On Generating Coset Representatives of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$

Jincheng Zhuang[1,2] ⋆ and Qi Cheng[3]⋆⋆

[1] State Key Laboratory of Information Security
Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China
[2] State Key Laboratory of Mathematical Engineering and Advanced Computing
Wuxi 214125, China
Email: zhuangjincheng@iie.ac.cn
[3] School of Computer Science
The University of Oklahoma
Norman, OK 73019, USA.
Email: qcheng@ou.edu

Abstract. There are q^3+q right $PGL_2(\mathbb{F}_q)-$cosets in the group $PGL_2(\mathbb{F}_{q^2})$. In this paper, we present a method of generating all the coset representatives, which runs in time $\tilde{O}(q^3)$, thus achieves the optimal time complexity up to a constant factor. Our algorithm has applications in solving discrete logarithms and finding primitive elements in finite fields of small characteristic.

Keywords: Projective linear group, Cosets, Discrete logarithm, Primitive elements

1 Introduction

The discrete logarithm problem (DLP) over finite fields underpins the security of many cryptographic systems. Since 2013, dramatic progresses have been made to solve the DLP when the characteristic is small [18, 15, 5, 16, 6, 17, 7, 19, 10, 9, 8, 3, 4, 20, 11, 21, 12, 13, 1, 2]. Particularly, for a finite field $\mathbb{F}_{q^n}$, Joux [19] proposed the first algorithm with heuristic running time at most $q^{n^{1/4+o(1)}}$. Subsequently, Barbulescu, Gaudry, Joux and Thomé[3] proposed the first algorithm with heuristic quasi-polynomial running time $q^{(\log n)^{O(1)}}$. In [20], these algorithms are coined

⋆ This work was partially supported by the National Natural Science Foundation of China under Grant 61502481, the Strategic Priority Research Program of the Chinese Academy of Sciences under Grant XDA06010701, and the Open Project Program of the State Key Laboratory of Mathematical Engineering and Advanced Computing for Jincheng Zhuang.

⋆⋆ This work was partially supported by China 973 Program under Grant 2013CB834201 and by US NSF under Grant CCF-1409294 for Qi Cheng.

as Frobenius representation algorithms. One key component of algorithms in [19] and [3] is the relation generation, which requires enumerating the cosets of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^d})$, where d is a small integer, e.g. $d = 2$ [19]. Huang and Narayanan [14] have applied Joux's relation generation method for finding primitive elements of finite fields of small characteristic. There is another method of generating relations, see [7].

To illustrate the application of enumerating cosets of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$, we briefly recall Joux's method [19] of generating relations among linear polynomials of a small characteristic finite field $\mathbb{F}_{q^{2k}} = \mathbb{F}_{q^2}[X]/(I(X))$, where $I(X) \in \mathbb{F}_{q^2}[X]$ is an irreducible factor of $h_1(X)X^q - h_0(X)$ with the requirement that the degrees of $h_0(X), h_1(X)$ are small. Let x be the image of $X \mod (I(X))$. Such Frobenius representation has the crucial property that $x^q = \frac{h_0(x)}{h_1(x)}$. It is well known that:

$$\prod_{\alpha \in \mathbb{F}_q} (y - \alpha) = y^q - y.$$

Applying the Mobius transformation

$$y \mapsto \frac{ax + b}{cx + d}$$

where the matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_{q^2}^{2\times 2}$ is nonsingular, we get

$$\prod_{\alpha \in \mathbb{F}_q} (\frac{ax + b}{cx + d} - \alpha) = (\frac{ax + b}{cx + d})^q - \frac{ax + b}{cx + d}.$$

We deduce [4]:

$$\begin{aligned} & h_1(x)(cx + d) \prod_{\alpha \in \mathbb{F}_q} ((ax + b) - \alpha(cx + d)) \\ = & (a^q h_0(x) + b^q h_1(x))(cx + d) - (ax + b)(c^q h_0(x) + d^q h_1(x)) \\ & \pmod{x^q h_1(x) - h_0(x)}. \end{aligned}$$

