Generalised Jacobians in Cryptography and Coding Theory

Florian Hess

Carl-von-Ossietzky Universität Oldenburg, Germany
http://www.staff.uni-oldenburg.de/florian.hess

Abstract. The use of generalised Jacobians in discrete logarithm based cryptosystems has so far been rather limited since they offer no advantage over traditional discrete logarithm based systems. In this paper we continue the search for possible applications in two directions.
Firstly, we investigate pairings on generalised Jacobians and show that these are insecure. Secondly, generalising and extending prior work, we show how the discrete logarithm problem in generalised Jacobians can be reduced to the minimal non zero weight word and maximum likelihood decoding problems in generalised algebraic geometric codes.

1 Introduction and Summary

The multiplicative group of finite fields and the point groups of Jacobian varieties of regular algebraic curves over finite fields, in particular point groups of elliptic curves, are the essential traditional building blocks of discrete logarithm based cryptography. Generalised Jacobian varieties of regular algebraic curves over finite fields can be thought of a combination of both of these traditional building blocks into one mathematical structure. Their use in cryptography has first been suggested in [6]. Soon thereafter, the lack in efficiency in comparison with multiplicative groups of finite fields and point groups of Jacobian varieties has been discussed in [10] and [7]. As a consequence, the use of generalised Jacobians in discrete logarithm based cryptosystems has so far been rather limited. In this paper we continue the search for possible interesting and useful applications of generalised Jacobians in two directions.

The first direction concerns pairings. Pairings have been a major topic in cryptography over the past decade. The only known generally suitable pairings are the Weil and Tate-Lichtenbaum pairings on Jacobians, and these pairings are bilinear. The construction of pairings in different mathematical contexts and the construction of multilinear pairings are important open research problems. Motivated by this we investigate a generalised form of the Tate-Lichtenbaum pairing on generalised Jacobians. As it turns out, these pairings are efficiently computable and also yield multilinear pairings. On the other hand we also have to show that the domain of these pairings suffers from a weak discrete logarithm problem, whence we do not get a useful application to cryptography.

The second direction concerns reductions of discrete logarithm problems to code based problems. Motivated by [3, 5] we define some generalised algebraic-geometric codes and show how the discrete logarithm problem in generalised Jacobians can be reduced to the minimal non zero weight word problem and to the maximum likelihood decoding problem in these generalised algebraic-geometric codes. An essential element of this reduction is the construction of efficient sets of generators for generalised Jacobians. Following the methodology of [17] we prove a theorem on the existence (and efficient construction) of such efficient sets of generators. The discrete logarithm reductions of [3, 5] then turn out to be essentially special cases of our general reduction.

The implication of the discrete logarithm reductions are not so clear at the moment. One point of view is that we obtain hardness results for the above mentioned code based computational problems. In this direction a further study of efficient generating sets and of special high genus curves could be of interest for the construction of codes over $\mathbb{F}_q$ with small q and large lower complexity bounds for the minimal non zero word or maximum likelihood decoding problems. Another point of view is that efficient algorithms for solving these code based computational problems might speed up algorithms for computing discrete logarithms. This latter point of view is for example taken in [1].

A different, but related way of combining the multiplicative group of finite fields and the point groups of Jacobian varieties of regular algebraic curves over finite fields into one mathematical structure is to consider Jacobians of singular algebraic curves over finite fields. This approach is taken in [18] where it is shown that one can achieve a compressed representation of finite fields elements from certain subgroups in this way. We do not consider Jacobians of singular curves in this paper though.

2 Preliminaries

Let C be an absolutely irreducible complete regular curve defined over the finite field $\mathbb{F}_q$ of characteristic p. The function field of C is denoted by $\kappa(C)$ and the genus of C by g.

We consider divisors as finite sums of places (closed points) of C. Let $\mathfrak{m}$ be an effective divisor of C. The group of divisors of C coprime to $\mathfrak{m}$ is denoted by $\mathcal{D}^{\mathfrak{m}}(C)$, and the subgroup of $\mathcal{D}^{\mathfrak{m}}(C)$ of principal divisors by $\mathcal{P}^{\mathfrak{m}}(C)$. Let $f \in \kappa(C)^{\times}$. Then by definition $f \equiv 1 \bmod \mathfrak{m}$ if $\mathrm{ord}_{\mathfrak{p}}(f-1) \geq 1$ for all $\mathfrak{p} \in \mathrm{supp}(\mathfrak{m})$. The ray modulo $\mathfrak{m}$ is defined as

$$\mathcal{P}_{\mathfrak{m}}(C) = \{f \in \kappa(C)^{\times} \mid f \equiv 1 \bmod \mathfrak{m}\}.$$

The ray class group modulo $\mathfrak{m}$ is

$$\mathrm{Pic}_{\mathfrak{m}}(C) = \mathcal{D}^{\mathfrak{m}}(C)/\mathcal{P}_{\mathfrak{m}}(C)$$

and the degree zero ray class group modulo $\mathfrak{m}$ is

$$\mathrm{Pic}^0_{\mathfrak{m}}(C) = \{y \in \mathrm{Pic}_{\mathfrak{m}}(C) \mid \deg(y) = 0\}.$$

The generalised Jacobian of C modulo $\mathfrak{m}$ is a semi-abelian variety $\mathrm{Jac}_{\mathfrak{m}}(C)$ that represents the functor $k \mapsto \mathrm{Pic}^0_{\mathfrak{m}}(C \times k)$ from $\mathbb{F}_q$-algebras to finite abelian groups. The generalised Jacobian $\mathrm{Jac}_{\mathfrak{m}}(C)$ exists for any C and $\mathfrak{m}$, see [20]. In this paper we will not (directly) use the geometric structure of $\mathrm{Jac}_{\mathfrak{m}}(C)$, and thus will essentially only consider the groups $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ and $\mathrm{Pic}_{\mathfrak{m}}(C)$. For $\mathfrak{m} = 0$ we have $\mathrm{Jac}_{\mathfrak{m}}(C) = \mathrm{Jac}(C)$, $\mathrm{Pic}^0_{\mathfrak{m}}(C) = \mathrm{Pic}^0(C)$ and $\mathrm{Pic}_{\mathfrak{m}}(C) = \mathrm{Pic}(C)$ as usual.

By the approximation theorem there is an exact sequence

$$1 \to \mathbb{F}_q^\times \to \prod_{\mathfrak{p} \in \mathrm{supp}(\mathfrak{m})} \left(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}\right)^\times \to \mathrm{Pic}^0_{\mathfrak{m}}(C) \to \mathrm{Pic}^0(C) \to 1. \quad (1)$$

Moreover,

$$\left(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}\right)^\times \cong \kappa(\mathfrak{p})^\times \times (1+\mathfrak{p})/(1+\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}), \quad (2)$$

where $\kappa(\mathfrak{p}) = \mathcal{O}_{C,\mathfrak{p}}/\mathfrak{p}$ is the residue class field of $\mathfrak{p}$ and $(1+\mathfrak{p})/(1+\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})})$ is a p-group. Some details about these definitions and facts can be found in [15].

In discrete logarithm based cryptography one considers cyclic groups G of prime order ℓ that are embedded into suitable algebraic groups. The standard cases are

$$G \subseteq \mathbb{G}_m(\mathbb{F}_q) = \mathbb{F}_q^\times, \text{ and } G \subseteq \mathrm{Jac}(C)(\mathbb{F}_q) \text{ or } G \subseteq \mathrm{Pic}^0(C)$$

respectively. The use of

$$G \subseteq \mathrm{Jac}_{\mathfrak{m}}(C)(\mathbb{F}_q)$$

has first been suggested in [6]. Since the group laws and maps in (1) and (2) are effective and G has prime order, this case leads to an effectively computable isomorphism $\phi : G \to H$ with either

$$H \subseteq \mathrm{Jac}(C)(\mathbb{F}_q),\ H \subseteq \mathbb{G}_m(\kappa(\mathfrak{p})) \text{ or } H \subseteq (1+\mathfrak{p})/(1+\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})})$$

for some $\mathfrak{p} \in \mathrm{supp}(\mathfrak{m})$. Since the discrete logarithm problem in $(1+\mathfrak{p})/(1+\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})})$ is easy (see for example [15]) the use of $G \subseteq \mathrm{Jac}_{\mathfrak{m}}(C)(\mathbb{F}_q)$ offers no advantage over the standard cases in terms of efficiency and security. This argumentation is carried out in more detail in [10]. For a discussion from a slightly different point of view see [7].

