FIFTY SHADES OF BLACK

ALEXANDRE BOROVIK AND ŞÜKRÜ YALÇINKAYA

Abstract. The paper proposes a new and systematic approach to the so-called black box group methods in computational group theory. As the starting point of our programme, we construct Frobenius maps on black box groups of untwisted Lie type in odd characteristic and then apply them to black box groups X encrypting groups $(\mathrm{P})\mathrm{SL}_2(q)$ in small odd characteristics. We propose an algorithm constructing a black box field $\mathbb{K}$ isomorphic to $\mathbb{F}_q$, and an isomorphism from $(\mathrm{P})\mathrm{SL}_2(\mathbb{K})$ to X. The algorithm runs in time quadratic in the characteristic of the underlying field and polynomial in $\log q$.

Due to the nature of our work we also have to discuss a few methodological issues of the black box group theory.

Contents

1. Introduction

Black box groups were introduced by Babai and Szemeredi [7] as an idealized setting for randomized algorithms for solving permutation and matrix group problems in computational group theory. This paper belongs to a series of works aimed

1991 *Mathematics Subject Classification.* Primary 20P05, Secondary 03C65.

at development of systematic structural analysis of black box groups [11, 12, 13, 15, 16, 49, 50].

The principal results of this paper are concerned with construction of Frobenius maps on black box Chevalley groups of untwisted type and odd characteristic, they are stated and proven in Section 2.7.

In Section 4, these constructions are applied to prove Theorem 4.1 concerned with recognition of black box groups (P)$\mathrm{SL}_2(q)$ for $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$.

Our approach requires a detailed discussion of some methodological issues of black box group theory; this discussion is spread all over the paper and is supported by some "toy" mathematical results, such as Theorem 3.1 that provides recognition of black box groups $SL_2(2^n)$ under a (rather hypothetical) assumption that we are given an involution in the group.

2. Black box groups and their automorphisms

2.1. **Axioms BB1 – BB3.** A black box group X is a black box (or an oracle, or a device, or an algorithm) operating with 0–1 strings of bounded length which encrypt (not necessarily in a unique way) elements of some finite group G (in various classes of black box problems the isomorphism type of G could be known in advance or unknown). The functionality of a black box is specified by the following axioms, where every operation is carried out in time polynomial in terms of $\log |G|$.

BB1 X produces strings of fixed length $l(X)$ encrypting random (almost) uniformly distributed elements from G; the string length $l(X)$ is polynomially bounded in terms of $\log |G|$.

BB2 X computes, in time polynomial in $l(X)$, 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 X compares, in time polynomial in $l(X)$, whether two strings encrypt the same element in G—therefore identification of strings is a canonical projection

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

We shall say in this situation that X is a *black box over* G or that a black box X *encrypts* the group G. Notice that we are not making any assumptions on computability 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 [26] 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 [5, 6, 17, 30, 37, 39, 41, 40, 42]). 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 X encrypting the group G. The group G could be unknown—in which case we are interested in its isomorphism type—or it could be known, as it happens in a variety of other black box problems.

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 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 multiplicative orders of matrices over finite fields are conditional and involve oracles either for the discrete logarithm problem in finite fields or for prime factorization of integers.

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

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

Usually, for a black box group 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 X.

One of the reasons why the axioms BB1–BB4, and, in particular, the concept of global exponent, appear to be natural, is provided by some surprising model-theoretic analogies. For example, D'Aquino and Macintyre [29] studied non-standard finite fields defined in a certain fragment of bounded Peano arithmetic; it is called $I\Delta_0 + \Omega_1$ and imitates proofs and computations of polynomial time complexity in modular arithmetic. It appears that such basic and fundamental fact as the Fermat Little Theorem has no proof which can be encoded in $I\Delta_0 + \Omega_1$; the best that had so far been proven in $I\Delta_0 + \Omega_1$ is that the multiplicative group $\mathbb{F}_p^*$ of the prime field $\mathbb{F}_p$ has a global exponent $E < 2p$ [29].

We shall discuss model theory and logic connections of black box group theory in some details elsewhere.

2.3. **Relations with other black box groups projects.**

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

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 [34]. Notice that we are not using the Discrete Logarithm Oracles for finite fields $\mathbb{F}_q$: in our original setup, we do not have fields. Nevertheless we are frequently concerned with black box groups encrypting classical linear groups; even so, some of our results (such as Theorems 3.2 and 3.3) do not even involve the assumption that we know the underlying field of the group but instead assume the knowledge of the characteristic of the field without imposing bounds on the size of the field. Finally, in the case of groups over fields of small characteristics we can prove much sharper results, see, for example, Theorem 4.1. Here, it is natural to call characteristic p "small", if it is known and if a linear or quadratic dependency of the running time of algorithm on p does not cause trouble and algorithms are computationally feasible.

So we attach to statements of our results one of the two labels:

- Known characteristic,
- Small characteristic.

Our next paper [15] is dominated by "known characteristic" results. In this one, we concentrate on black box groups of known or small characteristics.

2.4. **Morphisms.** Given two black boxes X and Y encrypting finite groups G and H, correspondingly, we say that a map α which assigns strings from Y to strings from X is a *morphism* of black box groups, if

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

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & Y \\ \vdots\!\downarrow{\scriptstyle \pi_X} & & \vdots\!\downarrow{\scriptstyle \pi_Y} \\ G & \xrightarrow{\beta} & H \end{array}$$

  where π_X and π_Y are the canonical projections of X and Y onto G and H, correspondingly.

We shall say in this situation that a morphism α *encrypts* the homomorphism β. For example, morphisms arise naturally when we replace a generating set for black box group 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 X and deal with a morphism $Y \longrightarrow X$ from the new black box into X. Also, a black box subgroup Z of X is a morphism $Z \hookrightarrow X$.

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

$$\hookrightarrow$$

stand for embeddings and doubleheaded arrows

$$\twoheadrightarrow$$

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

$$X \overset{\pi_X}{\dashrightarrow} \pi(X);$$

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.

We further discuss morphisms in Sections 2.6 and 3.4.

2.5. **Shades of black.** Polynomial time complexity is an asymptotic concept, to work with it we need an infinite class of objects. Therefore our theory refers to some infinite family $\mathcal{X}$ of black box groups ($\mathcal{X}$ of course varies from one black box problem to another). For $X \in \mathcal{X}$, we denote by $l(X)$ the length of 0–1 strings representing elements in X. We assume that, for every $X \in \mathcal{X}$, basic operations of generating, multiplying, comparing strings in X can be done in probabilistic polynomial time in $l(X)$. We assume that encryption of group elements in X is sufficiently economical and $l(X)$ is bounded by a polynomial in $\log |\pi(X)|$.

We also assume that the lengths $\log E(X)$ of global exponents $E(X)$ for $X \in \mathcal{X}$ are bounded by a polynomial in $l(X)$.

Morphism $X \longrightarrow Y$ in $\mathcal{X}$ are understood as defined in Section 2.4 and their running times are bounded by a polynomial in $l(X)$ and $l(Y)$.

At the expense of slightly increasing $\mathcal{X}$ and its bounds for complexity, we can include in $\mathcal{X}$ a collection of explicitly given "known" finite groups. Indeed, using standard computer implementations of finite field arithmetic, we can represent every group $Y = \mathrm{GL}_n(\mathbb{F}_{p^k})$ as an algorithm or computer routine operating on 0–1 strings of length $l(Y) = n^2 k \log p$. Using standard matrix representations for simple algebraic groups, we can represent every group of points $Y = \mathrm{G}(\mathbb{F}_{p^k})$ of a reductive algebraic group G defined over $\mathbb{F}_{p^k}$ as a black box Y generating and processing strings of length $l(Y)$ polynomial in $\log |\mathbb{F}_{p^k}|$ and the Lie rank of Y. Therefore an "explicitly defined" group can be seen a black box group, perhaps of a lighter shade of black.

We shall use direct products of black boxes: if X encrypts G and Y encrypts H then the black box $X \times Y$ generates pairs of strings (x, y) by sampling X and Y independently, with operations carried out componentwise in X and Y; of course, $X \times Y$ encrypts $G \times H$.

