ADJOINT REPRESENTATIONS OF BLACK BOX GROUPS $\mathrm{PSL}_2(\mathbb{F}_q)$

ALEXANDRE BOROVIK AND ŞÜKRÜ YALÇINKAYA

Abstract. In the area of computational group theory known as "black box group theory", the following problem by Babai and Beals [2, Problem 10.1] remained unsolved since 1999:

> Given a black-box group known to be isomorphic to $\mathrm{PSL}_2(p^k)$, find an element of order p.

We present a probabilistic algorithm that solves this problem in odd characteristic p. The running time of the algorithm is polynomial in k and $\log p$ if p is known, or linear in p and polynomial in k if p is not known. Our algorithm also finds the characteristic of the underlying field when it is not given as an input.

More generally, given a global exponent for a black box group $\mathbf{Y}$ (that is, an integer E such that $y^E = 1$ for all $x \in \mathbf{Y}$) encrypting PSL_2 over some finite field of unknown odd characteristic p, we construct, in probabilistic time polynomial in $\log E$,

- a black box group $\mathbf{X}$ encrypting SO_3 over the same field as $\mathbf{Y}$ and an effective embedding $\mathbf{Y} \hookrightarrow \mathbf{X}$;
- a black box field $\mathbf{K}$, and
- polynomial time, in $\log E$, isomorphisms

$$\mathrm{SO}_3(\mathbf{K}) \longrightarrow \mathbf{X} \longrightarrow \mathrm{SO}_3(\mathbf{K}).$$

Moreover, if p is known and $\mathbb{F}$ is a standard explicitly given finite field isomorphic to the field on which $\mathbf{Y}$ is defined, then we construct, in time polynomial in $\log E$, isomorphism

$$\mathrm{SO}_3(\mathbb{F}) \longrightarrow \mathrm{SO}_3(\mathbf{K}).$$

We implemented our algorithms on GAP for groups such as $\mathrm{PSL}_2(\mathbb{F})$ for $|\mathbb{F}| = 5463458053$ (a prime number).

Unlike many papers on black box groups, our algorithms make no reference to Discrete Logarithm Oracles or SL_2-oracles. Moreover, in case of small odd characteristics our result acts as an SL_2-oracle because effective recognition of black box finite fields is equivalent to effective recognition of black box fields of prime order p, with the latter solvable in time linear in p.

Our algorithms are Monte Carlo, but become Las Vegas if some additional information about $\mathbf{Y}$ is given, for example, the order of the ground field $\mathbb{F}$.

1. Introduction

1.1. **The principal results.** Black box groups were introduced by Babai and Szemeredi [4] as an idealized setting for randomized algorithms for solving permutation and matrix group problems in computational group theory. A black box group $\mathbf{X}$ is a black box (or an oracle, or a device, or an algorithm) operating with 0–1 strings of uniform length which encrypt (not necessarily in a unique way) elements of some

Date: 14 January 2015.
1991 *Mathematics Subject Classification.* Primary 20P05, Secondary 03C65.

finite group G. In various classes of black box problems the isomorphism type of G could be known in advance or unknown.

All black box groups in this paper are assumed to satisfy Axioms BB1–BB4 from Sections 2.1 and 2.2 although all algorithms in this paper work under weaker axioms BB1–BB3 and BB5 (the latter is from Section 2.3). In particular, we assume that for every black box groups $\mathbf{X}$ we are given a global exponent, that is, an integer E such that $x^E = 1$ for all $x \in \mathbf{X}$.

We propose an algorithm which solves the old problem by Babai and Beals [2, Problem 10.1] that remained open since 1999. We prove the following theorem.

Theorem 1.1. *Given a global exponent E for a black box group $\mathbf{Y}$ encrypting PSL_2 over some finite field of unknown odd characteristic p, we construct a non-trivial unipotent element in $\mathbf{Y}$ in time linear in p and polynomial in $\log E$. In particular, we find the characteristic p of the underlying field.*

If the characteristic p is known in advance, then we construct a non-trivial unipotent element in $\mathbf{Y}$ in time polynomial in $\log E$.

In case of $p = 2$, the Babai-Beals problem has been solved by Kantor and Kassabov [22], we briefly discuss its version in Section 3.8 as an illustration of our methods.

Note that, in the first part of the statement of Theorem 1.1, we do not have any information about the ground field of the group $\mathbf{Y}$. However, we use some form of an upper bound on the size of this field which is implicitly present in the global exponent E.

In the special case of matrix groups, Theorem 1.1 takes the form that also remained unknown until now.

Corollary 1.2. *Given matrices $g_1, \dots, g_m$ in a group $\mathrm{GL}_n(\mathbb{F})$ of matrices over a finite field $\mathbb{F}_{p^k}$ of odd characteristic p which generate subgroup G isomorphic to $\mathrm{SL}_2(\mathbb{F}_{p^l})$, we can find in G a non-trivial unipotent element in probabilistic time polynomial in k, l, m, n and $\log p$.*

Our next result is the solution to the problem of recognizing a black box group encrypting PSL_2 defined over a field of unknown odd characteristic.

Theorem 1.3. *Given a global exponent E for a black box group $\mathbf{Y}$ encrypting PSL_2 over some finite field of unknown odd characteristic p, we construct, in probabilistic time polynomial in $\log E$,*

- *a black box group $\mathbf{X}$ encrypting SO_3 over the same field as $\mathbf{Y}$ and an effective embedding $\mathbf{Y} \hookrightarrow \mathbf{X}$;*
- *a black box field $\mathbf{K}$, and*
- *the following isomorphisms*

$$\mathrm{SO}_3(\mathbf{K}) \longrightarrow \mathbf{X} \longrightarrow \mathrm{SO}_3(\mathbf{K}).$$

If p is known and $\mathbb{F}$ is the standard explicitly given finite field of characteristic p isomorphic to the field on which $\mathbf{Y}$ is defined, then we also construct, in $\log E$-time, an isomorphism

$$\mathrm{SO}_3(\mathbb{F}) \longrightarrow \mathrm{SO}_3(\mathbf{K}).$$

Since, by Theorem 1.1, we can find the characteristic p of the underlying field in time linear in p and polynomial in $\log E$, we have a stronger result in small odd characteristics:

Corollary 1.4. *We construct, in time linear in p and polynomial in $\log E$, an isomorphism*

$$\mathbf{X} \longleftrightarrow \mathrm{SO}_3(\mathbb{F}),$$

where $\mathbb{F}$ is the standard explicitly given finite field.

In particular this means that, in small odd characteristics, our algorithm fully replaces the so-called "SL_2 oracle", an assumption of existence of two-way polynomial time isomorphism between arbitrary black box group encrypting $\mathrm{SL}_2(\mathbb{F}_{p^k})$ and the group $\mathrm{SL}_2(\mathbb{F}_{p^k})$ over the standard explicitly given field $\mathbb{F}_{p^k}$. The first use of an "SL_2 oracle" appeared in 2001; quite a number of papers referring to SL_2 oracles followed.

1.2. **A very brief outline of the proof.** The proof of Theorem 1.3 will be achieved as a sequence of steps some of which are interesting on their own.

(a) We embed
$$\mathbf{Y} \hookrightarrow \mathbf{X},$$
where $\mathbf{X}$ encrypts $\mathrm{SO}_3(\mathbb{F})$, see Theorem 4.1.

(b) Using involutions in $\mathbf{X}$, we construct a black box projective plane $\mathfrak{P}$ that encrypts the projective plane of the 3-dimensional space of adjoint representation of $\mathrm{PGL}_2(\mathbb{F}) \simeq \mathrm{SO}_3(\mathbb{F})$ on its Lie algebra $\mathfrak{l} = \mathfrak{sl}_2(\mathbb{F})$.

(c) We coordinatize $\mathfrak{P}$ by homogeneous coordinates over a black box field $\mathbf{K}$ constructed in the projective plane $\mathfrak{P}$.

(d) We use the action of $\mathbf{X}$ on $\mathfrak{P}$ to construct a matrix representation
$$\mathbf{X} \longrightarrow \mathrm{SO}_3(\mathbf{K}).$$

(e) Coordinatizing $\mathrm{SO}_3(\mathbf{K})$ in a similar way, we construct an isomorphism
$$\mathrm{SO}_3(\mathbf{K}) \twoheadrightarrow \mathbf{X}.$$

(f) The map
$$\mathrm{SO}_3(\mathbb{F}) \twoheadrightarrow \mathrm{SO}_3(\mathbf{K})$$
is constructed from the canonical isomorphism
$$\mathbb{F} \twoheadrightarrow \mathbf{K}$$
from the standard finite field $\mathbb{F}$ onto a black box field $\mathbf{K}$; this isomorphism is polynomial time and exists due to a result by Maurer and Raub [27] formulated in our paper as Theorem 2.2 (the complexity of the inverse isomorphism is unknown).

1.3. **Monte-Carlo algorithms.** Recall that a *Monte-Carlo algorithm* is a randomized algorithm which gives a correct output to a decision problem with probability strictly bigger than $1/2$. The probability of having incorrect output can be made arbitrarily small by running the algorithm sufficiently many times. A Monte-Carlo algorithm with outputs "yes" and "no" is called *one-sided* if the output "yes" is always correct. A special case of Montes–Carlo algorithms is a *Las Vegas algorithm* which either outputs a correct answer or reports failure. A detailed comparison of Monte–Carlo and Las Vegas algorithms, both from practical and theoretical point, can be found in [1].

By the nature of our axioms, all algorithms for black box groups (in the sense of Axioms BB1–BB4 and BB5) are Monte-Carlo. In most applications, our algorithms

can be easily made Las Vegas if additional information of some kind is provided about $\mathbf{X}$—for example a set of its generators, that is, strings in $\mathbf{X}$ which represent a generating set of the group G encrypted by $\mathbf{X}$, or the order of the field $\mathbb{F}$.

The results of this paper suggest that the distinction between Monte-Carlo and Las Vegas probabilistic algorithms is external to the structural theory of black box groups although, of course, it remains quite natural and crucially important in its concrete applications.

1.4. **Terminology and notation.** In what follows we make extensive use of the language of projective geometry, see, for example Coxeter [15] and Hartshorne [20]. Group theoretic terminology mostly follows [18].

1.5. **Organization of the paper.** In Section 2, we discuss the axioms of black box groups and black box fields. We also prove the Tonelli-Shanks algorithm for black box groups. In Section 3, we introduce morphisms and protomorphisms of black box groups and the procedure called the reification of an involution. We also explain how our arguments work in the even characteristic producing a unipotent element in $\mathrm{PSL}_2(2^n)$. In Section 4, we prove a theorem about constructing a black box group encrypting SO_3 from a black box group encrypting PSL_2. In Section 5, we discuss the geometry of involutions in SO_3 and in Section 6, we construct the black box projective plane. In Section 7, we summarize the procedures we can handle in the black box projective plane. In Section 8, we construct a black box subgroup encrypting Sym_4 in a black box group encrypting SO_3 and in Section 9, we apply Hilbert's coordinatization to the black box projective plane and construct a black box field. In Section 10, we prove Theorem 1.1 and in Section 11, we prove Theorem 1.3. In Section 12, we present the complexities of the procedures presented in this paper. Finally, in Section 13, we make a few remarks about possible improvements in our algorithms.

2. Black box groups

2.1. **Axioms for black box groups.** The functionality of a black box $\mathbf{X}$ for a finite group G is specified by the following axioms.

- **BB1** $\mathbf{X}$ produces strings of fixed length $l(\mathbf{X})$ encrypting random (almost) uniformly distributed elements from G; this is done in probabilistic time polynomial in $l(\mathbf{X})$.
- **BB2** $\mathbf{X}$ computes, in probabilistic time polynomial in $l(\mathbf{X})$, a string encrypting the product of two group elements given by strings or a string encrypting the inverse of an element given by a string.
- **BB3** $\mathbf{X}$ decides, in probabilistic time polynomial in $l(\mathbf{X})$, whether two strings encrypt the same element in G—therefore identification of strings is a canonical projection

$$\mathbf{X} \overset{\pi}{\dashrightarrow} G.$$

We shall say in this situation that $\mathbf{X}$ is a *black box over* G or that a black box $\mathbf{X}$ *encrypts* the group G. Notice that we are not making any assumptions of practical computability or the time complexity of the projection π.

A typical example of a black box group is provided by a group G generated in a big matrix group $\mathrm{GL}_n(r^k)$ by several matrices $g_1, \dots, g_l$. The product replacement

algorithm [13] produces a sample of (almost) independent elements from a distribution on G which is close to the uniform distribution (see a discussion and further development in [3, 11, 17, 26, 31, 30, 32]). We can, of course, multiply, invert, compare matrices. Therefore the computer routines for these operations together with the sampling of the product replacement algorithm run on the tuple of generators $(g_1, \dots, g_l)$ can be viewed as a black box $\mathbf{X}$ encrypting the group G. The group G could be unknown—in which case we are interested in its isomorphism type—or its isomorphism type could be known, as it happens in a variety of other black box problems.

The concept of a black box can be applied to rings, fields, and, as we can see in this paper, even to projective planes.

2.2. **Global exponent and Axiom BB4.** Notice that even in routine examples the number of elements of a matrix group G could be astronomical, thus making many natural questions about the black box $\mathbf{X}$ over G—for example, finding the isomorphism type or the order of G—inaccessible for all known deterministic methods. Even when G is cyclic and thus is characterized by its order, existing approaches to finding exact multiplicative orders of matrices over large finite fields are conditional and involve prime factorization of large integers.

Nevertheless black box problems for matrix groups have a feature which makes them more accessible:

BB4 We are given a *global exponent* of $\mathbf{X}$, that is, a natural number E such that $\pi(x)^E = 1$ for all strings $x \in \mathbf{X}$ while computation of x^E is computationally feasible (say, $\log E$ is polynomially bounded in terms of $\log |G|$).

If we know factorization of E into prime factors, we can find the order of any element $x \in \mathbf{X}$ as the minimal divisor e of E such that $x^e = 1$. However, we wish to work with linear groups over fields of large characteristic where factorization of E is becoming unfeasible. Our approach allows us to avoid determination of orders of random elements from $\mathbf{X}$ and consequently avoid making any assumptions about the prime factorization of the global exponent.

For a black box group $\mathbf{X}$ arising from a subgroup in the ambient group $\mathrm{GL}_n(r^k)$, the exponent of $\mathrm{GL}_n(r^k)$ can be taken for a global exponent of $\mathbf{X}$.

2.3. **Axiom BB5.** Our last comment on the axiomatic of black box groups is an observation that in almost all our work in this and subsequent papers [8, 10, 38, 39] Axiom BB4 can be replaced by its corollary, Axiom BB5.

BB5 We are given a partial 1- or 2-valued function ρ of two variables on $\mathbf{X}$ that computes, in probabilistic time polynomial in $l(\mathbf{X})$, square roots in cyclic subgroups of $\mathbf{X}$ in the following sense:

> if $x \in \mathbf{X}$ and $y \in \langle x \rangle$ has square roots in $\langle x \rangle$ then $\rho(x, y)$ is the set of these roots.

In particular,

- if $|x|$ is even, $\rho(x, 1)$ is the subgroup of order 2 in $\langle x \rangle$;
- if $|x|$ is even, then, consecutively applying $\rho(x, \cdot)$ to 2-elements in $\langle x \rangle$, we can find 2-elements in $\langle x \rangle$ of every order present;
- if $|x|$ is odd, and $y \in \langle x \rangle$ then $\rho(x, y)$ is the unique square root of y in $\langle x \rangle$.

We emphasize that Axiom BB5 provides everything needed for construction of centralizers of involutions by the maps ζ_0 and ζ_1 [7].

Axiom BB5 follows from BB4 by the Tonelli-Shanks algorithm [35, 36] applied to the cyclic group $\langle x \rangle$, see the next lemma included here for completeness of exposition (usually the Tonelli-Shanks algorithm is formulated only for multiplicative groups of finite fields).

Lemma 2.1 (The Tonelli-Shanks Algorithm)**.** *Let* $\mathbf{T}$ *be a cyclic black box group of known global exponent* E*. Let* z *be an element in* $\mathbf{T}$ *that has a square root in* $\mathbf{T}$*. Then an element* $t \in \mathbf{T}$ *such that* $t^2 = z$ *can be found in probabilistic polynomial time in* $\log E$*.*

Proof. We set $E = 2^m n$ where $(2, n) = 1$. Given $g \in \mathbf{T}$, we shall say that l is the 2-height of g, if $|g^n| = 2^l$; notice that this is equivalent to 2^l being the largest power of 2 that divides the order $|g|$ of g.

