Black box, white arrow

Borovik, Alexandre and Yalcinkaya, Sukru

2014

MIMS EPrint: **2014.20**

ISSN 1749-9097

BLACK BOX, WHITE ARROW

ALEXANDRE BOROVIK AND ŞÜKRÜ YALÇINKAYA

Abstract. The present paper proposes a new and systematic approach to the so-called black box group methods in computational group theory. Instead of a single black box, we consider categories of black boxes and their morphisms. This makes new classes of black box problems accessible. For example, we can enrich black box groups by actions of outer automorphisms.

As an example of application of this technique, we construct Frobenius maps on black box groups of untwisted Lie type in odd characteristic (Section 6) and inverse-transpose automorphisms on black box groups encrypting $(\mathrm{P})\mathrm{SL}_n(\mathbb{F}_q)$.

One of the advantages of our approach is that it allows us to work in black box groups over finite fields of big characteristic. Another advantage is the explanatory power of our methods; as an example, we explain Kantor's and Kassabov's construction of an involution in black box groups encrypting $\mathrm{SL}_2(2^n)$.

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

1. Introduction

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

This original definition of a black box group appears to have gone out of vogue with the black box group community mostly because it is too abstract and demanding in the context of practical computations with matrix groups. The aim of this paper is to refresh and expand the concept by introducing and systematically using *morphisms*, that is, polynomial time computable homomorphisms of black box groups.

This modest change allows us to apply some basic category theoretic and model theoretic ideology. As we show in this and subsequent papers, this dramatically expands the range of available tools for structural analysis of black box groups and allows to solve black box problems previously not accessible to existing methods. The development of this new approach requires a detailed discussion of some methodological issues of black box group theory.

Date: 29 April 2014.

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

The paper contains a number of new results, and two of them deserve highlighting. They are concerned with construction of automorphisms of black box groups; the first one is construction of Frobenius maps on black box Chevalley groups of untwisted type and odd characteristic. This is stated and proven in Section 6.

The second—and the most important—result of the paper is the "reification of involutions", Theorem 7.1.

In our next work [15], these constructions are applied to recognition of black box groups $(\mathrm{P})\mathrm{SL}_2(q)$ for odd q.

Finally, we have to mention that the paper belongs to a series of works aimed at a systematic development of methods of structural analysis of black box groups [11, 12, 13, 15, 16, 17, 48, 49].

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

$$\begin{tikzcd}\mathbf{X} \arrow[r, dotted, "\pi"] & G.\end{tikzcd}$$

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 [25] 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 [2, 3, 18, 29, 39, 41, 43, 42, 44]). 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, in our next paper [15], even to projective planes. 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 our next paper [15] 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.

By the nature of our axioms, all algorithms for black box groups (in the sense of Axioms BB1–BB3) are Monte Carlo. In most applications, they 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 $\mathbf{X}$ that represent a generating set of G, or the isomorphism type of G.

In our subsequent papers, especially in [15], it becomes clear that the distinction between Monte Carlo and Las Vegas probabilistic algorithms is external to the theory of black box groups although it is quite natural in its concrete applications.

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 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 $\mathbf{X}$, 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 $\log |G|$).

Usually, 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 $\mathbf{X}$.

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 [28] studied nonstandard 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 a basic and fundamental fact as the Fermat Little Theorem has no proof that can be encoded in $I\Delta_0 + \Omega_1$; the best that has 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 $E < 2p$ [28]. Under a stronger version of bounded arithmetic, the Fermat Little Theorem is proven by Jeřábek [32]. These results have to be seen in the context of the earlier work by Krajíček and Pudlák [35] who proved that Buss’ subtheory S_2^1 does not prove the Fermat Little Theorem if the RSA system is secure. Another result by Jeřábek [31] directly links bounded arithmetic with the black box group theory: he showed that the Fermat Little Theorem in S_2^1 equivalent to the correctness of the Rabin-Miller primality testing [45], an archetypal example of a black box group algorithm.

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

2.3. **Cartan decomposition and Axiom BB5.** Our last comment on the axiomatics of black box groups is an observation that in almost all our work in subsequent papers Axiom BB4 can be replaced by its corollary, Axiom BB5, the latter is closely connected to the concept of Cartan decomposition in Lie groups, see the discussion of Cartan decomposition in [8].

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 all 2-elements in $\langle x \rangle$;
- 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 [9].

Axiom BB5 follows from BB4 by the Tonelli-Shanks algorithm [46, 47] applied to the cyclic group $\langle x \rangle$.

