New approaches in black box group theory

DOI:
10.1007/978-3-662-44199-2_10

Citation for published version (APA):
Borovik, A., & Yalcinkaya, S. (2014). New approaches in black box group theory. In *Mathematical Software { ICMS 2014 { 4th International Congress, Seoul, South Korea, August 5{9, 2014.* (Vol. 8592, pp. 53-58). (Lecture Notes in Computer Science). Springer Nature. https://doi.org/10.1007/978-3-662-44199-2_10

Published in:
Mathematical Software { ICMS 2014 { 4th International Congress, Seoul, South Korea, August 5{9, 2014.

New approaches in black box group theory

Alexandre Borovik[1] and Şükrü Yalçınkaya[2]

[1] University of Manchester, United Kingdom
`alexandre@borovik.net`,
[2] İstanbul University, Turkey
`sukru.yalcinkaya@istanbul.edu.tr`,

Abstract. We introduce a new approach in black box group theory which deals with black box group problems in the category of black boxes and their morphisms. This enables us to enrich black box groups by actions of outer automorphisms such as Frobenius maps or graph automorphisms of simple groups of Lie type. As an application of this new technique, we present a number of new results, including a solution of an old problem about constructing unipotent elements in groups of Lie type of odd characteristic.

Keywords: Black box groups, projective geometry, classical groups, unipotent elements

1 Black box groups

A black box group $\mathbf{X}$ is a black box (or an oracle, or an algorithm) operating on $0-1$ strings of uniform length which encrypt elements of some finite group G. The procedures performed by a black box are specified as follows.

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

$$\mathbf{X} \xrightarrow{\pi} G.$$

In this situation we say that $\mathbf{X}$ encrypts the group G.

A natural question here is to determine the isomorphism type of a black box group $\mathbf{X}$ or, if it is known, find an isomorphism between $\mathbf{X}$ and its natural copy. To that end, we need additional assumptions about $\mathbf{X}$, which we are keeping to a minimum by adopting an additional axiom.

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 $\log |G|$).

Note that axioms **BB1**–**BB4** hold, for example, in matrix groups over finite fields where we can take for E the exponent of the ambient $GL_n(q)$.

In this paper, we assume **BB1**–**BB4** and are concerned with *structure recovery* of black box groups $\mathbf{X}$ encrypting an explicitly given group G of Lie type over $\mathbb{F}_q$, that is, with constructing, in probabilistic polynomial time in $\log |G|$,

- a black box field $\mathbf{K}$ encrypting $\mathbb{F}_q$, and
- a morphism $\Psi : G(\mathbf{K}) \to \mathbf{X}$.

Unlike the constructive recognition algorithms of black box groups [7–11], we shall note here that we are not using a discrete logarithm oracle or an $\mathrm{SL}_2(q)$-oracle, see [4] for a detailed discussion of the hierarchy of black box group problems.

2 Morphisms and automorphisms

Let $\mathbf{X}$ and $\mathbf{Y}$ be two black box groups encrypting the groups G and H, respectively. We say that a map ζ, which assigns strings from $\mathbf{X}$ to $\mathbf{Y}$, 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:

$$\begin{tikzcd}
\mathbf{X} \arrow[r, "\zeta"] \arrow[d, "\pi_{\mathbf{X}}"'] & \mathbf{Y} \arrow[d, "\pi_{\mathbf{Y}}"] \\
G \arrow[r, "\phi"] & H
\end{tikzcd}$$

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

In this case we say that a morphism ζ encrypts the homomorphism ϕ. Observe that replacing a given generating set of a black box group $\mathbf{X}$ by a more suitable one means that we construct a new black box $\mathbf{Y}$ and work with the corresponding morphism $\mathbf{Y} \to \mathbf{X}$.

The first result based on this new philosophy is "amalgamation of local automorphisms":

Theorem 1. [4, Theorem 5.1] *Let $\mathbf{X}$ be a black box group encrypting a group G. Assume that G contains subgroups $G_1, \ldots, G_l$ invariant under an automorphism $\alpha \in \operatorname{Aut} G$ and that these subgroups are encrypted in $\mathbf{X}$ as black boxes $\mathbf{X}_i$, $i = 1, \ldots, l$, supplied with morphisms*

$$\phi_i : \mathbf{X}_i \longrightarrow \mathbf{X}_i$$

which encrypt restrictions $\alpha|_{G_i}$ *of* α *on* G_i*. Assume also that* $\langle G_i, i = 1, \ldots, l\rangle = G$*. Then we can construct, in time polynomial in* $l(\mathbf{X})$*, a morphism* $\phi : \mathbf{X} \longrightarrow \mathbf{X}$ *which encrypts* α*.*

This theorem can be applied, for example, to groups of Lie type and systems of root SL_2-subgroups corresponding to the nodes in the associated Dynkin diagrams. That way, we construct the following automorphisms of groups of Lie type.

(1) Frobenius maps on groups of Lie type of odd characteristic [4];
(2) Graph automorphisms of $\mathrm{SL}_n(q)$, $D_n(q)$ (including the triality of $\mathrm{D}_4(q)$), $\mathrm{F}_4(q)$, and $\mathrm{E}_6(q)$ (for odd q) [6].