On the other hand, given $G \subseteq \mathbb{G}_m(\kappa(\mathfrak{p}))$ there can exist efficiently computable isomorphisms $\phi : G \to H$ with $H \subseteq \mathrm{Jac}_{\mathfrak{m}}(C)(\mathbb{F}_q)$ or $H \subseteq \mathrm{Pic}^0_{\mathfrak{m}}(C)$ respectively. Such H are embedded in a context with richer or at least different structure than the context of G. In the following we investigate whether this structure can be used to obtain some new features relevant for cryptography or coding theory.

3 Pairings on Generalised Jacobians

Class field theory yields arithmetic duality pairings on generalised Jacobians. In this section we argue that these pairings indeed yield efficiently computable

pairings different from the pairings that have been used in cryptography so far. These pairings can even be applied iteratively, resulting in multilinear pairings. As demonstrated in [2, 19], non-degenerate multilinear pairings would be of great interest in cryptography, but no suitable such pairings have been found so far.

Unfortunately, we also have to argue that the domains of these pairings suffer from a weak discrete logarithm problem. The construction is thus not suitable for cryptography.

The construction of multilinear pairings is also discussed in [16] using a different approach. Contrary to our case, the obstacle in this work appears to be the efficient computability of the pairing.

3.1 A Generalised Tate-Lichtenbaum Pairing

Let n be a prime number such that $q \equiv 1 \bmod n$ and abbreviate $F = \kappa(C)$. Let

$$\mathrm{Sel}_{n,\mathfrak{m}}(C) = \{f \in F^\times \mid \mathrm{ord}_\mathfrak{p}(f) \equiv 0 \bmod n \text{ for all places } \mathfrak{p} \notin \mathrm{supp}(\mathfrak{m})\}$$

and denote the group of n-th root of unity of $\mathbb{F}_q^\times$ by μ_n. Class field theory yields the existence of a surjective pairing

$$\pi_\mathfrak{m} : \mathrm{Sel}_{n,\mathfrak{m}}(C) \times \mathrm{Pic}^0_\mathfrak{m}(C) \to \mu_n.$$

The left and right kernel of this pairing are $\mathbb{F}_q^\times \cdot (F^\times)^n$ and $n \cdot \mathrm{Pic}^0_\mathfrak{m}(C)$ respectively. Factoring out kernels thus yields a non-degenerate pairing

$$\pi'_\mathfrak{m} : \mathrm{Sel}_{n,\mathfrak{m}}(C) \,/\, \mathbb{F}_q^\times \cdot (F^\times)^n \times \mathrm{Pic}^0_\mathfrak{m}(C) \,/\, n \cdot \mathrm{Pic}^0_\mathfrak{m}(C) \to \mu_n.$$

A result of Hasse [12] on the algebraic representation of the Artin map gives an algebraic representation of the images under these pairings by means of function evaluation. The details of this are as follows.

Let $\mathfrak{d} = \sum_i \lambda_i \mathfrak{p}_i$ be a divisor of C where the $\mathfrak{p}_i$ are places. If $f \in F$ is a function with no pole at the place $\mathfrak{p}$ then $f + \mathfrak{p}$ denotes the image of f in the residue class field $\kappa(\mathfrak{p}) = \mathcal{O}_{C,\mathfrak{p}}/\mathfrak{p}$. Using the norm map $\mathrm{N}_{\kappa(\mathfrak{p}_i)/\mathbb{F}_q}$ of the extension $\kappa(\mathfrak{p}_i)/\mathbb{F}_q$ we can define an evaluation at divisors via

$$f(\mathfrak{d}) := \prod_i \mathrm{N}_{\kappa(\mathfrak{p}_i)/\mathbb{F}_q}(f + \mathfrak{p}_i)^{\lambda_i},$$

provided f has no zero at $\mathfrak{p}_i$ when $\lambda_i < 0$ and no pole when $\lambda_i > 0$. The evaluation map is multiplicative in f and additive in $\mathfrak{d}$.

Let $x = f \in \mathrm{Sel}_{n,\mathfrak{m}}(C)$ and $y = \mathfrak{d} + \mathcal{P}_\mathfrak{m}(C) \in \mathrm{Pic}^0_\mathfrak{m}(C)$. By the approximation theorem applied to f or $\mathfrak{d}$, f can be chosen modulo $(F^\times)^n$ or $\mathfrak{d}$ modulo $\mathcal{P}_\mathfrak{m}(C)$ such that $\mathrm{supp}(f) \cap \mathrm{supp}(\mathfrak{d}) = \emptyset$. Then

$$\pi_\mathfrak{m}(x, y) = f(\mathfrak{d})^{(q-1)/n}.$$

This definition also allows an efficient computation of $\pi_\mathfrak{m}(x, y)$. Using

$$\mathrm{Sel}_{n,0}(C)/\mathbb{F}_q^\times \cdot (F^\times)^n \cong \mathrm{Pic}^0(C)[n]$$

under $f \cdot \mathbb{F}_q^\times \cdot (F^\times)^n \mapsto \frac{1}{n}\mathrm{div}(f) + \mathcal{P}_0(C)$ we see that π_0 is essentially the usual Tate-Lichtenbaum pairing as discussed in [9, 14] and widely used in cryptography.

3.2 Variations – New Bilinear and Multilinear Pairings

The case $\mathrm{supp}(\mathfrak{m}) = \{\}$ essentially yields the usual and well known Tate-Lichtenbaum pairing. Next suppose $\mathrm{supp}(\mathfrak{m}) = \{\mathfrak{p}\}$. If $\deg(\mathfrak{p}) \not\equiv 0 \bmod n$ then the group $\prod_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} \left(\mathcal{O}_{C,\mathfrak{p}}/\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})}\right)^{\times}$ does not contain elements of n-power order other than those coming from $\mathbb{F}_q^{\times}$, and by (1) we are again reduced to the case of a Tate-Lichtenbaum pairing. If on the other hand $\deg(\mathfrak{p}) \equiv 0 \bmod n$ then $\pi_{\mathfrak{m}}$ cannot be efficiently computed anymore for cryptographic sizes of n.

So suppose now $\#\mathrm{supp}(\mathfrak{m}) \geq 2$. Then there are various choices of monomorphisms

$$\chi : \mu_n \to \mu_n^{\mathrm{supp}(\mathfrak{m})} = \prod_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} \mu_n$$

that extend according to $\mu_n \subseteq \mathbb{F}_q^{\times} \subseteq \kappa(\mathfrak{p})^{\times}$, (1) and (2) to monomorphisms

$$\phi : \mu_n \to \mathrm{Pic}^0_{\mathfrak{m}}(C).$$

If χ or C are suitably chosen, for example such that $\#\mathrm{Pic}^0(C) \not\equiv 0 \bmod n$, then we can also have that ϕ extends further to a monomorphism

$$\phi' : \mu_n \to \mathrm{Pic}^0_{\mathfrak{m}}(C) \,/\, n \cdot \mathrm{Pic}^0_{\mathfrak{m}}(C).$$

We obtain a surjective pairing

$$\psi : \mathrm{Sel}_{n,\mathfrak{m}}(C) \times \mu_n \to \mu_n$$

given by $\psi(x, y) = \pi_{\mathfrak{m}}(x, \phi(y))$. The right kernel is zero and the left kernel is a subgroup U with $U \supseteq \mathbb{F}_q^{\times} \cdot (F^{\times})^n$. Factoring out U yields a non-degenerate pairing

$$\psi' : \mathrm{Sel}_{n,\mathfrak{m}}(C)/U \times \mu_n \to \mu_n.$$

This pairing has the remarkable feature that pairing values can serve as second arguments. The r-fold iterated combination gives rise to a non-degenerate multilinear pairing

$$\psi'_r : \mathrm{Sel}_{n,\mathfrak{m}}(C)/U \times \cdots \times \mathrm{Sel}_{n,\mathfrak{m}}(C)/U \times \mu_n \to \mu_n$$

in $r + 1$ arguments.