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 [36]. 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. Nevertheless we are frequently concerned with black box groups encrypting classical linear groups; even so, some of our results (such as Theorems 8.2 and 9.1) do not even involve the assumption that we know the underlying field of the group but instead assume that we know 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, [12]. Here, it is natural to call the characteristic p "small" if it is known and small enough for the linear in p running time of algorithms to be feasible.

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

- known characteristic, or
- small characteristic.

Our next paper [16] is dominated by "known characteristic" results. In this one, we also obtain some more specific results for small odd characteristics.

3. Morphisms

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 $\mathbf{Y}$ to strings from $\mathbf{X}$ 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:

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

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

We shall say in this situation that a morphism ζ *encrypts* the homomorphism ϕ. For example, morphisms arise naturally when 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 $\mathbf{X}$.

Observe that a map

$$\begin{tikzcd}
G \arrow[r, dotted, "\phi"] & H
\end{tikzcd}$$

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 allow us to treat a morphism

$$\begin{tikzcd}
\mathbf{X} \arrow[r, dotted, "\zeta"] & \mathbf{Y}
\end{tikzcd}$$

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 could mean (although in some cases we use a more sophisticated construction) that we may be able to find strings $x_1, \ldots, x_k$ generating $\mathbf{X}$ with known to us 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.

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

$$\begin{tikzcd}
{} \arrow[r, hook] & {}
\end{tikzcd}$$

stand for embeddings and double-headed arrows

$$\longrightarrow\!\!\!\!\!\twoheadrightarrow$$

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

$$\begin{tikzcd} \mathbf{X} \arrow[r, dotted, "\pi_{\mathbf{X}}"] & \pi(\mathbf{X}); \end{tikzcd}$$

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. **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 $\mathbf{X} \in \mathcal{X}$, we denote by $l(\mathbf{X})$ the length of 0–1 strings representing elements in $\mathbf{X}$. We assume that, for every $\mathbf{X} \in \mathcal{X}$, basic operations of generating, multiplying, comparing strings in $\mathbf{X}$ can be done in probabilistic polynomial time in $l(\mathbf{X})$.

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

Morphisms $\mathbf{X} \longrightarrow \mathbf{Y}$ in $\mathcal{X}$ are understood as defined in Section 3.1 and their running times are bounded by a polynomial in $l(\mathbf{X})$ and $l(\mathbf{Y})$.

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 $Y = \mathrm{GL}_n(p^k)$ as an algorithm or computer routine operating on 0–1 strings of length $l(Y) = n^2k\lceil \log p \rceil$. Using standard matrix representations for simple algebraic groups, we can represent every group of points $Y = \mathrm{G}(p^k)$ of a reductive algebraic group G defined over $\mathbb{F}_{p^k}$ as a black box $\mathbf{Y}$ generating and processing strings of length $l(\mathbf{Y})$ polynomial in $k \log p$ and the Lie rank of $\mathbf{Y}$. Therefore an "explicitly defined" group can be seen a black box group, perhaps of a lighter shade of black.

We feel that the best way to analyze a black box group $\mathbf{X}$ encrypting a finite group G is by a step-by-step construction of a chain of morphisms

$$\begin{tikzcd} G & \mathbf{X} \arrow[l, dotted] & \mathbf{X}_1 \arrow[l, two heads] & \mathbf{X}_2 \arrow[l, two heads] & \cdots \arrow[l, two heads] & \mathbf{X}_n \arrow[l, two heads] & G \arrow[l, two heads] \end{tikzcd}$$

at each step changing the shade of black and increasing the amount of information provided by the black boxes $\mathbf{X}_i$.

Step-by-step transformation of black boxes into "white boxes" and their complex entanglement is captured well by Escher's famous woodcut, Figure 1.

3.3. **Randomized algorithms: Monte Carlo and Las Vegas.** This is a brief reminder of two canonical concepts for the benefit of those readers who do not come from a 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.

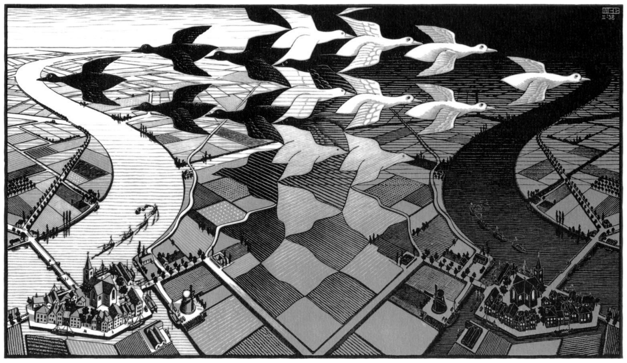

FIGURE 1. M.C. Escher, *Day and Night*, 1938

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 [1].