If the right-hand side can be factored into a product of linear factors over $\mathbb{F}_{q^2}$, we obtain a relation of the form

$$\lambda^{e_0} \prod_{i=1}^{q^2} (x + \alpha_i)^{e_i} = \prod_{i=1}^{q^2} (x + \alpha_i)^{e_i'} \pmod{x^q h_1(x) - h_0(x)}, \tag{1}$$

where λ is a multiplicative generator of $\mathbb{F}_{q^2}$, $\alpha_1 = 0, \alpha_2, \alpha_3, \ldots, \alpha_{q^2}$ is a natural ordering of elements in $\mathbb{F}_{q^2}$, and e_i's and e_i''s are non-negative integers.

Recall that for a given finite field $\mathbb{F}_q$, the projective general linear group $PGL_2(\mathbb{F}_q) = GL_2(\mathbb{F}_q)/E$, where E is the subgroup of $GL_2(\mathbb{F}_q)$ consisting of non-zero scalar matrices. Following the notion in [3], we denote $\mathcal{P}_q$ as a set of the right cosets of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$, namely,

$$\mathcal{P}_q = \{PGL_2(\mathbb{F}_q)t | t \in PGL_2(\mathbb{F}_{q^2})\}.$$

Note that the cardinality of $\mathcal{P}_q$ is q^3+q. It was shown in [19, 3] that the matrices in the same right coset produce the same relation. In [19], Joux suggested two ways to generate relations: the first is to investigate the structure of cosets of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$, and the second is to use hash values to remove duplicate relations. The second approach needs to enumerate the elements in $PGL_2(\mathbb{F}_{q^2})$ that has cardinality about q^6, hence has time complexity at least q^6. It may not be the most time-consuming part inside a subexponential algorithm. However, if we want a more efficient algorithm to compute the discrete logarithms of elements, or to construct a primitive element, this complexity can be a bottleneck. In this paper, we develop the first approach to generate cosets representatives efficiently.

1.1 Our result

In this work, we give an almost complete characterization of $\mathcal{P}_q$. The case of determining left cosets is similar. Our main result is the following:

Theorem 1 *There exists a deterministic algorithm that runs in time $\tilde{O}(q^3)$ and computes a set $S \subseteq PGL_2(\mathbb{F}_{q^2})$ such that*

1. $|S| \leq q^3 + 2q^2 - q + 2$;
2. $\mathcal{P}_q = \{PGL_2(\mathbb{F}_q)t | t \in S\}$.

Here we follow the convention that uses the notation $\tilde{O}(f(q))$ to stand for $O(f(q)\log^{O(1)} f(q))$. Note that the time complexity of our algorithm is optimal up to a constant factor, since the $\mathcal{P}_q$ has size q^3+q.

2 A Preliminary Classification

We deduce our main result by two steps. Firstly, we describe a preliminary classification. Then, we deal with the dominating case. In this section, the main technical tool we use is the fact that the following operations on a matrix over $\mathbb{F}_{q^2}$ will not change the membership in a right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$:

- Multiply the matrix by an element in $\mathbb{F}_{q^2}^*$;
- Multiply a row by an element in $\mathbb{F}_q^*$;
- Add a multiple of one row with an element in $\mathbb{F}_q$ into another row;
- Swap two rows.

Proposition 1. *Let g be an element in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Each right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$ is equal to $PGL_2(\mathbb{F}_q)t$, where t is one of the following four types:*

(I) $\begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}$, *where $b, c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q, bc \neq 1$.*

(II) $\begin{pmatrix} 1 & b_1 \\ g & d_2 g \end{pmatrix}$, *where $b_1, d_2 \in \mathbb{F}_q^*, b_1 \neq d_2$.*

(III) $\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}$, *where* $c \in \mathbb{F}_{q^2}^*, d \in \mathbb{F}_{q^2}$.