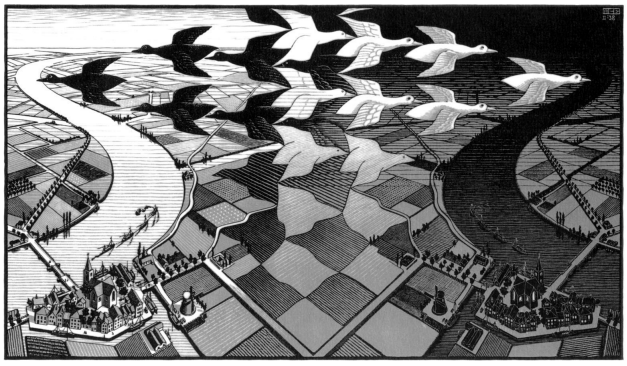

FIGURE 1. M.C. Escher, *Day and Night*, 1938

We feel that the best way to understand a black box group

$$G \blacktriangleleft\!\cdots\!\cdots X$$

is a step-by-step construction of a chain of morphisms

$$G \blacktriangleleft\!\cdots\!\cdots X \blacktriangleleft\!\!\blacktriangleleft\!\!- X_1 \blacktriangleleft\!\!\blacktriangleleft\!\!- X_2 \blacktriangleleft\!\!\blacktriangleleft\!\!- \cdots \blacktriangleleft\!\!\blacktriangleleft\!\!- X_n \blacktriangleleft\!\!\blacktriangleleft\!\!- G$$

at each step changing the shade of black and increasing amount of information provided by black boxes X_i.

Even in relatively simple black box problems we may end up dealing with a sophisticated category of black boxes and their morphisms. Step-by-step transformation of black boxes into "white boxes" and their complex entanglement is captured well by Escher's famous woodcut, Figure 1.

2.6. **Automorphisms as lighter shades of black.** The first application of the "shadows of black" philosophy is the following self-evident theorem which explains how an automorphism of a group can be added to a black box encrypting this group.

Theorem 2.1. *Let X be a black box group encrypting a finite group G and assume that each of k tuples of strings*

$$\tilde{x}^{(i)} = (x_1^{(i)}, \dots, x_m^{(i)}), \quad i = 1, \dots, k,$$

generate X in the sense that the projections $\pi\left(x_1^{(i)}\right), \dots, \pi\left(x_m^{(i)}\right)$ generate G. Assume that the map

$$\pi : x_j^{(i)} \mapsto \pi(x_j^{(i+1 \bmod k)}), \quad i = 0, \dots, k-1, \quad j = 1, \dots, m,$$

can be extended to an automorphism $a \in \operatorname{Aut} G$ of order k. The black box group Y generated in X^k by the strings

$$\bar{x}_j = \left(x_j^{(0)}, x_j^{(1)}, \dots, x_j^{(k-1)}\right), \quad j = 1, \dots, m,$$

encrypts G via the canonical projection on the first component

$$(y_0, \dots, y_{k-1}) \mapsto \pi(y_o),$$

and possess an additional unary operation, cyclic shift

$$\begin{array}{rcl} \alpha : Y & \longrightarrow & Y \\ (y_0, y_2, \dots, y_{k-1}, y_{k-1}) & \mapsto & (y_1, y_2, \dots, y_{k-1}, y_0) \end{array}$$

which encrypts the automorphism a of G in the sense that the following diagram commutes:

$$\begin{array}{ccc} Y & \xrightarrow{\alpha} & Y \\ \vdots & & \vdots \\ G & \xrightarrow{a} & G \end{array}$$

A somewhat more precise formulation of Theorem 2.1 is that we can construct, in polynomial in k and m time, a commutative diagram

$$\begin{array}{ccccccc} X & \xleftarrow{\{\pi_i\}_{0 \leqslant i \leqslant k-1}} & X^k & \xleftarrow{\delta} & Y & \xrightarrow{\alpha} & Y \\ \vdots & & \vdots & & \vdots & & \vdots \\ G & \xleftarrow{\{p_i\}_{1 \leqslant 0 \leqslant k-1}} & G^k & \xleftarrow{d} & G & \xrightarrow{a} & G \end{array} \tag{1}$$

where d is the twisted diagonal embedding

$$\begin{array}{rcl} d : G & \longrightarrow & G^k \\ x & \mapsto & (x, x^a, x^{a^2}, x^{a^{k-1}}), \end{array}$$

and p_i is the projection

$$\begin{array}{rcl} p_i : G^k & \longrightarrow & G \\ (g_0, \dots, g_i, \dots, g_{k-1}) & \mapsto & g_i. \end{array}$$

Of course, this construction leads to memory requirements increasing by factor of k, but, as our subsequent papers [15, 16] show, this is price worth paying. After all, in most practical problems the value of k is not that big, in most interesting cases $k = 2$.

A useful special case of Theorem 2.1 is the following result about amalgamation of black box automorphisms, stated here in an informal wording rather than expressed by a formal commutative diagram.

Theorem 2.2. *Let X be a black box group encrypting a group G. Assume that G contains subgroups $G_1, \dots, G_l$ invariant under an automorphism $\alpha \in \operatorname{Aut} G$ and that these subgroups are encrypted in X as black boxes X_i, $i = 1, \dots, l$, supplied with morphisms $\phi_i : X_i \longrightarrow X_i$ which encrypt restrictions $\alpha|_{G_i}$ of α on G_i.*

Finally, assume $\langle G_i, i = 1, \dots, l\rangle = G$.

Then we can construct, in polynomial in $l(X)$ time, a morphism $\phi : X \longrightarrow X$ which encrypts α.

2.7. **Construction of Frobenius maps.** We now use Theorem 2.1 to construct a Frobenius map on a black box group X encrypting $(\mathrm{P})\mathrm{SL}_2(q)$ with $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. We make sure that the Frobenius map constructed leaves invariant the specified Borel subgroup, thus giving us access to subtler structural properties of the group.

We shall use the following result from [12].

Theorem 2.3 (Small characteristic)**.** [12, Theorem 1.2] *Let X be a black box group encrypting $(\mathrm{P})\mathrm{SL}_2(q)$, where $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$. If $p \neq 5, 7$, then there is a Monte-Carlo algorithm which constructs in X strings u, h, n such that there exists an* (abstract) *isomorphism*

$$\Phi : X \longrightarrow (\mathrm{P})\mathrm{SL}_2(q)$$

with

$$\Phi(u) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \Phi(h) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \Phi(n) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

where t is some primitive element of the field $\mathbb{F}_q$. The running time of the algorithm is quadratic in p and polynomial in $\log q$.

If $p = 5$ or 7, and k has a small divisor ℓ, the same result holds where the running time is polynomial in $\log q$ and quadratic in p^ℓ.

In notation of Theorem 2.3, Theorem 2.1 immediately yields the following remarkably useful result, see its extensions and applications in our subsequent papers [15, 16].

Theorem 2.4 (Small characteristic)**.** (Informal formulation) *Let X be as in Theorem 2.3. Then there is a Monte-Carlo algorithm which constructs a map*

$$X \overset{\phi}{\longrightarrow\!\!\!\!\!\rightarrow} X$$

that corresponds to the Frobenius automorphism $a \mapsto a^p$ of the field $\mathbb{F}_q$ and leaves invariant subgroups U and T and the elements u and w of X.

The running time of the algorithm is quadratic in p and polynomial in $\log q$.

Proof. It suffices to observe that the action of the canonical Frobenius map

$$F : \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \mapsto \begin{bmatrix} a_{11}^p & a_{12}^p \\ a_{21}^p & a_{22}^p \end{bmatrix}$$

on the preimages of $\bar{u}, \bar{w}, \bar{h}$ in $\mathrm{PSL}_2(q)$ and their images under the powers of the Frobenius map looks like that:

$$\begin{aligned}
\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{F^i} &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \\
\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{F^i} &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \\
\begin{bmatrix} t^{p^l} & 0 \\ 0 & t^{p^{-l}} \end{bmatrix}^{F^i} &= \begin{bmatrix} t^{p^{l+i} \pmod k} & 0 \\ 0 & t^{p^{-l-i} \pmod k} \end{bmatrix} \\
&= \begin{bmatrix} t^{p^l} & 0 \\ 0 & t^{p^{-1}} \end{bmatrix}^{p^i}.
\end{aligned}$$

Therefore the black box group Y is generated in the direct product X^k by elements

$$\begin{aligned}
\bar{u} &= (u, u, \ldots, u) \\
\bar{w} &= (w, w, \ldots, w) \\
\bar{h} &= (h, h^p, \ldots, h^{p^{k-1}})
\end{aligned}$$

fits precisely in the construction described in Theorem 2.1.

