] Andreas Stein, *Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern*, Dissertation, Universität des Saarlandes, Saarbrücken, 1996.

MATHEMATISCHES INSTITUT, UNIVERSITÄT AUGSBURG, 86135 AUGSBURG, GERMANY
E-mail address: `enge@math.uni-augsburg.de`
URL: `www.math.uni-augsburg.de/~enge`
Current address: LIX, École Polytechnique, 91128 Palaiseau Cedex, France
E-mail address: `enge@lix.polytechnique.fr`