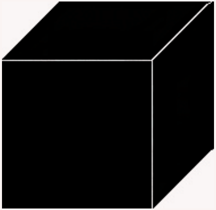
Black box methods to identify groups of Lie type

Şükrü Yalçınkaya
(joint with Alexandre Borovik)

Istanbul University

Black box groups

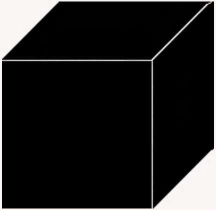
black box $\quad \mathbf{X} \overset{\pi}{\dashrightarrow} G \quad$ encrypted group



strings $\quad x \cdot y, \quad x^{-1}, \quad x = y \quad$ random

Black box rings

$$\mathbf{X} \xrightarrow{\pi} R$$



$x \cdot y, \qquad x + y, \qquad -x, \qquad x = y$

Similarly: black box everything

Axioms

BB1 $\mathbf{X}$ produces strings of fixed length $l(\mathbf{X})$ encrypting random (almost) uniformly distributed elements from G.

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

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

BB4 We are given a computationally feasible *global exponent* E of $\mathbf{X}$,

$$\pi(x)^E = 1 \text{ for all strings } x \in \mathbf{X}.$$

Black box group algorithms

Let X be a black box (simple) group

- Probabilistic Recognition
  - Determine the isomorphism type of X – X is $\mathrm{PSL}_2(13)$, Alt_9, etc.
- Constructive Recognition
  - Construct an explicit isomorphism between X and a known group G.

More on constructive recognition

Let **X** be a black box group encrypting a given group G.
An effective isomorphism

$$\varphi : G \to \mathbf{X}$$

1. Given $g \in G$, construct efficiently the string $\varphi(g)$ representing g in **X**.
2. Given a string x produced by **X**, construct efficiently the element $\varphi^{-1}(x) \in G$ represented by x.

Obstacles in constructive recognition algorithms

Let $\mathbf{X}$ be a group of Lie type over a field of size q.

- Involves construction of unipotent elements.
- Unipotents are astronomically rare!

If $\mathbf{X}$ is given as a matrix group, then one needs to solve discrete logarithm problem—in $\mathbb{F}_q$, not in the prime field.

More obstacles: The nature of non-reversibility

Let $\mathbf{K}$ be a black box field encrypting $\mathbb{F}_p$, p prime.

We always have a morphism

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

The existence of the reverse morphism

$$\mathbb{F}_p \longleftarrow \mathbf{K}$$

would follow from solution of the **discrete logarithm problem** in $\mathbf{K}$.

Our setup

We are given

- A black box group $\mathbf{X}$ with no additional oracles, and
- an exponent E of $\mathbf{X}$, that is, $x^E = 1$ for all $x \in \mathbf{X}$.

The decomposition $E = 2^k m$, $(m, 2) = 1$, suffices to produce efficient algorithms.

Morphisms of black box groups

A morphism $\zeta : \mathbf{X} \to \mathbf{Y}$ is an efficiently computable map which make the following diagram commutative:

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

We say that a morphism ζ *encrypts* the homomorphism ϕ.

BB subgroups are morphisms

When we

- have a generating set $y_1, \ldots, y_k$ for $\mathbf{Y} \leqslant \mathbf{X}$, and
- sample the "product replacement algorithm" (or something similar), for $\mathbf{Y}$

we deal with a morphism

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

Morphisms are BB subgroups

$$G \xrightarrow{\phi} H$$

is a homomorphism if and only if its graph

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

is a subgroup of $G \times H$.

$$\mathbf{X} \xrightarrow{\zeta} \mathbf{Y}$$

is a BB subgroup $\mathbf{Z} \hookrightarrow \mathbf{X} \times \mathbf{Y}$ encrypting F:

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

with the natural projection

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

Graphs of the morphisms

Let $x_1, x_2, \ldots, x_k \in \mathbf{X}$ with known images
$y1 = \zeta(x_1), y_2 = \zeta(x_2), \ldots y_k = \zeta(x_k) \in \mathbf{Y}$.

Then the subgroup

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

is the graph of the morphism ζ.

Random sampling on $\mathbf{Z}$ produces strings in $\mathbf{X}$ with their images $\zeta(x)$ in $\mathbf{Y}$ attached.

Automorphisms of black box groups of Lie type

Theorem (Borovik-Y.)