(IV) $\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}$, *where* $c \in \mathbb{F}_{q^2}, d \in \mathbb{F}_{q^2}^*$.

Proof. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a representative of a right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$. If any of a, b, c, d is zero, then we divide them by the other non-zero element in the same row, and swap rows if necessary, we will find a representative of type (III) or (IV). So we may assume that none of the entries are zero. Dividing the whole matrix by a, we can assume $a = 1$. Consider the nonsingular matrix

$$\begin{pmatrix} 1 & b_1 + b_2 g \\ c_1 + c_2 g & d_1 + d_2 g \end{pmatrix},$$

where $b_i, c_i, d_i \in \mathbb{F}_q$ for $1 \leq i \leq 2$. We distinguish the following cases. Note that we may also assume $c_1 = 0$, since we can add the multiple of the first row with $-c_1$ into the second. We start with the matrix

$$\begin{pmatrix} 1 & b_1 + b_2 g \\ c_2 g & d_1 + d_2 g \end{pmatrix}$$

where $c_2 \neq 0$.

Case 1. $b_2 \neq 0$

Subtracting $\frac{d_2}{b_2}$ times the first row from the second row, the matrix becomes

$$\begin{pmatrix} 1 & b_1 + b_2 g \\ -\frac{d_2}{b_2} + c_2 g & d_1 - \frac{b_1 d_2}{b_2} \end{pmatrix}.$$

We can assume that $d_1 - \frac{b_1 d_2}{b_2} \neq 0$. The matrix is in the same coset with a matrix of type (I) since we can divide the second row by $d_1 - \frac{b_1 d_2}{b_2}$, and b_2 and c_2 are not zero.

Case 2. $b_2 = 0$

We will assume $b_1 \neq 0$. After subtracting $\frac{d_1}{b_1}$ times the first row from the second row, the matrix becomes

$$\begin{pmatrix} 1 & b_1 \\ -\frac{d_1}{b_1} + c_2 g & d_2 g \end{pmatrix}$$

Assume $d_2 \neq 0$.

1. If $d_1 = 0$, then the matrix can be reduced to type (II) by dividing the second row by c_2.
2. If $d_1 \neq 0$, adding the product of the second row with $\frac{b_1}{d_1}$ into the first row, we get
$$\begin{pmatrix} \frac{b_1 c_2}{d_1} g & b_1 + \frac{b_1 d_2}{d_1} g \\ -\frac{d_1}{b_1} + c_2 g & d_2 g \end{pmatrix}.$$

Dividing all the entries in the matrix by g, we get

$$\begin{pmatrix} \frac{b_1c_2}{d_1} & \frac{b_1d_2}{d_1} + b_1g^{-1} \\ c_2 - \frac{d_1}{b_1}g^{-1} & d_2 \end{pmatrix}.$$

Dividing the first row by $\frac{b_1c_2}{d_1}$ and the second row by d_2, the matrix is reduced to type (I), since $\frac{b_1d_2}{d_1} + b_1g^{-1}$ and $c_2 - \frac{d_1}{b_1}g^{-1}$ are in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. □

There are only $O(q^2)$ many possibilities for Case (II). Next, we simplify cases (III) and (IV) further. As a conclusion, we can see that there are only $O(q^2)$ many possibilities in Case (III) and (IV) as well.

Proposition 2. *Let*

$$\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ c_1 + c_2g & d_1 + d_2g \end{pmatrix}$$

be one representative of a right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$, where $c_1, c_2, d_1, d_2 \in \mathbb{F}_q$. Then it belongs to $PGL_2(\mathbb{F}_q)t$, where t is of the following two types:

(III-a): $\begin{pmatrix} 0 & 1 \\ g & d_2g \end{pmatrix}$, *where* $d_2 \in \mathbb{F}_q$.

(III-b): $\begin{pmatrix} 0 & 1 \\ 1 + c_2g & d_2g \end{pmatrix}$, *where* $c_2 \in \mathbb{F}_q, d_2 \in \mathbb{F}_q$.