Let $g \in \mathbf{T}$ be an element with maximal 2-height l, that is, the order g is divisible by the maximum power of 2 dividing the order of $\mathbf{T}$. Then, clearly, g can not be a square in $\mathbf{T}$ namely there are no elements $y \in \mathbf{T}$ such that $y^2 = g$. We set

$$a := z^{(n+1)/2}, \quad b := z^n, \quad c := g^n$$

and run the loop:

- Find the smallest positive integer d such that $b^{2^d} = 1$.
- If $d = 0$, then return a since z has odd order.
- If $d > 0$ then repeat until $d = 0$:

$$\text{Set} \quad a := ac^{2^{l-d-1}}, \quad b := bc^{2^l - d}, \quad c := c^{2^{l-d}}, \quad l := d.$$

- When $d = 0$, the element a is the desired square root of z.

□

In this paper, we assume that all our black box groups satisfy assumptions BB1–BB4 or BB1–BB3 and B5.

We emphasize that we do not assume that black box groups under consideration in this paper are given as subgroups of ambient matrix groups; thus our approach is wider than the setup of the computational matrix group project [23]. Notice that we are not using the Discrete Logarithm Oracles for finite fields $\mathbb{F}_q$: in our setup, we start with a black box group without any access to the field over which the group is defined.

2.4. **Black box fields.** We define black box fields by analogy with black box groups, and the reader may wish to compare our exposition with [6]. We note here that, in this paper, we do not necessarily know the characteristic of the field. Therefore we slightly generalize the definition of a black box field given in [6, 27] by removing the assumption that the characteristic of the field is known.

A *black box* (finite) *field* $\mathbf{K}$ is an oracle or an algorithm operating on 0-1 strings of uniform length (input length) which encrypts some finite field $\mathbb{F}$. The oracle can compute $x + y$, xy and decides whether $x = y$ for any strings $x, y \in \mathbf{K}$. If the characteristic p is known, we say that $\mathbf{K}$ is a *black box field of known characteristic* p. We refer the reader to [6, 27] for more details of black box fields of known characteristic and their applications to cryptography.

In this paper, we shall be using some results about the isomorphism problem for black box fields of known characteristic p [27], that is, the problem of constructing an isomorphism and its inverse between $\mathbf{K}$ and an explicitly given finite field $\mathbb{F}_{p^n}$.

The explicit data for a finite field of cardinality p^n is defined to be a system of *structure constants* over the prime field, that is n^3 elements $(c_{ijk})_{i,j,k=1}^n$ of the prime field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (represented as integers in $[0, p-1]$) so that $\mathbb{F}_{p^n}$ becomes a field with ordinary addition and multiplication by elements of $\mathbb{F}_p$, and multiplication determined by

$$s_i s_j = \sum_{k=1}^{n} c_{ijk} s_k,$$

where $s_1, s_2, \ldots, s_n$ denotes a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. The concept of an explicitly given field of order p^n is robust; indeed, Lenstra Jr. has shown in [24, Theorem 1.2] that for any two fields A and B of order p^n given by two sets of structure constants $(a_{ijk})_{i,j,k=1}^n$ and $(b_{ijk})_{i,j,k=1}^n$ an isomorphism $A \longrightarrow B$ can be constructed in time polynomial in $n \log p$.

Maurer and Raub [27] proved that a construction of an isomorphism and its inverse between a black box field $\mathbf{K}$ of known characteristic p and an explicitly given field $\mathbb{F}_{p^n}$ is reducible in polynomial time to the same problem for the prime subfield in $\mathbf{K}$ and $\mathbb{F}_p$.

Using our terminology, their proof can be reformulated to yield the following result.

Theorem 2.2. *Let* $\mathbf{K}$ *and* $\mathbf{L}$ *be black box fields of known characteristic* p *encrypting the same finite field and* $\mathbf{K}_0$, $\mathbf{L}_0$ *their prime subfield. Then an isomorphism*

$$\mathbf{K}_0 \longrightarrow \mathbf{L}_0$$

can be extended in time polynomial in the input length to an isomorphism

$$\mathbf{K} \longrightarrow \mathbf{L}.$$

Obviously, if $\operatorname{char} \mathbf{K} = p$ and p is known, we can find multiplicative inverses easily and therefore we always have an isomorphism $\mathbb{F}_p \longrightarrow \mathbf{K}_0$. The existence of the reverse isomorphism $\mathbb{F}_p \longleftarrow \mathbf{K}_0$ would follow from solution of the discrete logarithm problem in $\mathbf{K}_0$. In particular, this means that, for small primes p, every black box field of order p^n is effectively isomorphic to $\mathbb{F}_{p^n}$.

3. Morphisms and protomorphisms

3.1. **Morphisms.** Given two black boxes $\mathbf{X}$ and $\mathbf{Y}$ encrypting finite groups G and H, respectively, we say that a map ζ which assigns strings from $\mathbf{X}$ to strings from $\mathbf{Y}$ is a *morphism* of black box groups, if

- the map ζ is computable in probabilistic time polynomial in $l(\mathbf{X})$ and $l(\mathbf{Y})$, and
- there is an abstract homomorphism $\phi : G \to H$ such that the following diagram is commutative:

$$\begin{array}{ccc} \mathbf{X} & \xrightarrow{\zeta} & \mathbf{Y} \\ \vdots\,{\scriptstyle \pi_{\mathbf{X}}} & & \vdots\,{\scriptstyle \pi_{\mathbf{Y}}} \\ G & \xrightarrow{\phi} & H \end{array}$$

  where $\pi_{\mathbf{X}}$ and $\pi_{\mathbf{Y}}$ are the canonical projections of $\mathbf{X}$ and $\mathbf{Y}$ onto G and H, respectively.

We shall say in this situation that a morphism ζ *encrypts* the homomorphism ϕ. For example, morphisms arise naturally when a black box group $\mathbf{X}$ is given by a generating set and we replace a generating set for the black box group $\mathbf{X}$ by a more convenient one and start sampling the product replacement algorithm for the new generating set; in fact, we replace a black box for $\mathbf{X}$ and deal with a morphism $\mathbf{Y} \longrightarrow \mathbf{X}$ from the new black box $\mathbf{Y}$ into $\mathbf{X}$.

Slightly abusing terminology, we say that a morphism ζ is an embedding, or an epimorphism, etc., if ϕ has these properties. In accordance with standard conventions, hooked arrows

$$\hookrightarrow$$

stand for embeddings and double-headed arrows

$$\twoheadrightarrow$$

for epimorphisms; dotted arrows are reserved for abstract homomorphisms, including natural projections

$$\mathbf{X} \overset{\pi_{\mathbf{X}}}{\dashrightarrow} \pi(\mathbf{X});$$

the latter are not necessarily morphisms, since, by the very nature of black box problems, we do not have efficient procedures for constructing the projection of a black box onto the (abstract) group it encrypts.

3.2. **Black box subgroups.** If we have an embedding of black box groups $\mathbf{Y} \hookrightarrow \mathbf{X}$, we shall say that $\mathbf{Y}$ is a subgroup of $\mathbf{X}$.

Black box subgroups will be constructed in this paper in one of the following three ways:

- We generate $\mathbf{Y}$ by some strings $y_1, \dots, y_m \in \mathbf{X}$ and use some version of the product replacement algorithm [13] for random sampling.
- Given black box subgroups $\mathbf{Y}_1, \dots, \mathbf{Y}_k$ in $\mathbf{X}$, we generate a subgroup $\mathbf{Y} = \langle \mathbf{Y}_1, \dots, \mathbf{Y}_k \rangle$ by taking generating sets in $\mathbf{Y}_i$ and combining them into a generating set in $\mathbf{Y}$.
- $\mathbf{Y}$ is the centralizer in $\mathbf{X}$ of an involution or a proto-involution in the sense of Section 3.5 when we apply a procedure described in Section 3.6 to "populate" $\mathbf{Y}$ and eventually find a generating set for $\mathbf{Y}$.

3.3. **Morphisms as black box groups.** Observe that a map

$$G \overset{\phi}{\dashrightarrow} H$$

from a group to a group is a homomorphism of groups if and only if its graph

$$F = \{(g, \phi(g)) : g \in G\}$$

is a subgroup of $G \times H$.

At this point it becomes useful to introduce direct products of black boxes: if $\mathbf{X}$ encrypts G and $\mathbf{Y}$ encrypts H then the black box $\mathbf{X} \times \mathbf{Y}$ produces pairs of strings (x, y) by sampling $\mathbf{X}$ and $\mathbf{Y}$ independently, with operations carried out componentwise in $\mathbf{X}$ and $\mathbf{Y}$; of course, $\mathbf{X} \times \mathbf{Y}$ encrypts $G \times H$.

This allows us to treat a morphism

$$\mathbf{X} \overset{\zeta}{\dashrightarrow} \mathbf{Y}$$

of black box groups as a black box subgroup $\mathbf{Z} \hookrightarrow \mathbf{X} \times \mathbf{Y}$ encrypting F:

$$\mathbf{Z} = \{(x, \zeta(x)) : x \in \mathbf{X}\}$$

with the natural projection

$$\begin{array}{rcl} \pi_{\mathbf{Z}} : \mathbf{Z} & \longrightarrow & F \\ (x, \zeta(x)) & \mapsto & (\pi_{\mathbf{X}}(x), \phi(\pi_{\mathbf{X}}(x)). \end{array}$$

In practice this means (although in some cases we use a more sophisticated construction) that we can find strings $x_1, \ldots, x_k$ generating $\mathbf{X}$ with known images $y_1 = \zeta(x_1), \ldots, y_k = \zeta(x_k)$ in $\mathbf{Y}$ and then use the product replacement algorithm to run a black box for the subgroup

$$\mathbf{Z} = \langle (x_1, y_1), \ldots, (x_k, y_k) \rangle \leqslant \mathbf{X} \times \mathbf{Y}$$

which is of course exactly the graph $\{ (x, \zeta(x)) \}$ of the homomorphism ζ. Random sampling of the black box $\mathbf{Z}$ returns strings $x \in \mathbf{X}$ with their images $\zeta(x) \in \mathbf{Y}$ already attached.

3.4. **Protomorphisms.** Let $\mathbf{X}$ and $\mathbf{Y}$ be black box groups encrypting groups G and H, respectively, and π the canonical projection of $\mathbf{X} \times \mathbf{Y}$ onto $G \times H$. A *protomorphism* $\mathbf{Z}$ between black box groups $\mathbf{X}$ and $\mathbf{Y}$ is a black box subgroup $\mathbf{Z} < \mathbf{X} \times \mathbf{Y}$ such that $\pi(\mathbf{Z})$ is a the graph of a homomorphism from G to H or from H to G—the direction of homomorphism is not set here. We say that $\mathbf{Z}$ *encrypts* this homomorphism.

We shall construct new black boxes from the given ones, and in these constructions strings in $\mathbf{X}$ will actually be pointers to other black boxes. Therefore it is convenient to think of elements of black boxes as other black boxes—the same way as in the ZF set theory all objects are sets, with some sets being elements of others. A projective plane constructed in Section 6 provides a good example: it could be seen as consisting of points and lines, where a "line" is a black box that produces random "points" on this line and a "point" is a black box that produces random "lines" passing through this point.

In a black box group $\mathbf{X}$, it is frequently useful to associate with an element encrypted by a string $x \in \mathbf{X}$ a black box for the graph of a specific homomorphism, namely, the conjugation by x, viewed as a subgroup of the direct product $\mathbf{X} \times \mathbf{X}$, the latter provided with group operations and equality relation in the obvious way:

$$\mathbf{C}_x = \{(y, y^x) : y \in \mathbf{X}\}.$$

From the computational point of view, treating a homomorphism $\mathbf{X} \longrightarrow \mathbf{Y}$ of black box groups $\mathbf{X}$ and $\mathbf{Y}$ as a black box subgroup in their direct product $\mathbf{X} \times \mathbf{Y}$ has happened to be an efficient conceptualization of previously inaccessible objects, as can be seen, for example, in "reification of involutions", see Section 3.7.

Given black box groups $\mathbf{X}_1, \ldots, \mathbf{X}_n$, we can define their direct product

$$\mathbf{X} = \mathbf{X}_1 \times \cdots \times \mathbf{X}_n$$

in an expected way, consecutively sampling strings $x_i \in \mathbf{X}_i$ to form a random n-tuple $(x_1, \ldots, x_n) \in \mathbf{X}$, and carrying out group operations on $\mathbf{X}$ component-wise. Later in the paper we are using semidirect products of black box groups. They

arise in a situation when we have two black box group $\mathbf{X}$ and $\mathbf{Y}$ and a polynomial time in $l(\mathbf{X})$ and $l(\mathbf{Y})$ procedure for the action of $\mathbf{Y}$ on $\mathbf{X}$ by automorphisms,

$$\begin{array}{ccc} \mathbf{X} \times \mathbf{Y} & \longrightarrow & \mathbf{X} \\ (x, y) & \mapsto & x^y; \end{array}$$

then $\mathbf{X} \rtimes \mathbf{Y}$ is defined as the set of pairs $\mathbf{X} \times \mathbf{Y}$ with multiplication

$$(x_1, y_1) \circ (x_2, y_2) := (x_1 x_2^{y_1^{-1}}, y_1 y_2).$$

3.5. **Amalgamation of local proto-involutions.** Let $\mathbf{X}$ be a black box group encrypting a group G. Expanding the terminology from the previous section, a proto-involution $\mathbf{F}$ on $\mathbf{X}$ is a black box subgroup $\mathbf{F} < \mathbf{X} \times \mathbf{X}$ for the graph of an involutive automorphism of $\mathbf{X}$.

Assume that black box subgroups $\mathbf{Y}_1, \dots, \mathbf{Y}_k$ in $\mathbf{X}$ encrypting, respectively, subgroups $H_1, \dots, H_k$ in G, and assume that $\langle H_1, \dots, H_k \rangle = G$. Assume that $\phi_1, \dots, \phi_k$ are involutive automorphisms of subgroups $H_1, \dots, H_k$, respectively, and $\mathbf{F}_i$ are proto-involutions on $\mathbf{Y}_i$ encrypting ϕ_i, $i = 1, \dots, k$. We say that the system of proto-involutions $\mathbf{F}_1, \dots, \mathbf{F}_k$ is *consistent* if, in addition to previous assumptions, there exists an automorphism ϕ of G such that $\phi_i = \phi \mid_{H_i}$ for all $i = 1, \dots, k$.

Theorem 3.1 (Amalgamation of local proto-involutions)**.** *If $\mathbf{F}_1, \dots, \mathbf{F}_k$ is a consistent system of proto-involutions on black box subgroups in $\mathbf{X}$, then*

$$\mathbf{F} = \langle \mathbf{F}_1, \dots, \mathbf{F}_k \rangle$$

is a proto-involution on $\mathbf{X}$.

Proof. The proof is self-evident. □

We shall call $\mathbf{F}$ the *amalgam* of proto-involutions $\mathbf{F}_1, \dots, \mathbf{F}_k$.

Theorem 3.2 (Augmentation of a black box group by a proto-involution)**.** *If $\mathbf{F} < \mathbf{X} \times \mathbf{X}$ is a proto-involution on $\mathbf{X}$ representing an involutive automorphism ϕ on G, we can construct an involutive automorphism α of $\mathbf{F}$ by setting*

$$\alpha : (x, x') \mapsto (x', x) \text{ for } (x, x') \in \mathbf{F}.$$

Then the semidirect product $\mathbf{F} \rtimes \{1, \alpha\}$ is a black box encrypting $G \rtimes \langle \phi \rangle$, with $\mathbf{F}$ canonically projecting onto G.

Proof. The proof is self-evident. □

Theorems 3.1 and 3.2 provide the conceptional frame of construction of a black group encrypting $\mathrm{SO}_3(\mathbb{F})$ from a black box group encrypting $\mathrm{PSL}_2(\mathbb{F})$, see Theorem 4.1.

3.6. **Centralizer of a proto-involution.** Let $\mathbf{F} < \mathbf{X} \times \mathbf{X}$ be a proto-involution on $\mathbf{X}$ as defined in Section 3.5. We shall denote pairs of strings in $\mathbf{F}$ as (x, x^φ) and set

$$C_{\mathbf{X}}(\varphi) = \{\, x \in \mathbf{X} \mid (x, x) \in \mathbf{F} \,\}.$$

By definition, φ encrypts some involutive automorphism $a \in \mathrm{Aut}(G)$ of G. It is easy to see that $C_{\mathbf{X}}(\varphi) = \pi^{-1}(C_G(a))$ is the preimage of $C_G(A)$ under the projection $\pi : \mathbf{X} \dashrightarrow G$.

Assume that $\mathbf{X}$ satisfies Axiom BB4 and has a global exponent $E = 2^k m$ with m odd.