The pairing ψ'_r is efficiently computable if the arguments from $\mathrm{Sel}_{n,\mathfrak{m}}(C)/U$ are for example represented as elements from $F^{\times}$ in a compact representation as power product of elements of $F^{\times}$ of small degree (see for example [13]).

3.3 Weak Discrete Logarithm Problem in the Domain

Suppose that the elements of $\mathrm{Sel}_{n,\mathfrak{m}}(C)/U$ are given by representatives in the group $\mathrm{Sel}_{n,\mathfrak{m}}(C)$. We will now argue that $\mathrm{Sel}_{n,\mathfrak{m}}(C)/U$ then has weak discrete logarithm problem. This implies, unfortunately, that the pairings ψ and ψ' are not useful in cryptography. A consequence of [11] is that all homomorphisms

$\mathrm{Sel}_{n,\mathfrak{m}}(C)/U \to \mu_n$, defined by their image on a generator, would necessarily be efficiently computable as well. This already hints a weak discrete logarithm problem.

We introduce some convenient notation. If $\zeta = (\zeta_\mathfrak{p})_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} \in \mu_n^{\mathrm{supp}(\mathfrak{m})}$ and $x = (x_\mathfrak{p})_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} \in \mathbb{Z}^{\mathrm{supp}(\mathfrak{m})}$ then let

$$\zeta^x = \prod_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} \zeta_\mathfrak{p}^{x_\mathfrak{p}} \in \mu_n.$$

If $f \in F^\times$ then let $\mathrm{ord}(f) = (\mathrm{ord}_\mathfrak{p}(f)\deg(\mathfrak{p}))_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})}$.

Theorem 1 *Let $f \in \mathrm{Sel}_{n,\mathfrak{m}}(C)$ and $\zeta \in \mu_n$. Then*

$$\psi(f,\zeta) = \chi(\zeta)^{\mathrm{ord}(f)}.$$

Proof. Let $\phi(\zeta) = \mathfrak{d} + \mathcal{P}_\mathfrak{m}(C)$. A closer look at the third map in (1) shows that $\mathfrak{d} = \mathrm{div}(g)$ for some $g \in F^\times$ with $g \equiv \chi_\mathfrak{p}(\zeta) \bmod \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{supp}(\mathfrak{m})$. Then

$$\psi(f,\zeta) = f(\mathfrak{d})^{(q-1)/n} = f(\mathrm{div}(g))^{(q-1)/n} = g(\mathrm{div}(f))^{(q-1)/n},$$

where the last equality holds by Weil reciprocity. Furthermore

$$g(\mathfrak{p}) = \mathrm{N}_{\kappa(\mathfrak{p})/\mathbb{F}_q}(\chi_\mathfrak{p}(\zeta)) = \chi_\mathfrak{p}(\zeta)^{\deg(\mathfrak{p})}$$

since $\chi_\mathfrak{p}(\zeta) \in \mathbb{F}_q$. Now $\mathrm{ord}_\mathfrak{p}(f) \equiv 0 \bmod n$ for all $\mathfrak{p} \notin \mathrm{supp}(\mathfrak{m})$, so we get

$$\begin{aligned} g(\mathrm{div}(f))^{(q-1)/n} &= \prod_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} g(\mathfrak{p})^{\mathrm{ord}_\mathfrak{p}(f)} = \prod_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{m})} \chi_\mathfrak{p}(\zeta)^{\mathrm{ord}_\mathfrak{p}(f)\deg(\mathfrak{p})} \\ &= \chi(\zeta)^{\mathrm{ord}(f)} \end{aligned}$$

as desired.

The ord map can be seen as a homomorphism

$$\mathrm{ord} : \mathrm{Sel}_{n,\mathfrak{m}}(C) \to \mathbb{Z}^{\mathrm{supp}(\mathfrak{m})}.$$

Let $G = \mathrm{ord}(\mathrm{Sel}_{n,\mathfrak{m}}(C))$ and $H = \mathrm{ord}(U)$. Since $\ker(\mathrm{ord}) \subseteq U$ by Theorem 1 it is clear that

$$\mathrm{Sel}_{n,\mathfrak{m}}(C)/U \;\cong\; G/H \tag{3}$$

via ord and that ψ is equivalent using ord to the pairing

$$\omega : G \times \mu_n \to \mu_n, \quad (x,\zeta) \mapsto \chi(\zeta)^x$$

with right kernel one and left kernel H. We can extend ω to the pairing

$$\omega_1 : \mathbb{Z}^{\mathrm{supp}(\mathfrak{m})} \times \mu_n \to \mu_n, \quad (x,\zeta) \mapsto \chi(\zeta)^x$$

with right kernel one and left kernel denoted by H_1. Then $H = G \cap H_1$ and

$$G/H \;\cong\; \mathbb{Z}^{\mathrm{supp}(\mathfrak{m})}/H_1 \tag{4}$$

via the inclusion $G \subseteq \mathbb{Z}^{\mathrm{supp}(\mathfrak{m})}$. Now H_1 can be easily computed from χ and the factor group $\mathbb{Z}^{\mathrm{supp}(\mathfrak{m})}/H_1$ has a weak discrete logarithm problem. Combining the effective isomorphisms of (3) and (4) shows that $\mathrm{Sel}_{n,\mathfrak{m}}(C)/U$ has weak discrete logarithm problem. We thus conclude that these pairings are indeed not useful in cryptography.

4 Lower Complexity Bounds for Codes

We continue the quest for a useful application of generalised Jacobians looking at coding theory. In [5], a reduction of the discrete logarithm problem in the multiplicative group of finite fields to the problem of maximum likelihood decoding in an associated Reed-Solomon code is given. In [3], a reduction of the discrete logarithm problem in elliptic curves to the problem of computing a non zero word of minimal weight in an associated elliptic code is given.

We now adapt and extend some of the ideas of [3, 5] to the case of generalised Jacobians. As it turns out, the discrete logarithm reductions of [3, 5] can both be seen as special cases of our general framework.

4.1 Generalised Algebraic Geometric Codes

Let S be a finite set of pairwise coprime effective divisors of C that are also coprime to $\mathfrak{m}$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be divisors of C that are of the form $\mathfrak{a} = \sum_{\mathfrak{d}\in S} \lambda_{\mathfrak{d}}\mathfrak{d}$ and $\mathfrak{b} = \sum_{\mathfrak{d}\in S} \mu_{\mathfrak{d}}\mathfrak{d}$ with $\lambda_{\mathfrak{d}}, \mu_{\mathfrak{d}} \in \mathbb{Z}$ such that $\mu_{\mathfrak{d}} > -\lambda_{\mathfrak{d}}$ for all $\mathfrak{d} \in S$ and thus $\mathfrak{a} + \mathfrak{b} \geq 0$. Let $\mathrm{ord}_{\mathfrak{d}}(\mathfrak{e})$ denote the maximal integer r such that $r\mathfrak{d} \leq \mathfrak{e}$ for any divisor $\mathfrak{e}$. Then $\mathfrak{a} = \sum_{\mathfrak{d}\in S} \mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})\mathfrak{d}$ and $\mathfrak{b} = \sum_{\mathfrak{d}\in S} \mathrm{ord}_{\mathfrak{d}}(\mathfrak{b})\mathfrak{d}$. Define

$$\mathcal{O}_{C,\mathfrak{d}} = \mathcal{O}_C(\mathrm{supp}(\mathfrak{d})) \text{ and } M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}} = (\mathcal{O}_C(\mathfrak{a})/\mathcal{O}_C(-\mathfrak{b}))(\mathrm{supp}(\mathfrak{d})).$$