In our setup, Las Vegas makes no sense unless we are given additional information about $X \dashrightarrow G$, for example

- generators $x_1, \ldots, x_k$ of $\mathbf{X}$, or
- the order of G, or
- the isomorphism type of G.

This additional information is frequently available in applications. Even so, it is frequently more practical and therefore preferable to recover the structure of a black box group $\mathbf{X}$ via a sequence of morphisms

$$\begin{tikzcd}
G & \mathbf{X} \arrow[l, dotted, "\pi"'] \arrow[d, two heads, "\mathrm{Id}"] & \mathbf{X}_1 \arrow[l, two heads, "\mu_1"'] & \cdots \arrow[l, two heads, "\mu_2"'] & \mathbf{X}_n \arrow[l, two heads, "\mu_n"'] & G \arrow[l, two heads, "\mu_{n+1}"'] \\
& \mathbf{X} \arrow[rrrr, two heads, "\lambda"] & & & & G \arrow[u, two heads, "\mathrm{Id}"']
\end{tikzcd}$$

with

- crude but *fast* Monte Carlo morphisms μ_i for $1 \leqslant i \leqslant n+1$, and
- a Las Vegas morphism λ;

then everything becomes Las Vegas.

Using a "real world" simile, we prefer to apply to black box groups the well-known *First Law of Metalworking*: **use the roughest file first**, see Figure 2.

Even in relatively simple black box problems we may end up dealing with a sophisticated category of black boxes and their morphisms—this is emphasized in the title of this paper.

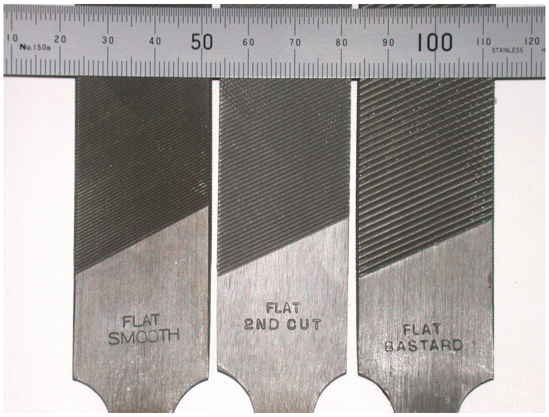

FIGURE 2. Relative tooth sizes for *smooth*, *second cut*, and *bastard* files. There are six different cuts altogether defined as (from roughest to smoothest): *rough, middle, bastard, second cut, smooth*, and *dead smooth*. Source: *Wikipedia*.

4. Black box fields

A *black box* (finite) *field* $\mathbf{K}$ is an oracle or an algorithm operating on 0-1 strings of uniform length (input length), $l(\mathbf{K})$, which encrypts a field of known characteristic p. The oracle produces random elements from $\mathbf{K}$ in probabilistic time polynomial in $l(\mathbf{K})$, computes $x+y$, xy, x^{-1} (for $x \neq 0$) and decides whether $x = y$ for strings $x, y \in \mathbf{K}$. We refer the reader to [7, 40] for more details on black box fields and their applications to cryptography.

In this and subsequent paper, we shall be using some results about the isomorphism problem of black box fields [40], 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 [38, 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 [40] proved that the cost of constructing an isomorphism between a black box field $\mathbf{K}$ 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 4.1. *Let* $\mathbf{K}$ *and* $\mathbf{L}$ *be black box fields encrypting the same finite field and* $\mathbf{K}_0$*,* $\mathbf{L}_0$ *their prime subfield. Then a morphism*

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

can be extended, with the help of polynomial time construction, to a morphism

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

Obviously, if $\operatorname{char} \mathbf{K} = p$, we always have a morphism $\mathbb{F}_p \longrightarrow \mathbf{K}_0$. The existence of the reverse morphism would follow from solution of the discrete logarithm problem in $\mathbf{K}_0$. In particular, this means that, for small primes p, any two black box fields of the same order p^n are effectively isomorphic.