If $x \in \mathbf{X}$ is an element of even order then the last non-identity element in the sequence

$$1 \neq x^m,\ (x^m)^2,\ (x^m)^{2^2}, \ldots, (x^m)^{2^{k-1}}, (x^m)^{2^k} = 1$$

is an involution and denoted by $\mathrm{i}(x)$.

If $x \in \mathbf{X}$ is an element of odd order then the element $y = x^{(m+1)/2}$ obviously satisfies $y^2 = x$ and is the unique square root of x in $\langle x \rangle$; we denote $y = \sqrt{x}$.

It follows from the arguments in [7, 12] that we have the map $\zeta = \zeta_0 \sqcup \zeta_1$:

$$\begin{array}{rcl} \zeta : \mathbf{F} & \longrightarrow & C_{\mathbf{X}}(\varphi) \\ (x, x^\varphi) & \mapsto & \begin{cases} \zeta_0((x, x^\varphi)) = \mathrm{i}(x^\varphi x^{-1}) & \text{if } o(x^\varphi x^{-1}) \text{ is even.} \\ \zeta_1((x, x^\varphi)) = \sqrt{x^\varphi x^{-1}} \cdot x & \text{if } o(x^\varphi x^{-1}) \text{ is odd} \end{cases} \end{array}$$

If $\mathbf{X}$ is a simple group of Lie type, then, as shown in [33], ζ_1 is defined with probability $O(1/n)$ where n is the Lie rank of $\mathbf{X}$. Furthermore, the same calculation as in [7, Section 6] proves that elements $\zeta_1((x, x^\varphi))$ are uniformly distributed over $C_{\mathbf{X}}(\varphi)$. Therefore ζ_1 provides an efficient black box for $C_{\mathbf{X}}(\varphi)$. Observe that this construction still works if Axiom BB4 is replaced by a weaker Axiom BB5.

The map ζ_0 is useful when we are interested mostly in involutions in $C_{\mathbf{X}}(\varphi)$, as it happens, for example, in reification of involutions, see Section 3.7.

3.7. **Reification of an involution.** We approach the most fascinating part of the story: identification of an involution in $\mathbf{X}$ from its description. We shall call this procedure the *reification of an involution*.

Following the notation from the previous subsection, assume that $\mathbf{F} < \mathbf{X} \times \mathbf{X}$ is a proto-involution on $\mathbf{X}$ corresponding to an inner automorphism of G, more specifically, to conjugation by an involution $h \in G$. We want to find in $\mathbf{X}$ a string x that represents h. Obviously, $x \in C_{\mathbf{X}}(\varphi)$, and $C_{\mathbf{X}}(\varphi)$ can be constructed as described in the previous subsection. Denote $\mathbf{Y}_1 = C_{\mathbf{X}}(\varphi)$ and observe that $x \in Z(\mathbf{Y}_1)$. Find in $\mathbf{Y}_1$ an involution y_1 and compute $Y_2 = C_{\mathbf{Y}_1}(y_1)$, and so on.

If G is a simple group of Lie type of odd characteristic and of Lie rank n, the length of chains of centralizers is bounded by a polynomial in its Lie rank (and in any case their centralizer chains are not longer than chains of subgroups in G), giving a crude upper bound of $\log |G|$. Also, elements of even order (hence involutions) in Lie groups of odd characteristic are abundant by [21]. Therefore in this particular situation the process quickly produces a subgroup $\mathbf{Y}_l$ which contains x and has the property that all involutions in $\mathbf{Y}_l$ belong to $Z(\mathbf{Y}_l)$ and therefore (taken together with the identity element) form an elementary abelian 2-subgroup $\mathbf{Z}$. Since $x \in \mathbf{Z}$, it can be identified in $\mathbf{Z}$ by testing every possibility. These crude estimates show that the reification procedure works in probabilistic time polynomial in $|\mathbf{Z}|$ and $\log E$, where E is the global exponent of $\mathbf{X}$.

In this paper, reification of involutions is applied to $\mathrm{SO}_3(\mathbb{F})$ in odd characteristic, where proper centralizers are abelian or dihedral, and where $\mathbf{Z}$ is at most of order 4, making the implementation of the procedure pretty fast.

More generally, if G is a simple group of Lie type and odd characteristic, then the computation of $Z(C_{\mathbf{X}}(\varphi))$ can be done in time polynomial in $\log E$ only by the technique of the analysis of centralizers of involutions developed in [8, 10, 38]; details of the enhanced procedure will be published elsewhere, they are not needed in this paper.

3.8. **Involutions in** $\mathrm{PSL}_2(2^n)$**.** Let $\mathbf{X}$ be a black box group encrypting $\mathrm{PSL}_2(2^n)$ for some $n \geqslant 2$. A paper by Kantor and Kassabov [22] contains a construction of an involution in $\mathbf{X}$, a result analogous to the results in this paper. We shall now show how involutions in $\mathrm{PSL}_2(2^n)$ can be most naturally constructed by our methods.

- Take in $\mathbf{X}$ two non-commuting elements y_1 and y_2 of odd orders > 3 (for large n, any two random elements would go with probability pretty close to 1) and generate $\mathbf{Y}_1 = \langle y_1 \rangle$ and $\mathbf{Y}_2 = \langle y_2 \rangle$.
- Generate the black box subgroup $\mathbf{Y} = \langle \mathbf{Y}_1, \mathbf{Y}_2 \rangle$ and observe that it is isomorphic to $\mathrm{PSL}_2(2^m)$ for some $m > 3$.
- It is a well-known property of subgroups $\mathrm{PSL}_2(2^m)$ that $\mathbf{Y}_1$ and $\mathbf{Y}_2$ are inverted by some involution $x \in \mathbf{Y}$. Hence we have two consistent proto-involutions $\mathbf{F}_1$ and $\mathbf{F}_2$ describing automorphisms $y \mapsto y^{-1}$ of $\mathbf{Y}_1$, $\mathbf{Y}_2$, respectively.
- Form the amalgam $\mathbf{F} = \langle \mathbf{F}_1, \mathbf{F}_2 \rangle$; and proto-involution φ is the action by conjugation by x.
- The centralizer $C_{\mathbf{X}}(\varphi)$ is a Sylow 2-subgroup containing x.

4. Construction of SO_3 from PSL_2

It will become clear later in this paper that black box groups $\mathrm{PGL}_2 \cong \mathrm{SO}_3$ are more open to analysis than SL_2 or PSL_2. Therefore, extending a black box group encrypting $\mathrm{PSL}_2(\mathbb{F})$ to a black box group encrypting $\mathrm{SO}_3(\mathbb{F})$ is important and it results from amalgamation of proto-involutions, Theorem 3.1, and augmentation of a black box group by a proto-involution, Theorem 3.2.

Theorem 4.1. *Let* $\mathbf{Y}$ *be a black box group encrypting a group* $G = \mathrm{PSL}_2(\mathbb{F})$*, where* $\mathbb{F}$ *is a finite field of unknown odd characteristic. Then, with a given exponent* E *for* $\mathbf{Y}$*, there is a polynomial time in* $\log E$ *algorithm which constructs an external automorphism* δ *of* $\mathbf{Y}$ *that encrypts a diagonal type automorphism* d *of* G *of order* 2 *so that the semidirect product* $\mathbf{X} = \mathbf{Y} \rtimes \langle \delta \rangle$ *encrypts* $G \rtimes \langle d \rangle \simeq \mathrm{SO}_3(\mathbb{F})$.

Proof. We recall from the table of the centralizers of involutions in [19, Table 4.5.1] that G has one conjugacy class of external involutive diagonal automorphisms. Let d be its representative, then $C_G(d) = S \rtimes \langle w \rangle$ where S is a torus of order $(q-1)/2$ or $(q+1)/2$ depending on $q \equiv -1 \bmod 4$ or $q \equiv 1 \bmod 4$, respectively, and w is an involution inverting S. Observe that the order of the torus S is odd. Take an involution $t \in C_G(d)$ inverting S and assume that t is contained in some maximal torus T. By Frattini argument, $G \cdot N_{G\langle d \rangle}(T) = G\langle d \rangle$ and we can assume without loss of generality that d normalizes T.

Notice that $\langle T, S \rangle = G$ and d centralizes S and inverts every element in T. Therefore we can apply amalgamation and augmentation of proto-involutions by using Theorem 3.1 and Theorem 3.2.

Construction of tori $\mathbf{T}$ and $\mathbf{S}$ in $\mathbf{Y}$ with these properties goes as follows. We construct an involution $u \in \mathbf{Y}$ and its centralizer $\mathbf{C} := C_{\mathbf{Y}}(u)$. Note that $\mathbf{C} = \mathbf{T} \rtimes \langle w \rangle$ for some torus $\mathbf{T}$ of even order containing the involution u. Now we find a random element $y \in \mathbf{Y}$ such that the element $z := uu^y$ has odd order and set $\mathbf{S} := \langle z \rangle$. Since w is an involution inverting $\mathbf{T}$, by [28, I.8], a random element in $\mathbf{C}$ is a generator of $\mathbf{T}$ with probability $O(1/\log\log|\mathbb{F}|)$. Moreover, by the similar arguments, the element z is also a generator of some maximal torus $\mathbf{S}$ of odd order with probability $O(1/\log\log|\mathbb{F}|)$.

Hence as soon as we have such tori $\mathbf{T}$ and $\mathbf{S}$ in $\mathbf{Y}$, the amalgam δ of local proto-involutions

$$\begin{aligned} \alpha : \mathbf{T} \to \mathbf{T}, \qquad & s \mapsto s \\ \beta : \mathbf{S} \to \mathbf{S}, \qquad & s \mapsto s^{-1} \end{aligned}$$

is a proto-involution of $\mathbf{Y}$ encrypting the external involutive diagonal automorphism d of G, see Theorem 3.1. All we need is to augment $\mathbf{Y}$ by δ, see Theorem 3.2. □

4.1. **Reification of involutions in $\mathrm{SO}_3(\mathbb{F})$.** Reification of proto-involutions, as desribed in Section 3.7, is the most important procedure involved in our construction of unipotent elements in $\mathrm{SO}_3(\mathbb{F})$ and in the proof of Theorem 1.3.

Theorem 4.2. *Let $\mathbf{X}$ be a black box group encrypting $\mathrm{SO}_3(\mathbb{F})$, where $\mathbb{F}$ is a finite field of unknown odd characteristic and $\mathbb{F} > 9$. Let $s, t \in \mathbf{X}$ be two distinct involutions such that st is not a unipotent element. Then, with a given exponent E for $\mathbf{X}$, there is an algorithm which runs in time polynomial in $\log E$ constructing the involution j commuting with s and t.*

For two distinct involutions $s, t \in \mathbf{X}$, we denote the only involution in $\mathbf{X}$ that commutes with both s and t (if such involution exists) as $\mathbf{j}(s, t)$.

Proof. Notice first of all that, due to basic properties of groups $\mathrm{SO}_3(\mathbb{F})$, the involution j commuting with s and t exists and unique in $\mathrm{Aut}(\mathrm{SO}_3(\mathbb{F})) = \mathrm{SO}_3(\mathbb{F})$.

We set $z := st$. Observe first that since z is not a unipotent element, the involution j commuting with both s and t exists. If the order of z is even, then j is the unique involution in $\langle z \rangle$ which can be computed by square-and-multiply method. If z has odd order, then observe that j centralizes $\mathbf{Z} = \langle z \rangle$ and inverts every element in the torus $\mathbf{T}_s$ containing s; construction of $\mathbf{T}_s$ is similar to construction of tori in the proof of Theorem 4.1. Since the order of z is odd, we have $|\mathbf{Z}| \geq 3$ and so $\mathbf{X} = \langle \mathbf{T}_s, \mathbf{Z} \rangle$.

Now the involution j can be found by amalgamating local proto-involutions

$$\begin{aligned} x \mapsto \quad & x^{-1} \quad \text{on } \mathbf{T}_s \\ x \mapsto \quad & x \quad \text{on } \mathbf{Z} \end{aligned}$$

and reifying the result. The last step can be run very efficiently due to the fact that, in $G = \mathrm{SO}_3(\mathbb{F})$ where $\mathbb{F}$ is a finite field of odd characteristic $|\mathbb{F}| > 9$, involutions $r \in G$ have the property that $Z(C_G(r)) = \langle r \rangle$, see details in Section 3.7. □

5. Geometry of involutions in $\mathrm{PGL}_2(\mathbb{F}) \simeq \mathrm{SO}_3(\mathbb{F})$

Let $G \simeq \mathrm{PGL}_2(\mathbb{F}) \simeq \mathrm{SO}_3(\mathbb{F})$, where $\mathbb{F}$ is a finite field of odd characteristic p. This is the most basic of all groups of Lie type, and for that reason it is very tightly built in the black box setting. We shall see that actions of involutions from G control properties of every facet of the structure of the group and its Lie algebra. Involutions are multifunctional: they act as pointers to tori in the group G, to toric subalgebras in the Lie algebra $\mathfrak{l} = \mathrm{Lie}(G)$ of G, to points and to lines in the projective plane associated with $\mathfrak{l}$ as $\mathbb{F}$-vector space, and they control the polarity in this plane.

5.1. **Involutions.** The Lie algebra $\mathfrak{l} = \mathfrak{sl}_2$ is a vector space of 2×2 matrices of trace 0 with the Lie bracket $[A, B] = AB - BA$. The isomorphism $\mathrm{PGL}_2(\mathbb{F}) \simeq \mathrm{SO}_3(\mathbb{F})$ comes from the adjoint action of $\mathrm{PGL}_2(\mathbb{F})$ on its Lie algebra $\mathfrak{sl}_2$, that is, action by conjugation on $\mathfrak{sl}_2$. In this action, the group PGL_2 becomes the group of automorphisms of $\mathfrak{l} = \mathfrak{sl}_2$ and therefore preserves the Killing form K on $\mathfrak{l}$,

$$K(\alpha, \beta) = \mathrm{Tr}\left(\mathrm{ad}(\alpha) \cdot \mathrm{ad}(\beta)\right);$$

moreover, it coincides with the orthogonal group $\mathrm{SO}_3(\mathfrak{l}, K)$ since K is a symmetric bilinear form.

We denote by $\mathfrak{l}$ the 3-dimensional $\mathbb{F}$-vector space of the canonical representation of $G = \mathrm{SO}_3(\mathbb{F})$. The vectors in $\mathfrak{l}$ will be denoted by low case Greek letters.

Note that a vector $\sigma \in \mathfrak{l}$ is semisimple in the Lie algebra sense if and only if $K(\sigma, \sigma) \neq 0$ and nilpotent if and only if $K(\sigma, \sigma) = 0$.

Every semisimple element σ in $\mathfrak{l}$ gives rise to an involution in G, the half-turn s_σ around the one-dimensional space generated by σ:

$$s_\sigma : \alpha \mapsto \frac{2K(\alpha, \sigma)}{K(\sigma, \sigma)}\sigma - \alpha.$$

Observe that the half-turn s_σ is not changed if we replace σ by a non-zero scalar multiple $c\sigma$.

Moreover, every involution in G is a half-turn. Indeed, in its adjoint action on $\mathfrak{l}$, every involution s from G has eigenvalues $+1, -1, -1$. If σ is an eigenvector for s for the eigenvalue $+1$ then obviously $s = s_\sigma$. Denote the $+1$-eigenspace (the *axis* of the half-turn) s as $\mathfrak{t}_s$. Obviously, $\mathfrak{t}_s$ is a 1-dimensional non-isotropic subspace of $\mathfrak{l}$ and thus a toric subalgebra of $\mathfrak{l}$. If T_s is a torus in G containing s then $\mathfrak{t}_s = \mathrm{Lie}(T_s)$, the Lie algebra of T_s.

Therefore the set $\mathfrak{I}$ of involutions in G is in one-to-one correspondence with the set of regular points of the projective plane $\mathfrak{P} = \mathfrak{P}(\mathfrak{l})$ (that is, images in $\mathfrak{P}$ of semisimple elements of $\mathfrak{l}$).

5.2. **Lines.** Notice that every 1-dimensional subspace $\mathfrak{a}$ in $\mathfrak{l}$ is a Lie subalgebra of $\mathfrak{l}$ and coincides with the Lie algebra $\mathrm{Lie}(A)$ of some 1-dimensional algebraic subgroup $A < G$. Assuming that $|\mathbb{F}| = q$, the latter belongs to one of the three conjugacy classes:

- split tori: cyclic subgroups of order $q - 1$,
- non-split tori: cyclic subgroups of order $q + 1$,
- maximal unipotent subgroups of order q,

see the beautiful paper by Boris Weisfeiler [37].

