axioms

MDPI

Article

Towards Effective Recognition of Black Box Rings

Alexandre Borovik [1,*] and Şükrü Yalçınkaya [2]

[1] Department of Mathematics, University of Manchester, Manchester M13 9PL, UK
[2] Department of Mathematics, Istinye University, Istanbul 34396, Turkey; sukru.yalcinkaya@istinye.edu.tr
* Correspondence: alexandre@borovik.net

Abstract

Black box algebra is a part of computational algebra focused on probabilistic methods of solving problems in very large finite algebraic objects where deterministic approaches simply do not work. The present paper provides a construction of structural proxies for black box rings encrypting rings of 2×2 matrices over finite fields.

Keywords: black box rings; black box groups; probabilistic methods

MSC: 20P05

1. Introduction

General discussion of problems in black box algebra, and extensive bibliography and historic remarks on black box groups, fields and rings, can be found in [1]. Terminology and notation in the present paper follow more updated papers [2,3].

As an example of application of black box analysis of an algebraic structure, we prove the following.

Theorem 1. *Let* R *be a black box ring encrypting the ring of* 2×2 *matrices* $\mathrm{M}_{2\times 2}(\mathbb{F})$*, where* $\mathbb{F}$ *is an unknown finite field* $\mathbb{F}$ *of unknown odd characteristic, and let* E *be a computationally feasible global exponent for invertible cryptoelements* x *of* R *(that is,* $\mathsf{x}^E = 1$*, see Axiom GE in Section 2). Then, there is a Las Vegas algorithm which constructs, in time polynomial in* $\log E$*, a black box field* $\mathsf{Z} = Z(\mathsf{R})$ *encrypting* $\mathbb{F}$*, and isomorphisms*

$$\mathsf{R} \longleftrightarrow \mathrm{M}_{2\times 2}(\mathsf{Z}).$$

Corollary 1. *Let* R *be a black box ring encrypting the ring of* 2×2 *matrices* $\mathrm{M}_{2\times 2}(\mathbb{F})$*, where* $\mathbb{F}$ *is a finite field of known odd order* q*. Then, there is a Las Vegas algorithm which constructs, in time polynomial in* $\log q$*, a black box field* Z *encrypting* $\mathbb{F}$*, and isomorphisms*

$$\mathsf{R} \longleftrightarrow \mathrm{M}_{2\times 2}(\mathsf{Z}).$$

Estimates for the complexity of the various algorithms in our construction are detailed in [1] (Section 12). The overall running time is fundamentally dominated by the construction of the two-way isomorphism $\mathsf{X}/Z(\mathsf{X}) \leftrightarrow \mathrm{PGL}_2(\mathsf{K})$, where X is the group of invertible elements of R and K is a specially constructed black box field. But the black box field $\mathsf{Z} = Z(\mathsf{R})$ has small fixed cost, negligible in comparison with that of K. Consequently, as stated in [1] (Sections 12.13 and 12.14) the algorithm runs in $O(\xi \log^2 E \log\log E + \mu \log^3 E \log\log E)$ time for Theorem 1 and $O(\xi \log^2 q \log\log q + \mu \log^3 q \log\log q)$ time for Corollary 1, where

Check for updates

Academic Editor: Yang Zhang

Received: 30 May 2026
Revised: 24 June 2026
Accepted: 6 July 2026
Published: 8 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

μ is an upper bound on the time required for a single group operation in X and ξ is an upper bound on the time requirement, per element, for the construction of random elements of X.

A few words about the nature of algorithms could be useful. Most probabilistic algorithms used in black box algebra are divided in two classes:

Monte-Carlo: they give correct answer with probability $> 1/2$. Repeating the calculation makes the probability of error exponentially small.
One-sided version: answer YES is always correct but answer NO may be wrong with probability $< 1/2$.

Las Vegas: they give always a correct answer or fail with probability $< 1/2$.

In the proof of Theorem 1, we construct and use Monte-Carlo algorithms, for example, constructing the field of scalars, see Step 4 of the proof. But the ultimate check of correctness of the answer is done by verifying the Identities (3) for the matrix elements e_{ij} of a standard matrix basis constructed in the proof:

$$\mathsf{e}_{ij}\mathsf{e}_{kl} = \begin{cases} e_{il} & \text{if} \quad j = k \\ 0 & \text{if} \quad j \neq k \end{cases}.$$

Therefore the full algorithm is Las Vegas.

This paper is designed to be self-contained as much as possible. An interested reader can find a more detailed discussion of the wider context of our work, of techniques used, and of methods to estimate computational complexity of algorithms in our paper [3], as well as a deeper discussion of methodology in [1]. Consulting these papers could be useful, but not necessary.

2. Axiomatic Description of Black Box Algebraic Structures

A *black box algebraic structure* X is a black box (device, algorithm, or oracle) which produces and operates with 0–1 strings of uniform length $l(\mathsf{X})$ encrypting (not necessarily in a unique way) elements of some fixed algebraic structure A: if x is one of these strings, then it corresponds to a unique (but unknown to us) element $\pi(\mathsf{x}) \in A$. Here, π is the decrypting map, not necessarily known to us in advance.

Our axioms for black boxes are the same as in [1–3], but stated in a more formal language.

BB1 On request, X produces a string x of fixed length $l(\mathsf{X})$, which depends on X, encrypting an element $\pi(\mathsf{x})$ for some fixed explicitly given algebraic structure A; this is done in time polynomial in $l(\mathsf{X})$. When this procedure is repeated, the elements $\pi(\mathsf{x}_1), \pi(\mathsf{x}_2), \ldots$ are independent and uniformly distributed in A.

In this paper, we work only with groups and fields so we assume that operations on A are unary or binary; a general case can be treated in exactly the same way.

BB2 On request, X performs algebraic operations on the encrypted strings which correspond to operations in A in a way which makes the map π (unknown to us!) a homomorphism: for every binary (unary case is similar) operation $\boxdot$ and strings x and y produced or computed by X,

$$\pi(\mathsf{x} \boxdot_{\mathsf{X}} \mathsf{y}) = \pi(\mathsf{x}) \boxdot_A \pi(\mathsf{y}).$$

We shall write $\mathsf{x} \in \mathsf{X}$ if the string x is produced by X.