It remains to notice that, by nature of its construction, the map α in Theorem 2.1 leaves invariant elements $\bar{u}$, $\bar{w}$ and the torus $\bar{T}$ generated by $\bar{h}$ and hence leaves invariant the unipotent group $\bar{U} = \langle \bar{u}^{\bar{T}} \rangle$ and the Borel subgroup $\bar{U}\bar{T}$ of Y. □

Actually we have a more general construction of Frobenius maps on all untwisted Chevalley groups over finite field of odd characteristic; unlike Theorem 2.4, it does not use unipotent elements.

Theorem 2.5 (Known characteristic)**.** *Let X be a black box group encrypting a simple Lie type group $G = G(q)$ of untwisted type over a field of order $q = p^k$ for p odd (and known) and $k > 1$. Then we can construct, in time polynomial in* $\log |G|$*,*

- *a black box Y encrypting G,*
- *a morphism $X \longleftarrow Y$, and*
- *a morphism $\phi : Y \longrightarrow Y$ which encrypts a Frobenius automorphism of G induced by the map $x \mapsto x^p$ on the field $\mathbb{F}_q$.*

Proof. The proof is based on two applications of Theorem 2.2. First we consider the case when X encrypts $\mathrm{PSL}_2(\mathbb{F}_q)$. Using the standard technique for dealing with involution centralizers, we can find in X a 4-subgroup V; let E be the subgroup in $G = \mathrm{PSL}_2(q)$ encrypted by V. Since all 4-subgroups in $\mathrm{PSL}_2(\mathbb{F}_q)$ are conjugate to a subgroup in $\mathrm{PSL}_2(\mathbb{F}_p)$, we can assume without loss of generality that E belongs to a subfield subgroup $H = \mathrm{PSL}_2(\mathbb{F}_p)$ of G and therefore E is fixed by a Frobenius map F on G. Now let e_1 and e_2 be two involutions in E, and C_1 and C_2 maximal cyclic subgroups in their centralizers in G; notice that C_1 and C_2 are conjugate by an element from H and are F-invariant.

It follows from the basic Galois cohomology considerations that F acts on C_1 and C_2 as power maps $\alpha_i : c \mapsto c^{\epsilon p}$ for $p \equiv \epsilon \bmod 4$. If now we take images X_i of groups C_i, we see that the morphisms $\phi_i : x \mapsto x^{\epsilon p}$ of X_i encrypt restrictions of F to C_i. Obviously, X_1 and X_2 generate a black box $Y \longrightarrow X$, and we can use Theorem 2.2 to amalgamate ϕ_1 and ϕ_2 into a morphism ϕ which encrypts F.

As usual, for groups $\mathrm{SL}_2(q)$ the same result can be achieved by essentially the same arguments as for $\mathrm{PSL}_2(q)$. Moving to other untwisted Chevalley groups, we apply amalgamation to (encryptions of) restrictions of a Frobenius map on G to (encryptions in X) of a family of root (P)SL_2-subgroups K_i in G forming a Curtis-Tits system in G (and therefore generating G). Black boxes for Curtis-Tits system in classical groups of odd characteristic are constructed in [11], in exceptional groups in [14]. This completes the proof. □

3. Oracles and revelations

In this section, we revise the classification of black box group problems and briefly discuss the role of "oracles".

3.1. **Monte-Carlo and Las Vegas.** This is a brief reminder of two canonical concepts for the benefit of those readers who came from the pure group theory rather than computational group theory background.

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 subclass of Monte-Carlo algorithm is a Las Vegas algorithm which either outputs a correct answer or reports failure (the latter with probability less than 1/2). The probability of having a report of failure is prescribed by the user. A detailed comparison of Monte-Carlo and Las Vegas algorithms, both from practical and theoretical point, can be found in Babai's paper [4].

3.2. **Constructive recognition.** We shall outline an hierarchy of typical black box group problems.

Verification Problem: Is the unknown group encrypted by a black box group X isomorphic to the given group G ("target group")?

Recognition Problem: Determine the isomorphism class of the group encrypted by X.

The Verification Problem arises as a sub-problem within more complicated Recognition Problems. The two problems have dramatically different complexity. For example, the celebrated Miller-Rabin algorithm [43] for testing primality of the given odd natural number n in nothing else but a black box algorithm for solving the verification problem for the multiplicative group $\mathbb{Z}/n\mathbb{Z}^*$ of residues modulo n (given by a simple black box: take your favorite random numbers generator and generate random integers between 1 and n) and the cyclic group $\mathbb{Z}/(n-1)\mathbb{Z}$ of order $n-1$ as the target group. On the other hand, if $n = pq$ is the product of primes p and q, the recognition problem for the same black box group means finding the direct product decomposition

$$\mathbb{Z}/n\mathbb{Z}^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z}$$

which is equivalent to factorization of n into product of primes.

The next step after finding the isomorphism type of the black box group X is

Constructive Recognition: Suppose that a black box group X encrypts a concrete and explicitly given group G. Rewording a definition given in [21],

> *The goal of a constructive recognition algorithm is to construct an effective isomorphism $\Psi : G \longrightarrow X$. That is, given $g \in G$, there is an efficient procedure to construct a string $\Psi(g)$ encrypting g in X and given a string x produced by X, there is an efficient procedure to construct the element $\Psi^{-1}(x) \in G$ encrypted by X.*

However, there are still no really efficient constructive recognition algorithms for black box groups X of (known) Lie type over a finite field of large order $q = p^k$. The first computational obstacles for known algorithms [19, 20, 21, 22, 23, 25, 28, 35] are the need to construct unipotent elements in black box groups, [19, 20, 21, 23, 22, 25] or to solve discrete logarithm problem for matrix groups [27, 28, 35].

Unfortunately, the proportion of the unipotent elements in X is $O(1/q)$ [31]. Moreover the probability that the order of a random element is divisible by p is also $O(1/q)$, so one has to make $O(q)$ (that is, *exponentially many*, in terms of the input length $O(\log q)$ of the black boxes and the algorithms) random selections of elements in a given group to construct a unipotent element. However, this brute force approach is still working for small values of q, and Kantor and Seress [33] used it to develop an algorithm for recognition of black box classical groups. Later the algorithms of [33] were upgraded to polynomial time constructive recognition algorithms [20, 21, 22, 23] by assuming the availability of additional *oracles*:

- the *discrete logarithm oracle* in $\mathbb{F}_q^*$, and
- the $\mathrm{SL}_2(q)$-*oracle*.

Here, the $\mathrm{SL}_2(q)$-*oracle* is a procedure for constructive recognition of $\mathrm{SL}_2(q)$; see discussion in [21, Section 3].

> ***We emphasize that in this and subsequent papers we are using neither the discrete logarithm oracle in $\mathbb{F}_q^*$ nor the $\mathrm{SL}_2(q)$-oracle.***

3.3. **On oracles and revelations: an example from even characteristic.** We have to admit that the concept of constructive recognition modulo the use of unrealistically powerful oracles makes us uncomfortable. We feel that the use of excessively powerful and blunt tools leads to loss of essential (and frequently very beautiful) theoretical details. Instead, we propose to use all "*fifty shades of black*" and exploit all available gradations of black (that is, a subtler hierarchy of complexity of black box problems) in development of practically useful algorithms. Our papers [12, 15, 16] provide a number of concrete examples where this alternative approach has happened to be fruitful.

In the present paper, we wish to dispel some mystic of the $\mathrm{SL}_2(q)$-oracle by analyzing the structure of the black box group X encrypting $\mathrm{SL}_2(2^n)$ using formally a more modest assumption: that we are given an involution $r \in X$. We shall say that r is obtained *by revelation*, to acknowledge that this assumption is quite unnatural in practical applications.

Still, we feel that there is a difference between a revelation or epiphany (which, by their nature, are non-reproducible, unique events) and an appeal to an oracle; indeed, there is an implicit assumption that the oracle can be approached for advice again and again.