Therefore the set $\mathfrak{W}$ of 1-dimensional algebraic subgroups A in G is in one-to-one correspondence

$$A \leftrightarrow \mathrm{Lie}(A)$$

with the set of points of the projective plane $\mathfrak{P}$. *We shall call* $\mathfrak{W}$ *the Weisfeiler plane.*

It will be convenient to identify $\mathfrak{W}$ with the dual plane $\mathfrak{P}^*$ of $\mathfrak{P}$ and treat elements of $\mathfrak{W}$ as *lines* of $\mathfrak{P}$. For that we need to describe the incidence relation, that is, the sets of points belonging to a line. There will be two kinds of points:

- *involutive* (or *toric*, or *semisimple*, or *regular*), and
- *unipotent* (or *parabolic*, or *tangent*).

The set of all involutive points in $\mathfrak{P}$ is simply the set of all involutions in G. If A is 1-dimensional subgroup in G, the line $\ell(A)$ associated with it contains all involutions inverting A; if w is one of these involutions, then $\ell(A)$ coincides with the coset Aw.

The key to our analysis is the following simple observation which is the basis of projective metric geometry in the sense of Bachmann [5].

Fact 5.1. *Involutions $r, s, t \in \mathfrak{I}$ are collinear in $\mathfrak{P}$ if and only if $rst \in \mathfrak{I}$.*

5.3. **$\mathfrak{I}$ as a finite symmetric space.** Now we shall study the action of $\mathfrak{I}$ on itself by conjugation.

For $s, t \in \mathfrak{I}$, denote

$$s \circ t = t^s.$$

This is a non-associative binary operation satisfying identities:

SD1 $s \circ s = s$
SD2 $s \circ (s \circ t) = t$
SD3 $r \circ (s \circ t) = (r \circ s) \circ (r \circ t)$

Loos [25] introduced these identities for algebraic axiomatization of symmetric spaces; axiom SD3 is called the *left self-distributivity*, see Dehornoy [16]. The involutary plane $\mathfrak{I}$ with the conjugation operation $\circ$ is a finite field analogue of the real hyperbolic (Lobachevsky) plane viewed as a symmetric space; we shall refer to its geometry as Lobachevsky geometry.

5.4. **Harmonic conjugation.** The following two simple observations will be useful in the analysis of our constructions.

Lemma 5.2. *Involutions s, t and $s \circ t = t^s$ are collinear.*

Proof. This immediately follows from Fact 5.1 since

$$s \cdot t^s \cdot t = s \cdot sts \cdot t = tst = s^t$$

is an involution. □

Lemma 5.3. *Let s and t be two distinct commuting involutions in $\mathfrak{I}$, and assume that $r \in \mathfrak{I}$ has the property that $s^r = t$. Then*

(a) *$r = sh^{\pm 1}$ where $h^{\pm 1}$ are two square roots of st in T_{st};*
(b) *the points $r_1 = sh$ and $r_2 = sh^{-1}$ are harmonic conjugate with respect to s and t.*

Proof. (a) The subgroup $\langle r, s, t\rangle$ is dihedral of order 8 and it lies in the dihedral group $C_G(st) = T_{st} \rtimes \langle r\rangle$, where the statement becomes obvious.

(b) Conjugation by s is a projective collineation of $\mathfrak{P}$; it centralizes s and t and swaps r_1 and r_2 which means that r_1 and r_2 are harmonic conjugate with respect to s and t. □

5.5. **Missing points in $\mathfrak{I}$.** Different lines in $\mathfrak{I}$ contain different number of points.

If A is of order $q-1$, the coset Aw contains $q-1$ involutions, while every line in a projective plane contains $q+1$ points. The missing points are *maximal unipotent* subgroups of G treated as points of $\mathfrak{P}$; the line associated with a 1-dimensional subgroup A contains the point associated with the maximal unipotent subgroup U if and only if A normalizes U. We know that every split torus normalizes exactly two

maximal unipotent subgroup, which adds the two missing points to the associated line.

If $|A| = q$, A is a maximal unipotent subgroup and therefore normalizes itself, which adds the missing point to its line $\ell(A)$.

Finally, if $|A| = q + 1$, then A is a non-split torus and therefore normalizes no unipotent subgroups; all $q + 1$ points in the associated line $\ell(A)$ are involutive.

5.6. **Quadric.** There is another way to map (partially) $\mathfrak{W}$ to $\mathfrak{P}$: assign to each torus $T < G$ the only involution $i(T)$ contained in T. Reversing this map, we assign to each involution $s \in \mathfrak{I}$ the torus $T_s \in \mathfrak{W}$ which contains s and identify s with the Lie subalgebra $\mathfrak{t}_s = \mathrm{Lie}(T_s)$ seen as a point in $\mathfrak{P}$.

If $U \in \mathfrak{W}$ is a maximal unipotent subgroup in G then its Lie algebra $\mathfrak{u} = \mathrm{Lie}(U)$ is a singular point in $\mathfrak{P}$ and belongs to the quadric $\mathfrak{Q}$ in $\mathfrak{P}$ given by the equation $K(\nu, \nu) = 0$ in terms of the Killing form $K(\cdot\,, \cdot)$ on $\mathfrak{l}$. Notice that

$$\mathfrak{Q} = \mathfrak{P} \smallsetminus \mathfrak{I};$$

so the quadric $\mathfrak{Q}$ is the missing (that is, not represented by involutions) part of the projective plane $\mathfrak{P}$. We find ourselves in the axiomatic set-up of projective metric geometry in terms of groups and involutions as it was developed by Bachmann [5] and his school, especially by Schröder [34]. The following result is the apex of projective metric geometry.

Fact 5.4. (Schröder [34]**)** *Let Γ be a projective plane and let Ω be a set of points that contains at most two points of any line of Γ. Assume further that the points in $\Gamma \smallsetminus \Omega$ are in a one-to-one correspondence with the set $\mathbb{I}$ of involutions of some group $\mathbb{G}$ in such a way that any three involutions $i, j, k \in \mathbb{I}$ correspond to collinear points in $\Gamma \smallsetminus \Omega$ if and only if their product $ijk \in \mathbb{I}$. Then there exist a field K and a quadratic form Q on the 3-dimensional vector space K^3 such that $\Gamma = \mathbb{P}^2(K)$ and Ω is the quadric in $\mathbb{P}^2(K)$ given by the equation $Q(x) = 0$.*

As we can see, the configuration that we are in is well understood in the abstract group theory; our task is to analyse it using black box group theory methods. Our principal difficulty is that when we look at the configuration where $\mathfrak{P}$, $\mathfrak{I}$, $\mathfrak{Q}$ are playing the roles of Γ, $\mathbb{I}$, and Ω, respectively, the quadric $\mathfrak{Q}$ is invisible. Indeed, the probability for a random element from G to be unipotent, or for two random involutions from G to produce a unipotent element as their product is $O(1/|\mathbb{F}|)$—that is, astronomically small for a large field $\mathbb{F}$. But, as we shall soon see, although we do not have in our possession the quadric $\mathfrak{Q}$ yet, we have the associated polarity.

5.7. **Polarity.** The key geometric property of half-turns is that two distinct involutions s_σ and s_τ commute if and only if σ and τ are orthogonal to each other, that is, $K(\sigma, \tau) = 0$, and even more so,

$$K(\mathfrak{t}_s, \mathfrak{t}_t) = 0.$$

We say that points $x, y \in \mathfrak{P}$ are *perpendicular* to each other if they represent 1-dimensional subspaces in $\mathfrak{l}$ which are orthogonal to each other; we shall denote this by $x \perp y$. The polar image $\pi(x)$ of a point $x \in \mathfrak{P}$ is defined as

$$\pi(x) = \{\, y \in \mathfrak{P} \mid x \perp y \,\}.$$

It is a straight line in $\mathfrak{P}$. Observe further that $x \in \mathfrak{P}$ is a toric point if and only if $x \notin \pi(x)$ and is a unipotent point if and only if $x \in \pi(x)$.

Now, we shall describe $\pi(U)$ for a unipotent point U seen as a maximal unipotent subgroup. A torus $\mathfrak{t} < \mathfrak{l}$ normalizes a nilpotent subalgebra $\mathfrak{u} < \mathfrak{l}$ if and only if $\mathfrak{b} = \mathfrak{t} \oplus \mathfrak{u}$ is a Borel subalgebra in $\mathfrak{l}$. Since $\mathfrak{u}$ is the nilpotent radical of $\mathfrak{b}$, the Killing form restricted to $\mathfrak{b}$ degenerates on $\mathfrak{u}$, which means that $\mathfrak{b} \perp \mathfrak{u}$; but this could happen if and only if $\mathfrak{t} \perp \mathfrak{u}$. Therefore, in terms of the Weisfeiler plane $\mathfrak{W}$,

$$\pi(U) = \{\, U \,\} \cup \{\, T \in \mathfrak{W} \mid T \ \text{ is a torus and normalizes } \ U \,\}.$$

For an involution $t \in \mathfrak{I}$, we denote $\varpi(t) = \pi(t) \cap \mathfrak{I}$. Then we have

$$\varpi(t) = \{\, x \in \mathfrak{I} \mid [x, t] = 1 \text{ and } x \neq t \,\}.$$

Observe that $\varpi(t) = Tw$ for some involution w, that is, the coset of $T = T_t$ consisting of involutions inverting T.

Similarly, for a unipotent point U, we have

$$\varpi(U) = \{\, x \in \mathfrak{I} \mid x \ \text{ inverts } \ U \,\}.$$

Depending on the nature of the point $t \in \mathfrak{P}$,

$$\varpi(t) = \pi(t) \smallsetminus (\pi(t) \cap \mathfrak{Q})$$

lacks 0, 1 or 2 points of intersection of the straight line $\pi(t)$ with the quadric $\mathfrak{Q}$ and contains, respectively, $q+1$, q, or $q-1$ points. These three types of lines are called *elliptic*, *parabolic*, and *hyperbolic*, respectively.

The parabolic lines are tangent lines to $\mathfrak{Q}$, that is, lines having exactly one point with $\mathfrak{Q}$ in common. In $\mathfrak{I}$, a parabolic line appears as the coset Ut of a maximal unipotent subgroup U in G with respect to an involution t inverting every element in U.

6. The black box projective plane

Let $\mathbf{X}$ be a black box group encrypting $\mathrm{PGL}_2(\mathbb{F}) \simeq \mathrm{SO}_3(\mathbb{F})$ where $\mathbb{F}$ is a finite field of odd characteristic.

Using the black box $\mathbf{X}$ as a computational engine, we shall construct a black box that encrypts the projective plane $\mathfrak{P}$; abusing notation, we shall denote it by the same letter $\mathfrak{P}$. Abusing notation again, we use the symbol $\mathfrak{I}$ to denote the set of involutions in $\mathbf{X}$ and view $\mathfrak{I}$ as a subset of $\mathfrak{P}$.

The elements or objects of $\mathfrak{P}$, *points* and *lines*, are pointers to certain black boxes which will be described now.

6.1. **Points.** There are two types of points in $\mathfrak{P}$; *regular* and *parabolic*.

A *regular point* is a pointer to a triple

$$(s, \mathbf{T}_s, \varpi(s))$$

where $s \in \mathfrak{I}$ is an involution, a $\mathbf{T}_s$ is its torus, that is, the cyclic subgroup of index 2 in $C_{\mathbf{X}}(s)$, and

$$\varpi(s) = \mathbf{T}_s w = \pi(s) \cap \mathfrak{I}$$

is the set of regular points in the polar line $\pi(s)$, where $w \in C_{\mathbf{X}}(s)$ is an involution inverting $\mathbf{T}_s$.

A *parabolic point* is the same as a parabolic line as defined below.

6.2. **Lines.** There are two types of lines in $\mathfrak{P}$; *toric* and *parabolic*.

A *parabolic line* $\mathbf{u}$ is a pointer to a black box for a subgroup $\mathbf{U} \rtimes \langle t \rangle$ where $\mathbf{U} < \mathbf{X}$ encrypts a maximal unipotent subgroup $U < G$ and $t \in \mathbf{X}$ encrypts an involution inverting every element in U. The line $\mathbf{u}$ is incident to two kinds of points:

- q regular points, involutions in the coset $\mathbf{U}t$; and
- $\mathbf{u}$ itself, seen as a point.

A *toric* or *regular line* $\mathbf{l}$ is a black box for a subgroup $\mathbf{T} \rtimes \langle w \rangle$ where $\mathbf{T} < \mathbf{X}$ encrypts a torus T in G and $w \in \mathbf{X}$ encrypts an involution that inverts every element in T. A toric line is incident to the following points:

- If $|T| = q + 1$ then $\mathbf{l}$ is incident only to points represented by involutions in the coset $\mathbf{T}w$;
- If $|T| = q - 1$ then $\mathbf{l}$ is incident to $q - 1$ points represented by involutions in the coset $\mathbf{T}w$ and, in addition, two parabolic points which will be constructed later but in abstract terms correspond to two maximal unipotent subgroups normalized by $\mathbf{T}$.

6.3. **Serendipity construction of parabolic lines.** It happens very rarely that a line through two random regular points s and t is parabolic; the probability of this event behaves asymptotically as $O(1/|\mathbb{F}|)$ and becomes astronomically small for a large field $\mathbb{F}$. However if it happens by a sheer strike of luck, we get a unipotent element $u = st$ and a black box for the parabolic subgroup

$$\mathbf{B} = \langle u^{\mathbf{T}_s} \rangle \rtimes \mathbf{T}_s,$$

its maximal unipotent subgroup

$$\mathbf{U} = \langle u^{\mathbf{T}_s} \rangle,$$

and the set $\mathbf{U}s$ of regular points in the parabolic line. We shall say in this occasion that we constructed a parabolic line

$$\mathbf{u} = s \vee t$$

as the joint of regular points s and t.

6.4. **A line through two regular points.** For two distinct involutions $s, t \in \mathfrak{I}$, define $\mathbf{j}(s, t)$ as the only involution in $\mathfrak{I}$ that commutes with both s and t.

If $\mathbf{j}(s, t)$ does not exist for some $s, t \in \mathfrak{I}$ then $u = st$ is an unipotent element and

$$s \vee t = \langle u^{\mathbf{T}_s} \rangle \rtimes \langle t \rangle$$

is a parabolic line through s and t.

If $\mathbf{j}(s, t)$ exists then the regular part of the line $s \vee t$ through s and t can be computed as

$$(s \vee t) \cap \mathfrak{I} = \varpi(\mathbf{j}(s, t)).$$

Therefore computing $\mathbf{j}(s, t)$ attains critical importance for our algorithms. This is easy when st is of even order, in that case $j(s, t)$ is defined as the only involution in the cyclic group $\langle st \rangle$. If $\mathbf{R} = \langle st \rangle$ is of odd order, we do not immediately have $j = \mathbf{j}(s, t)$ but we know that its action on $\mathbf{X}$ is uniquely defined by the following conditions:

- j centralizes $\mathbf{R}$; and
- j inverts every element in the torus $\mathbf{T} = \mathbf{T}_t$.

As a consequence, we can draw a line $x \vee y$ through any two distinct points $x, y \in \mathfrak{I}$; this is a black box which produces, among other useful goods, the following sets of involutions:

$$x \vee y = \begin{cases} \varpi(\mathbf{j}(x,y)) & \text{if} \quad |xy| \neq p \\ \langle (xy)^{\mathbf{T}_x} \rangle \cdot x & \text{if} \quad |xy| = p \end{cases}$$

6.5. **Intersection of two lines.** We use again reification of involutions for finding intersection $\mathbf{k} \wedge \mathbf{l}$ of any two non-parabolic lines $\mathbf{k}$ and $\mathbf{l}$:

$$\mathbf{k} \wedge \mathbf{l} = \begin{cases} \text{the common point of } \mathbf{k} \text{ and } \mathbf{l}, \text{ if this point belongs to } \mathfrak{I}; \\ \text{otherwise, the tangent line through the common parabolic point of } \mathbf{k} \text{ and } \mathbf{l}. \end{cases}$$

Indeed if the lines $\mathbf{k}$ and $\mathbf{l}$ contain a common involution w then their involutive parts $\mathbf{k} \cap \mathfrak{I}$ and $\mathbf{l} \cap \mathfrak{I}$ are

$$\begin{aligned} \mathbf{k} \cap \mathfrak{I} &= \mathbf{R}w \\ \mathbf{l} \cap \mathfrak{I} &= \mathbf{S}w \end{aligned}$$

for tori

$$\begin{aligned} \mathbf{R} &= \{\, ij \mid i, j \in \mathbf{k} \cap \mathfrak{I} \,\} \\ \mathbf{S} &= \{\, ij \mid i, j \in \mathbf{l} \cap \mathfrak{I} \,\} \end{aligned}$$

inverted by w. Obviously, w can be reified from these conditions.