Let $\mathbf{X}$ *be a black box group encrypting a Lie type group* $G(F)$, *where* F *is an unknown finite field. Given an exponent* E *for* $\mathbf{X}$, *we can construct, in polynomial in* $\log E$, *a cover*

$$\mathbf{X} \longleftarrow \mathbf{Y}$$

where a black box group $\mathbf{Y}$ *encrypts* $G(F)$ *and morphisms*

$$\mathbf{Y} \longleftarrow \mathbf{Y}$$

encrypting Frobenius and graph automorphisms of $G(F)$.

An example

Borovik–Y: Given a black box group encrypting $\mathrm{SL}_3(p^2)$ for a 60 decimal digits long prime number p:

$p = 622288097498926496141095869268883999563096063592498055290461,$

we can construct a black box subgroup

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

This is implemented on GAP!
Note that

$$|\mathrm{SL}_3(p^2)| \approx 10^{960}.$$

More constructions

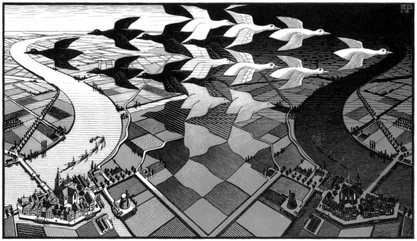
Borovik–Y: Let $\mathbf{X}$ be a black box group encrypting the group $\mathrm{SL}_8(F)$, where F is an unknown field. Given an exponent E for $\mathbf{X}$, we can construct, in time polynomial in $\log E$, a chain of black box groups and morphisms

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

that encrypts the chain of canonical embeddings

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

Fifty shades of black



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

Decryption of a BB group $\mathbf{X}$: a step-by-step construction of a chain of morphisms

$$G \overset{\pi}{\dashleftarrow} \mathbf{X} \overset{\zeta_1}{\twoheadleftarrow} \mathbf{X}_1 \overset{\zeta_2}{\twoheadleftarrow} \mathbf{X}_2 \twoheadleftarrow \cdots \twoheadleftarrow \mathbf{X}_n \overset{\zeta_{n+1}}{\twoheadleftarrow} G$$

at each step

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

Centralizers of involutions in black box groups (Cartan; Altseimer & Borovik; Bray)

$\mathbf{X}$ a black box group,
$i \in \mathbf{X}$ an involution,
$x \in \mathbf{X}$ a random element.

If $|ii^x| = m$ even, then $(ii^x)^{m/2}$ is an involution.

If $|ii^x| = m$ odd, then set $y := (ii^x)^{m+1/2}$. We have

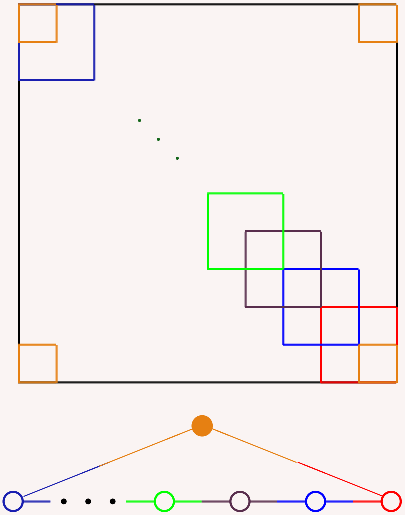
$$i^y = i^x.$$

Centralizers of involutions in black box groups (Cartan; Altseimer & Borovik; Bray)

Define

$$\begin{array}{rcl} \zeta : \mathbf{X} & \longrightarrow & C_{\mathbf{X}}(i) \\ x & \longmapsto & \begin{array}{ll} \zeta_0(x) = (ii^x)^{m/2}, & m = o(ii^x) \text{ even} \\ \zeta_1(x) = (ii^x)^{(m+1)/2}.x^{-1}, & m = o(ii^x) \text{ odd} \end{array} \end{array}$$

Shades of black for SL_n: Extended Curtis-Tits system



Reification of involutions

Let $\mathbf{S}$ be a generating set for $\mathbf{X}$,
i an involutive automorphism of $\mathbf{X}$.

Suppose that we know the action of i on $\mathbf{S}$:

$$x^i,\ x \in \mathbf{S}.$$

Since

$$ii^x = x^i x^{-1},$$

we construct $C_{\mathbf{X}}(i)$ and identify $i \in Z(C_{\mathbf{X}}(i))$.