5. Automorphisms

5.1. **Automorphisms as lighter shades of black.** The first application of the "shades 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 5.1. *Let* $\mathbf{X}$ *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 $\mathbf{X}$ *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* $\mathbf{Y}$ *generated in* $\mathbf{X}^k$ *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

$$\begin{array}{rcl} \alpha : \mathbf{Y} & \longrightarrow & \mathbf{Y} \\ (y_0, y_1, \dots, y_{k-2}, y_{k-1}) & \mapsto & (y_1, y_2, \dots, y_{k-1}, y_0) \end{array}$$

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

$$\begin{tikzcd}
\mathbf{Y} \arrow[r, two heads, "\alpha"] \arrow[d, dotted] & \mathbf{Y} \arrow[d, dotted] \\
G \arrow[r, dotted, "a"] & G
\end{tikzcd}$$

A somewhat more precise formulation of Theorem 5.1 is that we can construct, in time polynomial in k and m, k commutative diagrams

(1)
$$\begin{tikzcd}
\mathbf{X} \arrow[d, dotted] & \mathbf{X}^k \arrow[l, two heads, "\{\,\pi_i\,\}_{0\leqslant i\leqslant k-1}"'] \arrow[d, dotted] & \mathbf{Y} \arrow[l, hook', "\delta"'] \arrow[r, dotted, "\alpha"] \arrow[d, dotted] & \mathbf{Y} \arrow[d, dotted] \\
G & G^k \arrow[l, dotted, "\{\,p_i\,\}_{1\leqslant 0\leqslant k-1}"'] & G \arrow[l, dotted, "d"'] \arrow[r, dotted, "a"] & G
\end{tikzcd}$$

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

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

Of course, this construction leads to memory requirements increasing by a factor of k, but, as our subsequent papers [16, 17] show, this is price worth paying. After all, in most practical problems the value of k is not that big, in most interesting cases $k = 2$. Also, direct powers of black boxes appear to be very suitable for resorting to parallel computation [5, 6].

5.2. **Amalgamation of local automorphisms.** A useful special case of Theorem 5.1 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 5.2. *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.

We shall say in this situation that the automorphism ϕ is obtained by amalgamation of local automorphisms ϕ_i.

We can generalize Theorem 5.1 even further.

Theorem 5.3. *Let $\mathbf{X}$ be a black box group encrypting a group G. Assume that G contains subgroups $G_1, \ldots, G_l$ mapped by an automorphism $\alpha \in \operatorname{Aut} G$ to $H_1, \ldots, H_l$, respectively, and that these subgroups are encrypted in $\mathbf{X}$ as black boxes $\mathbf{Y}_i, \mathbf{Z}_i$, $i = 1, \ldots, l$, supplied with morphisms*

$$\phi_i : \mathbf{Y}_i \longrightarrow \mathbf{Z}_i$$

which encrypt restrictions

$$\alpha|_{G_i} : G_i \longrightarrow H_i.$$

Set $\mathbf{Y} = \langle \mathbf{Y}_i, i = 1, \ldots, l\rangle$ and $\mathbf{Z} = \langle \mathbf{Z}_i, i = 1, \ldots, l\rangle$. Then we can construct, in time polynomial in $l(\mathbf{X})$, a morphism

$$\phi : \mathbf{Y} \longrightarrow \mathbf{Z}$$

which encrypts the restriction of α to $\langle G_i, i = 1, \ldots, l\rangle$.

Theorem 5.3 will be used in the proof of Theorem 8.1 and 8.2, and also in the proof of Theorem 9.1 in [16].

6. Construction of Frobenius maps

We now use Theorems 5.1 and 5.2 to construct a Frobenius map on a black box group $\mathbf{X}$ encrypting (P)SL$_2(q)$.

We give a brief description of a Curtis-Tits system for groups of Lie type of rank at least 3 which is used in the proof of Theorems 6.1, 8.1 and 8.2 below. A Curtis-Tits system of a group $G = G(q)$ of Lie type of rank n is a set $\{K_1, \ldots, K_n\}$ of root SL$_2(q)$-subgroups of G where each K_i corresponds to a node in the Dynkin diagram of G. The realtions between K_i and K_j, $i \neq j$, are determined by the bonds connecting the nodes, that is, if there is no bond, then $[K_i, K_j] = 1$; if there is a single or double bonds, then $\langle K_i, K_j\rangle \cong \mathrm{SL}_3(q)$ or (P)Sp$_4(q)$, respectively, see [11, 12] for more details.