It should be noted that we do not assume the existence of an algorithm which allows us to decide whether a specific string can be potentially produced by X; requests for operations on strings can be made only in relation to strings previously output by X. Also, we do not make any assumptions on probabilistic distribution of strings.

BB3 On request, X determines, in time polynomial in $l(\mathsf{X})$, whether two strings x and y encrypt the same element in A, that is, check whether $\pi(\mathsf{x}) = \pi(\mathsf{y})$.

We say in this situation that a black box X *encrypts* the algebraic structure A and we write $\mathsf{X} \vDash A$. We shall call strings produced by X *cryptoelements*. If $\mathsf{x} \in \mathsf{X}$ and $\pi(\mathsf{x}) = a \in A$, we shall express that as $\mathsf{x} \vDash a$ and use the expressions x *encrypts* a and x *represents* a interchangeably.

In the specific case where A is a group (written multiplicatively), the following axiom formalizes a crucial property frequently encountered when applying black-box methods to computational finite algebra. This is especially relevant in the context of cryptography and computations involving matrix groups over finite fields.

GE We are given a *global exponent* of X, that is, a natural number $E := E(\mathsf{X})$ such that

- $\mathsf{x}^E = 1$ for all strings x produced by X; and
- $\log E$ is polynomially bounded in terms of $l(\mathsf{X})$.

Introducing Axiom **GE** dramatically clarifies the underlying sub-algorithms, resulting in cleaner and more structured GAP code for practical implementation. Its uniforming role is obvious in Theorem 3: in the proof of Theorem 1 we will be able to manipulate with elements in a black box group $\mathsf{X} \vDash \mathrm{PGL}_2(\mathbb{F})$ without even knowing the characteristic of the field $\mathbb{F}$.

Global exponents are ubiquitous. For example, if a black box group X encrypts a subgroup embedded in $\mathrm{GL}_n(\mathbb{F})$, we can simply take the exponent of $\mathrm{GL}_n(\mathbb{F})$ as the global exponent for X. This happens all the time in matrix algebra over finite fields, see [3] (Introduction) for more detail.

Clearly, in black box problems, the decrypting map π is not given in advance. However, it is useful to think about any algebraic structure (say, a finite field) implemented on a computer as a trivial black box, with π being the identity map, and with random elements produced with the help of a random number generator. In this situation, obviously, the axioms BB1–BB3 hold.

In our algorithms, we have to build new black boxes from existing ones and work with several black box structures at once: this is why we have to keep track of the length $l(\mathsf{X})$ on which a specific black box X operates. For example, in [1] it turns out that it is useful to consider an automorphism of A as a graph in $A \times A$. This produces another algebraic structure isomorphic to A which can be seen as being encrypted by a black box Z producing, and operating on, certain pairs of cryptoelements from X, see [1] for more examples. In this case, clearly, $l(\mathsf{Z}) = 2l(\mathsf{X})$.

Axiom BB1 is the only difference between our axioms and the original set-up of Babai and Szemerédi [4]: when we construct a new black box structure Y from X, operations on Y are usually more expensive than a direct construction of random cryptoelements in Y from random cryptoelements in X—this is the case, for example, of a black box field constructed from a black box projective plane constructed from a black box group $\mathrm{PGL}_2(\mathbb{F})$, which, in its turn, was constructed from a black box group $\mathrm{SL}_2(\mathbb{F})$ [1]. Another example where Axiom BB1 is very natural in analysis of an impersonation attack on homomorphic encryption [2]: here, supply of random cryptoelements is achieved simply by picking random codewords from the intercepted communication traffic.

3. Black Box Fields

We use Axioms BB1–BB3 to define black box fields with a few obvious changes in the wording. In Axiom BB2, we assume that the black box can perform the addition, multiplication, and inversion in the field. The reader may wish to compare our exposition with [5]. We remind that, in this paper, we do not necessarily know the characteristic of the

field. Therefore we slightly generalize the definition of a black box field given in [5,6] by removing the assumption that the characteristic of the field is known. We refer the reader to [5,6] for more details of black box fields of known characteristic.

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 [7] (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 $n \log p$.

By an *efficient isomorphism* between a black box field and an explicitly given finite field $\mathbb{F}_{p^n}$, we mean an algorithm constructing such an isomorphism in time polynomial in the input length, that is, we find a procedure which computes images and preimages, in time polynomial in n and $\log p$.

One of the key results on black box fields belongs to Maurer and Raub [6]; its statement and proof can be reformulated to yield the following result.

Theorem 2 (Maurer and Raub [6]). *Let* K *be a black box field of known characteristic* p *encrypting an explicitly given finite field* $\mathbb{F}_{p^n}$ *and* K_0 *the prime subfield of* K. *Then the isomorphism problem between* K *and* $\mathbb{F}_{p^n}$ *can be efficiently reduced to the isomorphism problem between* K_0 *and* $\mathbb{F}_p$. *In particular,*

- *an efficient isomorphism* $\mathsf{K}_0 \longrightarrow \mathbb{F}_p$ *can be extended in time polynomial in the input length* $l(\mathsf{K})$ *to an efficient isomorphism* $\mathsf{K} \longrightarrow \mathbb{F}_{p^n}$;
- *there exists an isomorphism* $\mathbb{F}_{p^n} \longrightarrow \mathsf{K}$ *computable in time polynomial in* $l(\mathsf{K})$.

In our terminology, Theorem 2 provides a *structural proxy* for black box fields of known characteristic, see Section 4. Indeed, if K is a black box field of known characteristic p, then we can construct an isomorphism $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathsf{K}_0$ by the map

$$m \mapsto 1 + 1 + \cdots + 1 \quad (m \text{ times})$$

where 1 is the unit in K_0; it is computable in linear in $\log p$ time by double-and-add method. Construction of an isomorphism $\mathsf{K}_0 \longrightarrow \mathbb{F}_p$ remains an open problem when p is an astronomically large prime.