If the lines $\mathbf{k}$ and $\mathbf{l}$ have no involution in common, then they intersect in a parabolic point and we find ourselves in a serendipity situation: this event is exceedingly rare and manifests itself in $\pi(\mathbf{k}) \vee \pi(\mathbf{l})$ being a parabolic line (and we identify parabolic lines with their tangent points on the quadric):

$$\mathbf{k} \wedge \mathbf{l} = \pi(\mathbf{k}) \vee \pi(\mathbf{l}).$$

6.6. **Polar projection.** If s is a regular point, then s is not incident to its polar line $\pi(s)$. If $x \neq s$ is another point, the line $s \vee x$ is different from $\pi(s)$, and therefore the lines $s \vee x$ and $\pi(s)$ have a unique common point

$$x' = \pi(x) \wedge (s \vee x).$$

We shall denote the map defined by the rule

$$x \mapsto \pi(x) \wedge (s \vee x)$$

by

$$x \mapsto \xi_s(x).$$

This map is nothing more but the central projection with the center s onto $\pi(s)$. We shall call it the *polar projection with center* s or polar projection on the (regular) line $\mathbf{l} = \pi(s)$. When s is chosen to be a point at infinity, ξ_s can be seen as the orthogonal projection of an affine part of $\mathfrak{P}$ onto $\mathbf{l} = \pi(s)$. It is easy to check that the following two formulae for ξ_s are equivalent:

$$\begin{aligned} \xi_s(x) &= \pi(x) \wedge (s \vee x) \\ &= \mathbf{j}(\mathbf{j}(x,s), s). \end{aligned}$$

6.7. **Bisection of angles.**

Lemma 6.1. *Let* $\mathbf{X}$ *be a black box group encrypting* $\mathrm{SO}_3(\mathbb{F})$*, where* $\mathbb{F}$ *is a finite field of unknown odd characteristic. Assume that* $i, j \in \mathbf{X}$ *be two conjugate involutions. Then, given an exponent* E *for* $\mathbf{X}$*, we can find an involution* $x \in \mathbf{X}$ *such that* $i^x = j$ *in time polynomial in* $\log E$*.*

Proof. We set $E = 2^m n$ where $(2, n) = 1$, and set $z = ij$. If the order of z is odd, that is, $z^n = 1$, then notice that $i^{z^{(n+1)/2}} = j$. Now, $z^{(n+1)/2} j$ is an involution conjugating i to j.

Assume now that the order of z is even and k is the involution in $\langle z \rangle$, which is obtained by repeated square-and-multiply method applied to the element $z^n \neq 1$. We denote by $\mathbf{Y}$ the subgroup in $\mathbf{X}$ encrypting $\mathrm{PSL}_2(\mathbb{F})$; it is well-known that $|\mathbf{X} : \mathbf{Y}| = 2$ and $\mathbf{Y} \lhd \mathbf{X}$. Let $\mathbf{T}$ be the maximal torus in $\mathbf{X}$ containing k and $\mathbf{T}^2 = \{t^2 \mid t \in \mathbf{T}\}$, then $\mathbf{T}^2$ is the subgroup of index 2 in $\mathbf{T}$ and $\mathbf{T}^2 = \mathbf{T} \cap \mathbf{Y}$. observe that $z = ij \in \mathbf{T}^2$ because i and j, being conjugate, simultaneously belong or do not belong to $\mathbf{Y}$.

We can now apply the Tonelli-Shanks Lemma 2.1 and find $t \in \mathbf{T}$ such that $t^2 = z$; after that we have

$$i^{tj} = jt^{-1}itj = jt^{-1}jjitj = tjitj = t^2jij = j.$$

□

Lemma 6.2. *Let* $\mathbf{X}$ *be a black box group encrypting* $\mathrm{SO}_3(\mathbb{F})$*, where* $\mathbb{F}$ *is a finite field of unknown odd characteristic. Then, with a given exponent* E *for* $\mathbf{X}$*, we can represent arbitrary element* $x \in \mathbf{X}$ *of order* $|x| > 2$ *as a product of two involutions from* $\mathbf{X}$ *in time polynomial in* $\log E$*.*

Proof. This is another application of reification of involutions. Take an arbitrary semisimple element $y \in \mathbf{X}$ and reify the involution r that inverts x and y. This works in the same way as in the construction of the intersection of the non-parabolic lines. If we end up with a serendipitous discovery of a unipotent element, we need to repeat reification with other choice of y. When we have the involution r, we can decompose

$$x = r \cdot rx.$$

□

7. Toolbox for constructions in the Lobachevsky plane

By restricting all our constructions to $\mathfrak{I}$, we can treat $\mathfrak{I}$ as a structure on its own, a black box Lobachevsky plane. It is a black box that

(a) produces uniformly distributed points from $\mathfrak{I}$;
(b) checks the equality of points;
(c) checks collinearity of triples of points;
(d) for any two points $s, t \in \mathfrak{I}$, computes the half turn of t around s, which we denote by $s \circ t$;
(e) for any involution $t \in \mathfrak{I}$, produces uniformly distributed regular points in the polar image of t:
$$\varpi(t) = \{\, s \in \mathfrak{I} \mid s \circ t = t \text{ and } s \neq t \,\};$$
(f) for any two distinct points $s, t \in \mathfrak{I}$, produces uniformly distributed regular points on the line $s \vee t$ through s and t;

(g) for a regular line $\mathbf{l}$ given by its two distinct points s and t, constructs its pole $\varpi(\mathbf{l})$ (uniquely determined by condition $\varpi(\varpi(\mathbf{l})) = \mathbf{l}$) as $\varpi(\mathbf{l}) = \mathbf{j}(s,t)$;
(h) for any two distinct lines $\mathbf{k}$ and $\mathbf{l}$, finds its intersection point $\mathbf{k} \wedge \mathbf{l}$ or, if the lines k and ℓ do not intersect in $\mathfrak{I}$ and therefore their intersection point z belongs to $\mathfrak{Q}$, computes the tangent line

$$\varpi(\mathbf{k}) \vee \varpi(\mathbf{l})$$

to $\mathfrak{Q}$ at the point z;
(i) for a point $s \in \mathfrak{I}$, computes the polar projection

$$\begin{aligned} \xi_s : \mathfrak{I} \smallsetminus \{ s \} &\longrightarrow \pi(s) \\ x &\mapsto \mathbf{j}(\mathbf{j}(x,s),s); \end{aligned}$$

(j) for any two points $s, t \in \mathfrak{I}$ conjugate under the action of $\mathbf{X}$, finds $r \in \mathfrak{I}$ such that $r \circ s = t$ (Lemma 6.1);
(k) represents any element of $\mathbf{X}$ as a product of two involutions from $\mathbf{X}$ (Lemma 6.2).

The key point is that operations (g), (h), and (i) may serendipitously fail; of course, this happens with asymptotically small probability $O(1/|\mathbb{F}|)$, but still, in theory it may happen. In this case, we accidentally leave $\mathfrak{I}$ and find a nontrivial unipotent element $u \in \mathbf{X}$. In our next paper [9] we explain what to do with u; in this paper, we can simply ignore it either by re-doing calculation from the beginning, or by extending our calculations to the whole plane $\mathfrak{P}$.

However, in Section 10 we show how *to enforce serendipity* by directing calculations towards a unipotent element in $\mathbf{X}$.

8. Construction of Sym_4

The fundamental procedure in the coordinatization of $\mathfrak{P}$ is to construct a black box subgroup encrypting Sym_4 in a black box group encrypting SO_3 over some finite field of odd characteristic. As we shall see, a Sym_4 subgroup provides us with a convenient basis triangle in $\mathfrak{P}$. Therefore, we first prove the following theorem.

Theorem 8.1. *Let $\mathbf{X}$ be a black box group encrypting $\mathrm{SO}_3(\mathbb{F})$, where $\mathbb{F}$ is a finite field of unknown odd characteristic. Then, with a given exponent E for $\mathbf{X}$, there is an algorithm constructing a subgroup encrypting Sym_4 which runs in time polynomial in $\log E$.*

Let $G \cong \mathrm{SO}_3(\mathbb{F})$, where $\mathbb{F}$ is a finite field of odd characteristic. It is well-known that G has two conjugacy classes of involutions. We say that an involution is of $+$-type if the order of its centralizer is $2(q-1)$ and $-$-type if the order of its centralizer is $2(q+1)$. Notice that $C_G(i) = T \rtimes \langle w \rangle$ where T is a torus of order $(q \pm 1)$ and w is an involution inverting T. We will consider the involutions of $+$-type if $q \equiv 1 \bmod 4$ and $-$-type if $q \equiv -1 \bmod 4$ so that the order of the torus T is always divisible by 4; we call them involutions of *right type*.

We set 5-tuple

$$(i, j, x, s, T)$$

where $i \in G$ is an involution of right type, $T < G$ is the torus in $C_G(i)$, $j \in G$ is an involution of right type which inverts T, $x \in G$ is an element of order 3 normalizing $\langle i, j \rangle$ and $s \in T$ is an element of order 4. We also set $k = ij$ and note that k is also of right type. Clearly $\langle i, j, x \rangle \cong \mathrm{Alt}_4$ and $\langle i, j, x, s \rangle \cong \mathrm{Sym}_4$.

The crucial part of the algorithm in the construction of Sym_4 in $\mathbf{X}$ encrypting $\mathrm{SO}_3(\mathbb{F})$ is the construction of an element $x \in \mathbf{X}$ of order 3 permuting some mutually commuting involutions $i, j, k \in \mathbf{X}$ of right type. The following lemma provides explicit construction of such an element.

Lemma 8.2. *Let $G \cong \mathrm{SO}_3(\mathbb{F})$, where $\mathbb{F}$ is a finite field of odd characteristic. Let $i, j, k \in G$ be mutually commuting involutions of right type and $g \in G$ be an arbitrary element. Assume that $h_1 = ij^g$ has odd order m_1 and set $n_1 = h_1^{\frac{m_1+1}{2}}$ and $s = k^{gn_1^{-1}}$. Assume also that $h_2 = js$ has odd order m_2 and set $n_2 = h_2^{\frac{m_2+1}{2}}$. Then the element $x = gn_1^{-1}n_2^{-1}$ permutes i, j, k and x has order 3.*

Proof. Observe first that $i^{n_1} = j^g$ and $j^{n_2} = s$. Then, since $s = k^{gn_1^{-1}}$, we have $j^{n_2} = k^{gn_1^{-1}}$. Hence $j = k^{gn_1^{-1}n_2^{-1}} = k^x$. Now, we prove that $j^x = i$. Since $j^{gn_1^{-1}} = i$, we have $j^x = j^{gn_1^{-1}n_2^{-1}} = i^{n_2^{-1}}$. We claim that $h_2 \in C_G(i)$, which implies that $n_2 \in C_G(i)$, so $j^x = i^{n_2^{-1}} = i$. Now, since $j \in C_G(i)$, $h_2 = js \in C_G(i)$ if and only if $s = k^{gn_1^{-1}} \in C_G(i)$. Moreover, since $i^{n_1} = j^g$, $s \in C_G(i)$ if and only if $k^g \in C_G(j^g)$, equivalently, $k \in C_G(j)$ and the claim follows. It is now clear that $i^x = k$ since $ij = k$, and x has order 3. □

Lemma 8.3. *Let G, i, j, k, h_1 and h_2 be as in Lemma 8.2. Then the probability that h_1 and h_2 have odd orders is bounded from below by $\frac{1}{2} - \frac{1}{2|\mathbb{F}|}$.*

Proof. We first note that the subgroup $\langle i, x\rangle \cong \mathrm{Alt}_4$ is a subgroup of $L \leq G$ where $L \cong \mathrm{PSL}_2(\mathbb{F})$, so the involutions i, j, k belong to a normal subgroup isomorphic to $\mathrm{PSL}_2(\mathbb{F})$. Therefore it is enough to compute the estimate in $H \cong \mathrm{PSL}_2(\mathbb{F})$. Notice that all involutions in H are conjugate. Therefore the probability that h_1 and h_2 have odd orders is the same as the probability of the product of two random involutions from H to be of odd order.

We set $|\mathbb{F}| = q$ and we denote by a one of these numbers $(q \pm 1)/2$ which is odd and by b the other one. Then $|H| = q(q^2-1)/2 = 2abq$ and $|C_H(i)| = 2b$ for any involution $i \in H$. Hence the total number of involutions is

$$\frac{|H|}{|C_H(i)|} = \frac{2abq}{2b} = aq.$$

Now we compute the number of pairs of involutions (i, j) such that their product ij belongs to a torus of order a. Let T be a torus of order a. Then $N_H(T)$ is a dihedral group of order $2a$. Therefore the involutions in $N_H(T)$ form the coset $N_H(T)\backslash T$ since a is odd. Hence, for every torus of order a, we have a^2 pairs of involutions whose product belong to T. The number of tori of order a is $|H|/|N_H(T)| = 2abq/2a = bq$. Hence, there are bqa^2 pairs of involutions whose product belong to a torus of order a. Thus the desired probability is

$$\frac{bqa^2}{(aq)^2} = \frac{b}{q} \geqslant \frac{q-1}{2q} = \frac{1}{2} - \frac{1}{2q}.$$

□

Proof of Theorem 8.1. Let $E = 2^m n$ where $(2, n) = 1$. We first construct an involution $i \in \mathbf{X}$ of right type and an element $s \in C_{\mathbf{X}}(i)$ of order 4. Let $i \in \mathbf{X}$ be an involution constructed from a random element by taking its power using square-and-multiply method. To check whether i is an involution of right type or not, we

search for an element $s \in \mathbf{C} := C_{\mathbf{X}}(i)$ of order 4. Note that a random element from $\mathbf{C}$ can be constructed efficiently by the method described in [7, 12] together with the results in [33]. If i is of right type, then $\mathbf{C}$ contains elements of order 4. Since $\mathbf{C} = \mathbf{T} \rtimes \langle w \rangle$ where $\mathbf{T}$ is a torus of order $q \pm 1$ and w is an involution which inverts $\mathbf{T}$, a random element from $\mathbf{C}$ has order divisible by 4 with probability at least $1/4$. As soon as we find an element $h \in \mathbf{C}$ such that $h^n \neq 1$ and $h^{2n} \neq 1$, then we construct an element $s \in \langle h \rangle$ of order 4 by repeated square-and-multiple method. If we can not find an element of order 4 in $\mathbf{C}$, we deduce that i is not of right type and we start from the beginning.

Let $i \in \mathbf{X}$ be a right type involution. The coset $\mathbf{T}w$ of $\mathbf{T}$ in $\mathbf{C}$ consists of the involutions inverting $\mathbf{T}$, so half of the elements of $\mathbf{C}$ are the involutions inverting $\mathbf{T}$ and half of the involutions in $\mathbf{T}w$ are of the same type as i. We construct an involution $j \in \mathbf{C}$ and check whether j is an involution of right type by following the same arguments above.

Finally, for commuting right type involutions $i, j \in \mathbf{X}$, we construct an element x of order 3 normalizing $\langle i, j \rangle$ by using Lemma 8.2. The probability of constructing such an element $x \in \mathbf{X}$ is at least $\frac{1}{2} - \frac{1}{2|\mathbb{F}|}$ by Lemma 8.3. Hence $\langle s, x \rangle$ is a black box subgroup encrypting Sym_4. □

9. Coordinatization

All we need now is to carry out Hilbert's coordinatization of $\mathfrak{P}$ [20] using our toolbox from Section 7. Then the action of $\mathbf{X}$ on $\mathfrak{I}$ by conjugation will give us a morphism

$$\mathbf{X} \longrightarrow \mathrm{SO}_3(\mathbf{K})$$

for some black box field $\mathbf{K}$ that encrypts a finite field $\mathbb{F}$ of odd characteristic.

9.1. **The spinor basis.** A construction from Section 8 yields a subgroup $\mathbf{H} \simeq \mathrm{Sym}_4$ and all its 24 elements as concrete strings in $\mathbf{X}$, and we shall need to introduce special notation for most of these elements, they will play the central role in later calculations. The symbol $\mathbf{H}$ is chosen to emphasize that the group $\mathbf{H} \simeq \mathrm{Sym}_4$ controls the quaternionic structure on $\mathfrak{l}$ as well as cross-ratio and harmonic conjugation on $\mathfrak{P}$.