Reifying an involution in $\mathrm{SO}_3(q)$

Let $\mathbf{X} = \mathrm{SO}_3(q)$, q odd,
$i, j \in \mathbf{X}$ involutions and ij is not a unipotent element.

Question

Find the involution which commutes with both i and j, call it k.

- Set $z = ij$.
- If z has even order, then k is the unique involution in $\langle z \rangle$.
- Assume that z has odd order.
  - k centralises z, and
  - k inverts the torus $\mathbf{T}_j$ containing j.
- $k : z \mapsto z, \quad t \mapsto t^{-1}$ for all $t \in \mathbf{T}_j$.
- $\langle z, \mathbf{T}_j \rangle = \mathbf{X}$.

From PSL_2 to PGL_2

A reification of a diagonal automorphism of $\mathbf{X} \simeq \mathrm{PSL}_2(q)$, $q \equiv 1 \bmod 4$:

- Produce an involution $i \in \mathbf{X}$.
- Construct $\mathbf{T}_+ < C_{\mathbf{X}}(i)$, where $|\mathbf{T}_+| = (q-1)/2$.
- Find $g \in \mathbf{X}$ such that $ii^g \in \mathbf{T}_-$, where $|\mathbf{T}_-| = (q+1)/2$.
- We have $\langle \mathbf{T}_+, \mathbf{T}_- \rangle = \mathbf{X}$.
- The amalgam δ of the local automorphisms

$$\begin{aligned} \alpha_+ : \mathbf{T}_+ \to \mathbf{T}_+, &\qquad s \mapsto s \\ \alpha_- : \mathbf{T}_- \to \mathbf{T}_-, &\qquad s \mapsto s^{-1} \end{aligned}$$

  encrypts a diagonal automorphism of $\mathrm{PSL}_2(q)$.

Involutions in $\mathbf{X} := \mathrm{PSL}_2(2^n)$

- Let x_1, x_2 be two non-commuting elements of odd order > 3.
- $\langle x_1, x_2 \rangle = \mathrm{PSL}_2(2^m)$ for some m.
- There is an involution $i \in \mathbf{X}$ inverting both x_1 and x_2.
- Construct an element in $C_{\mathbf{X}}(i)$.

Structural recognition, $(\mathrm{P})\mathrm{SL}_2(q)$

Theorem (Borovik and Y.)

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

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

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

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

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

Unipotents

Theorem (Borovik and Y.)

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

$\mathrm{PGL}_2(q) \cong \mathrm{SO}_3(q)$

Lie algebra $\mathfrak{l}$ of $\mathfrak{sl}_2$: 2×2 matrices of trace 0 with Lie bracket $[A, B] = AB - BA$.

$\mathrm{PGL}_2(\mathbb{F})$: Via action by conjugation, group of automorphisms of the Lie algebra $\mathfrak{l} = \mathfrak{sl}_2$ and it preserves the Killing form K on $\mathfrak{l}$,

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

$\mathrm{SO}_3(\mathfrak{l}, K)$: Group of orthogonal transformations of $\mathfrak{l}$ preserving K.

Denote by $\mathfrak{l}$ the 3-dimensional $\mathbb{F}_q$ vector space of the canonical representation of $\mathrm{SO}_3(q)$.

$\mathrm{PGL}_2(q) \cong \mathrm{SO}_3(q)$

$\mathfrak{l} := \mathfrak{sl}_2$, $G := \mathrm{SO}_3(q)$.

An element $\sigma \in \mathfrak{l}$ is

- semisimple iff $K(\sigma, \sigma) \neq 0$
- unipotent iff $K(\sigma, \sigma) = 0$.

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

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

Every involution in G is a half turn.

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

Weisfeiler plane

Fact

The set $\mathfrak{W}$ (Weisfeiler plane) of 1-dimensional algebraic subgroups A in G is in one-to-one correspondence

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

with the set of points of the projective plane $\mathfrak{P}$.

1-dimensional subgroups of $\mathrm{SO}_3(q)$:

- split tori: cyclic groups of order $q-1$;
- non-split tori: cyclic groups of order $q+1$;
- maximal unipotent subgroups of order q.