4. Structural Proxy and Structure Recovery

Most groups of Lie type (we exclude ${}^2B_2$, ${}^3D_4$, ${}^2F_4$ and ${}^2G_2$ to avoid technical details) can be seen as functors $G : \mathcal{F} \longrightarrow \mathcal{G}$ from the category of fields $\mathcal{F}$ with an automorphism of order $\leqslant 2$ to the category of groups $\mathcal{G}$. There are also other algebraic structures which can be defined in a similar way as functors from $\mathcal{F}$, for example, projective planes or simple Lie algebras (viewed as rings). The following problem is natural and, as our results show, useful in this context.

Structure recovery: Suppose that we are given a black box structure $\mathsf{X} \vDash A(\mathbb{F})$. Construct, in time polynomial in $l(\mathsf{X})$,

- a black box field $\mathsf{K} \vDash \mathbb{F}$, and
- an isomorphism $A(\mathsf{K}) \longrightarrow \mathsf{X}$.

https://doi.org/10.3390/axioms15070511

If we construct a black box field K by using X as a computational engine, then we can construct the natural representation $A(\mathsf{K})$ of the structure A over the black box field K. A trickier part of structure recovery is construction of isomorphism $A(\mathsf{K}) \longrightarrow \mathsf{X}$. If we achieved that, then by Maurer and Raub [6] (see also [1] (Theorem 3.1)), we have a computable in probabilistic polynomial time isomorphism $\mathbb{F}_q \longrightarrow \mathsf{K}$ and, hence, isomorphisms

$$A(\mathbb{F}_q) \longrightarrow A(\mathsf{K}) \longrightarrow \mathsf{X}$$

producing a more powerful and useful structure recovery of X.

If a structural recovery is achieved, this means that we can force the black box to produce cryptoelements with specific properties.

A much stronger and harder-to-achieve version of structure recovery is the concept of structure proxy.

Construction of a structural proxy: Suppose that we are given a black box structure $\mathsf{X} \vDash A(\mathbb{F})$. Construct, in time polynomial in $l(\mathsf{X})$,

- a black box field $\mathsf{K} \vDash \mathbb{F}$
- two-way bijective morphisms $A(\mathsf{K}) \longleftrightarrow \mathsf{X}$.

In this situation, we call $A(\mathsf{K})$ a *structural proxy* of the black box X.

Structure recoveries and structural proxies play a crucial role in our papers [1,3]. We construct the structural proxies for

- a black box projective plane with polarity $\mathsf{Z} \vDash \mathbb{P}(\mathbb{F}_q)$;
- the projectivisation of a black box Lie algebra $\mathsf{Y} \vDash \mathfrak{sl}_2(\mathbb{F}_q)$ (this one appears in disguise as construction of the "cross product" on the projective plane);
- black box groups $\mathsf{X}_1 \vDash \mathrm{SO}_3(\mathbb{F}_q) \simeq \mathrm{PGL}_2(\mathbb{F}_q)$, $\mathsf{X}_2 \vDash \mathrm{PSL}_2(\mathbb{F}_q)$, $\mathsf{X}_3 \vDash \mathrm{SL}_2(\mathbb{F}_q)$.

In all these cases, q is odd.

Corollary 1 of the present paper adds to this list

- a structural proxy for the black box ring $\mathsf{R} \vDash \mathrm{M}_2(\mathbb{F}_q)$, q odd.

Proof of Theorem 1 critically depends on the use of a structural proxy for groups PGL_2 constructed in our previous paper [3] (Theorem 2).

Theorem 3 (Borovik and Yalçınkaya [3])**.** *Let* X *be a black box group encrypting* $\mathrm{PSL}_2(\mathbb{F})$ *or* $\mathrm{PGL}_2(\mathbb{F})$*, where* $\mathbb{F}$ *is an unknown finite field of unknown odd characteristic, and let* E *be a global exponent for* X*. Then there is a Las Vegas algorithm which constructs, in probabilistic time polynomial in* $\log E$*, structural proxies*

$$\mathsf{X} \longleftrightarrow \mathrm{PSL}_2(\mathsf{K})$$

or

$$\mathsf{X} \longleftrightarrow \mathrm{PGL}_2(\mathsf{K}),$$

respectively.

The present paper is evidence of the power of this approach to black box algebra.

These observations strongly suggest that the black box analysis of most structures built from finite fields (and they dominate finite algebra) could be most likely reduced to black box analysis of fields, with implications for algebraic cryptography discussed in [2].

https://doi.org/10.3390/axioms15070511

5. Preparing Proof of Theorem 1: Dihedral Subgroups of Order 8 in $\mathbf{GL_2(\mathbb{F})}$

We prove the following useful lemmas.

Lemma 1. *Let $G = \mathrm{GL}_2(\mathbb{F})$ where $\mathbb{F}$ is a finite field of odd characteristic. Then the subgroups isomorphic to a dihedral group of order 8 in G are all conjugate.*

Proof. Let $e_1 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ and $w_1 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Then, it is easy to check that

$$e_1^2 = w_1^4 = 1 \text{ and } e_1^{-1} w_1 e_1 = w_1^{-1}.$$

Therefore $D = \langle e_1, w_1 \rangle$ is a dihedral group of order 8. Assume that $H = \langle r, s \mid r^2 = s^4 = 1, r^{-1}sr = s^{-1} \rangle$ is any other dihedral group of order 8 in G and $e_1 \mapsto r$, $w_1 \mapsto s$ is an isomorphism. As r is an element of order 2, its characteristic polynomial is the same as the characteristic polynomial of the element e_1 and its matrix representation with respect to the ordered basis consisting of its eigenvectors corresponding to the eigenvalues -1 and 1 is the same matrix element e_1. This means that there exists $g \in G$ such that $r^g = e_1$. By a direct computation, we see that the elements of order 4 in G which are inverted by e_1 have the form

$$\begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$$

for some $0 \neq t \in \mathbb{F}$. Since $\langle r^g, s^g \rangle$ is a dihedral group of order 8, we must have $s^g = \begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix}$ for some $0 \neq t \in \mathbb{F}$. Since

$$\begin{bmatrix} 0 & t \\ -t^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & t^{-1} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

setting $h = \begin{bmatrix} 1 & 0 \\ 0 & t^{-1} \end{bmatrix}$, we have

$$r^{gh} = e_1 \text{ and } s^{gh} = w_1$$

which proves that $H^{gh} = D$ and all dihedral groups of order 8 in G are conjugate. □