We denote the three involutions in the 4-group $\mathbf{E} = O_2(\mathbf{H})$ by e_1, e_2, e_3. If $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$ are their centralizers in $\mathfrak{l}$, we know that they are orthogonal to each other and

$$\mathfrak{l} = \mathfrak{t}_1 \oplus \mathfrak{t}_2 \oplus \mathfrak{t}_3$$

is the weight decomposition for the action of $\mathbf{E}$ on $\mathfrak{l}$ and is therefore a grading of $\mathfrak{l}$:

$$[\mathfrak{t}_1, \mathfrak{t}_2] = \mathfrak{t}_3, \quad [\mathfrak{t}_2, \mathfrak{t}_3] = \mathfrak{t}_1, \quad [\mathfrak{t}_3, \mathfrak{t}_1] = \mathfrak{t}_2.$$

Moreover, an element θ of order 3 from $\mathbf{H}$ cyclically permutes $\mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{t}_3$, which allows us to select a basis in $\mathfrak{l}$ made of

$$\epsilon_1 \in \mathfrak{t}_1, \quad \epsilon_2 = \epsilon_1^\theta \in \mathfrak{t}_2, \quad \text{and} \quad \epsilon_3 = \epsilon_2^\theta \in \mathfrak{t}_3.$$

Since $\mathbf{E}$ lies in the commutator of $\mathbf{H}$, the involutions $e_i \in \mathbf{E}$ have spinor norm 1 and therefore vectors ϵ_i can be chosen to satisfy

$$K(\epsilon_i, \epsilon_i) = 1$$

forming an orthonormal basis in $\mathfrak{l}$,

$$K(\epsilon_i, \epsilon_j) = \delta_{ij}.$$

In particular, the quadric $\mathfrak{Q}$ in $\mathfrak{P}$ can be written by the equation

$$x_1^2 + x_2^2 + x_3^2 = 0$$

in the coordinates x_1, x_2, x_3 associated with the basis $\epsilon_1, \epsilon_2, \epsilon_3$.

In addition, the basis $\epsilon_1, \epsilon_2, \epsilon_3$ seen as a basis of Lie algebra $\mathfrak{l}$ obviously satisfies the Lie relations

$$[\epsilon_1, \epsilon_2] = a\epsilon_3, \quad [\epsilon_2, \epsilon_3] = a\epsilon_1, \quad [\epsilon_3, \epsilon_1] = a\epsilon_2,$$

for some fixed $a \in \mathbb{F}_q^*$. What we found is an analogue of a *spinor basis* (or *Pauli basis*) from quantum mechanics and will be discussed in detail elsewhere.

9.2. **First steps towards the coordinatization of $\mathfrak{P}$.** We know that $\epsilon_1, \epsilon_2, \epsilon_3$ form an orthonormal basis in $\mathfrak{l}$ and e_1, e_2, e_3 have homogeneous coordinates

$$(1, 0, 0), (0, 1, 0), (0, 0, 1);$$

and the quadric $\mathfrak{Q}$ is given in coordinates x_1, x_2, x_3 associated with this basis by the equation

$$x_1^2 + x_2^2 + x_3^2 = 0.$$

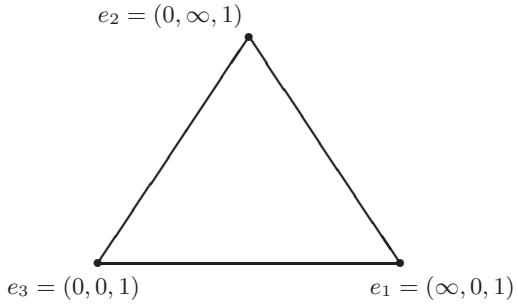
Following traditional notation, we represent lines in $\mathfrak{P}$ by equations of the form

$$X_1x_1 + X_2x_2 + X_3x_3 = 0$$

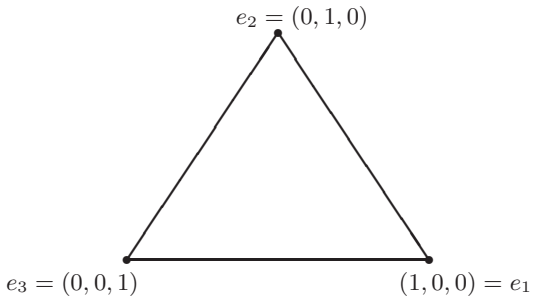
and treat the tuple $[X_1, X_2, X_3]$ as the homogeneous coordinates of the line.

We shall now construct a black box field $\mathbf{K}$. Towards this end, let us take for the extended field $\mathbf{K} \cup \{\infty\}$ the set of points on the coordinate line $e_1 \vee e_3$ assigning the coordinate $x_1 = 0$ to e_3 and $x_1 = \infty$ to e_1.

Taking into account that the coordinatization of $\mathfrak{P}$ has to be consistent with the action of $\mathbf{X}$, and, in particular, with the action of $\mathbf{H}$ on the basis e_1, e_2, e_3, we see that if we take the line $e_1 \vee e_2$ for the line at infinity, we have the following:



And this is the same picture in homogeneous coordinates:



We shall gradually assign coordinates to more and more points in $\mathfrak{P}$, at every step ensuring that the coordinatization is consistent with the action of $\mathbf{X}$ on $\mathfrak{I}$ and $\mathfrak{P}$ and hence with the vector space structure on $\mathfrak{l}$. If a point $x \in \mathfrak{P}$ has coordinates x_1, x_2, x_3, we shall write

$$x = (x_1, x_2, x_3)$$

and similarly denote lines by their coordinates,

$$\ell = [X_1, X_2, X_3]$$

which denote the line

$$\ell = \{\, (x_1, x_2, x_3) \mid X_1x_1 + X_2x_2 + X_3x_3 = 0 \,\}.$$

We note that (x_1, x_2, x_3) and $[X_1, X_2, X_3]$ are homogeneous coordinates, they are defined up to multiplication by a non-zero scalar.

Observe that polarity has a very simple meaning in terms of homogeneous coordinates associated with an orthonormal basis:

$$\pi((x_1, x_2, x_3)) = [X_1, X_2, X_3] \text{ if and only if } X_1 = x_1,\ X_2 = x_2,\ X_3 = x_3.$$

In particular, polar images of the base points ϵ_i have equations $x_i = 0$, $i = 1, 2, 3$, and homogeneous coordinates

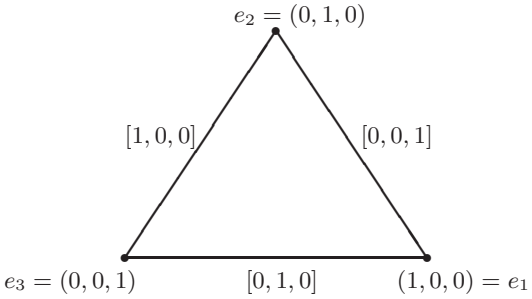
$$\pi(\epsilon_1) = [1, 0, 0], \quad \pi(\epsilon_2) = [0, 1, 0], \quad \pi(\epsilon_3) = [0, 0, 1].$$

When restricted to $\mathfrak{I}$, the polar image of a point $s \in \mathfrak{I}$,

$$\varpi(s) = \mathbf{T}_s w,$$

is a coset of the torus $\mathbf{T}_s$ containing s in the centralizer $C_{\mathbf{X}}(s) = \mathbf{T}_s \rtimes \langle w \rangle$ where w is an involution inverting $\mathbf{T}_s$. Therefore they can be easily computed by the Altseimer-Bray algorithm [7, 12].

So we have, in the black box setup, the following picture.



We shall soon add new points to this picture.

9.3. **The unity element in K.** So far, we know which elements on the x_1-coordinate line represent point 0 and ∞ and now we construct the point $x_1 = 1$. We shall do that by exploiting the group $\mathbf{H}$ in full.

Let θ be an element of order 3 in $\mathbf{H}$ which permutes the basis points e_1, e_2, e_3. Pick in $N_{\mathbf{H}}(\langle\theta\rangle)$ an involution d_1 which commutes with e_1. Observe that $\mathbf{E} \rtimes \langle d_1\rangle$ is a dihedral group of order 8 and therefore $e_2^{d_1} = e_3$.

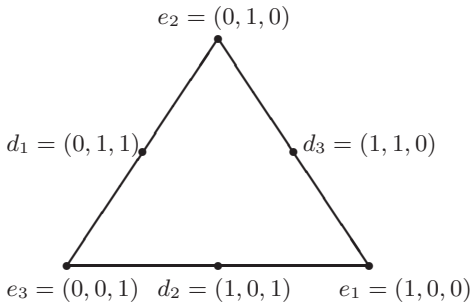
Now turn to the use of homogeneous coordinates. Recall that $e_2 = (0,1,0)$ and $e_3 = (0,0,1)$. There are two involutions which conjugate e_2 and e_3:

$$\begin{aligned}
s_{(0,1,1)}(e_2) &= s_{(0,1,1)}((0,1,0)) \\
&= \frac{2(0\cdot 0 + 1\cdot 1 + 1\cdot 0)}{0^2+1^2+1^2}(0,1,1) - (0,1,0) \\
&= (0,0,1) \\
&= e_3 \\
s_{(0,1,-1)}(e_2) &= s_{(0,1,-1)}((0,1,0)) \\
&= \frac{2(0\cdot 0 + 1\cdot 1 + (-1)\cdot 0)}{0^2+1^2+1^2}(0,1,-1) - (0,1,0) \\
&= (0,0,-1) \\
&= e_3
\end{aligned}$$

We can assign to d_1 the coordinates $(0,1,1)$ and set

$$d_2 = d_1^{\theta} = (1,0,1) \text{ and } d_3 = d_1^{\theta^2} = (1,1,0).$$

So we have now a richer picture:



9.4. **More about H.** We record for future use that the natural isomorphism

$$\mathbf{H} \longrightarrow \mathrm{Sym}_4,$$

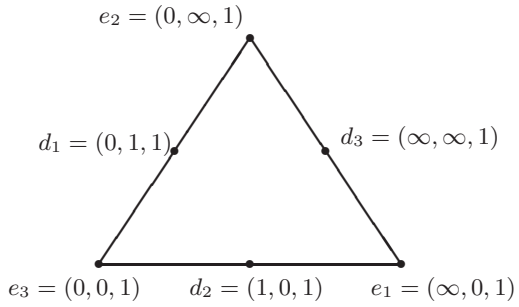
where Sym_4 is seen as the symmetric group of the set $\{\,0,1,2,3\,\}$ in notation chosen in such a way that

$$\begin{array}{lll} e_1 \mapsto (01)(23) & \theta \mapsto (123) & d_1 \mapsto (23) \\ e_2 \mapsto (02)(13) & & d_2 \mapsto (13) \\ e_3 \mapsto (03)(12) & & d_3 \mapsto (12) \end{array} .$$

In particular,

$$d_2^{d_3} = d_3 \circ d_2 = d_1, \quad e_1^{d_3} = d_3 \circ e_1 = e_2.$$

9.5. **Affine coordinates.** Taking, as we have already did, the line $x_3 = 0$ for the line at infinity and the lines $x_2 = 0$ and $x_1 = 0$ for the coordinate axes, we get



Observe that this assignment of coordinates agrees with action by $\mathbf{H}$. In particular, conjugations by d_3 moves the points with x_1-coordinates 0, 1, ∞ on the x_1-axis $e_1 \vee e_3$ to the points with x_2-coordinates 0, 1, ∞, respectively, on the x_2-axis $e_2 \vee e_3$. Therefore we can treat both coordinate axes, the x_1-axis $e_1 \vee e_3$ and the x_2-axis $e_2 \vee e_3$ as the two copies of the projective line $\mathbf{K} \cup \{\infty\}$ over the black box field $\mathbf{K}$ that we will construct on the x_1-axis.

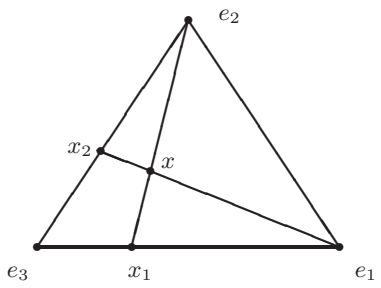
Now on "this side of infinity", on the affine plane $x_3 \neq 0$, the homogeneous coordinates of arbitrary point x can be written as

$$(x_1, x_2, 1),$$

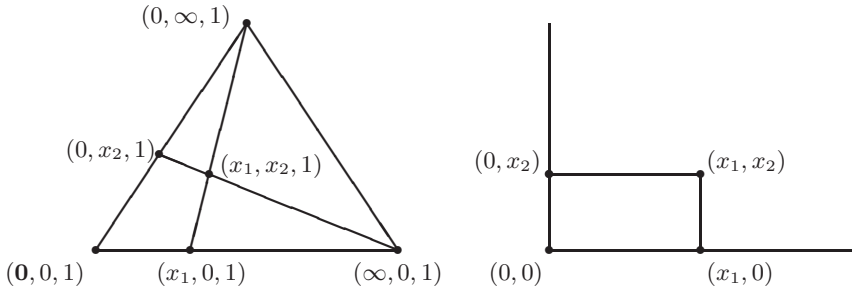
where

$$x_1 = \xi_{e_2}(x) \ \text{ and } \ x_2 = \xi_{e_1}(x)$$

are polar projections of x onto the coordinate axes:



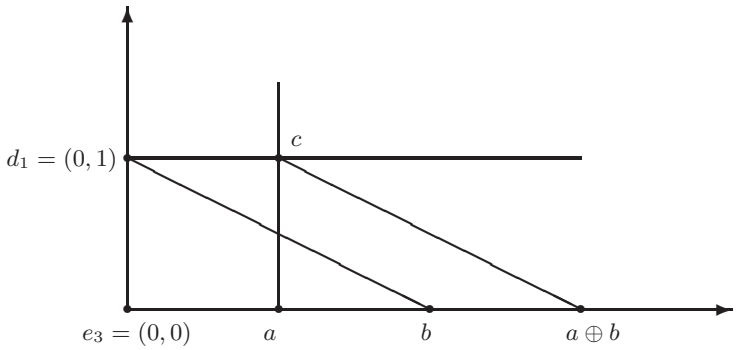
and we get the classical coordinatization of the affine plane [15]:



even before we defined operations of the field $\mathbf{K}$—the latter will be done in the rest of this section.

If x lies on the line at infinity $x_3 = 0$ then we can take any point x' on the line $e_3 \vee x$, construct its affine coordinates $(x'_1, x'_2, 1)$ as above and take the triple $(x'_1, x'_2, 0)$ for the homogeneous coordinates of x.

9.6. **Addition $\oplus$ on K.** Now we can introduce the field operations in the usual way, as shown on the following two diagrams, see Hartshorne [20] for details.



In terms of our toolbox, we first construct

$$c = (a \vee e_2) \wedge (d_1 \vee e_1),$$

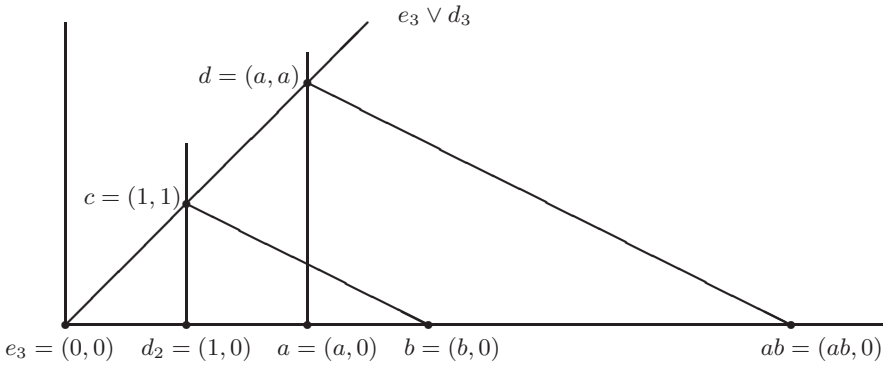
then we construct the point at infinity on the line $d_1 \vee b$ and denote it $\infty_{d_1,b}$:

$$\infty_{d_1,b} = (d_1 \vee b) \wedge (e_1 \vee e_2),$$

then $a \oplus b$ is the point of intersection of the line $c \vee d$ parallel to $d_1 \vee b$ with the x_1-coordinate axis $e_1 \vee e_3$:

$$a \oplus b = (c \vee \infty_{d_1,b}) \wedge (e_1 \vee e_3).$$

9.7. **Multiplication $\otimes$ on K.**



In terms of our toolbox, we first construct the line $x_1 = x_2$ as $e_3 \vee d_3$, then the point $c = (1, 1)$ as

$$(e_3 \vee d_3) \wedge (d_2 \vee e_2),$$

and point $d = (a, a)$ as

$$d = (e_3 \vee d_3) \wedge (a \vee e_2),$$

then the point at infinity of the line $b \vee c$ as

$$\infty_{b,c} = (b \vee c) \wedge (e_1 \vee e_2),$$

the line through the point d parallel to $b \vee c$ as

$$d \vee \infty_{b,c},$$

and, finally, the product $a \otimes b$ as the point of intersection of that line with the x_1-axis $e_1 \vee e_3$:

$$a \otimes b = (e_1 \vee e_3) \wedge (d \vee \infty_{b,c}).$$

9.8. **Inversion and negation in K.** Forming the negative

$$x \mapsto \ominus x$$

and inversion

$$x \mapsto x^{\ominus}$$

on **K** are much easier compute than addition and multiplication. Here are two useful observations.