Proof. There are two cases to consider.

1. Assume $c_1 = 0$. Subtracting the second row by the first row times d_1 , we get
$$\begin{pmatrix} 0 & 1 \\ c_2g & d_2g \end{pmatrix}.$$
Since $c_2 \neq 0$, after dividing the second row by c_2, the matrix is reduced to type (III-a).
2. Assume $c_1 \neq 0$. Subtracting the second row by the first row times d_1, we get
$$\begin{pmatrix} 0 & 1 \\ c_1 + c_2g & d_2g \end{pmatrix}.$$
Dividing the second row by c_1, we get
$$\begin{pmatrix} 0 & 1 \\ 1 + c_2g & \frac{d_2}{c_1}g \end{pmatrix}.$$
Thus the matrix is reduced to type (III-b), which completes the proof. □

Similarly, we have the following proposition.

Proposition 3. *Let*

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c_1 + c_2 g & d_1 + d_2 g \end{pmatrix}$$

be one representative of a right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$. Then it belongs to $PGL_2(\mathbb{F}_q)t$, where t is of the following two types:

(IV-a): $\begin{pmatrix} 1 & 0 \\ c_2 g & g \end{pmatrix}$, *where* $c_2 \in \mathbb{F}_q$.

(IV-b): $\begin{pmatrix} 1 & 0 \\ c_2 g & 1 + d_2 g \end{pmatrix}$, *where* $c_2 \in \mathbb{F}_q, d_2 \in \mathbb{F}_q$.

3 The dominating case

In this section, we show how to reduce the cardinality of type (I) in Proposition 1 from $O(q^4)$ to $O(q^3)$, which is the main case of representative of cosets. The following proposition shows that if

$$A_1 = \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & b' \\ c' & 1 \end{pmatrix}$$

are of type (I) and

$$\frac{b^q - b}{c - c^q} = \frac{b'^q - b'}{c' - c'^q}, \frac{1 - bc^q}{b - c^q} = \frac{1 - b'c'^q}{b' - c'^q},$$

then A_1 and A_2 are in the same coset. Note that the first value is in $\mathbb{F}_q$. Considering parameters of the above special format is inspired by the equations appeared in [19].

Proposition 4. *Fix $v \in \mathbb{F}_q^*$ and $w \in \mathbb{F}_{q^2}$. Suppose that we solve the equations*

$$\begin{cases} \frac{x^q - x}{y - y^q} = v, \\ \frac{1 - xy^q}{y - y^q} = w, \end{cases} \tag{2}$$

under conditions $x, y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $xy \neq 1$, and find two pairs of solutions $(b, c), (b', c')$, then A_1 and A_2 are in the same right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$, where

$$A_1 = \begin{pmatrix} 1 & b \\ c & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & b' \\ c' & 1 \end{pmatrix}.$$

Proof. The proof consists of two steps. Firstly, we will parametrize the variety corresponding to solutions of $(x, y)'s$ to equations (2). Then we will deduce the desired result.

Note that x, y are in $\mathbb{F}_{q^2}$, we have $x^{q^2} = x$ and $y^{q^2} = y$. From equations (2), it follows that

$$w^q = (\frac{1 - xy^q}{y - y^q})^q = \frac{1 - x^q y}{y^q - y}.$$

So $\frac{w^q}{v} = \frac{1-x^q y}{x-x^q}$ and $y - \frac{w^q}{v} = \frac{xy-1}{x-x^q}$. Thus

$$(y - \frac{w^q}{v})^{q+1} = \frac{(xy-1)(x^q y^q - 1)}{(x^q - x)(x - x^q)} = \frac{(1-xy^q)(1-x^q y)}{(x^q - x)(x - x^q)} - \frac{y - y^q}{x^q - x},$$

which equals $(\frac{w^q}{v})^{q+1} - \frac{1}{v}$. Besides, we have

$$-vy + w + w^q = \frac{y(x - x^q)}{y - y^q} + \frac{1 - xy^q}{y - y^q} + \frac{x^q y - 1}{y - y^q} = x.$$