Dual plane $\mathfrak{P}^*$ of $\mathfrak{P}$

$\mathfrak{W}$ becomes the lines of $\mathfrak{P}$.
Points of $\mathfrak{P}$:

- involutive (or, semisimple, or regular)
- unipotent (or, parabolic, or tangent)

Incidence relation:

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

Missing points

Projective lines over $\mathbb{F}_q$ have $q+1$ points.

$|A| = q-1$:

- maximal unipotent subgroups normalizing A.

$|A| = q$:

- A itself.

$|A| = q+1$:

- None.

Quadric

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

We have

$$\mathfrak{Q} = \mathfrak{P} \setminus \mathfrak{I}.$$

Black box projective plane

Let **X** be a black box group encrypting $\mathrm{SO}_3(q)$, q, odd.

Using **X**, we construct a black box encrypting the projective plane $\mathfrak{P}$.

Points:

- Regular points:

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

  $s \in \mathfrak{I}$, $\mathbf{T}_s$ is its torus and $\varpi(s) = \mathbf{T}_s w$, the coset of involutions inverting $\mathbf{T}_s$.
- Parabolic point: same as the parabolic line.

Black box projective plane

Lines:

- Parabolic line, $\mathbf{u}$: pointer to a black box subgroup $\mathbf{U} \rtimes \langle t \rangle$. Incidence:
  - Involutions in $\mathbf{U}t$, and
  - $\mathbf{U}$ itself.
- Regular line, $\mathbf{l}$: pointer to a black box subgroup $\mathbf{T} \rtimes \langle w \rangle$. Incidence:
  - If $|\mathbf{T}| = q + 1$, then the involutions in $\mathbf{T}w$.
  - If $|\mathbf{T}| = q - 1$, then
    - the involutions in $\mathbf{T}w$, and
    - two maximal unipotent subgroups normalised by $\mathbf{T}$.

Line through two regular points

Let $s, t \in \mathfrak{I}$ be two involutions.

- Set $z = st$. If z is unipotent, then $\langle z^{\mathbf{T}_s} \rangle s$ is a parabolic line.
- Otherwise, we construct an involution $j := j(s, t)$ commuting with both s and t.
- Construct $C_{\mathbf{X}}(j)$ and the involutions inverting $T_j < C_{\mathbf{X}}(j)$ form the desired line.

Intersection of two lines

Let $\mathbf{k} \wedge \mathbf{l}$ be any two non-parabolic lines. Then

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

Coordinatisation of $\mathfrak{I}$

- Construct three involutions e_1, e_2, e_3 mutually commuting with each other (Spinor basis) and $\mathbf{H} := \mathrm{Sym}_4$ containing e_1, e_2, e_3. Set $\mathbf{E} := \langle e_1, e_2, e_3 \rangle$.
- $\mathbf{E} \leq [\mathbf{H}, \mathbf{H}]$. Therefore the involutions e_i have spinor norm 1 and the vectors ϵ_i can be chosen to satisfy

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

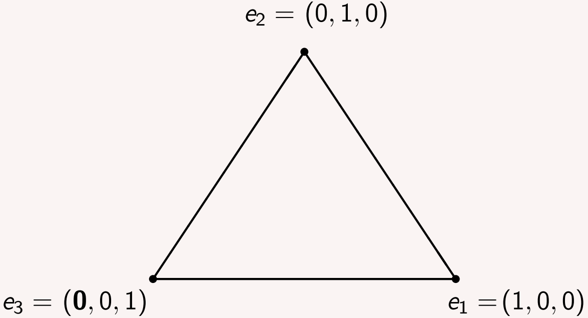
  forming an orthonormal basis in $\mathfrak{l}$,