If $x = (\chi, 0, 1)$ is a point in the x_1-axis,

$$\begin{aligned} s_{(0,0,1)}(x) &= s_{(0,0,1)}((\chi,0,1)) \\ &= \frac{2(0\cdot\chi + 0\cdot 0 + 1\cdot 1)}{0^2+0^2+1^2}(0,0,1) - (\chi,0,1) \\ &= (0,0,2) - (\chi,0,1) \\ &= (-\chi,0,1) \\ &= \ominus x \end{aligned}$$

and

$$\begin{aligned} s_{(1,0,1)}(x) &= s_{(1,0,1)}((\chi,0,1)) \\ &= \frac{2(1\cdot\chi + 0\cdot 0 + 1\cdot 1)}{1^2+0^2+1^2}(1,0,1) - (\chi,0,1) \\ &= (\chi+1,0,\chi+1) - (\chi,0,1) \\ &= (1,0,\chi) \\ &= (1/\chi,0,1) \\ &= x^{\ominus}. \end{aligned}$$

Therefore the field operations of taking negative and inversion

$$x \mapsto \ominus x, \quad x \mapsto x^{\ominus}$$

on $\mathbf{K}$ are computable by single conjugations.

This completes the construction of the black box field $\mathbf{K}$.

9.9. **Square roots in K.** Given an element $x \in \mathbf{K}$, a number of polynomial time Las Vegas algorithms allow us to find a square root of x in $\mathbf{K}$, if it exists. In our context, the most suitable appears to be Ozdemir's singular elliptic curve algorithm [29].

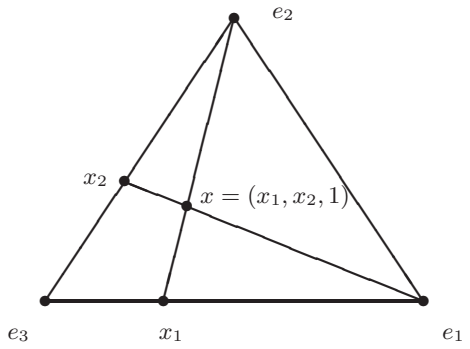
10. Enforced serendipity: construction of unipotent elements

10.1. **Subplane over $\mathbb{F}_p$.** Denote by $\mathbf{K}_0$ the prime subfield (of order p) of $\mathbf{K}$. Starting from element $1 \in \mathbf{K}$, we can construct the image of every residue modulo p by double-and-add algorithm, that is, we can compute the canonical map

$$\mathbb{F}_P = \mathbf{Z}/p\mathbf{Z} \longrightarrow \mathbf{K}_0.$$

This can be carried on the both x_1- and x_2-axes. After computing points x_1 and x_2 on the corresponding axes, we can find the point $x = (x_1, x_2, 1)$ as

$$x = (x_1 \vee e_2) \wedge (x_2 \vee e_1)$$



Hence we can construct the image in $\mathfrak{P}$ of any point $(x_1, x_2, 1)$ in the affine plane over $\mathbb{F}_p$.

10.2. **A serendipitous path to parabolic points, Proof of Theorem 1.1.** Let $\mathbf{Y}$ be a black box group encrypting $\mathrm{PSL}_2(\mathbb{F})$ for some finite field $\mathbb{F}$ of unknown odd characteristic p. By Theorem 4.1, we construct a black box group $\mathbf{X}$ encrypting $\mathrm{SO}_3(\mathbb{F})$. Then, we construct a black box subgroup $\mathbf{H}$ of $\mathbf{X}$ encrypting Sym_4 containing three commuting involutions e_1, e_2, e_3 of right type. By following the procedures described in Section 9, we have a black box field $\mathbf{K}$ with addition, $\oplus$, and multiplication, $\otimes$, together with the procedures for computing multiplicative and additive inverses. Let $\mathbf{K}$ be defined on the axis $e_1 \vee e_3$, that is,

$$\mathbf{K} = \{te_3 \mid t \in \mathbf{T}_{e_2}\}.$$

Let d_1 be the unit element on the axis $e_1 \vee e_3$ found as described in Subsection 9.3.

Observe that if $p \equiv -1 \bmod 4$, then adding d_1 to itself on the coordinate axis $e_1 \vee e_3$ results in constructing the zero element e_3 in the field $\mathbf{K}$ after p iterations whereas if $p \equiv 1 \bmod 4$ then there exists a positive integer $c < p$ such that $c^2 + 1 \equiv 0 \bmod p$ and so $(c-1)d_1 \oplus d_1$ fails, that is, the procedure for this addition produces two involutions t and s whose product $u = ts$ is a nontrivial unipotent element in $\mathbf{X}$.

Thus, if $p \equiv 1 \bmod 4$, then we check whether the element u has order $c^2 + 1$ by using repeated square-and-multiply method. In this case, clearly, $p = c^2 + 1$. If $p \equiv -1 \bmod 4$, then obtaining the involution e_3 by adding d_1 to itself repeatedly determines the characteristic p. To construct a unipotent element, in this case, we first find field elements $c, d \in \mathbb{F}_p$ satisfying $c^2 + d^2 + 1 = 0$ by using the Tonelli-Shanks algorithm. Note that the half of the elements in $\mathbb{F}_p$ are square. Then, the construction of the image in $\mathfrak{P}$ of the point $(c, d, 1)$ results in one of the functions in our toolbox returning the result outside of $\mathfrak{I}$, that is, in discovery of two involutions t and s whose product $u = ts$ is a nontrivial unipotent element in X.

So far we tested our algorithm for finding unipotent elements in $\mathrm{SO}_3(\mathbb{F}_p)$ (in an old version of GAP on an old laptop) for 10-digit primes like $p = 5463458053$, which had provided a sufficient proof of concept.

11. Coordinatization of the action of $\mathbf{X}$ on $\mathfrak{I}$, Proof of Theorem 1.3

11.1. **Construction of the morphism $\mathbf{X} \longrightarrow \mathrm{SO}_3(\mathbf{K})$.** Abusing notation, let us denote strings in $\mathbf{X}$ by the same symbols as elements in $G \simeq \mathrm{SO}_3(\mathbb{F})$ that they encrypt.

The aim of this section is to represent the action of an arbitrary element $x \in \mathbf{X}$ on the projective plane $\mathfrak{P}$ by a 3×3 matrix $\rho(x)$ with coefficient in $\mathbf{K}$. We shall consider several cases:

Case 1. We set

$$\rho(e_1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \rho(e_2) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \rho(e_3) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Case 2. Now we compute $\rho(u)$ for an arbitrary involution $u \in \mathbf{X}$ in "general position" in the sense that u does not commute with any of e_i, $i = 1, 2, 3$.

If now $u \in \mathbf{X}$, involutions $u_i = e_i^u$, $i = 1, 2, 3$, represent in the projective plane $\mathfrak{P}$ vectors ϵ_i^u. We can compute the homogeneous coordinates (u_{i1}, u_{i2}, u_{i3}) of u_i using construction from Section 9.5. The vector (u_{i1}, u_{i2}, u_{i3}) is a scalar multiple of ϵ_i^u. We have to normalize it by finding a scalar $c_i \in \mathbf{K}$ such that

$$c_i^2(u_{i1}^2 + u_{i2}^2 + u_{i3}^2) = 1$$

which is done by taking a square root

$$c_i = \pm\sqrt{\frac{1}{u_{i1}^2 + u_{i2}^2 + u_{i3}^2}}$$

(see Section 9.9). The choice of signs $\pm$ is dictated by the need to make the matrix

$$U = \left(u'_{ij}\right) = \left(\frac{u_{ij}}{c_i}\right)$$

an involution from $\mathrm{SO}_3(\mathbf{K})$; that is, U has to have determinant 1 and be symmetric.

The choice of signs could happen to be not unique and defined up to simultaneous change of two signs, that is, up to multiplication of U on the right by one of the matrices $\rho(e_i)$. Since U and $\rho(e_i)$ are involutions, their product $U\rho(e_i)$ can happen to be an involution if and only if U and $\rho(e_i)$ commute, which is excluded by our choice of u.

Case 3. Now let $u \in \mathbf{X}$ be an involution not in general position, say $u \in C_{\mathbf{X}}(e_1)$. Recall that $\mathbf{C} = C_{\mathbf{X}}(e_1)$ is a dihedral group. If $u = e_1$, we are in Case 1. If $u \neq e_1$, we do random search for an involution $v \in \mathbf{X}$ such that v and $w := u^v$ do not commute with any e_1, e_2, e_3 (this condition is satisfied with probability $1 - O(\frac{1}{q})$). Then $u = vwv$ and we can compute $\rho(v)$ and $\rho(w)$ as in Case 2 and then compute

$$\rho(u) = \rho(v)\rho(w)\rho(v).$$

Case 4. This is the general case. By Lemma 6.2, we know that every $x \in \mathbf{X}$ is either an involution, or a product of two or three involutions, say $x = uv$; so we compute

$$\rho(x) = \rho(u)\rho(v),$$

where $\rho(u)$ and $\rho(v)$ are computed as in Cases 2 and 3.

This gives us an algorithm constructing a morphism

$$\mathbf{X} \longrightarrow \mathrm{SO}_3(\mathbf{K}).$$

11.2. **Construction of the morphism $\mathrm{SO}_3(\mathbf{K}) \longrightarrow \mathbf{X}$.** It is well known that each element in $\mathrm{SO}_3(\mathbf{K})$ is an involution or a product of two involutions, therefore it will suffice to compute $\rho^{-1}(r)$ for an involution $r \in \mathrm{SO}_3(\mathbf{K})$.

We shall think of r as matrix in the same orthonormal basis in which

$$\rho(e_1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \rho(e_2) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \quad \rho(e_3) = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

As it was with computation of ρ, we can easily reduce computation of $\rho^{-1}(r)$ to the case when r is in general position, that is, does not commute with any $\rho(e_i)$, $i = 1, 2, 3$.

Being an involution, r is a symmetric matrix; denote its rows as r_1, r_2, r_3. Now construct in $\mathfrak{P}$ points s_i which have in the homogeneous coordinates associated with the basis e_1, e_2, e_3 the coordinated vectors r_i, $i = 1, 2, 3$. The preimage $s = \rho^{-1}(r)$ satisfies the condition

$$e_i^s = s_i, \quad i = 1, 2, 3.$$

and is in general position with respect to $\{e_i\}$; therefore s is uniquely defined by these conditions.

We can compute an involution $t_1 \in \mathbf{X}$ such that $e_1^{t_1} = s_1$. Then the element (not necessarily an involution) $x = st_1$ belongs to $\mathbf{C} = C_{\mathbf{X}}(e_1)$ and sends e_2 to $e_2^x = e_2^{st_1} = s_2^{t_1} \in \mathbf{C}$. We solve the conjugation problem once more, this time in $\mathbf{C}$, and identify this element $x \in \mathbf{C}$; it is defined uniquely up to multiplication by an element from $\mathbf{E} = \langle e_1, e_2 \rangle$, so we get a coset $\mathbf{E}x$ as an answer. Now $s \in \mathbf{E}xt_1$, and, being in general position, is the only involution there.

11.3. **Construction of the morphism $\mathrm{SO}_3(\mathbb{F}) \to \mathrm{SO}_3(\mathbf{K})$.** Since, in this case, p is known, the order q of the field on which $\mathbf{X}$ is defined can be found by Algorithm 5.5 in [39]. Let $\mathbb{F}$ be standard explicitly given finite field of order q and $\mathbb{F}_0$ be the prime subfield. Assume also that $\mathbf{K}_0$ is the prime subfield of $\mathbf{K}$. Then the isomorphism $\mathbb{F}_0 \to \mathbf{K}_0$ can be extended to an isomorphism in time polynomial in the input length to an isomorphism $\mathbb{F} \to \mathbf{K}$ [27].

12. Complexities

In this section, we compute the complexities of the main procedures presented in this paper.

Let $\mathbf{X}$ be a black box group encrypting $\mathrm{SO}_3(\mathbb{F})$ for some finite field $\mathbb{F}$ of odd characteristic. Let μ denote an upper bound on the time requirement for each group operation in $\mathbf{X}$ and ξ an upper bound on the time requirement, per element, for the construction of random elements of $\mathbf{X}$.

Recall that we are working under the assumptions of Axioms BB1–BB3 and either BB4 or BB5. To that end, we denote by ρ an upper bound for time required for any of the following operations:

- given an element $x \in \mathbf{X}$, determine whether it is of odd or even order;
- given an element $x \in \mathbf{X}$ of even order, compute an involution in $\langle x \rangle$;
- given an element $x \in \mathbf{X}$ of odd order, compute its square root $\sqrt{x}$ in $\langle x \rangle$.

If E is a global exponent of $\mathbf{X}$, then it is easy to see that $\rho = O(\mu \log E)$.

We shall express complexities of our procedures in terms of μ, ξ, ρ and E. If the size $|\mathbb{F}| = q$ of the underlying field is known in advance, then we have $\rho = O(\mu \log q)$

and E can be chosen to be $O(\log q)$ but we do not assume that knowledge in the estimates that follow. We set $E = 2^m n$ where $(2, n) = 1$.

12.1. **Constructing an involution in X.** At least the quarter of elements in $\mathbf{X}$ are of even order [21, Corollary 5.3], therefore an involution can be constructed from a random element in time $O(\xi + \rho)$.

12.2. **Centralizer of an involution s in X.** We shall use the map ζ_1 from [7], which produces uniformly distributed random elements in $C_{\mathbf{X}}(s)$. By the structure of tori and their conjugacy classes in $\mathbf{X}$, it is easy to see that the product of two conjugate involutions has odd order with probability bounded from below by constant, see, for example, [33]. Since $\mathbf{C} := C_{\mathbf{X}}(s) = \mathbf{T}_s \rtimes \langle w \rangle$, where $\mathbf{T}_s$ is a torus of order $(|\mathbb{F}| \pm 1)$ and w is an involution inverting $\mathbf{T}_s$, the half of the elements in $\mathbf{C}$ are the involutions inverting $\mathbf{T}_s$ and, by [28, I.8], the probability of finding a generator of $\mathbf{T}_s$ is $O(1/\log\log|\mathbb{F}|)$. Hence the black box group $\mathbf{C}$ can be constructed in time $O((\xi + \mu + \rho)\log\log E)$.

12.3. **Reification of an involution in X, Lemma 4.2.** Given two involutions $s, t \in \mathbf{X}$, we shall find the complexity of constructing the involution $j := \mathbf{j}(s, t)$ which commutes with both s and t.

Set $z = st$; it is computed in time μ. Testing z for being of odd or even order takes time ρ.

If z has even order, then $j \in \langle z \rangle$ can be computed in time ρ, giving the total time $\mu + 2\rho$.

If z has odd order, then we construct $C_{\mathbf{X}}(s)$ in time $O((\xi+\mu+\rho)\log\log E)$ as in Subsection 12.2. Note that the elements in the generating set for $C_{\mathbf{X}}(s)$ which are not involutions can be taken to be generators for the torus T_s containing s. Let S_{T_s} be a generating set for T_s. By [28, I.8], we can take $|S_{T_s}| = O(\log\log|\mathbb{F}|)$. Clearly $S = S_{T_s} \cup \{z\}$ is a generating set for $\mathbf{X}$ and computing the action of j on S takes $O(\mu\log\log|\mathbb{F}|)$ time. Hence, we run the product replacement algorithm on S to construct a random element x together with its conjugate x^j. This takes time 2ξ. Since the elements of the form $x^j x$ have odd orders with probability bounded from below by a constant, see [33], the construction of $C_{\mathbf{X}}(j)$ takes $O((\xi+\mu+\rho)\log\log E)$ time. Finally, the involution j can be constructed from an element of even order from the torus in $C_{\mathbf{X}}(j)$ by square-and-multiply method. Hence, if z has odd order, the overall cost is $O((\xi + \mu + \rho)\log\log E)$.

12.4. **A line through s and t.** Given two involutions $s, t \in \mathbf{X}$, the line passing through s and t is the coset $\mathbf{T}_j s$ where $j = \mathbf{j}(s, t)$ is the involution commuting with both s and t and $C_{\mathbf{X}}(j) = \mathbf{T}_j \rtimes \langle s \rangle$. Therefore, by Subsection 12.3, the total time needed to construct j and $C_{\mathbf{X}}(j)$ is $O((\xi + \mu + \rho)\log\log E)$.