Theorem 6.1 (Known characteristic)**.** *Let $\mathbf{X}$ 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 $\mathbf{Y}$ encrypting G,*
- *a morphism $\mathbf{X} \longleftarrow \mathbf{Y}$, and*
- *a morphism $\phi : \mathbf{Y} \longrightarrow \mathbf{Y}$ 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 5.2. First we consider the case when $\mathbf{X}$ encrypts PSL$_2(q)$. Using the standard technique for dealing with involution centralizers, we can find in $\mathbf{X}$ a 4-subgroup V; let E be the subgroup in $G = \mathrm{PSL}_2(q)$ encrypted by V. Since all 4-subgroups in PSL$_2(q)$ are conjugate to a subgroup in PSL$_2(p)$, we can assume without loss of generality that E belongs to a subfield subgroup $H = \mathrm{PSL}_2(p)$ of G and therefore E is centralized 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 basic Galois cohomology considerations that F acts on C_1 and C_2 as power maps $\alpha_i : c \mapsto c^{\epsilon p}$ for $p \equiv \epsilon \bmod 4$, $\epsilon = \pm 1$. If now we take images $\mathbf{X}_i$ of groups C_i, we see that the morphisms $\phi_i : x \mapsto x^{\epsilon p}$ of $\mathbf{X}_i$ encrypt restrictions of F to C_i. Obviously, $\mathbf{X}_1$ and $\mathbf{X}_2$ generate a black box $\mathbf{Y} \longrightarrow \mathbf{X}$, and we can use Theorem 5.2 to amalgamate ϕ_1 and ϕ_2 into a morphism ϕ which encrypts F.

As usual, for groups SL$_2(q)$ the same result can be achieved by essentially the same arguments as for 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 $\mathbf{X}$) 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. □

7. Reification of involutions

Another application of Theorem 5.1 is a simple, but powerful procedure which we call "reification of involutions".

7.1. **From amalgamation of local automorphisms to reification of involutions.** Let G be a finite group, $a \in \operatorname{Aut} G$ an automorphism of order 2 and $H \leqslant G$ an a-invariant subgroup. We say that the action of a on H is *clean* if a either centralizes H or inverts every elements in H.

The following theorem is partly a special case and partly an easy corollary of the amalgamation of local automorphisms, Theorems 5.2 and 5.3.

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 $H_1, \ldots, H_n$ with a clean action of a on each of them.*

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 $\mathbf{Z}$ covering $\Omega_1(Z(C_H(a)))$, 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 $\mathbf{Z}$.*

Notice that in many situations (in particular, when G is a Lie type group of odd characteristic), $\mathbf{Z}$ is small, and identification of α in $\mathbf{Z}$ is easy.

The full strength of reification of involutions will become obvious in [15].

7.2. **Kantor's and Kassabov's construction of involutions in $\mathrm{SL}_2(2^n)$.** The construction of involutions in $\mathrm{SL}_2(2^n)$ as done by Bill Kantor and Martin Kassabov [33] is the special case of reification of involutions.

Indeed, let $\mathbf{X}$ be a black box group encrypting $\mathrm{SL}_2(q)$ with $q = 2^n$.

7.2.1. *First construction.* Tori of order $q-1$ in $\mathbf{X}$ are pointwise stabilisers of pairs of points on the projective line over $\mathbb{F}_q$. Let g and h be two elements of odd orders dividing $q-1$, and assume $[g,h] \neq 1$. If both g and h are contained in the same Borel subgroup of $\mathbf{X}$ then $[g,h]$ belongs to its unipotent radical and is therefore an involution.

Borel subgroups are stabilisers of points on the projective line. If g and h do not belong to the same Borel subgroup, they belong to some tori S and T whose pairs of fixed points are disjoint, say, a, b and c, d. Since $\mathbf{X}$ acts sharply 3-transitively on the projective line, there is a unique element w in $\mathbf{X}$ that maps

$$a \mapsto b, \quad b \mapsto a, \quad c \mapsto d;$$

since this permutation contains a 2-cycle (a, b), it is of even order and is therefore an involution. Now w is an involution that inverts S and T and can therefore be reified by Theorem 7.1, thus becoming the desired involution. □

7.2.2. *A shorter construction.* However there is a shortcut in the construction above. Take $f = gh$ and observe that

$$f^w = g^w h^w = g^{-1} h^{-1};$$

for this calculation, we do not need w as such, its role as a "virtual" involution suffices.