Lemma 2. *In any black box field K of odd or zero characteristics, we can construct cryptoelements 0, 1, and -1—without even knowing the characteristic of K. After that, it can be directly checked that the matrices*

$$\mathsf{e} \vDash \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad -\mathsf{e} \vDash \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \mathsf{e}_1 \vDash \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathsf{e}_2 \vDash \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1}$$

together with

$$\mathsf{w}_1 \vDash \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad -\mathsf{w}_1 \vDash \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \quad \mathsf{w}_2 \vDash \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad -\mathsf{w}_2 \vDash \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{2}$$

form a dihedral subgroup of order 8 in the matrix group $\mathsf{G} = \mathrm{GL}_2(\mathsf{K})$.

Proof. Obvious. □

We denote this group as D. Elements listed in (1) form the elementary abelian subgroup $\mathsf{E} \lhd \mathsf{D}$ of order 4. The element e is of course the identity of G and of the matrix ring $\mathrm{M}_{2\times 2}(\mathsf{K})$. Elements e and $-\mathsf{e}$ belong to $Z(\mathsf{G})$.

6. Proof of Theorem 1

We start with an obvious observation that even if the zero $0 \vDash 0$ is not given explicitly in the set-up of the black box ring R, we can easily construct it by taking a random $\mathsf{r} \in \mathsf{R}$ and computing $0 = \mathsf{r} - \mathsf{r}$.

Construction of a structural proxy of R is explained in the steps below. The crucial ingredient of the proof is to construct the field of scalars and a dihedral group of order 8 in the multiplicative group of R.

For the purpose of estimating probabilities, we formally assume that the underlying field has order $|\mathbb{F}| = q$. We use q simply as a variable to help express these probabilities clearly.

Step 1: Construction of the black box group $\mathsf{X} \vDash \mathrm{GL}_2(\mathbb{F})$. Observe first that a random element in $R = \mathrm{M}_{2\times 2}(\mathbb{F})$ is invertible with probability $1 - O\left(\frac{1}{q}\right)$. Therefore a random element $\mathsf{r} \in \mathsf{R}$ is invertible with probability close to 1 when q is large. Now we use the global exponent E: For an invertible cryptoelement $\mathsf{r} \in \mathsf{R}$, we have $\mathsf{r}^E = 1$ where 1 encrypts the multiplicative identity of R. Therefore we can easily construct the identity cryptoelement in R. Hence the invertible cryptoelements in R give us the black box group $\mathsf{X} \vDash \mathrm{GL}_2(\mathbb{F})$.

Step 2: Generation of trace 0 cryptoelements. Our next task is to construct in R a black box subring Z encrypting the subring $Z = Z(R)$ of scalar matrices in R. Of course, Z is a field, and therefore $\mathsf{Z} \vDash \mathbb{F}$. When Z is constructed, it will turn R into a black box Z-algebra.

It is easy to check that, for any matrices $a, b \in \mathrm{M}_{2\times 2}(\mathbb{F})$ over any field $\mathbb{F}$, the matrix $[a,b]^2 = (ab-ba)^2$ is a scalar matrix; hence we have a natural map

$$\begin{array}{ccc} \mathsf{R}\times\mathsf{R} & \longrightarrow & \mathsf{Z} \\ (\mathsf{r},\mathsf{s}) & \mapsto & [\mathsf{r},\mathsf{s}]^2 \end{array}$$

with values in $\mathsf{Z} = Z(\mathsf{R})$. We need to check that this map gives almost uniformly distributed cryptoelements in Z.

Matrices of trace zero in $\mathrm{M}_{2\times 2}(\mathbb{F})$ form the Lie subalgebra $\mathfrak{sl}_2(\mathbb{F})$. The Lie algebra $\mathfrak{gl}_2(\mathbb{F})$ of $\mathrm{M}_{2\times 2}(\mathbb{F})$ can be decomposed as the sum of two ideals

$$\mathfrak{z} \oplus \mathfrak{sl}_2(\mathbb{F}),$$

where $\mathfrak{z}$ is the center of $\mathfrak{gl}_2(\mathbb{F})$. Therefore, the probability of an element $c \in \mathfrak{sl}_2(\mathbb{F})$ to be a commutator of two independent random elements from $\mathfrak{gl}_2(\mathbb{F})$ is the same as the probability of being a commutator of two independent random elements from $\mathfrak{sl}_2(\mathbb{F})$. For estimating the latter, observe that if $c = [a,b]$ and $c \neq 0$, then a and b belong to the plane in $\mathfrak{gl}_2(\mathbb{F})$ orthogonal to c with respect to the Killing form on $\mathfrak{gl}_2(\mathbb{F})$. This plane, denoted by $c^\perp$, does not contain c if c is semisimple, and contains c if c is nilpotent.