Theorem 3.1 (Small characteristic)**.** *Let X be a black box group encrypting $\mathrm{SL}_2(2^n)$ for some (perhaps unknown) n. We assume that we are given an involution $u \in X$.*

Then there exists a Monte-Carlo algorithm which constructs, in polynomial in $l(X)$ *time,*

- *a black box field* $\mathbb{U}$ *encrypting* $\mathbb{F}_{2^n}$*, and*
- *a polynomial in* $l(X)$ *time isomorphism*

$$\Phi : \mathrm{SL}_2(\mathbb{U}) \longrightarrow X.$$

3.4. **Structure recovery.** Theorem 3.1 is an example of a class of results which we call *structure recovery theorems.*[1]

Suppose that a black box group X encrypts a concrete and explicitly given group $G = G(\mathbb{F}_q)$ of Chevalley type G over a explicitly given finite field $\mathbb{F}_q$. To achieve *structure recovery* in X means to construct, in probabilistic polynomial time in $\log |G|$,

- a black box field $\mathbb{K}$ encrypting $\mathbb{F}_q$, and
- a probabilistic polynomial time morphism

$$\Psi : G(\mathbb{K}) \longrightarrow X.$$

This new concept requires a detailed discussion.

Recall that simple algebraic groups (in particular, Chevalley groups over finite fields) are understood in the theory of algebraic groups as functors from the category of unital commutative rings into the category of groups; most structural properties of a Chevalley group are encoded in the functor; the field mostly provides the flesh on the bones. Remarkably, this separation of flesh from the bones is very prominent in the black box group theory. Here, we wish to mention a few from many constructions from our subsequent paper [15] which illustrate this point.

Theorem 3.2 (Known characteristic)**.** [15] *Let* X *be a black box group encrypting the group* $\mathrm{SL}_n(q^2)$ *for* q *odd,* $q = p^k$ *for some* k *(perhaps unknown) and a known prime number* p*. Then we can construct, in time polynomial in* $\log q$ *and* n*, a black box group* Y *encrypting the group* $\mathrm{SU}_n(q)$ *and a morphism* $Y \hookrightarrow X$*. If in addition* n *is even and* $n = 2m$*, we can do the same with a black box group* Z *encrypting* $\mathrm{Sp}_{2m}(q)$ *and a morphism* $Z \hookrightarrow Y$*.*

An important feature of the proofs of this and other similar results in [15] is that they never refer to the ground fields of groups and do not involved any computations with unipotent elements. In fact, we interpret morphisms between functors

$$\mathrm{Sp}_{2m}(\cdot) \hookrightarrow \mathrm{SU}_n(\cdot) \hookrightarrow \mathrm{SL}_n(\cdot^2).$$

within our black boxes.

This example shows that a modicum of categorical language is useful for the theory as well as for its implementation in the code since it suggests a natural structural approach to development of the computer code.

Another example of a "category-theoretical" approach is provided by a very elementary, but also very important observation that the graph of a group homomorphism $G \longrightarrow H$ is a subgroup of $G \times H$. Therefore it is natural to identify a morphism $\mu : X \longrightarrow Y$ of black box groups with its graph $M < X \times Y$. In its turn, the black box M is a morphism $M \longrightarrow X \times Y$. In practice this could mean (although in some cases a more sophisticated construction is used) that we take some

[1]We extend our definition from [12] where it refers to a special case of the present one.

strings $x_1, \dots, x_k$ generating X and their images $y_1 = \mu(x_1), \dots, y_k = \mu(x_k)$ in Y and use the product replacement algorithm to run a black box for the subgroup

$$M = \langle (x_1, y_1), \dots, (x_k, y_k) \rangle \leqslant X \times Y$$

which is of course exactly the graph $\{ (x, \mu(x)) \}$ of the homomorphism μ. Random sampling of the black box M returns strings $x \in X$ with their images $\mu(x) \in Y$ already attached. This doubles the computational cost of the black box for X, but allows us to do constructions like the following one.

Theorem 3.3 (Known characteristic)**.** [15] *Let X be a black box group encrypting the group $\mathrm{SL}_8(F)$ for a field F of (unknown) odd order $q = p^k$ but known $p = \mathrm{char}\, F$. Then we can construct, in time polynomial in $\log |F|$, a chain of black box groups and morphisms*

$$U \hookrightarrow V \hookrightarrow W \hookrightarrow X$$

that encrypts the chain of canonical embeddings

$$G_2(F) \hookrightarrow \mathrm{SO}_7(F) \hookrightarrow \mathrm{SO}_8^+(F) \hookrightarrow \mathrm{SL}_8(F).$$

Again, these our constructions (and even the embedding ${}^3\mathrm{D}_4(q) \hookrightarrow \mathrm{SO}_8^+(q^3)$, also done in [15]) are "field-free" and, moreover, "characteristic-free".

Another aspect of the concept of "structure recovery" is that it follows an important technique from the model-theoretic algebra: interpretability of one algebraic structure in another, see, for example, [10]. Construction of a black box field in a black box group in Theorems 3.1 and 4.1 closely follows this model-theoretic paradigm.

3.5. **Black box fields.** We define black box fields by analogy with black box groups, the reader may wish to compare the exposition in this section with [8].

A *black box* (finite) *field* $\mathbb{K}$ is an oracle or an algorithm operating on 0-1 strings of uniform length (input length) which encrypts a field of known characteristic p. The oracle can compute $x + y$, xy and compares whether $x = y$ for any strings $x, y \in \mathbb{K}$. We refer the reader to [8, 38] for more details of black box fields and their applications to cryptography.

In this paper, we shall be using some results about the isomorphism problem of black box fields [38], that is, the problem of constructing an isomorphism and its inverse between $\mathbb{K}$ 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 is determined by

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

where $s_1, s_2, \dots, s_n$ denotes a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. The concept of explicitly given field of order p^n is robust; indeed, Lenstra Jr. has shown in [36, 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 polynomial in $n \log p$ time.

Maurer and Raub [38] proved that the isomorphism problem for a black box field $\mathbb{K}$ and an explicitly given field $\mathbb{F}_{p^n}$ is reducible in polynomial time to the same

problem for the prime subfield in $\mathbb{K}$ and $\mathbb{F}_p$. Hence, for small primes p, one can construct an isomorphism between $\mathbb{K}$ and $\mathbb{F}_{p^n}$ in time polynomial in $n \log p$ and linear in p.

In our construction of a black box field, we use the so called *primitive prime divisor* elements in the field of size p^n. A prime number r is said to be a primitive prime divisor of $p^n - 1$ if r divides $p^n - 1$ but not $p^i - 1$ for $1 \leqslant i < n$. By [51], there exists a primitive prime divisor of $p^n - 1$ except when $(p, n) = (2, 6)$, or $n = 2$ and p is a Mersenne prime. Here, we shall note that the Mersenne primes which are less than 1000 are 3, 7, 31, 127. We call a group element a $ppd(n, p)$-element if its order is odd and divisible by a primitive prime divisor of $p^n - 1$.

4. Application of Frobenius maps: structure recovery of (P)$\mathrm{SL}_2(q)$, $q \equiv 1 \bmod 4$

We remind that in all theorems and conjectures stated in this paper, we assume that black boxes for groups satisfy Axioms BB1–BB4; in particular, they come with known and computationally feasible global exponent (Axiom BB4).

For the structure recovery of (P)$\mathrm{SL}_2(q)$, we need to recall the Steinberg generators of (P)$\mathrm{SL}_2(q)$ as introduced by Steinberg [44, Theorem 8]. We use notation from [12].

Let $G = \mathrm{SL}_2(q)$. Then set the Steinberg generators of G as

$$\mathbf{u}(t) = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}, \mathbf{v}(t) = \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}, \mathbf{h}(t) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \mathbf{n}(t) = \begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$$

where $t \in \mathbb{F}_q$ and in addition $t \neq 0$ in $\mathbf{h}(t)$ and $\mathbf{n}(t)$.

The group $\mathrm{PSL}_2(q)$ is obtained from $\mathrm{SL}_2(q)$ by factorizing over the relation

$$\mathbf{h}(t) = \mathbf{h}(-t).$$

Abusing notation, we are using for elements in $\mathrm{PSL}_2(q)$ the same matrix notation as for their pre-images in $\mathrm{SL}_2(q)$.