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

Hence we have the quadric given by the equation

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

Coordinatisation of $\mathfrak{I}$



Unity in $\mathbf{K}$

Let $\Theta \in \mathbf{H}$ be an element of order 3 with

$$\Theta : e_1 \longrightarrow e_2 \longrightarrow e_3 \longrightarrow e_1$$

Let $d_1 \in N_{\mathbf{H}}(\langle \Theta \rangle)$ be an involution such that

$$e_1^{d_1} = e_1.$$

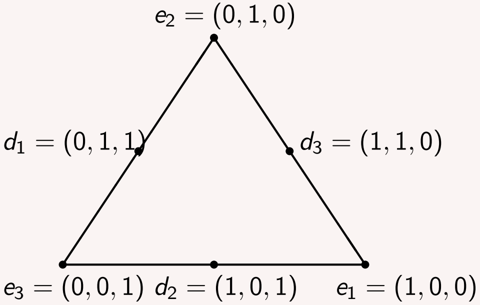
Then

$$e_2^{d_1} = e_3.$$

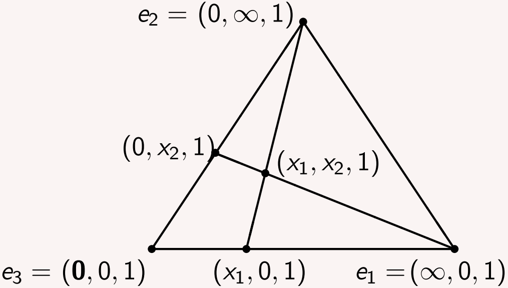
Unity in $\mathbf{K}$

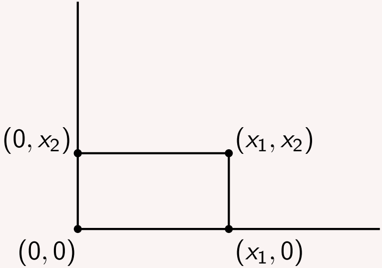
Assign to d_1 the coordinates $(0, 1, 1)$.

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

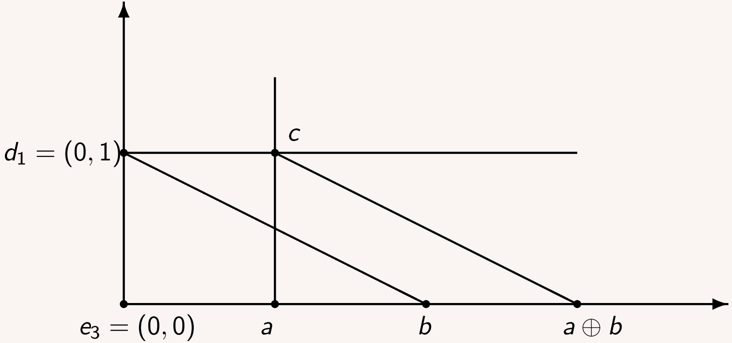


Coordinatisation of $\mathfrak{I}$

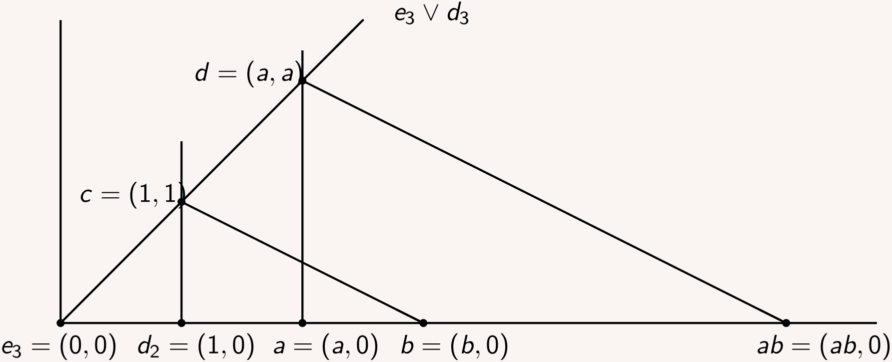




Addition in **K** on the axis $e_1 \vee e_3$



Multiplication on $\mathbf{K}$



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

The action of $\mathbf{X}$ on $\mathfrak{I}$ gives morphisms

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

Black box fields

Theorem (Lenstra Jr 1991; Maurer and Raub 2007)

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 a polynomial time construction, to a morphism

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

Unipotents are not invisible anymore!

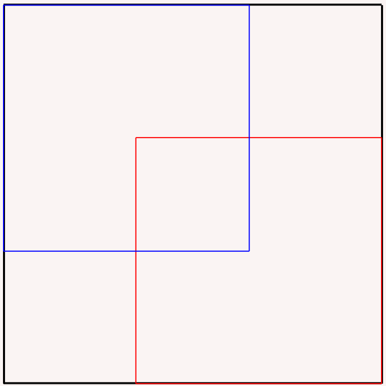
On $e_1 \vee e_3$, start adding the unity $\mathbf{1}$ to itself.