Because a and b are restricted to this 2-dimensional plane $c^\perp$, we can evaluate the commutator map strictly on $c^\perp$. Observe that, for any $x, y \in c^\perp$, $[x,y]$ is orthogonal to all of $c^\perp$. Thus, $[x,y] \in (c^\perp)^\perp = \mathrm{Span}(c)$. Choosing a basis $\{e_1, e_2\}$ for $c^\perp$, any $a, b \in c^\perp$ can be written as $a = x_1e_1 + y_1e_2$ and $b = x_2e_1 + y_2e_2$, making their commutator $[a,b] = (x_1y_2 - x_2y_1)[e_1,e_2]$. Since $[e_1,e_2]$ is a non-zero multiple of c, setting $[a,b] = c$ is equivalent to solving the determinant equation $x_1y_2 - x_2y_1 = k$ for some non-zero constant $k \in \mathbb{F}^*$. The

number of solutions corresponds to the number of 2×2 matrices over $\mathbb{F}$ with determinant k. The general linear group $\mathrm{GL}_2(\mathbb{F})$ has $(q^2-1)(q^2-q)$ elements, evenly distributed across the $q-1$ non-zero determinants, yielding exactly $q(q^2-1) = q^3 - q$ valid pairs for (a, b). Given $(q^3)^2 = q^6$ total pairs in $\mathfrak{sl}_2(\mathbb{F}) \times \mathfrak{sl}_2(\mathbb{F})$, the probability of c being a commutator of random elements from $\mathfrak{sl}_2(\mathbb{F}_q)$ is $\frac{q^3-q}{q^6} = \frac{1}{q^3} - \frac{1}{q^5}$.

Step 3: The quadratic form on $\mathfrak{sl}_2$. Now we turn our attention to the square map

$$\begin{array}{ccc} \sigma : \mathfrak{sl}_2(\mathbb{F}) & \longrightarrow & Z \\ s & \mapsto & s^2. \end{array}$$

Let s be a trace zero matrix,

$$s = \begin{bmatrix} a & b \\ c & -a \end{bmatrix},$$

then it is easy to check that

$$s^2 = \begin{bmatrix} a^2+bc & 0 \\ 0 & a^2+bc \end{bmatrix},$$

and that $a^2 + bc = -\det s$ is proportional to the Killing quadratic form on $\mathfrak{sl}_2(\mathbb{F})$.

To determine the probability that a random element maps to a given scalar matrix $xI \in Z$, we must count the number of preimages $(a, b, c) \in \mathbb{F}^3$ satisfying $a^2 + bc = x$. If $b \neq 0$, there are $q-1$ choices for b and q choices for a, which uniquely determine $c = b^{-1}(x - a^2)$, yielding $q(q-1)$ solutions. If $b = 0$, then c can take any of the q values in $\mathbb{F}$, and we must solve $a^2 = x$. Since the characteristic of $\mathbb{F}$ is odd, this yields 1, 2, or 0 solutions for a depending on whether x is zero, a non-zero quadratic residue, or a quadratic non-residue, respectively. Summing these cases gives q^2, $q^2 + q$, or $q^2 - q$ total preimages. Dividing by $|\mathfrak{sl}_2(\mathbb{F})| = q^3$, the probability of mapping to a specific element in Z is either $\frac{1}{q}$, $\frac{1}{q} + \frac{1}{q^2}$, or $\frac{1}{q} - \frac{1}{q^2}$. Thus, elements of Z are images of random elements from $\mathfrak{sl}_2(\mathbb{F})$ with probability $\frac{1}{q} + O\left(\frac{1}{q^2}\right)$.

Step 4: Construction of the field of scalars. Combining these two estimates, we see that the square map

$$\begin{array}{ccc} R \times R & \longrightarrow & Z \\ (a, b) & \mapsto & [a, b]^2 \end{array}$$

hits specific elements in Z with probabilities $\frac{1}{q} + O\left(\frac{1}{q^2}\right)$, that is, it is essentially the uniform distribution. Therefore the map

$$\begin{array}{ccc} \mathsf{R} \times \mathsf{R} & \longrightarrow & \mathsf{Z} \\ (\mathsf{x}, \mathsf{y}) & \mapsto & [\mathsf{x}, \mathsf{y}]^2 \end{array}$$

can be taken for a generator of random cryptoelements for the black box Z; operations of addition, multiplication, inversion on Z are inherited from R and its multiplicative group.

Notice that construction of random elements in Z comes at remarkably low fixed cost: two generations of random elements in R, three multiplications and one subtraction. It is negligible in comparison with complexity of construction and running of the black box field $\mathsf{K} \vDash \mathbb{F}$ which will make its appearance in Step 5. An estimate for complexity of K can be found in [1] (Section 12): $O(\xi \log^2 E \log\log E + \mu \log^3 E \log\log E)$, where μ is an upper bound on the time required for a single group operation in X and ξ is an upper bound on the time requirement, per element, for the construction of random elements of X.

Step 5: Construction of a dihedral group of order 8. Our aim is to construct a dihedral group of order 8 in X.

To construct in X a dihedral group of order 8, we consider the factor group $\widetilde{X} = X/Z \vDash \mathrm{PGL}_2(\mathbb{F})$. Observe that we can use the black box X to carry out computations in $\widetilde{X}$ by replacing the equality relation in X by the new one:

$$x \equiv y$$

if and only if $x^{-1}y$ commutes with cryptoelements r, s of odd order and $[r, s] \neq 1$.

By Theorem 3 we can construct a black box field K inside the black box group $\widetilde{X}$ and then surjective homomorphisms

$$\widetilde{X} \xleftarrow{\Phi} \mathrm{PGL}_2(K) \xleftarrow{\beta} \mathrm{GL}_2(K).$$

We denote $\Psi = \Phi \circ \beta$.

Notice that the black box fields Z and K come from completely different origins; the latter was constructed in [1] by coordinatisation of a projective plane structure on the set of involutions in $\widetilde{X}$.

Also notice that $\mathrm{GL}_2(K)$ comes with the matrix algebra $M_{2\times 2}(K)$ and that the image $\alpha \circ \beta(e)$ of the identity cryptoelement $e \in M_{2\times 2}(K)$ is the identity cryptoelement of Z. In later calculations, this will allow us to identify the cryptoelements representing $0, 1, -1, 2, \frac{1}{2}$ in the two fields and use the same notation for them. In our calculations we will be using only a tiny 'shared' fragment of the two fields. From now on we shall call cryptoelements in K, $M_{2\times 2}(K)$, and $\mathrm{GL}_2(K)$ just 'elements'—this level of deciphering will suffice for our purposes because the field K does not appear in the formulation of our results, Theorem 1 K and Corollary 1; it plays only a temporary role.