12.5. **Intersection of two distinct lines k and l.** Given involutions $s_1, s_2, t_1, t_2 \in \mathbf{X}$, where s_1, s_2 define a line $\mathbf{k}$ and t_1, t_2 define a line $\mathbf{l}$, the intersection of $\mathbf{k}$ and $\mathbf{l}$, if exists, is the involution $\mathbf{j}(\mathbf{j}(s_1, s_2), \mathbf{j}(t_1, t_2))$. Therefore it can be computed in time $O((\xi + \mu + \rho)\log\log E)$.

12.6. **Tonelli-Shanks algorithm, Lemma 2.1.** We follow the outline presented in the proof of Lemma 2.1. Let $\mathbf{T}$ be a cyclic black box group and let $E = 2^m n$ be an exponent for $\mathbf{T}$ with n odd. Let $z \in \mathbf{T}$ be an element that has a square root in $\mathbf{T}$. Checking whether z has odd or even order takes ρ time. If $|z|$ is odd,

then the square root of z, which is $z^{(|z|+1)/2}$, can be constructed in time ρ. If $|z|$ is even, then we need to look for an element of maximal 2-height. Observe that the proportion of the elements of maximal 2-height in $\mathbf{T}$ is at least $1/2$ and computing the 2-height of an arbitrary element takes time ρ. The elements a, b, c in the proof of Lemma 2.1 can be set up in time $\mu \log E$ and finding the smallest d takes at most μm time. As the recursion has at most m steps and each step takes at most $\mu \log E$ time, the over all construction takes $O(\rho + \xi + \mu m^2 \log E)$ time.

12.7. **Bisection of angles, Lemma 6.1.** Given two conjugate involutions $i, j \in \mathbf{X}$, we shall find the complexity of constructing a conjugating involution $x \in \mathbf{X}$, that is, $i^x = j$. The construction of x involves only finding the square root of $z = ij$. Therefore it takes $O(\rho + \xi + \mu m^2 \log E)$ time, see Subsection 12.6.

12.8. **Representation of an arbitrary element as a product of involutions, Lemma 6.2.** This is an another application of a reification of an involution and it takes $O((\xi + \mu + \rho) \log \log E)$ time.

12.9. **Construction of Sym_4, Theorem 8.1.** We construct an involution $i \in \mathbf{X}$ and check whether i is of right type. If i is of right type, then the proportion of elements in $C_{\mathbf{X}}(i)$ whose orders are divisible by 4 is at least $1/4$. Therefore, constructing an involution i and checking whether i is of right type or not takes $O(\xi + \rho + \mu \log E)$ time. Similarly, constructing another right type involution j which commutes with i takes $O(\xi + \rho + \mu \log E)$ time. Finally the construction of an element of order 3 permuting, i, j, ij takes $O(\xi + \mu \log E)$ time. Hence the overall construction takes $O(\xi + \rho + \mu \log E)$ time.

12.10. **Coordinate axes and unit elements.** The construction of coordinate axes involves the construction of three commuting involutions of right type and their centralizers, so it takes $O((\xi + \rho) \log \log E + \mu \log E \log \log E)$ time, see Sections 12.2 and 12.9. Moreover, constructing the unit element on one of the axes takes $O(\mu)$ time.

12.11. **Addition and multiplication in K.** On the coordinate axis $e_1 \vee e_3$, that is, $\mathbf{T}_{e_2} e_3$ where $\mathbf{T}_{e_2}$ is the torus in $C_{\mathbf{X}}(e_2)$, we shall find the complexity of $a \oplus b$ and $a \otimes b$ for given two involutions $a, b \in \mathbf{T}_{e_2} e_3$.

Addition involves process of four reifications of involutions and three intersections of lines, and multiplication involves process of six reifications of involutions and four intersections of lines. Hence both addition and multiplication takes $O((\xi + \mu + \rho) \log \log E)$ time.

12.12. **Finding the characteristic and constructing a unipotent element, Theorem 1.1.** Let p denote the characteristic of the underlying field. The construction of a coordinate axis, say $e_1 \vee e_3 = \mathbf{T}_{e_2} e_3$, and the unit element $u \in e_1 \vee e_3$ take $O((\xi + \rho) \log \log E + \mu \log E \log \log E)$ time, see Subsection 12.10.

Computing the characteristic p of the underlying field involves at most p additions in $\mathbf{K}$. Therefore, it can be computed in time $O(p(\xi + \mu + \rho) \log \log E) + \mu \log E)$.

Note that if $p \equiv 1 \bmod 4$, the procedure for the computation of the characteristic p also produces a unipotent element. To construct a unipotent element when $p \equiv -1 \bmod 4$, we first find field elements $c, d \in \mathbb{F}_p$ satisfying $c^2 + d^2 + 1 = 0$ by using Tonelli-Shanks algorithm. By [14, page 212], this takes $O(k^2 \log^2 p)$ time where k is the maximum power of 2 such that 2^k divides $p - 1$. Then, the construction of

the involutions $u \in e_1 \vee e_3$ with the coordinate $(c, 0, 1)$ and $v \in e_1 \vee e_2$ with the coordinate $(0, d, 1)$ takes $O(\log p(\xi + \mu + \rho) \log\log E)$. The intersection of the lines passing through e_2 and u, and e_1 and v has the coordinate $(c, d, 1)$. Clearly the point $(c, d, 1)$ lies on the quadric, so the procedure to construct the intersection of these two lines produces a unipotent element. Thus if $p \equiv -1 \bmod 4$, the the construction of a unipotent element takes $O(p(\xi+\mu+\rho)\log\log E)+\mu \log E \log\log E+k^2 \log^2 p)$.

We note here that if p is given as an input, then, by using double-and-add method, one can construct a unipotent element in time $O(\log p(\xi+\mu+\rho)\log\log E)+\mu \log E \log\log E)$ if $p \equiv 1 \bmod 4$, or $O(\log p((\xi+\mu+\rho)\log\log E)+\mu \log E \log\log E+k^2 \log^2 p)$ if $p \equiv -1 \bmod 4$.

12.13. **Morphism $\mathbf{X} \to \mathrm{SO}_3(\mathbf{K})$.** We shall find the complexity to represent an involution $u \in \mathbf{X}$ in $\mathrm{SO}_3(\mathbf{K})$. Observe that it is enough to compute the complexity when u does not commute with some commuting right type involutions $e_1, e_2, e_3 \in \mathbf{X}$. Then, together with the computations in Subsection 12.8 the complexity of the representation of an arbitrary element follows.

1: Construction of right type involutions e_1, e_2, e_3 in $\mathbf{X}$ takes $O(\xi+\rho+\mu \log E)$ time.

2: Computing the homogenous coordinates of $e_i^u = (u_{i1}, u_{i2}, u_{i3})$ involves the construction of coordinate axes, unit elements on the corresponding axes and the intersection of the corresponding lines. Hence the overall cost is $O((\xi + \rho)\log\log E + \mu \log E \log\log E)$.

3: Normalization of (u_{i1}, u_{i2}, u_{i3}) involves the computation of $\frac{1}{u_{i1}^2+u_{i2}^2+u_{i3}^2}$ and its square root c_i in $\mathbf{K}$. The computation of the quotient takes $O((\xi + \mu + \rho)\log\log E)$ time and, by using, for example, [29, Algorithm 1], the computation of square roots in $\mathbf{K}$ involves constant number of field operations and double-and-add method in $\mathbf{K}$ so it takes $O((\xi + \mu + \rho)\log E \log\log E)$ time.

4: The time needed to compute the matrix $U = \left(\frac{u_{ij}}{c_i}\right)$ is $O((\xi+\mu+\rho)\log\log E)$.

5: Adding all the complexities above, we get $O((\xi + \mu + \rho)\log E \log\log E)$.

12.14. **Morphism $\mathrm{SO}_3(\mathbf{K}) \to \mathbf{X}$.** Let $r \in \mathrm{SO}_3(\mathbf{K})$ be an involution. As in Subsection 12.13, it is enough to find the complexity for the construction of a black box group element representing r when r does not commute with $\rho(e_1), \rho(e_2), \rho(e_3)$. Let r_1, r_2, r_3 be the rows of r. Constructing the involutions $s_1, s_2, s_3 \in \mathfrak{P}$ with the homogenous coordinates r_1, r_2, r_3 involve only reifications of involutions and intersections of lines. Therefore it takes $O((\xi + \mu + \rho)\log\log E)$ time.

Constructing the desired involution $s \in X$ such that $e_i^s = s_i$ involves two times bisection of angles so it takes $O((\xi+\mu+\rho)\log\log E+\mu m^2 \log E)$ time by Subsection 12.7.

Writing an arbitrary element $x \in \mathrm{SO}_3(\mathbf{K})$ as a product of involutions involves only reification of an involution r that inverts x and a random element $y \in \mathrm{SO}_3(\mathbf{K})$. Since a matrix multiplication and taking inverse of an element in $\mathrm{SO}_3(\mathbf{K})$ involves only constant number of multiplications and additions in $\mathbf{K}$, it takes $O((\xi + \mu + \rho)\log\log E)$ time by Subsection 12.11. Therefore, constructing $C_{\mathrm{SO}_3(\mathbf{K})}(r)$ takes $O((\xi + \mu + \rho)\log\log^2 E \log E)$ time.

Hence the overall cost to construct the black box group element representing r is $O((\xi + \mu + \rho)\log\log^2 E \log E + \mu m^2 \log E)$.

13. Concluding remarks

Without doubt, algorithms presented in this paper can be considerably improved.

First of all, in many applications the embedding $\mathrm{PSL}_2 \hookrightarrow \mathrm{PGL}_2$ (Theorem 4.1) is already given for free. In particular, root SL_2-subgroups in groups of Lie type of rank at least 2 already live inside GL_2.

Secondly, it is likely that some gains in speed can come from treating separately the cases $q \equiv 1 \bmod 4$ and $q \equiv -1 \bmod 4$ of black box group encrypting $(\mathrm{P})\mathrm{SL}_2(\mathbb{F}_q)$.

There is a possibility that multiplication and addition of points on a line can be made faster by a fuller use of technique from projective-metric geometry [34].

In this paper, we described several different algebraic and geometric structures associated with SO_3. Our aim was to prepare ground for a more systematic study of possible—and, among them, optimal—data formats for subgroups, lines and points in the black box group environment.

Acknowledgements

This paper would have never been written if the authors did not enjoy the warm hospitality offered to them at the Nesin Mathematics Village in Şirince, Izmir Province, Turkey, in August 2011, August 2012, July 2013, and August 2014; our thanks go to Ali Nesin and to all volunteers, staff, and students who have made the Village a mathematical paradise.

We thank Adrien Deloro for many fruitful discussions, in Şirince and elsewhere.

Our work was partially supported by the Marie Curie FP7 Initial Training Network MALOA (PITN-GA-2008-MALOA no. 238381).

We gratefully acknowledge the use of Paul Taylor's *Commutative Diagrams* package, `http://www.paultaylor.eu/diagrams/`.

References

1. L. Babai, *Randomization in group algorithms: conceptual questions*, Groups and Computation II (L. Finkelstein and W. M. Kantor, eds.), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 1–17.
2. L. Babai and R. Beals, *A polynomial-time theory of black box groups. I*, Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 30–64.
3. L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, J. Algorithms **50** (2004), no. 2, 215–231, SODA 2000 special issue.
4. L. Babai and E. Szemerédi, *On the complexity of matrix group problems*, Proc. 25th IEEE Sympos. Foundations Comp. Sci. (1984), 229–240.
5. F. Bachmann, *Aufbau der geometrie aus dem spiegelungsbegriff: eine vorlesung*, Grundlehren der mathematischen Wissenschaften, Springer, 1959 (German).
6. D. Boneh and R. J. Lipton, *Algorithms for black-box fields and their application to cryptography*, Advances in Cryptology CRYPTO 96 (Neal Koblitz, ed.), Lecture Notes in Computer Science, vol. 1109, Springer Berlin Heidelberg, 1996, pp. 283–297 (English).
7. A. V. Borovik, *Centralisers of involutions in black box groups*, Computational and statistical group theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 7–20.
8. A. V. Borovik and Ş. Yalçınkaya, *Construction of Curtis-Phan-Tits system for black box classical groups*, Available at arXiv:1008.2823v1 [math.GR].
9. ———, *Effective recognition of black box groups* $\mathrm{PSL}_2(q)$ *in small odd characteristic*, in preparation.
10. A.V. Borovik and Ş. Yalçınkaya, *The Curtis-Tits theorem and its generalizations*, in preparation.

11. S. Bratus and I. Pak, *On sampling generating sets of finite groups and product replacement algorithm (extended abstract)*, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 91–96.
12. J. N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245.
13. F. Celler, C. R. Leedham-Green, S. H. Murray, A. C. Niemeyer, and E. A. O'Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), no. 13, 4931–4948.
14. H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006.
15. H.S.M. Coxeter, *Projective geometry*, Springer New York, 2003.
16. P. Dehornoy, *Braids and self-distributivity*, Progress in Mathematics, vol. 192, Birkhäuser Verlag, Basel, 2000.
17. A. Gamburd and I. Pak, *Expansion of product replacement graphs*, Combinatorica **26** (2006), no. 4, 411–429.
18. D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups. Number 1*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1994.
19. ———, *The classification of the finite simple groups. Number 3. Part I. Chapter A*, Mathematical Surveys and Monographs, vol. 40, American Mathematical Society, Providence, RI, 1998.
20. R. Hartshorne, *Foundations of projective geometry*, Lecture Notes, Harvard University, vol. 1966/67, W. A. Benjamin, Inc., New York, 1967.
21. I. M. Isaacs, W. M. Kantor, and N. Spaltenstein, *On the probability that a group element is p-singular*, J. Algebra **176** (1995), no. 1, 139–181.
22. W. M. Kantor and M. Kassabov, *Black box groups $PGL(2, 2^e)$*, J. Algebra **421** (2015), 12–15.
23. C. R. Leedham-Green, *The computational matrix group project*, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 229–247.
24. H. W. Lenstra Jr., *Finding isomorphisms between finite fields*, Mathematics of Computation **56** (1991), no. 193, pp. 329–347 (English).
25. O. Loos, *Symmetric spaces. I: General theory*, W. A. Benjamin, Inc., New York-Amsterdam, 1969.
26. A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363.
27. U. Maurer and D. Raub, *Black-box extension fields and the inexistence of field-homomorphic one-way permutations*, Advances in cryptology—ASIACRYPT 2007, Lecture Notes in Comput. Sci., vol. 4833, Springer, Berlin, 2007, pp. 427–443.
28. D. S. Mitrinović, J. Sándor, and B. Crstici, *Handbook of number theory*, Mathematics and its Applications, vol. 351, Kluwer Academic Publishers Group, Dordrecht, 1996.
29. E. Ozdemir, *Computing square roots in finite fields*, Information Theory, IEEE Transactions on **59** (2013), no. 9, 5613–5615.
30. I. Pak, *The product replacement algorithm is polynomial*, Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci. (2001), 476–485.
31. ———, *What do we know about the product replacement algorithm?*, Groups and Computation III (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 301–347.
32. I. Pak and A. Żuk, *On Kazhdan constants and mixing of random walks*, Int. Math. Res. Not. (2002), no. 36, 1891–1905.
33. C. W. Parker and R. A. Wilson, *Recognising simplicity of black-box groups by constructing involutions and their centralisers*, J. Algebra **324** (2010), no. 5, 885–915.
34. E. M. Schröder, *Eine gruppentheoretisch-geometrische kennzeichnung der projektiv-metrischen geometrien*, Journal of Geometry **18** (1982), no. 1, 57–69 (German).
35. D. Shanks, *Five number-theoretic algorithms*, Proceedings of the Second Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1972) (Winnipeg, Man.), Utilitas Math., 1973, pp. 51–70. Congressus Numerantium, No. VII.

36. A. Tonelli, *Bemerkung ber die auflösung quadratischer congruenzen*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen (1891), 344–346 (German).
37. B. Weisfeiler, *On abstract monomorphisms of k-forms of $PGL(2)$*, J. Algebra **57** (1979), 522–543.
38. Ş. Yalçınkaya, *Construction of long root $SL_2(q)$-subgroups in black-box groups*, Available at arXiv, math.GR/1001.3184v1.
39. Ş. Yalçınkaya, *Black box groups*, Turkish J. Math. **31** (2007), no. suppl., 171–210.

School of Mathematics, University of Manchester, UK; alexandre@borovik.net

Department of Mathematics, İstanbul University, Turkey; sukru.yalcinkaya@gmail.com