We know that

$$\zeta(f) = f \cdot \sqrt{g \cdot g^w} = gh \cdot \sqrt{ghg^{-1}h^{-1}}$$

belongs to $C_{\mathbf{X}}(w)$; but the latter is a 2-group, therefore it is an involution or 1. But

$$gh \cdot \sqrt{ghg^{-1}h^{-1}} = 1$$

quickly yields $gh = hg$, which is excluded by our initial choice of g and h. Hence $\zeta(f)$ is the desired involution. □

8. The inverse-transpose map

In this section, we use Theorems 5.1 and 5.3 to construct the inverse-transpose map on $G = (\mathrm{P})\mathrm{SL}_n(q)$, q odd.

8.1. **Construction of the inverse-transposed map.**

Theorem 8.1. *Let $\mathbf{X}$ be a black box group encrypting $G = (\mathrm{P})\mathrm{SL}_n(q)$, q odd. Then we can construct, in time polynomial in $\log |G|$, a morphism*

$$\mathbf{X} \xrightarrow{\varphi} \mathbf{X}$$

that encrypts an inverse-transpose map composed with some inner automorphism of G.

Proof. We will prove the result for the black box groups encrypting $\mathrm{SL}_n(q)$, q odd and the result follows from the same arguments for $\mathrm{PSL}_n(q)$.

The key observation is that inverse-transpose map is an inner automorphism of $\mathrm{SL}_2(q)$ but not for $\mathrm{SL}_n(q)$ for $n \geq 3$.

Let $G = \mathrm{SL}_2(q)$ and $w = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Then, conjugation by w is the inverse-transpose map of G. Note that w is a Weyl group element corresponding to the diagonal subgroup T (split torus) of G, that is, w inverts T. In general, the Weyl group elements corresponding to T are of the form $w_t = \begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$ for some $t \in \mathbb{F}_q^*$. Notice that conjugation by w_t is the composition of the inverse-transpose map with an inner automorphism associated to the diagonal element $\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}$.

Let $G \cong \mathrm{SL}_n(q)$, $\{K_1, \ldots, K_{n-1}\}$ be a Curtis-Tits system of G and T be the maximal split torus of G normalizing K_i for each $i = 1, \ldots, n-1$. Assume also that $w_i \in K_i$ be Weyl group elements which inverts the tori $T_i = T \cap K_i$ for each $i = 1, \ldots, n-1$. Then amalgamation on $\{K_1, \ldots, K_{n-1}\}$ the maps

$$K_i \xrightarrow{\varphi_i} K_i,$$

where each φ_i is a conjugation by w_i on K_i, are conjugate to an inverse-transpose map of K_i.

A construction of a Curtis-Tits system $\{\mathbf{K}_1, \ldots, \mathbf{K}_{n-1}\}$ of a black box group $\mathbf{X}$ encrypting $\mathrm{SL}_n(q)$ is presented in [11] and the construction of the tori $\mathbf{T}_i$ and $\mathbf{T} = \langle \mathbf{T}_1, \ldots, \mathbf{T}_{n-1} \rangle$ together with Weyl group elements $w_i \in \mathbf{K}_i$ inverting $\mathbf{T}_i$ is presented in [12]. Since $\mathbf{X}$ is generated by $\{\mathbf{K}_1, \ldots, \mathbf{K}_{n-1}\}$, applying amalgamation to the conjugation by $w_i \in \mathbf{K}_i$, we have an automorphism of $\mathbf{X}$ which encrypts the inverse transpose map composed with some inner automorphism of G. □

8.2. **An application:** $\mathrm{SU}_n(q) \hookrightarrow \mathrm{SL}_n(q^2)$**.** We apply our arguments for the construction of $\mathrm{SU}_n(q)$ inside $\mathrm{SL}_n(q^2)$. We note that the centralizer of inverse transpose map composed with Frobenius map in $\mathrm{SL}_n(q^2)$ is the subgroup $\mathrm{SU}_n(q)$.

Theorem 8.2 (Known characteristic)**.** *Let $\mathbf{X}$ 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 $\mathbf{Y}$ encrypting the group $\mathrm{SU}_n(q)$ and a morphism $\mathbf{Y} \hookrightarrow \mathbf{X}$.*

An important feature of the proof of this theorem (and other similar results in [16]) is that they never refer to the ground fields of the groups and do not involve any computations with unipotent elements. In fact, we interpret morphisms between functors

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

within our black boxes. At a practical level, it means that given a black box group encrypting $\mathrm{SL}_3(p^2)$ for a 60 decimal digits long prime number p, say

$$p = 622288097498926496141095869268883999563096063592498055290461$$

(one of the examples run in GAP on a pretty old and underpowered laptop computer), we can construct a black box subgroup

$$\mathrm{SU}_3(p) \hookrightarrow \mathrm{SL}_3(p^2).$$

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.