Now we apply Lemma 2 to construct in $G = \mathrm{GL}_2(K)$ the dihedral subgroup D, its elements are listed in Equations (1) and (2). The image $\widetilde{D} = \Psi(D)$ of D in $\widetilde{X}$ is the factor group $D/Z(D)$, we have to lift it to a dihedral group of order 8 in X which we will denote, abusing notation, by the same symbol D, with the same notation for elements.

So far we know only elements e and $-e$ from $Z(D) < Z$.

The full preimage of $\Psi(D) < \widetilde{X}$ in X is ZD. We need to look with some attention at the cosets of Z in ZD. The factor group $\widetilde{D} = ZD/Z$ is elementary abelian; therefore, if T is a coset of Z in $ZD \setminus Z$ then $Z \cup T$ is an abelian group which contains elements from $D \setminus Z$ and of course these elements belong to T. These elements can be of order 2 or 4.

Assume that the coset T contains an element of order 2 (involution). It is easy to see that T contains only two involutions, say x and $-x$. Pick an arbitrary element $t \in T$, then $t = zx$ for some $z \in Z$ and $t^2 = z^2x^2 = z^2$. We can construct square roots of $\widetilde{z}^2$ in the cyclic group Z^* by using the analog of Tonelli-Shanks algorithm for cyclic groups, see [1] (Lemma 5.6). There are two of them,

$$\pm s = \sqrt{z^2},$$

and is easy to check that $(\pm st)^2 = (\pm szx)^2 = 1$, hence elements $\pm st$ coincide with $\pm x$ and belong to D.

So we know involutions $\pm e_1$ and $\pm w_1$, but do not know the correct choice of signs.

Step 6: Construction of a basis for R**.** Our task now is to construct in R cryptoelements $\{ e_{ij} \}_{i,j=1,2}$ which are linearly independent over Z and satisfy the relation

$$e_{ij}e_{kl} = \begin{cases} e_{il} & \text{if} \quad j = k \\ 0 & \text{if} \quad j \neq k \end{cases}. \tag{3}$$

https://doi.org/10.3390/axioms15070511

We shall call a system of cryptoelements $\{ e_{ij} \}_{i,j=1,2}$ a *standard basis* for R.

We will do that by manipulating elements from the subgroup D in the additive group of the ring R. We have to consider four cases each one for a different choice of the signs $\pm$ of elements $\pm e_1$ and $\pm w_1$.

Case 1, the lucky case. We pick at random an element in each pair of elements $\pm e_1$ and $\pm w_1$ and denote them e'_1 and w'_1, respectively. If we are lucky and have picked

$$w'_1 \vDash \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } e'_1 \vDash \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

(and this should definitely happen in one of the cases) then the following calculations

$$\begin{aligned}
w'_2 &:= w'_1 \cdot e'_1 \vDash \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \\
e_{11} &:= \frac{1}{2}(e - e'_1) \vDash \frac{1}{2}\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \\
e_{22} &:= \frac{1}{2}(e + e'_1) \vDash \frac{1}{2}\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \\
e_{12} &:= \frac{1}{2}(w'_1 + w'_2) \vDash \frac{1}{2}\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \\
e_{21} &:= \frac{1}{2}(w'_1 - w'_2) \vDash \frac{1}{2}\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}
\end{aligned} \tag{4}$$

The symbol $\vDash$ here and from now on means that a particular cryptoelement from the ring R represents a particular element from $M_{2\times 2}(K)$. Obviously, $\{ e_{ij} \}_{i,j=1,2}$ is a standard matrix basis in R because its cryptoelements represent canonical matrix units in $M_{2\times 2}(K)$. This is obvious for a human observer—but the algorithm *must* check that by substituting cryptoelements e_{ij}'s in Equation (3).

Cases 2, 3, and 4. If we are not lucky in our choice of elements e'_1 and w'_1 and the system of cryptoelements $\{ e_{ij} \}_{i,j=1,2}$ found in Equation (4) does not satisfy the criteria of Equation (3), we adjust them within group D, realizing the three remaining choices of signs.

Case 2: We keep e'_1 and replace w'_1 by setting $w'_1 := -ew'_1$, so that now $w'_1 \vDash \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$.

Case 3: We replace e'_1 by setting $e'_1 := -ee'_1$, so that now $e'_1 \vDash \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, and keep w'_1.

Case 4: We replace e'_1 and w'_1 by setting $e'_1 := -ee'_1$ and $w'_1 := -ew'_1$, so that now $e'_1 \vDash \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $w'_1 \vDash \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$.

We do calculations formulated in Equation (4) only once but without knowing in which of the Cases 1–4 we are. But in each of these cases we come to a standard basis in R which could be different from the one we get in Case 1.

Indeed, in Case 2, we get

$$e_{11} \vDash \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad e_{22} \vDash \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad e_{12} \vDash \begin{bmatrix} 0 & -1 \\ 0 & 0 \end{bmatrix}, \quad e_{21} \vDash \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}$$

which satisfy Equation (3) and therefore form a standard basis in R.

But in Case 3 we get

$$\mathsf{e}_{11} \vDash \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad \mathsf{e}_{22} \vDash \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathsf{e}_{12} \vDash \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad \mathsf{e}_{21} \vDash \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Equation (3) fail because $\mathsf{e}_{12} \cdot \mathsf{e}_{21} = \mathsf{e}_{22}$ instead of e_{11}. Swapping notation between e_{11} and e_{22} and between e_{12} and e_{21} fixes the problem and produces a standard basis for R —the same as in Case 1.

In Case 4 we get the same standard basis as in Case 2.

Step 7: Representation of cryptoelements in R by 2 × 2 matrices over Z. Let $\{e_{ij}\}_{i,j=1,2}$ be a standard basis for $R = \mathrm{M}_{2\times 2}(\mathbb{F})$ constructed in Step 6.