It is straightforward to check that

$$\mathbf{u}(t)^{\mathbf{n}(s)} = \mathbf{v}(-s^{-2}t),\ \mathbf{u}(1)^{\mathbf{h}(t)} = \mathbf{u}(t^{-2}) \text{ and } \mathbf{n}(1)^{\mathbf{h}(t)} = \mathbf{n}(t^{-2}). \tag{2}$$

Moreover,

$$\mathbf{n}(t) = \mathbf{u}(t)\mathbf{v}(-t^{-1})\mathbf{u}(t) \text{ and } \mathbf{h}(t) = \mathbf{n}(t)\mathbf{n}(-1). \tag{3}$$

It is well-known that

$$G = \langle \mathbf{u}(t), \mathbf{v}(t) \mid t \in \mathbb{F}_q \rangle,$$

see, for example, [24, Lemma 6.1.1]. Therefore, by (2) and (3),

$$G = \langle \mathbf{u}(1), \mathbf{h}(t), \mathbf{n}(1) \mid t \in \mathbb{F}_q^* \rangle;$$

notice that actually G is generated by three elements

$$G = \langle \mathbf{u}(1), \mathbf{h}(t), \mathbf{n}(1) \rangle$$

where we can take t as an arbitrary $ppd(k, p)$-element of the field $\mathbb{F}_{p^k}$.

In this section, we prove the following theorem.

Theorem 4.1 (Small characteristic)**.** *Let X be a black box group encrypting the group $G \cong$ (P)$\mathrm{SL}_2(q)$, where $q \equiv 1 \bmod 4$ and $q = p^k$ for some $k \geqslant 1$ (perhaps unknown). If $p \neq 5, 7$, then there is a Monte-Carlo algorithm which constructs, in time quadratic in p and polynomial in $\log q$,*

- *a black box field* $\mathbb{K}$ *encrypting* $\mathbb{F}_q$*, and*
- *a quadratic in* p *and polynomial in* $\log q$ *time isomorphism*

$$\Phi : (P)SL_2(\mathbb{K}) \longrightarrow X.$$

If $p = 5$ *or* 7*, and* k *has a small divisor* ℓ*, the same result holds where the running time is polynomial in* $\log q$ *and quadratic in* p^ℓ*.*

Theorem 4.1 is used in our paper [13] as the basis of recursion in the proof of the following structure recovery theorem for classical groups in small characteristics.

Theorem 4.2 (Small characteristic)**.** [13] *Let* X *be a black box group encrypting one of the classical groups* $\mathrm{G}(q) \simeq (\mathrm{P})\mathrm{SL}_{n+1}(q)$*,* $(\mathrm{P})\mathrm{Sp}_{2n}(q)$*,* $\Omega_{2n+1}(q)$ *or* $(\mathrm{P})\Omega^+_{2n}(q)$*, where* $q \equiv 1 \bmod 4$ *and* $q = p^k$ *for some* $k \geqslant 1$ *(*k *and the type of the group are perhaps unknown).*

If $p \neq 5, 7$*, then there is a Monte-Carlo algorithm which constructs, in time quadratic in* p *and polynomial in* $\log q$*,*

- *a black box field* $\mathbb{K}$ *encrypting* $\mathbb{F}_q$*, and*
- *a quadratic in* p *and polynomial in* $\log q$ *time isomorphism*

$$\Phi : \mathrm{G}(\mathbb{K}) \longrightarrow X.$$

If $p = 5$ *or* 7*, and* k *has a small divisor* ℓ*, the same result holds where the running time is polynomial in* $\log q$ *and quadratic in* p^ℓ*.*

4.1. **Proof of Theorem 4.1, general case.** Our aim is to present an algorithm which produces a black box field $\mathbb{K}$ and an isomorphism

$$\varphi : \mathrm{SL}_2(\mathbb{K}) \to X.$$

(1) We use Theorem 2.3 as applied to our black box group X, so u, h, n are string in X such that

$$\Phi(u) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \Phi(h) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \Phi(n) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

for some abstract isomorphism

$$\Phi : X \longrightarrow (\mathrm{P})\mathrm{SL}_2(q);$$

here, t is some primitive element in $\mathbb{F}_q$, $q = p^k$. We shall note that we only know the existence of the map Φ. Let $\tilde{h}$ be a $ppd(k, p)$-element produced by taking some power of h and

$$\Phi(\tilde{h}) = \begin{bmatrix} \tilde{t} & 0 \\ 0 & \tilde{t}^{-1} \end{bmatrix}.$$

(2) We consider the cyclic subgroup $T = \langle \tilde{h} \rangle$ and the unipotent subgroup $U = \langle u^T \rangle$ in X. Observe that U is the full unipotent subgroup of X since the order of $\tilde{h}$ is a $ppd(k, p)$-element in $\mathbb{F}_{p^k}$.

(3) Now we start introducing on U a structure of field $\mathbb{K}$ isomorphic to $\mathbb{F}_q$. First, for any $u_1, u_2 \in U$, we define an addition on $\mathbb{K}$ by setting

$$u_1 \oplus u_2 = u_1 u_2.$$

For the multiplication on $\mathbb{K}$, we set the element u as the unity of $\mathbb{K}$. Since $\tilde{h}$ is a $ppd(k,p)$-element, it has odd order m and the element $\sqrt{\tilde{h}} := \tilde{h}^{(m+1)/2}$ has the property that $\sqrt{\tilde{h}}^2 = \tilde{h}$. We also set

$$s := u^{\sqrt{\tilde{h}}}.$$

Notice that

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \sqrt{\tilde{t}} & 0 \\ 0 & \sqrt{\tilde{t}^{-1}} \end{bmatrix} = \begin{bmatrix} 1 & \tilde{t}^{-1} \\ 0 & 1 \end{bmatrix}.$$

Hence s can be seen as an element in $\mathbb{K}$ corresponding to $\tilde{t}^{-1}$, and after setting $s^i = u^{(\sqrt{\tilde{h}})^i}$, the elements

$$s, s^2, \ldots, s^{k-1}, s^k$$

form a polynomial basis of $\mathbb{K}$ over the prime field $\mathbb{L} \simeq \mathbb{F}_p$. The additive groups of $\mathbb{L}$ is cyclic of order p. We have already fixed the identity element 1 of $\mathbb{K}$ and hence of $\mathbb{L}$, which uniquely defines the multiplicative structure on $\mathbb{L}$.

For $w \in U$, we define the product

$$w \otimes s^l = w^{h^l}$$

and expanded by linearity to product of any two elements in $\mathbb{K}$. We still do not know, however, why this operation can be carried out in feasible time—but we should be reassured that at least the product $w \otimes s^l$ can be computed in time polynomial in $\log q$. So at this stage we treat $\mathbb{K}$ a *partially* polynomial time black box field: random generation, comparison, and addition of elements in $\mathbb{K}$ can be carried out in polynomial in $\log q$, as well as multiplication of an arbitrary element in $\mathbb{K}$ by some specific elements.

(4) In view of Theorem 2.4, we have the Frobenius map ϕ on our black box group $X \simeq (\mathrm{P})\mathrm{SL}_2(q)$ which leaves U and T invariant and induces the Frobenius map F on U. This allows us to introduce on U the Frobenius trace $\mathrm{Tr} : U \to \mathbb{F}_p$

$$\mathrm{Tr}(x) = x \oplus x^F \oplus x^{F^2} \oplus \cdots \oplus x^{F^{k-1}}$$

and the trace form, that is, the non-degenerate symmetric $\mathbb{F}_p$-bilinear form given by

$$\langle x, y \rangle = \mathrm{Tr}(x \otimes y).$$

It is interesting that the Frobenius map and the trace form of our future black box field are introduced *before* the field multiplication!