Then $\mathcal{O}_{C,\mathfrak{d}} = \cap_{\mathfrak{p}\in\mathrm{supp}(\mathfrak{d})}\mathcal{O}_{C,\mathfrak{p}}$ and $M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}$ is the factorisation of the fractional ideal of $\mathcal{O}_{C,\mathfrak{d}}$ defined by $\mathfrak{a}$ by the fractional ideal of $\mathcal{O}_{C,\mathfrak{d}}$ defined by $-\mathfrak{b}$. This is an $\mathcal{O}_{C,\mathfrak{d}}$-module and finite $\mathbb{F}_q$-vector space of dimension $\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a}+\mathfrak{b})\deg(\mathfrak{d})$. For example, if $\mathfrak{d}$ is a place of degree one, this essentially means that we are looking at truncated Laurent series rings starting at the exponent $-\lambda_{\mathfrak{d}} = -\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})$ and ending at the exponent $\mu_{\mathfrak{d}} = \mathrm{ord}_{\mathfrak{d}}(\mathfrak{b})$. Furthermore, define $U = \cup_{\mathfrak{d}\in S}\mathrm{supp}(\mathfrak{d})$ and

$$\mathcal{O}_{C,S} = \mathcal{O}_C(U) = \cap_{\mathfrak{d}\in S}\mathcal{O}_{C,\mathfrak{d}} \text{ and}$$
$$M_{S,\mathfrak{a},\mathfrak{b}} = (\mathcal{O}_C(\mathfrak{a})/\mathcal{O}_C(-\mathfrak{b}))(U) = \prod_{\mathfrak{d}\in S} M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}.$$

Then $M_{S,\mathfrak{a},\mathfrak{b}}$ is an $\mathcal{O}_{C,S}$-module and finite $\mathbb{F}_q$-vector space of dimension $\deg(\mathfrak{a}+\mathfrak{b})$. The canonical epimorphism $\mathcal{O}_C(\mathfrak{a}) \to \mathcal{O}_C(\mathfrak{a})/\mathcal{O}_C(-\mathfrak{b})$ gives us the "evaluation" map

$$\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}} : \mathcal{O}_C(\mathfrak{a})(U) \to M_{S,\mathfrak{a},\mathfrak{b}}.$$

It is also the product of the restrictions to $\mathcal{O}_C(\mathfrak{a})(U)$ of the residue class epimorphisms $\mathcal{O}_C(\mathfrak{a})(\mathrm{supp}(\mathfrak{d})) \to M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}$.

We regard the $\mathfrak{d}$-components of $M_{S,\mathfrak{a},\mathfrak{b}}$ as symbols and the elements of $M_{S,\mathfrak{a},\mathfrak{b}}$ as words. Given $x_{\mathfrak{d}} \in \mathcal{O}_C(\mathfrak{a})(\mathrm{supp}(\mathfrak{d}))$ with $x_{\mathfrak{d}} \neq 0$ let $z_{\mathfrak{d}}(x_{\mathfrak{d}}) = r\deg(\mathfrak{d})$ with r the maximal integer such that $x_{\mathfrak{d}} \in \mathcal{O}_C(\mathfrak{a} - r\mathfrak{d})(\mathrm{supp}(\mathfrak{d}))$. For $x_{\mathfrak{d}} = 0$ we let $z_{\mathfrak{d}}(x_{\mathfrak{d}}) = \infty$. If $x_{\mathfrak{d}} \in M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}$ we define $z_{\mathfrak{d}}(x_{\mathfrak{d}})$ similarly with the additional maximal value $z_{\mathfrak{d}}(0) = \mathrm{ord}_{\mathfrak{d}}(\mathfrak{a}+\mathfrak{b})\deg(\mathfrak{d})$. We say that $x_{\mathfrak{d}}$ has a zero

of multiplicity $z_{\mathfrak{d}}(x_{\mathfrak{d}})$ at $\mathfrak{d}$. The weight of $x_{\mathfrak{d}} \in M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}$ is defined as $w_{\mathfrak{d}}(x_{\mathfrak{d}}) = \mathrm{ord}_{\mathfrak{d}}(\mathfrak{a}+\mathfrak{b})\deg(\mathfrak{d}) - z_{\mathfrak{d}}(x_{\mathfrak{d}})$.

The number of zeros of $x \in \mathcal{O}_C(\mathfrak{a})(U)$ and $x \in M_{S,\mathfrak{a},\mathfrak{b}}$ respectively (counted with multiplicity) is then

$$z_S(x) = \sum_{\mathfrak{d}\in S} z_{\mathfrak{d}}(x_{\mathfrak{d}})$$

where the $x_{\mathfrak{d}}$ are the images of x in $\mathcal{O}_C(\mathfrak{a})(\mathrm{supp}(\mathfrak{d}))$ and $M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}$ respectively. The weight of $x \in \mathcal{O}_C(\mathfrak{a})(U)$ and $x \in M_{S,\mathfrak{a},\mathfrak{b}}$ respectively is

$$w_S(x) = \sum_{\mathfrak{d}\in S} w_{\mathfrak{d}}(x_{\mathfrak{d}})$$

where the $x_{\mathfrak{d}}$ are the images of x in $\mathcal{O}_C(\mathfrak{a})(\mathrm{supp}(\mathfrak{d}))$ and $M_{\mathfrak{d},\mathfrak{a},\mathfrak{b}}$ respectively. The weight defines a Hamming metric on $M_{S,\mathfrak{a},\mathfrak{b}}$ in a standard way. Obviously,

$$z_S(x) + w_S(x) = \deg(\mathfrak{a}+\mathfrak{b})$$

for $x \in M_{S,\mathfrak{a},\mathfrak{b}}$. For example $z_S(0) = \deg(\mathfrak{a}+\mathfrak{b})$.

If $\mathfrak{d}$ is any divisor coprime to $\mathfrak{m}$, we define

$$L_{\mathfrak{m}}(\mathfrak{d}) = \{f \in F^{\times} \mid \mathrm{div}(f) \geq -\mathfrak{d} \text{ and } f \equiv c \bmod \mathfrak{m} \text{ for some } c \in \mathbb{F}_q\} \cup \{0\}.$$

This is a finite dimensional $\mathbb{F}_q$-vector space. For $\mathfrak{m} = 0$ we recover the standard spaces $L(\mathfrak{d})$. Finally, let $\mathfrak{e}$ be a divisor of C coprime to $\sum_{\mathfrak{d}\in S}\mathfrak{d}$ and to $\mathfrak{m}$ with $\deg(\mathfrak{e}) < \deg(\mathfrak{b})$ and define a generalised algebraic-geometric code

$$C(S,\mathfrak{a},\mathfrak{b},\mathfrak{e},\mathfrak{m}) = \{\,\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f) \mid f \in L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})\,\}.$$

If S is a set of places of degree one, $\mathfrak{a} = \mathfrak{m} = 0$ and $\mathfrak{b}$ has no multiplicities, then $C(S,\mathfrak{a},\mathfrak{b},\mathfrak{e},\mathfrak{m})$ is a standard algebraic-geometric code. If $\mathfrak{a}$ and $\mathfrak{b}$ are sums of places of degree one and $\mathrm{ord}_{\mathfrak{d}}(\mathfrak{b}) = -\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})+1$ then $C(S,\mathfrak{a},\mathfrak{b},\mathfrak{e},\mathfrak{m})$ is a code with Hamming distance w_S in the standard sense.

Proposition 1 *For any $f \in L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})$ with $f \neq 0$ it holds that*

$$z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) \leq \deg(\mathfrak{a}+\mathfrak{e}) \quad \textit{and} \quad w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) \geq \deg(\mathfrak{b}-\mathfrak{e}).$$

In particular, $\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f) \neq 0$.