Take an arbitrary $\mathsf{x} \in \mathsf{R}$ and assume that

$$\mathsf{x} \vDash \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \sum_{i,j} a_{ij} e_{ij}, \ a_{ij} \in \mathbb{F}.$$

We should construct proxies for a_{ij}, $i, j = 1, 2$, that is, we should construct cryptoelements $\mathsf{z}_{ij} \in \mathsf{Z}$ such that $\mathsf{z}_{ij} \vDash a_{ij}$ and

$$\mathsf{x} = \sum_{i,j} \mathsf{z}_{ij} \mathsf{e}_{ij},$$

where e_{ij}, $i, j = 1, 2$, are the cryptoelements constructed in Step 6. Since we have made an exhaustive search there, we may assume that cryptoelements e_{ij} represent the standard matrix units and

$$\mathsf{w}_1' \vDash \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

We start by setting the cryptoelements $\mathsf{x}_{ij} \in \mathsf{R}$:

$$\begin{aligned} \mathsf{x}_{11} &:= \mathsf{e}_{11}\mathsf{x}\mathsf{e}_{11} \vDash a_{11}e_{11} \\ \mathsf{x}_{22} &:= \mathsf{e}_{22}\mathsf{x}\mathsf{e}_{22} \vDash a_{22}e_{22} \\ \mathsf{x}_{12} &:= \mathsf{e}_{11}\mathsf{x}\mathsf{e}_{22} \vDash a_{12}e_{12} \\ \mathsf{x}_{21} &:= \mathsf{e}_{22}\mathsf{x}\mathsf{e}_{11} \vDash a_{21}e_{21} \end{aligned}$$

Notice that $\mathsf{e}_{11}^{\mathsf{w}_1'} = \mathsf{e}_{22}$ and $\mathsf{e}_{22}^{\mathsf{w}_1'} = \mathsf{e}_{11}$. This allows us to produce scalar matrices:

$$\mathsf{z}_{11} := \mathsf{x}_{11} + \mathsf{x}_{11}^{\mathsf{w}_1'} \vDash \begin{bmatrix} a_{11} & 0 \\ 0 & a_{11} \end{bmatrix},$$

hence

$$\mathsf{x}_{11} = \mathsf{z}_{11}\mathsf{e}_{11}.$$

Similarly,

$$\mathsf{z}_{22} := \mathsf{x}_{22} + \mathsf{x}_{22}^{\mathsf{w}_1'} \vDash \begin{bmatrix} a_{22} & 0 \\ 0 & a_{22} \end{bmatrix},$$

hence

$$\mathsf{x}_{22} = \mathsf{z}_{22}\mathsf{e}_{22}.$$

https://doi.org/10.3390/axioms15070511

Two other matrix element of x can be obtained as follows:

$$\mathsf{z}_{12} := \mathsf{w}_1'\mathsf{x}_{12} + \mathsf{x}_{12}\mathsf{w}_1' \vDash \begin{bmatrix} a_{12} & 0 \\ 0 & a_{12} \end{bmatrix},$$

yielding

$$\mathsf{x}_{12} = \mathsf{z}_{12}\mathsf{e}_{12},$$

and similarly

$$\mathsf{z}_{21} := \mathsf{w'}_1\mathsf{x}_{21} + \mathsf{x}_{21}\mathsf{w}_1' \vDash \begin{bmatrix} a_{21} & 0 \\ 0 & a_{21} \end{bmatrix},$$

yielding

$$\mathsf{x}_{21} = \mathsf{z}_{21}\mathsf{e}_{21}.$$

Hence, we have

$$\sum_{i,j} \mathsf{z}_{ij}\mathsf{e}_{ij} \vDash \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

and

$$\sum_{i,j} \mathsf{z}_{ij}\mathsf{e}_{ij} = \mathsf{x}$$

which establishes a two-way isomorphism between R and $M_{2\times 2}(\mathsf{Z})$.

7. The Characteristic 2 Case

Theorem 1 deals only with fields of odd characteristic. The case of even characteristic is much simpler and allows us to re-use large chunks of proof Theorem 1.

Here is the result:

Theorem 4. *Let* R *be a black box ring encrypting the ring of* 2×2 *matrices* $\mathrm{M}_{2\times 2}(\mathbb{F})$*, where* $\mathbb{F}$ *is an unknown finite field* $\mathbb{F}$ *of characteristic* 2*, and let* E *be a computationally feasible global exponent for invertible cryptoelements* x *of* R *(that is,* $\mathsf{x}^E = 1$*), see Axiom* ***GE*** *in Section 2. Then there is a Las Vegas algorithm which constructs, in time polynomial in* $\log E$*, a black box field* Z *encrypting* $\mathbb{F}$*, and isomorphisms*

$$\mathsf{R} \longleftrightarrow \mathrm{M}_{2\times 2}(\mathsf{Z}).$$

We shall use the following structure recovery theorem [8] (Theorem 3.1).

Theorem 5 (Borovik and Yalçınkaya [8])**.** *Let* Y *be a black box group of global exponent* E *encrypting a group* $\mathrm{SL}_2(\mathbb{F})$ *for some unknown field* $\mathbb{F}$ *of characteristic 2. We assume that we are given an involution* $\mathsf{u} \in \mathsf{X}$*.*

Then there exists a Monte-Carlo algorithm which constructs, in polynomial in $\log E$ *time,*

- *a black box field* $\mathsf{U} \vDash \mathbb{F}$*, and*
- *a polynomial in* $\log E$ *time isomorphism*

$$\Phi : \mathrm{SL}_2(\mathsf{U}) \longrightarrow \mathsf{Y}.$$

Now we can turn our attention to proof of Theorem 4.

Proof. We use the same notation as in proof of Theorem 1: $\mathsf{Z} = Z(\mathsf{R})$ and X is the group of invertible elements in R.

https://doi.org/10.3390/axioms15070511

The same way as in Theorem 1, the map

$$\begin{array}{ccc} R \times R & \longrightarrow & Z \\ (x, y) & \mapsto & [x, y]^2 \end{array}$$

can be taken for a generator of random cryptoelements for the black box field Z. The structure of the group X is more transparent than in the odd characteristic case because

$$X = Z \times Y,$$

where $Y \vDash SL_2(\mathbb{F})$. To apply Theorem 5 to the group Y, we need to construct an involution in Y. This was done by Kantor and Kassabov in [9] (Proposition 4), but only in the case when the order of $\mathbb{F}$ is known. So we could not use their result in the set-up of the present paper, and used instead our construction of involutions from [1] (Section 4.9) where the size of the field remains unknown.