We do not know yet whether the evaluation of the trace form on $\mathbb{K}$ is computationally feasible, but we can compute in polynomial in $\log q$ time the values $w \otimes s^l = w^{h^l}$ and of $\langle w, s^l \rangle$ for arbitrary $w \in \mathbb{K}$ and powers of s. In particular, this allows us to compute the matrix of the trace form

$$A = (a_{ij})_{k \times k}, \quad a_{i,j} = \langle s^i, s^j \rangle, \quad i, j, = 1, 2, \ldots, k.$$

(5) We are now in position to introduce in $\mathbb{K}$ an explicit structure of a $\mathbb{L}$ vector space by computing the decomposition of an arbitrary element $w \in \mathbb{K}$ with respect to the basis $s, s^2, \dots, s^k$. Indeed, for an arbitrary element $w \in \mathbb{K}$, set

$$w = \alpha_1 s \oplus \alpha_2 s^2 \oplus \cdots \oplus \alpha_k s^k$$

and

$$\beta_j = \langle w, s^j \rangle, \quad j = 1, 2, \dots, k.$$

The coefficients β_j are computable in time polynomial in $\log p$ and k:

$$\beta_j = \langle w, s^j \rangle = \sum_{i=1}^{k} \alpha_i a_{ij},$$

which in matrix notation becomes

$$(\beta_1, \dots, \beta_k) = (\alpha_1, \dots, \alpha_k) \cdot A,$$

and therefore

$$(\alpha_0, \dots, \alpha_{k-1}) = (\beta_0, \dots, \beta_{k-1}) \cdot A^{-1}.$$

(6) We can now decompose products $s^i \otimes s^j$ with respect to the basis $s, s^2, \dots, s^k$ and thus find the structure constants c_{ijl} for this basis:

$$s^i \otimes s^j = \sum_{l=1}^{k} c_{ijl} s^l.$$

Of course now we are in position to multiply any two elements in $\mathbb{K}$, and, as we can easily see, in time polynomial in $\log q$. Now, we shall use the algorithms in [1, 36, 38] to construct the isomorphism between $\mathbb{F}_{p^k}$ and $\mathbb{K}$, see discussion in Section 3.5.

(7) Now, we construct (P)$\mathrm{SL}_2(\mathbb{K})$ by using the Steinberg generators, see Section 4. Recall that the element $s \in \mathbb{K}$ corresponds to the element $\tilde{t}^{-1} \in \mathbb{F}_q$ where $\tilde{t}$ is a $ppd(k,p)$-element in $\mathbb{F}_q$, so s is a $ppd(k,p)$-element in $\mathbb{K}$. We construct, in (P)$\mathrm{SL}_2(\mathbb{K})$, the elements encrypting the strings

$$\mathbf{u}(1), \mathbf{h}(s^{-1}), \mathbf{n}(1)$$

by using the isomorphism between the fields $\mathbb{F}_{p^k}$ and $\mathbb{K}$ constructed in Step 6.

(8) Our first assignments are $\mathbf{u}(1) \mapsto u$ and $\mathbf{h}(s^{-1}) \mapsto \tilde{h}$. Now we need to construct the element in X encrypting the string $\mathbf{n}(1)$. Note that the element $n \in X$, which was constructed in Step 1, need not necessarily be the element corresponding to $\mathbf{n}(1)$. Therefore we shall replace the original element n by the one that corresponds to $\mathbf{n}(1)$. Recall that the elements $u, n \in X$ are indeed computed inside a subgroup isomorphic to (P)$\mathrm{SL}_2(p)$ or $\mathrm{PSL}_2(p^2)$ depending on $p \equiv 1 \bmod 4$ or $p \equiv -1 \bmod 4$, respectively [12]. For simplicity, we may assume that this subgroup encrypts (P)$\mathrm{SL}_2(p)$ and the following computations are carried out in this black box subgroup. Note that raising the element h to the power so that the resulting element h_0 has order $(p-1)/2$ and belongs to this subgroup isomorphic to (P)$\mathrm{SL}_2(p)$.

We compute all $v := (u^{-1})^{h_0^k n}$ for $k = 1, \dots p-1$, and check which of the elements of the form

$$uv^{-1}u$$

has order 4 (Recall that, by (2) and (3), we have $\mathbf{u}(1)^{\mathbf{n}(s)} = \mathbf{v}(-s^{-2})$ and $\mathbf{n}(t) = \mathbf{u}(t)\mathbf{v}(-t^{-1})\mathbf{u}(t)$). Observe that there are only two elements of the form $uv^{-1}u$ of order 4 and they correspond to the elements $\mathbf{n}(1)$ and $\mathbf{n}(-1)$. Now we need to distinguish $\mathbf{n}(1)$ from $\mathbf{n}(-1)$. Recall also that, by (2) and (3), we have

$$\mathbf{n}(1)^{\mathbf{h}(t)} = \mathbf{n}(t^{-2}), \mathbf{u}(1)^{\mathbf{h}(t)} = \mathbf{u}(t^{-2}), \mathbf{v}(1)^{\mathbf{h}(t)} = \mathbf{v}(t^2)$$

and

$$\mathbf{n}(t^{-2}) = \mathbf{u}(t^{-2})\mathbf{v}(-t^2)\mathbf{u}(t^{-2}). \tag{4}$$

Now it is easy to see that if one of the elements of the form $uv^{-1}u$ of order 4 corresponds to the Weyl group element $\mathbf{n}(-1)$, then Equation (4) is not satisfied. Hence the Weyl group element $h_0^k n$ which produces the element $uv^{-1}u$ satisfying Equation (4) is the desired Weyl group element, say $\tilde{n}$.

(9) Observe that the following map

$$\begin{array}{rcl} (\mathrm{P})\mathrm{SL}_2(\mathbb{K}) & \longrightarrow & Y \\ \mathbf{u}(1) & \mapsto & u \\ \mathbf{h}(s^{-1}) & \mapsto & \tilde{h} \\ \mathbf{n}(1) & \mapsto & \tilde{n} \end{array}$$

is an isomorphism.

Notice that the algorithm described above provides a proof of Theorem 4.1.

4.2. **A more straightforward treatment of** $\mathrm{SL}_2(p)$**.** Because of its importance, we give a streamlined construction of an isomorphism between $\mathrm{SL}_2(p)$, $p \equiv 1 \bmod 4$, and a black box group X encrypting $\mathrm{SL}_2(p)$. Notice, in this case, that we may assume that the field structure of $\mathbb{F}_p$ is available. Hence, we shall construct the elements in X encrypting the images of $\mathbf{u}(1), \mathbf{h}(t)$ and $\mathbf{n}(1)$ where $0, 1 \neq t \in \mathbb{F}_p$ in X.

Step 1: Using Theorem 2.3, we select in X a unipotent element u, a toral element h normalizing the root subgroup containing u, and n a Weyl group element for the torus containing h. Our fist assignment is $\mathbf{u}(1) \mapsto u$.

Step 2: Recall that for a given $\mathbf{h}(t)$ we have $\mathbf{u}(1)^{\mathbf{h}(t)} = \mathbf{u}(t^{-2})$. Assume that $\mathbf{u}(t^{-2}) = \mathbf{u}(k) = \mathbf{u}(1)^k$ for some $k \in \{1, 2, \ldots, p-1\}$.

Now we check whether $u^h = u^k$ in X. If not, then some power ℓ of h has this property, that is, $u^{h^\ell} = u^k$. Observe that ℓ is necessarily relatively prime to $p-1$ so that the resulting element h^ℓ generates the torus. We replace h with h^ℓ and assign $\mathbf{h}(t) \mapsto h$.

Step 3: Now we compute $\mathbf{n}(1)$ by using the same arguments in Step 9 of the algorithm in Section 4.1. Thus we have an isomorphism

$$\begin{array}{rcl} \mathrm{SL}_2(p) & \longrightarrow & X \\ \mathbf{u}(1) & \mapsto & u \\ \mathbf{h}(t) & \mapsto & h \\ \mathbf{n}(1) & \mapsto & n. \end{array}$$