Proof. Since $f \neq 0$ we can write $\mathrm{div}(f) = \mathfrak{e}_1 + \mathfrak{e}_2$ with $\mathrm{supp}(\mathfrak{e}_1) \subseteq U$ and $\mathrm{supp}(\mathfrak{e}_2) \cap U = \emptyset$. Then $\mathfrak{e}_1 \geq \sum_{\mathfrak{d}\in S}\mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))\mathfrak{d}$ and $\mathfrak{e}_2 \geq -\mathfrak{e}$. We obtain

$$\begin{aligned} z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) &\leq \deg(\mathfrak{a}) + \sum_{\mathfrak{d}\in S}\mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))\mathfrak{d} \\ &\leq \deg(\mathfrak{a}) + \deg(\mathfrak{e}_1) = \deg(\mathfrak{a}) - \deg(\mathfrak{e}_2) \\ &\leq \deg(\mathfrak{a}) + \deg(\mathfrak{e}) = \deg(\mathfrak{a}+\mathfrak{e}). \end{aligned}$$

The other inequality follows from $z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) + w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \deg(\mathfrak{a}+\mathfrak{b})$.

4.2 Reduction of the Discrete Logarithm Problem to Code Based Computational Problems

Words of minimal non zero weight in the code $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ correspond to relations in the group $\mathrm{Pic}_{\mathfrak{m}}(C)$ in the following way. If $\mathfrak{d} \in \mathcal{D}^{\mathfrak{m}}(C)$ then $[\mathfrak{d}]_{\mathfrak{m}}$ denotes the class of $\mathfrak{d}$ in $\mathrm{Pic}_{\mathfrak{m}}(C)$.

Theorem 2 *Words of $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ of minimal non zero weight $\deg(\mathfrak{b} - \mathfrak{e})$ correspond bijectively to linear combinations*

$$[\mathfrak{e}]_{\mathfrak{m}} = \sum_{\mathfrak{d} \in S} \gamma_{\mathfrak{d}} \cdot [\,\mathfrak{d}\,]_{\mathfrak{m}}$$

with $\mathrm{ord}_{\mathfrak{d}}(\mathfrak{b}) \geq \gamma_{\mathfrak{d}} \geq -\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})$ for all $\mathfrak{d} \in S$. If $x \in C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ is such a word then the corresponding linear combinations satisfies

$$\gamma_{\mathfrak{d}} = \mathrm{ord}_{\mathfrak{d}}(\mathfrak{b}) - w_{\mathfrak{d}}(x_{\mathfrak{d}})/\deg(\mathfrak{d})$$

for all $\mathfrak{d} \in S$.

Proof. Let $[\mathfrak{e}]_{\mathfrak{m}} - \sum_{\mathfrak{d} \in S} \gamma_{\mathfrak{d}} \cdot [\,\mathfrak{d}\,]_{\mathfrak{m}} = 0$. Then there is $f \in F^{\times}$ with $f \equiv 1 \bmod \mathfrak{m}$, $\mathrm{div}(f) = -\mathfrak{e} + \sum_{\mathfrak{d} \in S} \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))\mathfrak{d}$ and $\gamma_{\mathfrak{d}} = \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))$. Since $\mathrm{ord}_{\mathfrak{d}}(\mathfrak{b}) \geq \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f)) \geq -\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})$ by assumption and $\deg(\mathrm{div}(f)) = 0$ we have

$$\begin{aligned} z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) &= \sum_{\mathfrak{d} \in S} z_{\mathfrak{d}}(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)_{\mathfrak{d}}) = \sum_{\mathfrak{d} \in S} (\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f)))\deg(\mathfrak{d}) \\ &= \sum_{\mathfrak{d} \in S} \mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})\deg(\mathfrak{d}) + \sum_{\mathfrak{d} \in S} \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))\deg(\mathfrak{d}) \\ &= \deg(\mathfrak{a}) + \deg(\mathfrak{e}) = \deg(\mathfrak{a} + \mathfrak{e}). \end{aligned}$$

Thus $w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \deg(\mathfrak{a}+\mathfrak{b}) - z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \deg(\mathfrak{b}-\mathfrak{e})$. This maps every linear combination to a word of minimal non zero weight in a well defined way. From

$$\begin{aligned} \gamma_{\mathfrak{d}} &= \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f)) = z_{\mathfrak{d}}(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)_{\mathfrak{d}})/\deg(\mathfrak{d}) - \mathrm{ord}_{\mathfrak{d}}(\mathfrak{a}) \\ &= \mathrm{ord}_{\mathfrak{d}}(\mathfrak{b}) - w_{\mathfrak{d}}(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)_{\mathfrak{d}})/\deg(\mathfrak{d}) \end{aligned}$$

we see that the map is injective and also the formula for $\gamma_{\mathfrak{d}}$ is proved.

To prove surjectivity, assume that $f \in L_{\mathfrak{m}}(\mathfrak{a} + \mathfrak{e})$ such that $w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \deg(\mathfrak{b} - \mathfrak{e})$. Then $z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \deg(\mathfrak{a} + \mathfrak{e})$. All inequalities in the proof of Proposition 1 are thus equalities. We obtain

$$\mathrm{div}(f) = \mathfrak{e}_1 + \mathfrak{e}_2 = \sum_{\mathfrak{d} \in S} \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))\mathfrak{d} - \mathfrak{e}.$$

Since $f \in L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})$ and f is coprime to $\mathfrak{m}$ there is $c \in \mathbb{F}_q$ such that $cf \equiv 1 \bmod \mathfrak{m}$. Thus f indeed yields $[\mathfrak{e}]_{\mathfrak{m}} - \sum_{\mathfrak{d} \in S} \gamma_{\mathfrak{d}} \cdot [\,\mathfrak{d}\,]_{\mathfrak{m}} = 0$ with $\gamma_{\mathfrak{d}} = \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f))$. Finally, $\gamma_{\mathfrak{d}} \geq \mathrm{ord}_{\mathfrak{d}}(\mathfrak{a})$ holds by $f \in L_{\mathfrak{m}}(\mathfrak{a} + \mathfrak{e})$, and

$$z_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \sum_{\mathfrak{d} \in S} (\mathrm{ord}_{\mathfrak{d}}(\mathfrak{a}) + \mathrm{ord}_{\mathfrak{d}}(\mathrm{div}(f)))\deg(\mathfrak{d})$$

implies $\mathrm{ord}_{\mathfrak{d}}(\mathfrak{b}) \geq \gamma_{\mathfrak{d}}$ for all $\mathfrak{d} \in S$.

It is also possible to make a reduction of the minimal non zero weight word problem to the maximum likelihood decoding problem as in [3], under some additional assumptions.

Theorem 3 *Let* $\mathfrak{q} \in \mathrm{supp}(\mathfrak{e})$ *be a place of degree one and let*

$$\deg(\mathfrak{a}+\mathfrak{e}) \geq 2g + \deg(\mathfrak{m}).$$

There is $h \in L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})$ *such that* $\mathrm{ord}_{\mathfrak{q}}(h) = \mathrm{ord}_{\mathfrak{q}}(\mathfrak{e})$. *Assume that* $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ *contains a word of minimal non zero weight* $\deg(\mathfrak{b}-\mathfrak{e})$. *Let* $x \in C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}-\mathfrak{q}, \mathfrak{m})$ *such that*

$$w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - x)$$

is minimal. Then $\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - x$ *is a word in* $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ *of minimal non zero weight* $\deg(\mathfrak{b}-\mathfrak{e})$.

Proof. We have $L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e}-\mathfrak{q}) \subseteq L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})$ and $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}-\mathfrak{q}, \mathfrak{m}) \subseteq C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$. If one of them exists, the minimal non zero distance of $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}-\mathfrak{q}, \mathfrak{m})$ and $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ is thus equal to the minimal non zero weight of $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$.