Proof of Theorem 8.2. Let $\{\mathbf{K}_1, \ldots, \mathbf{K}_{n-1}\}$ be a Curtis-Tits system for $\mathbf{X}$. Assume also that, for each $i = 1, 2, \ldots, n-1$, $\mathbf{T}_i$ is a maximal split torus of $\mathbf{K}_i$ where $\langle \mathbf{T}_1, \ldots, \mathbf{T}_{n-1} \rangle$ encrypts a maximal split torus of G normalizing each $\mathbf{K}_i$, and $w_i \in \mathbf{K}_i$ are the Weyl group elements, that is, w_i inverts $\mathbf{T}_i$. Furthermore, set $W_i = C_{\mathbf{K}_i}(w_i)$ and $\mathbf{T}_{w_i}$ is the maximal torus in W_i for each $i = 1, 2, \ldots, n-1$.

Let ϕ_i denote the restriction of the Frobenius map on $\mathbf{K}_i$.

Since the inverse transpose map is amalgamated over the conjugation by Weyl group elements w_i, the inverse transpose map inverts $\mathbf{T}_i$ and fixes $\mathbf{T}_{w_i}$. Moreover the restriction of the Frobenius map ϕ_i acts on $\mathbf{T}_i$ and $\mathbf{T}_{w_i}$ as $x \mapsto x^{\epsilon q}$ for $q \equiv \epsilon \bmod 4$, $\epsilon = \pm 1$. Therefore, the centralizer of $w_i \circ \phi_i$ consists of the elements from $\mathbf{K}_i$ satisfying

$$t = t^{-\epsilon q} \text{ or, equivalently } t^{\epsilon q + 1} = 1 \text{ for } t \in \mathbf{T}_i,$$

and

$$t = t^{\epsilon q} \text{ or, equivalently } t^{\epsilon q - 1} = 1 \text{ for } t \in \mathbf{T}_{w_i}.$$

Since $\mathbf{K}_i = \langle \mathbf{T}_i, \mathbf{T}_{w_i} \rangle$, we can compute $\mathbf{C}_i := C_{\mathbf{K}_i}(w_i \circ \phi_i)$. Moreover, since $\mathbf{X} = \langle \mathbf{K}_1, \ldots, \mathbf{K}_{n-1} \rangle$, amalgamation over $\mathbf{C}_i$ gives the subgroup encrypting the fixed points of the inverse transpose map composed with Frobenius map which is isomorphic to $\mathrm{SU}_n(q)$. □

9. Structure recovery

In this section, we revise the classification of black box group problems and outline our vision of the hierarchy of typical black box group problems.

9.1. The hierarchy of black box problems.

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

Recognition Problem: Determine the isomorphism class of the group encrypted by $\mathbf{X}$.

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 [45] for testing primality of the given odd number n is simply 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 $\mathbf{X}$ is

Constructive Recognition: Suppose that a black box group $\mathbf{X}$ 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 $\mathbf{X}$ and given a string x produced by $\mathbf{X}$, there is an efficient procedure to construct the element $\Psi^{-1}(x) \in G$ encrypted by $\mathbf{X}$.*

However, there are still no really efficient constructive recognition algorithms for black box groups $\mathbf{X}$ 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, 24, 27, 37] are the need to construct unipotent elements in black box groups, [19, 20, 21, 23, 22, 24] or to solve discrete logarithm problem for matrix groups [26, 27, 37].

Unfortunately, the probability that the order of a random element is divisible by p is $O(1/q)$ [30], 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 [34] used it to develop an algorithm for recognition of black box classical groups. Later the algorithms of [34] 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.***

9.2. **Structure recovery.** Suppose that a black box group $\mathbf{X}$ 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 $\mathbf{X}$ means to construct, in probabilistic polynomial time in $\log |G|$,

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

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

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

An example of a structure recovery is presented in our next paper [15] for black box groups $(\mathrm{P})\mathrm{SL}_2(q)$.

9.3. **Separation of flesh from bones.** 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.

A "category-theoretical" approach allows us to carry out constructions like the following one.