Hence equations (2) imply the following

$$\begin{cases} (y - \frac{w^q}{v})^{q+1} = (\frac{w^q}{v})^{q+1} - \frac{1}{v} \in \mathbb{F}_q, \\ x = -vy + w + w^q. \end{cases} \tag{3}$$

Let γ be one of the $(q+1)$-th roots of $(\frac{w^q}{v})^{q+1} - \frac{1}{v}$. Suppose that

$$c = \frac{w^q}{v} + \zeta_1 \gamma, c' = \frac{w^q}{v} + \zeta_2 \gamma,$$

where ζ_1, ζ_2 are two distinct $(q+1)$-th roots of unity, and

$$b = -vc + w + w^q = w - v\zeta_1 \gamma,$$

$$b' = -vc' + w + w^q = w - v\zeta_2 \gamma.$$

It follows that

$$A_1 = \begin{pmatrix} 1 & w - v\zeta_1\gamma \\ \frac{w^q}{v} + \zeta_1\gamma & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & w - v\zeta_2\gamma \\ \frac{w^q}{v} + \zeta_2\gamma & 1 \end{pmatrix}.$$

Since A_2 is not singular, we deduce

$$A_2^{-1} = \frac{1}{\det(A_2)} \begin{pmatrix} 1 & -w + v\zeta_2\gamma \\ -\frac{w^q}{v} - \zeta_2\gamma & 1 \end{pmatrix}.$$

Thus,

$$\begin{aligned} A_1 A_2^{-1} &= \frac{1}{\det(A_2)} \begin{pmatrix} (v\zeta_1\gamma - w)(\frac{w^q}{v} + \zeta_2\gamma) + 1 & -v(\zeta_1\gamma - \zeta_2\gamma) \\ \zeta_1\gamma - \zeta_2\gamma & (v\zeta_2\gamma - w)(\frac{w^q}{v} + \zeta_1\gamma) + 1 \end{pmatrix} \\ &= \frac{1}{\det(A_2)} \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}. \end{aligned}$$

Note that $m_{12} = -vm_{21}, m_{11} - m_{22} = (w^q + w)m_{21}$. They imply that $\frac{m_{12}}{m_{21}} \in \mathbb{F}_q$ and $\frac{m_{11} - m_{22}}{m_{21}} \in \mathbb{F}_q$. It remains to prove $\frac{m_{11}}{m_{21}} \in \mathbb{F}_q$. Let $\delta = \frac{m_{11}}{m_{21}}$. Note that

$$\begin{aligned} \delta \in \mathbb{F}_q &\iff \delta = \delta^q \\ &\iff m_{11} m_{21}^q = m_{11}^q m_{21} \\ &\iff m_{11} m_{21}^q \in \mathbb{F}_q. \end{aligned}$$

Since $\gamma^{q+1} = (\frac{w^q}{v})^{q+1} - \frac{1}{v} = \frac{w^{q+1}-v}{v^2}$, we have $\frac{w^{q+1}}{v} = v\gamma^{q+1} + 1$. Hence

$$m_{11} = w^q\zeta_1\gamma + v\zeta_1\gamma\zeta_2\gamma - w\zeta_2\gamma - v\gamma^{q+1}.$$

Thus

$$m_{11}m_{21}^q = \gamma^{q+1}\{(w^q + w) - (w\zeta_1^q\zeta_2 + w^q\zeta_1\zeta_2^q) + v(\zeta_2\gamma + \zeta_2^q\gamma^q) - v(\zeta_1\gamma + \zeta_1^q\gamma^q)\}.$$