Interestingly, construction of graph automorphisms in black box groups of Lie type of odd characteristic does not use information about the underlying field. Further manipulation with morphisms between root $\mathrm{SL}_2(q)$-subgroups yields, for example, the following (field-independent) black box embeddings constructed in time polynomial in $\log q$ and n:

- $\mathrm{SU}_n(q) \hookrightarrow \mathrm{SL}_n(q^2)$;
- $\mathrm{G}_2(q) \hookrightarrow \mathrm{SO}_7(q) \hookrightarrow \mathrm{SO}_8^+(q) \hookrightarrow \mathrm{SL}_8(q)$;
- ${}^3\mathrm{D}_4(q) \hookrightarrow \mathrm{SO}_8^+(q) \hookrightarrow \mathrm{SL}_8(q)$;

These embeddings are implemented in GAP for various fields but notably we construct the embedding $\mathrm{SU}_3(p) \hookrightarrow \mathrm{SL}_3(p^2)$ for the 60 digit prime

$$p = 622288097498926496141095869268883999563096063592498055290461.$$

Notice that the size of $\mathrm{SL}_3(p^2)$ is bigger than 10^{960}.

Another very important corollary of Theorem 1 is that if the action of an involutive automorphism a of G is known on some a-invariant subgroups of G generating G, then we can transfer the action of a on these subgroups to whole group G. We call this process a *reification* of a. More precisely, we have

Theorem 2. [4, Theorem 7.1] *Let* $\mathbf{X}$ *be a black box group encrypting a finite group* G*. Assume that* G *admits an involutive automorphism* $a \in \operatorname{Aut} G$ *and contains* a*-invariant subgroups* $H_1, \ldots, H_n$ *where* a *either inverts or centralizes each* H_i*.*

Assume also that we are given black boxes $\mathbf{Y}_1, \ldots, \mathbf{Y}_n$ *encrypting subgroups* $H_1, \ldots, H_n$*. Then we can construct, in polynomial time,*

- *a black box for the structure* $\{\,\mathbf{Y}, \alpha\,\}$*, where* $\mathbf{Y}$ *encrypts* $H = \langle H_1, \ldots, H_n\rangle$ *and* α *encrypts the restriction of* $a\,|_H$ *of* a *to* H*;*
- *a black box subgroup* $\mathbf{Z}$ *encrypting* $\Omega_1(Z(C_H(a)))$*, the subgroup generated by involutions from* $Z(C_H(a))$*;*
- *if, in addition, the automorphism* $a \in G$ *and* $H = G$ *then* α *is induced by one of the involutions in* $\mathbf{Z}$*.*

An immediate application of Theorem 2 is that we can append a diagonal automorphism d of $\mathrm{PSL}_2(q)$ to a black box group $\mathbf{X}$ encrypting $\mathrm{PSL}_2(q)$ to obtain a black box group $\mathbf{Y} = \mathbf{X} \rtimes \langle \delta \rangle$ encrypting $\mathrm{PGL}_2(q)$, where δ encrypts d, see [5] for details. This construction plays a crucial role in the proof of Theorem 3 below.

In addition, if a is an *inner* involutive automorphism in a group G of small 2-rank, after reification it can be identified with a string in X.

It turns out that construction of an involution in black box groups encrypting $\mathrm{PGL}_2(2^k)$ by Kantor and Kassabov [12] is a special case of Theorem 2, see [4] for further discussion. Moreover, the construction of a black box projective plane is based on reification of involutions.

3 PSL$_2$(q): structure recovery and unipotent elements

This is our principal result.

Theorem 3. [5] *Let* $\mathbf{Y}$ *be a black box group encrypting* $\mathrm{PSL}_2(\mathbb{F}_q)$ *for* $q = p^k$ *of known odd characteristic* p*. Then we construct, in probabilistic time polynomial in* $\log q$*,*

- *a black box group* $\mathbf{X}$ *encrypting* $\mathrm{PGL}_2(\mathbb{F}_q)$ *and an effective embedding*

$$\mathbf{Y} \hookrightarrow \mathbf{X};$$

- *a black box field* $\mathbf{K}$ *of order* q*, and*
- *polynomial in* $\log q$ *time isomorphisms*

$$\begin{tikzcd} & & \mathbf{Y} \arrow[d] & \\ \mathrm{PGL}_2(\mathbb{F}_q) \arrow[r, two heads] & \mathrm{PGL}_2(\mathbf{K}) \arrow[r, two heads] & \mathbf{X} \arrow[r] & \mathrm{SO}_3(\mathbf{K}) \end{tikzcd}$$

where $\mathbb{F}_q$ *is the standard explicitly given field of order* q*.*

Construction of unipotent elements in $\mathbf{X}$ is an automatic corollary, but can be actually done at early stages of the proof of this theorem.