So now we have a polynomial in $\log E$ time isomorphism $\Phi : SL_2(U) \longrightarrow Y$. In any black box field we can locate elements 0 and 1, so we can construct in $SL_2(U)$ matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

and denote by $y_1, \ldots, y_6$, respectively, their Φ-images in Y.

Then basic arithmetic modulo 2 shows that

$$e_{11} = y_2 + y_3 \vDash \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad e_{12} = y_1 + y_5 \vDash \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$e_{21} = y_1 + y_6 \vDash \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad e_{22} = y_2 + y_4 \vDash \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

are matrix units satisfying Equation (3).

Now we can rename $w_1' := y_2$ and repeat *verbatim* arguments from Step 7 of the proof of Theorem 1. □

8. Conclusions

Theorem 1 demonstrates that probabilistic methods of black box group theory can be successfully applied to black box rings.

What is most important, Theorem 1 is the basis of recursive algorithms for cryptanalysis of black box rings encrypting matrix rings $M_{n\times n}(\mathbb{F})$ over finite fields $\mathbb{F}$ of odd order and $n > 2$. This will be done in a separate paper because it requires completely different methods, work with the so-called Curtis-Phan-Tits systems defined for all simple algebraic group: they are systems of root $SL_2(\mathbb{F})$-subgroups associated with the nodes of the extended Dynkin diagram of the corresponding group [10]. Similarly, rings $M_{n\times n}(\mathbb{F})$ are built from subrings $M_{2\times 2}(\mathbb{F})$ corresponding to $SL_2(\mathbb{F})$-subgroups in $SL_n(\mathbb{F})$.

Theorem 1 allows us to start this delicate analysis.

Why do we focus on fields of odd characteristics (and, moreover, large characteristics)? Because a simple algebraic group over a *large* finite field behaves in probabilistic computations as a compact Lie group: a randomly chosen element is semisimple with probability astronomically close to 1. This affinity between finite groups and compact Lie groups is best explained in a remarkable paper of Boris Zilber [11] (Theorem 4.2):

Theorem 6 (Zilber [11]). *Every simple compact Lie group is locally approximated by finite groups.*

This means that simple compact Lie groups are "limits at infinity" of algebraic groups over finite fields of unboundedly growing characteristic. This "limit" is defined by means of (logical) model theory.

As Zilber explains [11] (p. 2),

> [Simple compact Lie] groups are the backbone of the Standard Model of particle physics and also of the String Theory.

Zilber's theorem explains why black box algebra adequately captures important aspects of mathematical objects and structures of quantum physics.

Author Contributions: Conceptualization, A.B. and Ş.Y.; methodology, A.B. and Ş.Y.; software, Ş.Y.; validation, A.B. and Ş.Y.; formal analysis, A.B. and Ş.Y.; investigation, A.B. and Ş.Y.; resources, A.B. and Ş.Y.; data curation, A.B. and Ş.Y.; writing—original draft preparation, A.B. and Ş.Y.; writing—review and editing, A.B. and Ş.Y.; visualization, A.B. and Ş.Y.; supervision, A.B. and Ş.Y.; project administration, A.B. and Ş.Y.; funding acquisition, none. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: This paper—and other papers in our project—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, as part of their Research in Pairs programme; our thanks go to Ali Nesin and to all volunteers, staff, and students who have made the Village a mathematical paradise. We also thank the anonymous referees whose comments led to improvements in this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Borovik, A.; Yalçınkaya, Ş. Adjoint representations of black box groups $\mathrm{PSL}_2(\mathbb{F}_q)$. *J. Algebra* **2018**, *506*, 540–591. [CrossRef]
2. Borovik, A.; Yalçınkaya, Ş. Homomorphic encryption and some black box attacks. In *Proceedings of Mathematical Software—ICMS 2020—7th International Conference, Braunschweig, Germany, 13–16 July 2020*; Lecture Notes in Computer Science, volume 12097; Springer: Cham, Switzerland, 2020; pp. 115–124.
3. Borovik, A.; Yalçınkaya, Ş. Natural representations of black boxgroups $\mathrm{SL}_2(\mathbb{F})$. *Axioms* **2025**, 14, 895. [CrossRef]
4. Babai, L.; Szemerédi, E. On the complexity of matrix group problems. In *Proceedings of 25th IEEE Symposium on Foundations of Computer Science (1984)*; IEEE: Piscataway, NJ, USA, 1984; pp. 229–240.
5. Boneh, D.; Lipton, R.J. Algorithms for black-box fields and their application to cryptography. In *Advances in Cryptology—CRYPTO '96*; Koblitz, N. Ed.; Lecture Notes in Computer Science, volume 1109; Springer: Berlin/Heidelberg, Germany, 1996; pp. 283–297.
6. Maurer, U.; Raub, D. Black-box extension fields and the inexistence of field-homomorphic one-way permutations. In *Advances in Cryptology—ASIACRYPT 2007*; Lecture Notes in Computer Science, volume 4833; Springer: Berlin, Germany, 2007; pp. 427–443.
7. Lenstra, H.W., Jr. Finding isomorphisms between finite fields. *Math. Comput.* **1991**, *56*, 329–347. [CrossRef]
8. Borovik, A.; Yalçınkaya, Ş. Fifty shades of black. *arXiv* **2013**, arXiv:1308.2487.
9. Kantor, W.M.; Kassabov, M. Black box groups isomorphic to $PGL(2, 2^e)$. *J. Algebra* **2015**, *421*, 16–26.
10. Borovik, A.; Yalçınkaya, Ş. Construction of Curtis-Phan-Tits system for black box classical groups. *arXiv* **2010**, arXiv:1008.2823.
11. Zilber, B. Approximation of structures: Local and global. *arXiv* **2026**, arXiv:2604.00720v1.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.