Since

$$\gamma^{q+1} \in \mathbb{F}_q,$$
$$w^q + w \in \mathbb{F}_q, w\zeta_1^q\zeta_2 + w^q\zeta_1\zeta_2^q \in \mathbb{F}_q,$$
$$\zeta_2\gamma + \zeta_2^q\gamma^q \in \mathbb{F}_q, \zeta_1\gamma + \zeta_1^q\gamma^q \in \mathbb{F}_q,$$

we deduce $m_{11}m_{21}^q \in \mathbb{F}_q$, which implies $\frac{m_{11}}{m_{21}} \in \mathbb{F}_q$ and $\frac{m_{22}}{m_{21}} \in \mathbb{F}_q$. Thus

$$\begin{aligned} A_1A_2^{-1} &= \frac{\zeta_1\gamma - \zeta_2\gamma}{\det(A_2)} \begin{pmatrix} \frac{m_{11}}{m_{21}} & -v \\ 1 & \frac{m_{22}}{m_{21}} \end{pmatrix} \\ &\in PGL_2(q), \end{aligned}$$

which implies that A_1 and A_2 are in the same right coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$. This completes the proof. □

Remark 1. Following a similar approach, it can be shown that A_1 and A_2 are also in the same left coset of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$.

The map sending x to x^{q+1} is a group endomorphism from $\mathbb{F}_{q^2}^*$ to $\mathbb{F}_q^*$. Observe that $(\frac{w^q}{v})^{q+1} - \frac{1}{v}$ is in $\mathbb{F}_q$. If it is not zero, then

$$(y - \frac{w^q}{v})^{q+1} = (\frac{w^q}{v})^{q+1} - \frac{1}{v} \tag{4}$$

has $q+1$ distinct solutions in $\mathbb{F}_{q^2}$. Out of these solutions, at most two of them satisfy $(-vy + w + w^q)y = 1$ because the degree on y is two. All the other solutions satisfy $xy \neq 1$.

Lemma 2 *Of all the solutions of equation (4), at most two of them are in $\mathbb{F}_q$.*

Proof. The number of solution in $\mathbb{F}_q$ is equal to the degree of $gcd(y^q - y, (y - \frac{w^q}{v})^{q+1} - (\frac{w^q}{v})^{q+1} + \frac{1}{v})$. And

$$\begin{aligned} &(y - \frac{w^q}{v})^{q+1} - (\frac{w^q}{v})^{q+1} + \frac{1}{v} \\ =&(y^q - \frac{w}{v^q})(y - \frac{w^q}{v}) - (\frac{w^q}{v})^{q+1} + \frac{1}{v} \\ \equiv&(y - \frac{w}{v^q})(y - \frac{w^q}{v}) - (\frac{w^q}{v})^{q+1} + \frac{1}{v} \pmod{y^q - y}. \end{aligned}$$

The last polynomial has degree 2. □

We observe that $-vy+w+w^q$ is in $\mathbb{F}_q$ if and only if y is in $\mathbb{F}_q$. Thus we have

Corollary 3 *Suppose that $q \geq 4$, and $(\frac{w^q}{v})^{q+1} - \frac{1}{v} \neq 0$. There must exist one solution of equation (3) that satisfy $x, y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $xy \neq 1$.*

Remark 2. To list all coset representatives of type (I) in Proposition 1, one can find one pair of $(b, c) \in (\mathbb{F}_{q^2} \setminus \mathbb{F}_q) \times (\mathbb{F}_{q^2} \setminus \mathbb{F}_q)$ for every $(v, w) \in \mathbb{F}_q^* \times \mathbb{F}_{q^2}$ by solving equations (3). Assume that $q \geq 4$. In order to solve equations (3), one can build a table indexed by elements in $\mathbb{F}_q^*$. In the entry of index $\alpha \in \mathbb{F}_q^*$, we store 5 distinct $(q+1)$-th roots of α in $\mathbb{F}_{q^2}$. The table will be built in advance, in time at most $\tilde{O}(q^2)$. For given $v \in \mathbb{F}_q^*$ and $w \in \mathbb{F}_{q^2}$, one can find $y \in \mathbb{F}_{q^2}$ satisfying equation (4) and x as $-vy+w+w^q$ in time $\log^{O(1)} q$ such that $xy \neq 1$ and $x, y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ since there are at most 4 such pairs from the discussion above. Thus, determining the dominating case can be done in time $\tilde{O}(q^3)$.