5. A Revelation and Its Reverberations: Proof of Theorem 3.1

5.1. **Proof of Theorem 3.1.** We describe an algorithm which produces a black box field $\mathbb{U}$ and an isomorphism

$$\Phi : \mathrm{SL}_2(\mathbb{U}) \longrightarrow X.$$

(1) We take our revelation involution r and consider strongly real elements of the form $r^x \cdot r$ for random $x \in X$, and raising them to appropriate powers, find an element θ of order 3 inverted by r.
(2) Set $v = \theta r$ and $w = \theta^2 r$. Observe that v and w are involutions and $L = \langle\theta\rangle\langle r\rangle$ is the dihedral group of order 6.
(3) Observe that all dihedral subgroups of order 6 in X are conjugate in X and therefore we can assume without loss of generality that $L \cong \mathrm{SL}_2(2)$ encrypts a subfield subgroup of $\mathrm{SL}_2(2^n)$. In particular, there exist a system of Steinberg generators of $\mathrm{SL}_2(2^n)$,

$$\mathbf{u}(t) = \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}, \mathbf{v}(t) = \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix}, \mathbf{h}(t) = \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}, \mathbf{n}(t) = \begin{bmatrix} 0 & t \\ t^{-1} & 0 \end{bmatrix}$$

for $t \in \mathbb{F}_{2^n}$ and $t \neq 0$ for $\mathbf{h}(t)$ and $\mathbf{n}(t)$, and such that r, v and n encrypt $\mathbf{u}(1)$, $\mathbf{v}(1)$, and $\mathbf{n}(1)$, correspondingly.
(4) The standard procedure for construction of centralizers of involutions [9, 18] produces unipotent subgroups $U = C_X(r)$ and $V = C_X(v)$. If we set

$$H = \langle h(t) \mid t \in \mathbb{F}_{2^n}\rangle$$

(warning: this subgroup is not constructed yet) then $B^+ = UH = N_X(U)$ and $B^- = VH = N_X(V)$ are Borel subgroups in X.
(5) Observe that if $x \in X$ is such that $u^x \in U$ for some $1 \neq u \in U$ then $x \in B$.
(6) We can identify action of H on U by conjugation with the action of B/U on U. Observe that for any two involutions $s, t \in U$ there is a unique $\bar{b} \in B/U$ such that $s^{\bar{b}} = t$.
(7) Using the double conjugation trick, we can find, for any given involutions s and t in U an element x in X (and hence in B) such that $s^x = t$. This is done in the following way: notice that the exponent of $\mathrm{SL}_2(2^n)$ is $2 \cdot (2^n - 1)(2^n + 1)$ and therefore if $y \in X$ is an element of odd order than $y^{2^{2n}-1} = 1$. By conjugating s by a random element $z \in X$, find an involution $r = s^z$ such that elements $y_1 = sr$ and $y_2 = rt$ have odd order. Then it can be checked directly that

$$s^{\left((sr)^{2^{2n-1}}\right)} = r \quad \text{and} \quad r^{\left((rt)^{2^{2n-1}}\right)} = t$$

and

$$x = (sr)^{2^{2n-1}} \cdot (rt)^{2^{2n-1}}$$

has the desired property $s^x = t$. By the previous point, the coset xU in B/U is uniquely determined.

(The same idea of "local conjugation" of involutions is used by Ballantyne and Rowley for construction of centralizers of involutions in black box groups with expensive generation of random elements [32].)
(8) Treating the subgroup B as a black box, we have

$$U = \{\, x \in B \mid x^2 = 1\}.$$

Therefore after introducing on B a new equality relation

$$x \equiv y \text{ if and only if } (xy^{-1})^2 = 1$$

we get a black box $\mathbb{T}$ for the factor group $T = B/U$. Notice that there is a natural action of $\mathbb{T}$ on U by conjugation and that notation u^t for $u \in U$ and $t \in \mathbb{T}$ is not ambiguous.

(9) Now we construct a black box field $\mathbb{U}$. We start with the multiplicative group $\mathbb{U}^*$ of $\mathbb{U}$ which we define as the graph of the orbit action map of $\mathbb{T}$ onto the orbit $r^{\mathbb{T}}$. Namely, $\mathbb{U}^*$ is the set of all pairs (t, s) with $t \in \mathbb{T}$ and $s \in U \setminus \{1\}$ such that $r^t = s$. We define in $\mathbb{U}$ multiplication $\otimes$ by the rule

$$(t_1, u_1) \otimes (t_2, u_2) = (t_1 t_s, r^{t_1 t_2}).$$

In particular, the element $\mathbf{1} = (1, r)$ plays the role of the identity element in $\mathbb{U}^*$.

Then we define the zero element of $\mathbb{U}$ as

$$\mathbf{0} = (1, 1),$$

set

$$\mathbb{U} = \mathbb{U}^* \cup \{0\}$$

(and use lower case boldfaced letter to denote elements $\mathbf{u} \in \mathbb{U}$), and define

$$\mathbf{0} \otimes \mathbf{u} = \mathbf{u} \otimes \mathbf{0} \text{ for all } \mathbf{u} \in \mathbb{U}^*.$$

Finally, we define on $\mathbb{U}$ addition $\oplus$ by setting

$$\begin{aligned} \mathbf{0} \oplus \mathbf{u} = \mathbf{u} \oplus \mathbf{0} &= \mathbf{u} \\ \mathbf{u} \oplus \mathbf{u} &= \mathbf{0} \\ (t_1, u_1) \oplus (t_2, u_2) &= (t, u_1 u_2) \end{aligned}$$

where in the last line $u_1 \neq u_2$ (and thus $u_1 u_2 \neq 1$) and $t \in \mathbb{T}$ is chosen to send r to $u_1 u_2$, that is, $r^t = u_1 u_2$. It follows that the inverse $\mathbf{u}^{-1}$ of $\mathbf{u} = (t, u) \neq \mathbf{0}$ with respect to multiplication $\otimes$ is equal to $(t^{-1}, r^{t^{-1}})$.

(10) So we have a black box field $\mathbb{U}$ interpreted in the Borel subgroup $B = N_X(C_X(r)))$ of the black box group X and such that X encrypts $\mathrm{SL}_2(\mathbb{U})$.

It will be convenient to use traditional notation and denote $1 = u(\mathbf{0})$, and write, for elements $\mathbf{t} \in \mathbb{U}^*$, $u = u(\mathbf{t})$ if $\mathbf{t} = (t, u)$. In particular, $r = u(\mathbf{1})$. This gives us a parametrization of U by elements of the black box field $\mathbb{U}$.

(11) Now we transfer the black box field parametrization from U to V by setting $v(\mathbf{0}) = 1$ and for setting for non-identity elements $v \in V$

$$v = v(\mathbf{t}) \text{ if } v^w = u(\mathbf{t}).$$

We set further

$$n(\mathbf{t}) = u(\mathbf{t}) v(\mathbf{t}^{-1}) u(\mathbf{t}),$$

so that this agrees with computation in $L \cong \mathrm{SL}_2(2)$, yielding

$$n(\mathbf{1}) = w,$$

and finally set

$$h(\mathbf{t}) = n(\mathbf{t}) n(\mathbf{1}).$$

Notice that

$$\{h(\mathbf{t}) \mid \mathbf{t} \in \mathbb{U}^*\} = N_X(V) \cap N_X(U)$$

is the uniquely determined maximal torus in X normalizing the both V and U. We denote it by H.

(12) We can now construct an isomorphism

$$\Psi : \mathrm{SL}_2(\mathbb{U}) \longrightarrow X.$$

First of all, recall that matrices from $\mathrm{SL}_2(\mathbb{U})$ are quadruples

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

of strings a_{ij} generated by black box $\mathbb{U}$, with matrix addition and multiplication defined with respect to operations $\oplus$ and $\otimes$.

(a) Notice easy-to-check identities over any field of characteristic 2:

(i) given a, b, and d such that $bc = 1$, we have

$$\begin{bmatrix} 0 & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & bd \\ 0 & 1 \end{bmatrix};$$

(ii) for $a \neq 0$ and $ad - bc = 1$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ac & 1 \end{bmatrix} \begin{bmatrix} 1 & a^{-1}b \\ 0 & 1 \end{bmatrix}.$$

(b) Therefore we can map

$$\Psi : \begin{bmatrix} \mathbf{0} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix} \mapsto n(\mathbf{1})h(\mathbf{c})u(\mathbf{b} \otimes \mathbf{d})$$

$$\Psi : \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix} \mapsto h(\mathbf{a})v(\mathbf{a} \otimes \mathbf{c})u(\mathbf{a}^{-1} \otimes \mathbf{b}).$$

This is an isomorphism.

This completes the proof of Theorem 3.1. □

5.2. **Other groups of characteristic 2.** We expect that Theorem 4.2 is mirrored by the following conjecture.

Conjecture 5.1. *Let X be a black box group encrypting one of the untwisted Chevalley groups $\mathrm{G}(2^n)$. We assume that we are given an involution $u \in X$.*

Then there is a Monte-Carlo algorithm which constructs a polynomial time (in $l(X)$) isomorphism

$$\Phi : \mathrm{G}(2^n) \longrightarrow X.$$

The running time of the algorithm is polynomial in n and the Lie rank of $\mathrm{G}(2^n)$.