Consider the $\mathbb{F}_q$-linear map $\phi : L(\mathfrak{a}+\mathfrak{e}) \to \mathcal{O}_{C,\mathfrak{m}}/\mathfrak{m}$. Since $\mathfrak{a}+\mathfrak{e}-\mathfrak{m}$ is non special, the adele spaces satisfy $A_F = A_F(\mathfrak{a}+\mathfrak{e}-\mathfrak{m}) + F$, whence ϕ is surjective (like in the proof of the strong approximation theorem, see for example [21, p. 33]). As $\dim_{\mathbb{F}_q} \mathcal{O}_{C,\mathfrak{m}}/\mathfrak{m} = \deg(\mathfrak{m})$ we get

$$\dim_{\mathbb{F}_q} L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e}) = \dim_{\mathbb{F}_q} L(\mathfrak{a}+\mathfrak{e}) - \deg(\mathfrak{m}) + 1.$$

Now $\deg(\mathfrak{a}+\mathfrak{e}) \geq 2g$ implies $L(\mathfrak{a}+\mathfrak{e}-\mathfrak{q}) \subsetneq L(\mathfrak{a}+\mathfrak{e})$, whence $L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e}-\mathfrak{q}) \subsetneq L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})$ by the dimension formula, and this yields the existence of h.

By the above observation, $w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - x) \geq \deg(\mathfrak{b}-\mathfrak{e})$. To prove the reverse inequality, let $f \in L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e})$ such that that $w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(f)) = \deg(\mathfrak{b}-\mathfrak{e})$. This exists by assumption. Then $\mathrm{ord}_{\mathfrak{p}}(f) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{e})$ for all $\mathfrak{p} \in \mathrm{supp}(\mathfrak{e})$, including $\mathfrak{p} = \mathfrak{q}$. Since $\mathrm{ord}_{\mathfrak{q}}(h) = \mathrm{ord}_{\mathfrak{q}}(\mathfrak{e}) = \mathrm{ord}_{\mathfrak{q}}(f)$ and $\deg(\mathfrak{q}) = 1$ there is $\lambda \in \mathbb{F}_q^{\times}$ such that $h - \lambda f \in L_{\mathfrak{m}}(\mathfrak{a}+\mathfrak{e}-\mathfrak{q})$. Then $w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - \mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h-\lambda f)) = \deg(\mathfrak{b}-\mathfrak{e})$ and thus $w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - x) \leq \deg(\mathfrak{b}-\mathfrak{e})$, so we have

$$w_S(\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - x) = \deg(\mathfrak{b}-\mathfrak{e}).$$

Clearly $\mathrm{ev}_{S,\mathfrak{a},\mathfrak{b}}(h) - x \in C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$, and the theorem is proved.

We continue the discussion with ways of applying Theorem 2 and in particular working within $\mathrm{Pic}_{\mathfrak{m}}(C)$.

Theorem 4 *Every class of* $\mathrm{Pic}_{\mathfrak{m}}(C)$ *of degree greater or equal to* $2g+\deg(\mathfrak{m})-1$ *contains an effective divisor.*

Proof. Let $\mathfrak{d} \in \mathcal{D}^{\mathfrak{m}}(C)$ with $\deg(\mathfrak{d}) \geq 2g + \deg(\mathfrak{m}) - 1$. The divisor $\mathfrak{d} - \mathfrak{m}$ is not special, since $\deg(\mathfrak{d} - \mathfrak{m}) \geq 2g - 1$. The adele spaces then satisfy $A_F = A_F(\mathfrak{d} - \mathfrak{m}) + F$, whence there is $f \in L(\mathfrak{d})$ such that $f \equiv 1 \bmod \mathfrak{m}$. The divisor $\mathfrak{a} = \mathfrak{d} + \mathrm{div}(f)$ is effective and defines the same class as $\mathfrak{d}$ in $\mathrm{Pic}_{\mathfrak{m}}(C)$.

Let $\mathfrak{e}$ be an arbitrary divisor of C. By replacing $\mathfrak{m}$ by $\mathfrak{m}$ plus the sum of the places in $\mathrm{supp}(\mathfrak{e})$ the theorem can also be applied to conclude that every class of $\mathrm{Pic}_{\mathfrak{m}}(C)$ contains an effective divisor coprime to $\mathfrak{e}$.

Corollary 1 *Let $\mathfrak{o}$ be a place of degree one of C. Every class of $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ contains a divisor of the form*

$$\mathfrak{d} - \deg(\mathfrak{d})\mathfrak{o},$$

where $\mathfrak{d}$ is an effective divisor of degree less than or equal to $\leq 2g + \deg(\mathfrak{m}) - 1$. If $\mathfrak{d}$ has minimal degree then $\mathfrak{d}$ is uniquely determined.

Using these results we see that expressing any divisor $\mathfrak{e}$ as a linear combination of elements of any S in $\mathrm{Pic}_{\mathfrak{m}}(C)$, where the coefficients are bounded by $\mathfrak{a}$ and $\mathfrak{b}$, is equivalent to the minimal non zero weight word problem in $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$. Note that this reduction is polynomial time in the length of the input and the occurring degrees or multiplicities in $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{m}$, by well known algorithms for algebraic curves and function fields (see for example [13]). In order to get a meaningful reduction we need to exhibit supposedly hard instances of the problem of finding linear combinations or of the minimal non zero weight word problem that are related by sufficiently small S, $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{m}$.

Suppose S defines a generating set of $\mathrm{Pic}_{\mathfrak{m}}(C)$ with $\#S$ small such that every element of $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ can be written as a linear combination of the $[\mathfrak{d}]_{\mathfrak{m}}$ with $\mathfrak{d} \in S$ with small coefficients bounded by $-\lambda$ from below and μ from above. Choose

$$\mathfrak{a} = \lambda \sum_{\mathfrak{d} \in S} \mathfrak{d} \quad \text{and} \quad \mathfrak{b} = \mu \sum_{\mathfrak{d} \in S} \mathfrak{d}.$$

Suppose $[\mathfrak{e}_1]_{\mathfrak{m}} = \lambda[\mathfrak{e}_2]_{\mathfrak{m}}$ in $\mathrm{Pic}^0_{\mathfrak{m}}(C)$. By the corollary, for any λ_1 and λ_2 there is an effective $\mathfrak{e}$ with $\deg(\mathfrak{e}) \leq 2g + \deg(\mathfrak{m}) - 1$ such that

$$[\mathfrak{e} - \deg(\mathfrak{e})\mathfrak{o}]_{\mathfrak{m}} = \lambda_1[\mathfrak{e}_1]_{\mathfrak{m}} - \lambda_2[\mathfrak{e}_2]_{\mathfrak{m}}.$$

The complexity of the computation of such an $\mathfrak{e}$ is polynomial in $\log(\lambda_1)$ and $\log(\lambda_2)$ and thus efficient if $\mathfrak{e}_1$ and $\mathfrak{e}_2$ satisfy a similar degree bound to start with (see [13]). Given an oracle for the minimal non zero weight word problem in the codes $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$ we can thus efficiently compute linear combinations

$$\lambda_1[\mathfrak{e}_1]_{\mathfrak{m}} - \lambda_2[\mathfrak{e}_2]_{\mathfrak{m}} = [\mathfrak{e} - \deg(\mathfrak{e})\mathfrak{o}]_{\mathfrak{m}} = \sum_{\mathfrak{d} \in S} \gamma_{\mathfrak{d}}[\mathfrak{d}]_{\mathfrak{m}}$$

for randomly chosen λ_1 and λ_2. After more than $\#S$ linear combinations we get linear dependencies of the right hand sides and can solve for λ in the usual way. The discrete logarithm problem in $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ is thus reduced to the minimal non zero weight word problem in the codes $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$.

In a similar fashion, using random linear combinations of the $\mathfrak{d} \in S$ on the left hand side, we can also compute all relations between the $\mathfrak{d} \in S$ in $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ and thus deduce the structure of $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ as an abelian group. For both problems the best known algorithms have subexponential complexity or

only exponential complexity on average. Depending on the point of view we can obtain hardness statements for the minimal non zero weight word problem in the codes $C(S, \mathfrak{a}, \mathfrak{b}, \mathfrak{e}, \mathfrak{m})$, or we get a possible way of improving said algorithms for the computation of discrete logarithms or for the computation of all relations.