4 Concluding remarks

We summarise our algorithm in Algorithm 1. Based on the discussions above, the number of representatives of type (I), (II), (III) and (IV) is no more than $q^3 - q^2, q^2 - 3q + 2, q^2 + q$ and $q^2 + q$ respectively, thus the total number of representatives of all four types (counting repetitions) is no more than $q^3 + 2q^2 - q + 2$. From Remark 2, we can see that the time complexity is $\tilde{O}(q^3)$. Hence Theorem 1 follows.

Acknowledgements

The authors would like to thank anonymous reviewers, Eleazar Leal, Robert Granger and Frederik Vercauteren for helpful comments and discussions.

References

1. Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodríguez-Henríquez. Computing discrete logarithms in $\mathbb{F}_{3^{6*137}}$ and $\mathbb{F}_{3^{6*163}}$ using Magma. In *Arithmetic of Finite Fields - 5th International Workshop, WAIFI 2014*, pages 3–22, 2014.
2. Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodríguez-Henríquez. Weakness of $\mathbb{F}_{3^{6*1429}}$ and $\mathbb{F}_{2^{4*3041}}$ for discrete logarithm cryptography. *Finite Fields and Their Applications*, 32:148–170, 2015.
3. Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in Cryptology - EUROCRYPT 2014*, pages 1–16, 2014.
4. Qi Cheng, Daqing Wan, and Jincheng Zhuang. Traps to the BGJT-algorithm for discrete logarithms. *LMS Journal of Computation and Mathematics (Special issue for ANTS 2014)*, 17:218–229, 2014.
5. Faruk Göloglu, Robert Granger, Gary McGuire, and Jens Zumbrägel. Discrete logarithms in GF(2^{1971}). NMBRTHRY list, 19/2/2013.

6. Faruk Göloglu, Robert Granger, Gary McGuire, and Jens Zumbrägel. Discrete logarithms in GF(2^{6120}). NMBRTHRY list, 11/4/2013.
7. Faruk Göloglu, Robert Granger, Gary McGuire, and Jens Zumbrägel. On the function field sieve and the impact of higher splitting probabilities. In Ran Canetti and Juan A. Garay, editors, *CRYPTO*, volume 8043 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2013.
8. Faruk Göloglu, Robert Granger, Gary McGuire, and Jens Zumbrägel. Solving a 6120-bit DLP on a desktop computer. In *Selected Areas in Cryptography - SAC 2013*, pages 136–152, 2014.
9. Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. Discrete logarithms in GF(2^{9234}). NMBRTHRY list, 31/1/2014.
10. Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. Discrete logarithms in the Jacobian of a genus 2 supersingular curve over GF(2^{367}). NMBRTHRY list, 30/1/2014.
11. Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. Breaking a '128-bit secure' supersingular binary curve-(or how to solve discrete logarithms in $\mathbb{F}_{2^{4*1223}}$ and $\mathbb{F}_{2^{12*367}}$). In *Advances in Cryptology-CRYPTO 2014*, pages 126–145, 2014.
12. Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the powers of 2. Cryptology ePrint Archive, Report 2014/300, 2014. http://eprint.iacr.org/.
13. Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. arXiv:1507.01495v1, 2015.
14. Ming-Deh Huang and Anand Kumar Narayanan. Finding primitive elements in finite fields of small characteristic. In *Proc. 11th Int. Conf. on Finite Fields and Their Applications, Topics in Finite Fields, AMS Contemporary Mathematics Series*, 2013.
15. Antoine Joux. Discrete logarithms in GF(2^{1778}). NMBRTHRY list, 11/2/2013.
16. Antoine Joux. Discrete logarithms in GF(2^{4080}). NMBRTHRY list, 22/3/2013.
17. Antoine Joux. Discrete logarithms in GF(2^{6168}). NMBRTHRY list, 21/5/2013.
18. Antoine Joux. Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 177–193. Springer, 2013.
19. Antoine Joux. A new index calculus algorithm with complexity L(1/4+o(1)) in small characteristic. In *Selected Areas in Cryptography - SAC 2013*, pages 355–379, 2014.
20. Antoine Joux and Cécile Pierrot. Improving the polynomial time precomputation of frobenius representation discrete logarithm algorithms - simplified setting for small characteristic finite fields. In *Advances in Cryptology - ASIACRYPT 2014*, pages 378–397, 2014.
21. Thorsten Kleinjung. Discrete logarithms in GF(2^{1279}). NMBRTHRY list, 17/10/2014.