As a comment to Conjecture 5.1, we formulate here the following easy result.

Theorem 5.2. *Let X be a black box group encrypting an untwisted Chevalley group $\mathrm{G}(2^n)$ (with n known) and $U < X$ an unipotent long root subgroup given as a black box subgroup of X. Then there is a polynomial time, in n and Lie rank of $\mathrm{G}(2^n)$, Monte-Carlo algorithm which constructs a black box for $N_X(U)$ and a black box $\mathbb{U}$ for the field $\mathbb{F}_{2^n}$ interpreted in the action of $N_X(U)$ on U, with U becoming the additive group of the field $\mathbb{U}$.*

The proof of this theorem is an immediate and obvious generalization of Step 8 in the proof of Theorem 3.1 in Section 5. Indeed, it suffices to observe that U is a TI-subgroup of X (that is, $U \cap U^g = 1$ or U for all $g \in G$) and that all involutions in U are conjugate in $N_X(U)$.

Theorem 5.2 suggests that structure recovery of black box Chevalley groups $G(2^n)$ is likely to share some of the conceptual framework of Franz Timmesfeld's classification of groups generated by root type subgroups [45, 46, 47, 48]. If so, then this will be strikingly similar to the use of Aschbacher's classical involutions [2, 3] and root SL_2-subgroups in our structural theory of classical black box groups in odd characteristic [11, 13, 12, 15, 49, 50].

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, and July 2013; our thanks go to Ali Nesin and to all volunteers and staff who have made the Village a mathematical paradise.

We thank Adrien Deloro for many fruitful discussions, in Şirince and elsewhere, and Bill Kantor and Rob Wilson for their helpful comments.

Special thanks go to our logician colleagues: Paola D'Aquino, Gregory Cherlin, Jan Krajíček, Angus Macintyre, Jeff Paris, Jonathan Pila, and Alex Wilkie for pointing to fascinating connections with logic and complexity theory.

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

References

1. B. Allombert, *Explicit computation of isomorphisms between finite fields*, Finite Fields and Their Applications **8** (2002), no. 3, 332 – 342.
2. M. Aschbacher, *A characterization of Chevalley groups over fields of odd order. I, II*, Ann. of Math. (2) **106** (1977), no. 3, 353–468.
3. ———, *Correction to: "A characterization of Chevalley groups over fields of odd order. I, II" [Ann. of Math. (2) **106** (1977), 353–468]*, Ann. of Math. (2) **111** (1980), no. 2, 411–414.
4. L. Babai, *Randomization in group algorithms: conceptual questions*, Groups and computation, II (New Brunswick, NJ, 1995), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 28, Amer. Math. Soc., Providence, RI, 1997, pp. 1–17. MR 1444127 (98k:68092)
5. L. Babai and I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 2000) (New York), ACM, 2000, pp. 627–635.
6. ———, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, J. Algorithms **50** (2004), no. 2, 215–231, SODA 2000 special issue.
7. L. Babai and E. Szemerédi, *On the complexity of matrix group problems*, Proc. 25th IEEE Sympos. Foundations Comp. Sci. (1984), 229–240.
8. 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).
9. 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.
10. A. V. Borovik and A. Nesin, *Groups of finite Morley rank*, The Clarendon Press Oxford University Press, New York, 1994, Oxford Science Publications. MR 96c:20004
11. A. V. Borovik and Ş. Yalçınkaya, *Construction of Curtis-Phan-Tits system for black box classical groups*, Available at arXiv:1008.2823v1 [math.GR].
12. ———, *Steinberg presentations of black box classical groups in small characteristics*, Available at arXiv:1302.3059v1 [math.GR].
13. ———, *Classical black box groups in small odd characteristics*, in preparation.
14. ———, *Construction of Curtis-Phan-Tits systems in black box twisted Chevalley and exceptional groups of Lie type and odd characteristic*, in preparation.

15. ———, *Subgroup structure and automorphisms of black box classical groups*, in preparation.
16. ———, *Subgroup structure and automorphisms of black box groups of exceptional groups of odd characteristic*, in preparation.
17. 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.
18. J. N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245.
19. P. A. Brooksbank, *A constructive recognition algorithm for the matrix group* $\Omega(d, q)$, 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. 79–93.
20. ———, *Fast constructive recognition of black-box unitary groups*, LMS J. Comput. Math. **6** (2003), 162–197.
21. ———, *Fast constructive recognition of black box symplectic groups*, J. Algebra **320** (2008), no. 2, 885–909.
22. P. A. Brooksbank and W. M. Kantor, *On constructive recognition of a black box* $\mathrm{PSL}(d, q)$, 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. 95–111.
23. ———, *Fast constructive recognition of black box orthogonal groups*, J. Algebra **300** (2006), no. 1, 256–288.
24. R. W. Carter, *Simple Groups of Lie Type*, John Wiley & Sons, London, 1972.
25. F. Celler and C. R. Leedham-Green, *A constructive recognition algorithm for the special linear group*, The atlas of finite groups: ten years on (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, Cambridge, 1998, pp. 11–26.
26. 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.
27. M. D. E. Conder and C. R. Leedham-Green, *Fast recognition of classical groups over large fields*, Groups and Computation III (Berlin) (W. M. Kantor and Á. Seress, eds.), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, 2001, pp. 113–121.
28. M. D. E. Conder, C. R. Leedham-Green, and E. A. O'Brien, *Constructive recognition of* $\mathrm{PSL}(2, q)$, Trans. Amer. Math. Soc. **358** (2006), no. 3, 1203–1221.
29. P. D'Aquino and A. Macintyre, *Non-standard finite fields over* $i\delta_0 + \omega_1$, Israel Journal of Mathematics **117** (2000), 311–333 (English).
30. A. Gamburd and I. Pak, *Expansion of product replacement graphs*, Combinatorica **26** (2006), no. 4, 411–429.
31. R. M. Guralnick and F. Lübeck, *On p-singular elements in Chevalley groups in characteristic p*, 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. 169–182.
32. J. John Ballantyne and P. Peter Rowley, *A note on computing involution centralizers*, Journal of Symbolic Computation (2013), no. 0, –.
33. W. M. Kantor and Á. Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708, viii+168.
34. 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.
35. C. R. Leedham-Green and E. A. O'Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881.
36. H. W. Lenstra Jr., *Finding isomorphisms between finite fields*, Mathematics of Computation **56** (1991), no. 193, pp. 329–347 (English).
37. A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363.
38. 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.
39. I. Pak, *The product replacement algorithm is polynomial*, 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), IEEE Comput. Soc. Press, Los Alamitos, CA, 2000, pp. 476–485.

40. ———, *The product replacement algorithm is polynomial*, Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci. (2001), 476–485.
41. ———, *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.
42. I. Pak and A. Żuk, *On Kazhdan constants and mixing of random walks*, Int. Math. Res. Not. (2002), no. 36, 1891–1905.
43. M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.
44. R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968, Notes prepared by John Faulkner and Robert Wilson.
45. F. G. Timmesfeld, *Groups generated by k-transvections*, Invent. Math. **100** (1990), no. 1, 167–206.
46. ———, *Groups generated by k-root subgroups*, Invent. Math. **106** (1991), no. 3, 575–666.
47. ———, *Groups generated by k-root subgroups—a survey*, Groups, combinatorics & geometry (Durham, 1990), London Math. Soc. Lecture Note Ser., vol. 165, Cambridge Univ. Press, Cambridge, 1992, pp. 183–204.
48. ———, *Abstract root subgroups and simple groups of Lie type*, Monographs in Mathematics, vol. 95, Birkhäuser Verlag, Basel, 2001.
49. Ş. Yalçınkaya, *Construction of long root $SL_2(q)$-subgroups in black-box groups*, Available at arXiv, math.GR/1001.3184v1.
50. Ş. Yalçınkaya, *Black box groups*, Turkish J. Math. **31** (2007), no. suppl., 171–210. MR 2369830 (2009a:20081)
51. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), no. 1, 265–284.

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

Nesin Mathematics Village, Izmir, Turkey; sukru.yalcinkaya@gmail.com