4.3 Efficient Generating Sets of Generalised Jacobians

The crucial point to discuss now are suitable generating systems of $\mathrm{Pic}_{\mathfrak{m}}(C)$ in the above sense. Assume there exists a place $\mathfrak{o}$ of degree one of C. Let X be a multiset with $\mathrm{supp}(X) \subseteq \mathrm{Pic}^0_{\mathfrak{m}}(C)$ such that $-y \in X$ for all $y \in X$. The Cayley graph

$$\mathrm{Cay}(\mathrm{Pic}^0_{\mathfrak{m}}(C), X)$$

has the set of vertices $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ and the multiset $\{(x, yx) \,|\, x \in \mathrm{Pic}^0_{\mathfrak{m}}(C), y \in X\}$ of edges. For every $x \in \mathrm{Pic}^0_{\mathfrak{m}}(C)$ there are exactly $\#X$ edges leaving x.

Theorem 5 *Let X_r be a multiset containing*

$$[(r/\deg(\mathfrak{p}))\mathfrak{p} - r\mathfrak{o}]_{\mathfrak{m}} \quad \textit{and} \quad [r\mathfrak{o} - (r/\deg(\mathfrak{p}))\mathfrak{p}]_{\mathfrak{m}}$$

each with multiplicity $\deg(\mathfrak{p})$, where $\mathfrak{p}$ ranges over all places $\neq \mathfrak{o}$ with $\deg(\mathfrak{p})|r$ and $\mathfrak{p} \notin \mathrm{supp}(\mathfrak{m})$. Let $r, t \in \mathbb{Z}^{\geq 1}$ with

$$\begin{aligned} q^r - 2gq^{r/2} - \deg(\mathfrak{m}) \;&>\; 0, \\ (q^r - 2gq^{r/2} - \deg(\mathfrak{m}))^t \;&>\; 2(q^{1/2}+1)^{2g}(q^{\deg(\mathfrak{m})} - 1)/(q-1) \\ &\quad \cdot ((2g + \deg(\mathfrak{m}))q^{r/2} + \deg(\mathfrak{m}))^t. \end{aligned}$$

Let $x_0, x_1 \in \mathrm{Pic}^0_{\mathfrak{m}}(C)$. Then any random walk in $\mathrm{Cay}(\mathrm{Pic}^0_{\mathfrak{m}}(C), X_r)$ of length t starting in x_0 will end in x_1 with probability $p_{r,t}$ satisfying

$$\frac{1}{2}\#\mathrm{Pic}^0_{\mathfrak{m}}(C)^{-1} \;\leq\; p_{r,t} \;\leq\; \frac{3}{2}\#\mathrm{Pic}^0_{\mathfrak{m}}(C)^{-1}.$$

Proof. We will make use of the methodology in [17] that estimates rapid mixing properties of random walks of length t on the Cayley graph of $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ with edges X_r. For this we need to estimate character sums over X_r.

Let $\chi : \mathrm{Pic}^0_{\mathfrak{m}}(C) \to \mathbb{C}^\times$ be a character. We extend χ to $\mathrm{Pic}_{\mathfrak{m}}(C)$ via $\chi([\mathfrak{o}]_{\mathfrak{m}}) = 1$. Then $\chi : \mathrm{Pic}_{\mathfrak{m}}(C) \to \mathbb{C}^\times$ is a character of finite order. Let $\mathfrak{f}(\chi)$ be its conductor. The theory of L-series gives

$$\sum_{\deg(\mathfrak{p})|r, \mathfrak{p} \not\leq \mathfrak{f}(\chi)} \deg(\mathfrak{p}) \cdot \chi([\mathfrak{p}]_{\mathfrak{m}})^{r/\deg(\mathfrak{p})} = \rho_\chi(q^r + 1) - \sum_{i=1}^{2(g-1+\rho_\chi)+\deg(\mathfrak{f}(\chi))} \omega_i(\chi)^r,$$

where $\rho_\chi = 1$ if χ is the trivial character on $\mathrm{Pic}^0_{\mathfrak{m}}(C)$, $\rho_\chi = 0$ otherwise, and $\omega_i(\chi)$ are complex numbers of absolute value $q^{r/2}$. This gives

$$\begin{aligned} \lambda_\chi &:= \sum_{x \in X_r} \chi(\,x\,) \\ &= \sum_{\deg(\mathfrak{p})|r, \mathfrak{p} \not\leq \mathfrak{m}+\mathfrak{o}} \deg(\mathfrak{p}) \cdot \big(\chi\big((r/\deg(\mathfrak{p})) \cdot [\mathfrak{p}]_{\mathfrak{m}}\big) + \chi^{-1}\big((r/\deg(\mathfrak{p})) \cdot [\mathfrak{p}]_{\mathfrak{m}}\big)\big)\,. \end{aligned}$$

Furthermore,

$$\sum_{\deg(\mathfrak{p})|r,\mathfrak{p}\not\leq\mathfrak{m}+\mathfrak{o}} \deg(\mathfrak{p})\cdot\chi\big((r/\deg(\mathfrak{p}))\cdot[\mathfrak{p}]_{\mathfrak{m}}\big) = \sum_{\deg(\mathfrak{p})|r,\mathfrak{p}\not\leq\mathfrak{m}+\mathfrak{o}} \deg(\mathfrak{p})\cdot\chi([\mathfrak{p}]_{\mathfrak{m}})^{r/\deg(\mathfrak{p})}$$
$$= \sum_{\deg(\mathfrak{p})|r,\mathfrak{p}\not\leq\mathfrak{f}(\chi)} \deg(\mathfrak{p})\cdot\chi([\mathfrak{p}]_{\mathfrak{m}})^{r/\deg(\mathfrak{p})} - \sum_{\deg(\mathfrak{p})|r,\mathfrak{p}\not\leq\mathfrak{f}(\chi),\mathfrak{p}\leq\mathfrak{m}+\mathfrak{o}} \deg(\mathfrak{p})\cdot\chi([\mathfrak{p}]_{\mathfrak{m}})^{r/\deg(\mathfrak{p})}$$
$$= \rho_\chi(q^r+1) - \sum_{i=1}^{2(g-1+\rho_\chi)+\deg(\mathfrak{f}(\chi))} \omega_i(\chi)^r - \sum_{\deg(\mathfrak{p})|r,\mathfrak{p}\not\leq\mathfrak{f}(\chi),\mathfrak{p}\leq\mathfrak{m}+\mathfrak{o}} \deg(\mathfrak{p})\cdot\chi([\mathfrak{p}]_{\mathfrak{m}})^{r/\deg(\mathfrak{p})}.$$

We obtain

$$|\lambda_1/2 - (q^r+1)| \leq 2gq^{r/2} + \deg(\mathfrak{m}) + 1 \tag{5}$$

and

$$|\lambda_\chi/2| \leq (2g-2+\deg(\mathfrak{m}))q^{r/2} + \deg(\mathfrak{m}) + 1. \tag{6}$$

By the proof of [17, Lemma 2.1], the number of paths of length t starting and ending in any two fixed elements of $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ is equal to

$$\frac{\lambda_1^t}{\#\mathrm{Pic}^0_{\mathfrak{m}}(C)} + w$$

with $|w| \leq \max_{\chi\neq 1}|\lambda_\chi|^t$. If r and t are chosen such that

$$\frac{\lambda_1^t}{\#\mathrm{Pic}^0_{\mathfrak{m}}(C)} > 2\max_{\chi\neq 1}|\lambda_\chi|^t \tag{7}$$

then the assertion of the theorem holds for S_r and t by [17, Lemma 2.1]. Observing

$$\#\mathrm{Pic}^0_{\mathfrak{m}}(C) \leq (q^{1/2}+1)^{2g}(q^{\deg(\mathfrak{m})}-1)/(q-1)$$

the inequality of the assertion follows by combining (5), (6) and (7).