Algorithm 1 Algorithm of generating right coset representatives of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$

Input: A prime power $q \geq 4$ and an element $g \in \mathbb{F}_{q^2} - \mathbb{F}_q$
Output: A set S including all right coset representatives of $PGL_2(\mathbb{F}_q)$ in $PGL_2(\mathbb{F}_{q^2})$.

for $\alpha \in \mathbb{F}_q$ **do**
  $R[\alpha] \leftarrow \emptyset$
end for
for $\beta \in \mathbb{F}_{q^2}$ **do**
  $\alpha \leftarrow \beta^{q+1}$
  if the cardinality of $R[\alpha]$ is < 5 **then**
    $R[\alpha] \leftarrow R[\alpha] \cup \{\beta\}$
  end if
end for ▷ Now $R[\alpha]$ is a set consisting of at most 5 $(q+1)$-th root of α.
$S \leftarrow \emptyset$ ▷ Initialize S
for $(v, w) \in \mathbb{F}_q^* \times \mathbb{F}_{q^2}$ **do** ▷ Adding elements of type (I) in Proposition 1
  $\alpha \leftarrow (\frac{w^q}{v})^{q+1} - \frac{1}{v}$
  for $r \in R[\alpha]$ **do**
    $y \leftarrow \frac{w^q}{v} + r$
    $x \leftarrow -vy + w + w^q$
    if $xy \neq 1$ and $x \notin \mathbb{F}_q$ and $y \notin \mathbb{F}_q$ **then**
      $S \leftarrow S \cup \{\begin{pmatrix} 1 & x \\ y & 1 \end{pmatrix}\}$
      break
    end if
  end for
end for
for $(b_1, d_2) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ **do** ▷ Adding elements of type (II) in Proposition 1
  if $b_1 \neq d_2$ **then**
    $S \leftarrow S \cup \{\begin{pmatrix} 1 & b_1 \\ g & d_2 g \end{pmatrix}\}$
  end if
end for
for $d_2 \in \mathbb{F}_q$ **do** ▷ Adding elements of type (III) in Proposition 1
  $S \leftarrow S \cup \{\begin{pmatrix} 0 & 1 \\ g & d_2 g \end{pmatrix}\}$
end for
for $(c_2, d_2) \in \mathbb{F}_q \times \mathbb{F}_q$ **do**
  $S \leftarrow S \cup \{\begin{pmatrix} 0 & 1 \\ 1 + c_2 g & d_2 g \end{pmatrix}\}$
end for
for $c_2 \in \mathbb{F}_q$ **do** ▷ Adding elements of type (IV) in Proposition 1
  $S \leftarrow S \cup \{\begin{pmatrix} 1 & 0 \\ c_2 g & g \end{pmatrix}\}$
end for
for $(c_2, d_2) \in \mathbb{F}_q \times \mathbb{F}_q$ **do**
  $S \leftarrow S \cup \{\begin{pmatrix} 1 & 0 \\ c_2 g & 1 + d_2 g \end{pmatrix}\}$
end for
return S;