Theorem 9.1 (Known characteristic [16])**.** *Let* $\mathbf{X}$ *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*

$$\mathbf{U} \hookrightarrow \mathbf{V} \hookrightarrow \mathbf{W} \hookrightarrow \mathbf{X}$$

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 constructions (and even the embedding

$${}^3\mathrm{D}_4(q) \hookrightarrow \mathrm{SO}_8^+(q^3),$$

also done in [16]) are "field-free" and, moreover, "characteristic-free".

Another aspect of the concept of "structure recovery" is that it follows an important technique from 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 [15] closely follows this model-theoretic paradigm.

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.

Final touches to the paper were put during the Workshop on Model Theory and Groups at İstanbul Center for Mathematical Sciences in March 2014.

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

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

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 (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)
2. 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.
3. ———, *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. R. Behrends, A. Konovalov, S. Linton, F. Lübeck, and M. Neunhöffer, *Parallelising the computational algebra system GAP*, Proceedings of the 4th International Workshop on Parallel and Symbolic Computation (New York, NY, USA), PASCO '10, ACM, 2010, pp. 177–178.
6. R. Behrends, A. Konovalov, F. Lübeck, and M. Neunhöffer, *Towards high-performance computational algebra with GAP*, Proceedings of the Third International Congress on Mathematical Software. Kobe, Japan, September 13–17, 2010 (K. Fukada, J. van der Hoeven, Joswig. M., and N. Takayama, eds.), Springer, 2010, pp. 58–61.
7. 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).
8. A. Borovik, *Mathematics discovered, invented, and inherited*, Selected Passages from Correspondence with Friends **1** (2013), 13–28.
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. ———, *Construction of some subgroups in black box groups* $\mathrm{PGL}_2(q)$ *and* $(\mathrm{P})\mathrm{SL}_2(q)$, Available at arXiv:1403.2224 [math.GR].
14. ———, *Construction of Curtis-Phan-Tits systems in black box twisted Chevalley and exceptional groups of Lie type and odd characteristic*, in preparation.
15. ———, *Revelations and reifications: Adjoint representations of black box groups* $\mathrm{PSL}_2(q)$, in preparation.
16. ———, *Subgroup structure and automorphisms of black box classical groups*, in preparation.
17. ———, *Subgroup structure and automorphisms of black box groups of exceptional groups of odd characteristic*, in preparation.
18. 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.
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. 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.
25. 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.
26. 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.
27. 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.
28. 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).
29. A. Gamburd and I. Pak, *Expansion of product replacement graphs*, Combinatorica **26** (2006), no. 4, 411–429.
30. 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.
31. E. Jeřábek, *Dual weak pigeonhole principle, Boolean complexity, and derandomization*, Annals of Pure and Applied Logic **129**, no. 1–3.
32. ———, *Abelian groups and quadratic residues in weak arithmetic*, Mathematical Logic Quarterly **56** (2010), no. 3, 262–278.
33. W. M. Kantor and M. Kassamov, *Black box groups* $\mathrm{PGL}(2, 2^e)$, arXiv:1309.3715v2 [math.GR].
34. W. M. Kantor and Á. Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708, viii+168.
35. J. Krajíček and P. Pudlák, *Some consequences of cryptographical conjectures for* S_2^1 *and* EF, Inform. and Comput. **140** (1998), no. 1, 82–94. MR 1492845 (99c:03092)
36. 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.
37. 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.
38. H. W. Lenstra Jr., *Finding isomorphisms between finite fields*, Mathematics of Computation **56** (1991), no. 193, pp. 329–347 (English).
39. A. Lubotzky and I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363.
40. 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.
41. 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.
42. ———, *The product replacement algorithm is polynomial*, Proc. FOCS'2000, The 41st Ann. Symp. on Foundations of Comp. Sci. (2001), 476–485.
43. ———, *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.
44. I. Pak and A. Żuk, *On Kazhdan constants and mixing of random walks*, Int. Math. Res. Not. (2002), no. 36, 1891–1905.

45. M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.
46. 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. MR 0371855 (51 #8072)
47. 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).
48. Ş. Yalçınkaya, *Construction of long root $SL_2(q)$-subgroups in black-box groups*, Available at arXiv, math.GR/1001.3184v1.
49. Ş. Yalçınkaya, *Black box groups*, Turkish J. Math. **31** (2007), no. suppl., 171–210. MR 2369830 (2009a:20081)

School of Mathematics, University of Manchester, UK

alexandre@borovik.net

İstanbul University, previously Nesin Mathematics Village, Izmir, Turkey

sukru.yalcinkaya@gmail.com