Corollary 2 *Choose r and t as in the theorem and let S_r be the set containing the divisors $\mathfrak{o}$ and $(r/\deg(\mathfrak{p}))\mathfrak{p}$ for all places $\neq\mathfrak{o}$ with $\deg(\mathfrak{p})|r$ and $\mathfrak{p}\notin\mathrm{supp}(\mathfrak{m})$. Then S_r is a generating system of $\mathrm{Pic}_{\mathfrak{m}}(C)$ and every $[\mathfrak{e}]_{\mathfrak{m}}\in\mathrm{Pic}^0_{\mathfrak{m}}(C)$ can be written as*

$$[\mathfrak{e}]_{\mathfrak{m}} = \sum_{\mathfrak{d}\in S_r}\lambda_{\mathfrak{d}}\mathfrak{d} \text{ with } \lambda_{\mathfrak{d}}\in\mathbb{Z} \text{ and } \sum_{\mathfrak{d}\in S_r}|\lambda_{\mathfrak{d}}| \leq 2t.$$

We remark that it is convenient but not really necessary to assume that there exists a place $\mathfrak{o}$ of degree one. We could also adapt the statements to the case that $\mathfrak{o}$ is only a divisor of degree one.

According to the corollary, S_r is a set of generators that can be used for an efficient reduction as described above. A drawback for the construction of the codes $C(S,\mathfrak{a},\mathfrak{b},\mathfrak{m},\mathfrak{e})$ is that the $\lambda_{\mathfrak{d}}$ can also be negative, thus we get non standard codes and Hamming weights. It is also possible to prove the existence of a small set of low degree prime generators such that $\lambda_{\mathfrak{d}}\in\{0,1\}$ for $\mathfrak{d}\neq\mathfrak{o}$, see

the method of [4] in a special context. The bounds of this method appear to be weaker than the bounds in Theorem 5 though. Alternatively, using Theorem 5, we can probabilistically construct such a set of $\{0,1\}$-generators by the following theorem of [8].

Theorem 6 *Let G be an abelian group and $n = \#G$. Choose k elements $a_1, \ldots, a_k$ from G uniformly and independently at random. If $k \geq \log_2(n) + 2\log(\log(n))$, then*

$$G = \left\{ \sum_{i=1}^{k} \lambda_i a_i \mid \lambda_i \in \{0,1\} \right\}$$

with probability tending to 1 for $n \to \infty$.

Besides the additional probabilistic computation, the drawback here is that the a_i will be represented as $[\mathfrak{d} - \deg(\mathfrak{d})\mathfrak{o}]_{\mathfrak{m}}$ with $\mathfrak{d}$ effective by Corollary 1, where $\mathfrak{d}$ has in general degree of order $O(g + \deg(\mathfrak{m}))$. These degrees are much bigger than those of Theorem 5. The $\mathfrak{d}$ are not necessarily prime, but allowing for larger degrees, still of order $O(g+\deg(\mathfrak{m}))$, we could even achieve that the $\mathfrak{d}$ are places.

4.4 Examples

In [5], the discrete logarithm problem in $\mathbb{F}_{q^h} = \mathbb{F}_q[\alpha]$ is solved by decomposing $f(\alpha) \in \mathbb{F}_q[\alpha]$ as products of linear polynomials $\alpha + a$ in α with $a \in \mathbb{F}_q$ by an oracle to Reed-Solomon decoding. In our setting, we take $C = \mathbb{P}^1$, $\mathfrak{m}$ is defined as the place of degree h corresponding to the minimal polynomial of α over $\mathbb{F}_q$ and $\mathfrak{o}$ is the place "at infinity". By Corollary 1, the classes of $\mathrm{Pic}^0_{\mathfrak{m}}(C)$ can be represented as polynomials $f(\alpha)$ in α of degree $\leq h-1$. In [5], h is chosen in comparison to q (as large as possible) such that the linear polynomials $\alpha + a$ in α with $a \in \mathbb{F}_q$ are a $\{0,1\}$-generating system. By Theorem 5 we obtain similar generating systems.

In [3], the discrete logarithm problem in an elliptic curve is cast as a minimal non zero weight word problem of an elliptic code. In our setting, we take C as elliptic curve, $\mathfrak{m} = 0$, $\mathfrak{a} = 0$, $\mathfrak{b}$ as divisor sum of point group multiples of a generator of the point group and $\mathfrak{e} = k\mathfrak{o}$, where $\mathfrak{o}$ is again a place "at infinity". Note that Theorem 5 does not apply in this context, since q is large. Estimates for incomplete character sums can be used to obtain a variant of Theorem 5 that does apply, but the resulting sizes of the generating systems are of order $q^{1/2}$ and hence completely unsatisfactory.

References

1. Daniel Augot and François Morain. Discrete logarithm computations over finite fields using Reed-Solomon codes. `http://hal.inria.fr/hal-00672050`, 2012.
2. Dan Boneh and Alice Silverberg. Applications of multilinear forms to cryptography. Melles, Caroline Grant (ed.) et al., Topics in algebraic and noncommutative geometry. Proceedings in memory of Ruth Michler, Luminy, France, July 20-22, 2001 and Annapolis, MD, USA, October 25-28, 2001. Providence, RI: American Mathematical Society (AMS). Contemp. Math. 324, 71-90 (2003)., 2003.

3. Qi Cheng. Hard problems of algebraic geometry codes. *IEEE Trans. Inform. Theory*, 54(1):402–406, 2008.
4. Qi Cheng and Daqing Wan. On the list and bounded distance decodability of Reed-Solomon codes. *SIAM J. Comput.*, 37(1):195–209, 2007.
5. Qi Cheng and Daqing Wan. Complexity of decoding positive-rate Reed-Solomon codes. Aceto, Luca (ed.) et al., Automata, languages and programming. 35th international colloquium, ICALP 2008, Reykjavik, Iceland, July 7–11, 2008. Proceedings, Part I. Berlin: Springer. Lecture Notes in Computer Science 5125, 283-293 (2008)., 2008.
6. Isabelle Déchène. Arithmetic of generalized Jacobians. Hess, Florian (ed.) et al., Algorithmic number theory. 7th international symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 4076, 421-435 (2006)., 2006.
7. Isabelle Déchène. On the security of generalized Jacobian cryptosystems. *Adv. Math. Commun.*, 1(4):413–426, 2007.
8. P. Erdős and A. Rényi. Probabilistic methods in group theory. *J. Analyse Math.*, 14:127–138, 1965.
9. G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.
10. S. D. Galbraith and Benjamin Smith. Discrete Logarithms in Generalized Jacobians. `http://hal.inria.fr/inria-00537887`, 2006.
11. Steven D. Galbraith, Florian Hess, and Frederik Vercauteren. Aspects of pairing inversion. *IEEE Trans. Inf. Theory*, 54(12):5719–5728, 2008.
12. Helmut Hasse. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper. *J. Reine Angew. Math.*, 172:37–54, 1934.
13. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.*, 33(4):425–445, 2002.
14. F. Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math.*, 82:28–32, 2004.
15. Florian Hess, Sebastian Pauli, and Michael E. Pohst. Computing the multiplicative group of residue class rings. *Math. Comp.*, 72(243):1531–1548 (electronic), 2003.
16. Ming-Deh Huang and Wayne Raskind. A multilinear generalization of the Tate pairing. McGuire, Gary (ed.) et al., Finite fields. Theory and applications. Proceedings of the 9th international conference on finite fields and applications, Dublin, Ireland, July 13–17, 2009. Providence, RI: American Mathematical Society (AMS). Contemporary Mathematics 518, 255-263 (2010)., 2010.
17. David Jao, Stephen D. Miller, and Ramarathnam Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *J. Number Theory*, 129(6):1491–1504, 2009.
18. David Kohel. Constructive and destructive facets of torus-based cryptography. `http://echidna.maths.usyd.edu.au/kohel/pub/torus.ps`, 2004.
19. Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos. Optimal authenticated data structures with multilinear forms. Joye, Marc (ed.) et al., Pairing-based cryptography – Pairing 2010. 4th international conference, Yamanaka Hot Spring, Japan, December 13–15, 2010. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 6487, 246-264 (2010)., 2010.
20. Jean-Pierre Serre. *Algebraic groups and class fields. Transl. of the French edition. Transl. of the French Edition.* Graduate Texts in Mathematics, 117. New York etc.: Springer-Verlag. ix, 207 p., 1988.

21. Henning Stichtenoth. *Algebraic function fields and codes. 2nd ed.* Graduate Texts in Mathematics 254. Berlin: Springer. xiii, 355 p., 2009.