- If the addition fails at $(c-1)\mathbf{1} \oplus \mathbf{1}$, it means that
  - $p \equiv 1 \bmod 4$, and
  - $c^2 + 1 = p$, that is, the coordinate of one of the unipotents on the axis $e_1 \vee e_3$ is at c. The other one is at $-c$.
  - This failure produces a unipotent element.
- If the addition never fails and produces the involution e_3 at a coordinate, then
  - $p \equiv -1 \bmod 4$, and
  - the characteristic of the field is this coordinate.
  - Solve $x_1^2 + c^2 + 1 = 0$ for a random involution c on $e_1 \vee e_3$.

GAP

Construction of unipotent elements has been tested on GAP up to 10 digit primes.

Brauer: Characterisation of $\mathrm{PGL}_3(q)$, q odd



Spinor basis

$$e_1 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ e_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix},\ e_3 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Desarguesian Plane: Points and lines of $\mathfrak{P}$

Let $M_1 = \{ \begin{bmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \mid * \in \mathbb{F}\}$ and $\tilde{M}_1 = \{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ * & * & 1 \end{bmatrix} \mid * \in \mathbb{F}\}$

- Points: $\{(e_1 M_1)^g \mid g \in G\} = \{ \begin{bmatrix} -1 & 0 & * \\ 0 & -1 & * \\ 0 & 0 & 1 \end{bmatrix}^g \mid g \in G\}$
- Lines: $\{(e_1 \tilde{M}_1)^h \mid h \in G\} = \{ \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ * & * & 1 \end{bmatrix}^h \mid h \in G\}$

Incidence relation

The point p lies on a line ℓ if $p \cap \ell = \emptyset$.

The plane consisting of these points and lines is a projective plane $\mathfrak{P}$ associated with PGL_3.

Black box projective plane

Let $\mathbf{X} = \mathrm{PGL}_3(q)$, q odd.

Involutions in $\mathbf{X}$ are pointers to both the points and the lines.

Two involutions i, j represents the same point if and only if ij is unipotent. Similarly, for the lines.

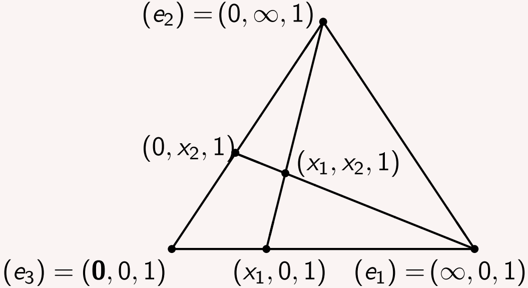
Lines through two points: Reification strikes back!

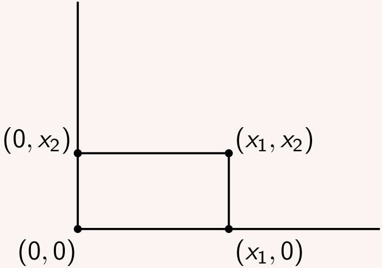
Fact

Let $x, y \in \mathbf{X}$ be two distinct commuting involutions, then the point (x) lies on the line $[y]$.

Let $x, y \in \mathbf{X}$ be two involutions and $z \in \mathbf{X}$ be an involution commuting with both x, y. Then $(x), (y) \in [z]$.

Coordinatisation





Black box field $\mathbf{K}$

Addition and multiplication involves

1. constructing lines from two points, and
2. finding the intersection point of two lines.

Same as before!

Morphisms $\mathrm{PGL}_3(\mathbf{K}) \to \mathbf{X} \to \mathrm{PGL}_3(\mathbf{K})$

The action of $\mathbf{X}$ on $\mathfrak{P}$ gives morphisms

$$\mathbf{X} \leftrightarrow \mathrm{PGL}_3(\mathbf{K}).$$

Recursion step: PGL_3-oracle

Theorem (Borovik and Y.)

Given a global exponent E for a black box group $\mathbf{X}$ encrypting PGL_3 over some finite field of unknown odd characteristic p, we construct, in probabilistic time polynomial in $\log E$,

- *a black box field $\mathbf{K}$, and*
- *the following isomorphisms*

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

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

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

Structural recognition of Lie type groups

Borovik–Y, work in progress:

For BB groups **X** encrypting simple group of Lie type $G = \mathrm{G}(F)$, where F is an unknown field of odd order, we have a probabilistic algorithm which constructs

- a BB field **K** encrypting F, and
- an effective isomorphisms between $G(\mathbf{K})$ and **X**.

The algorithm runs in time polynomial in $\log |G|$.