Our approach to the proof is recovery, within $\mathbf{X}$, of geometric structures arising from the adjoint representation of the group $\mathrm{PGL}_2(q)$ on its Lie algebra $\mathfrak{sl}_2$ seen as an inner product space with respect to its Killing form—this explains appearance of the morphism

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

in the statement of Theorem 3.

Our proof in [5] starts by exploiting the fact that the set of involutions in $\mathbf{X}$ is the set $\mathfrak{I} = \mathfrak{P} \smallsetminus \mathfrak{Q}$ of regular points in projective plane $\mathfrak{P}$ over $\mathfrak{sl}_2$ with a quadric $\mathfrak{Q}$ (coming from the Killing form), and the points in $\mathfrak{Q}$ are the Borel subgroups in $\mathbf{X}$. There are also two types of lines in $\mathfrak{P}$: regular and parabolic. The regular lines are the polar images of regular points

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

The parabolic lines correspond to Borel subgroups B in $\mathbf{X}$ and consist of involutions inverting a maximal unipotent subgroup U of B, together with U itself seen as a point in $\mathfrak{P}$.

It turns out that the set $\mathfrak{I}$ is a finite symmetric space with the conjugation operation $\circ$, for $s,t \in \mathfrak{I}$, $s \circ t = t^s$, forming a finite field analogue of the real hyperbolic (Lobachevsky) plane viewed as a symmetric space. The black box field $\mathbf{K}$ is built by applying the Hilbert's coordinatization on this Lobachevsky plane $\mathfrak{I}$. The analysis of the action of $\mathbf{X}$ on $\mathfrak{I}$ produces the morphism

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

Constructing the black box field by coordinatizing the Lobachevsky plane enables us to construct arbitrary elements in $\mathfrak{P}$ with specified coordinates. In particular, we can construct unipotent elements in $\mathbf{X}$ encrypting $\mathrm{PGL}_2(q)$, which are precisely the points on the quadric $\mathfrak{Q}$.

4 Toolbox in Lobachevsky plane

It is shown in [5] that the following procedures are performed in time polynomial in $\log q$ inside the Lobachevsky plane constructed in $\mathbf{X}$. So we construct 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 through two distinct points s and t, constructs its pole, which is the involution commuting with both s and 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 $\mathbf{k}$ and $\mathbf{l}$ do not intersect in $\mathfrak{I}$ and therefore their intersection point z belongs to $\mathfrak{Q}$, computes the unipotent element.
(i) for a point $s \in \mathfrak{I}$, computes the polar projection

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

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

As an example, we show how we draw the line passing through two distinct points $s, t \in \mathfrak{I}$ as in item (f). For an involution $x \in \mathbf{X}$ denote by $\mathbf{T}_x$ the maximal torus in $C_{\mathbf{X}}(x)$.

If $z = st$ is a unipotent element then $\langle z^{\mathbf{T}_s} \rangle s$ is a parabolic line. Otherwise observe that it suffices to construct the involution $j := j(s,t)$ which commutes with both s and t. Indeed, the line passing through s and t is the coset $\mathbf{T}_j w$ where w is an involution inverting $\mathbf{T}_j$, see Equation (1). If $z = st$ has even order, then j is the involution in $\langle z \rangle$ which can be constructed by using square and multiply method. However, if z has odd order, then we can not construct j immediately but we know its action on $\mathbf{X}$:

- j centralizes $\langle z \rangle$,
- j inverts every element in the torus $\mathbf{T}_s$.

Hence, $j(s,t)$ can be reified from these two conditions by using Theorem 2.

References

1. A. V. Borovik and Ş. Yalçınkaya, *Construction of Curtis-Phan-Tits system for black box classical groups*, Available at arXiv:1008.2823v1.
2. A. V. Borovik and Ş. Yalçınkaya, *Steinberg presentations of black box classical groups in small characteristics*, Available at arXiv:1302.3059v1.
3. A. V. Borovik and Ş. Yalçınkaya, *Fifty shades of black*, Available at arXiv:1308.2487.
4. A. V. Borovik and Ş. Yalçınkaya, *Black box, white arrow*, Available at arXiv:1404.7700.
5. A. V. Borovik and Ş. Yalçınkaya, *Revelations and reifications: Adjoint representations of black box groups* $\mathrm{PSL}_2(q)$, in preparation.
6. A. V. Borovik and Ş. Yalçınkaya, *Subgroup structure and automorphisms of black box classical groups*, in preparation.
7. 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.
8. P. A. Brooksbank, *Fast constructive recognition of black-box unitary groups*, LMS J. Comput. Math. **6** (2003), 162–197.
9. P. A. Brooksbank, *Fast constructive recognition of black box symplectic groups*, J. Algebra **320** (2008), no. 2, 885–909.
10. 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.
11. P. A. Brooksbank and W. M. Kantor, *Fast constructive recognition of black box orthogonal groups*, J. Algebra **300** (2006), no. 1, 256–288.
12. W. M. Kantor and M. Kassabov, *Black box groups* $\mathrm{PGL}(2,2^e)$, arXiv:1309.3715v2.
13. Ş. Yalçınkaya, *Black box groups*, Turkish J. Math. **31** (2007), no. suppl., 171–210.