Finite groups, black box groups, algebraic groups.

Alexandre Borovik Pinar Ugurlu Şükrü Yalçınkaya

Isaac Newton Institute
Algebraic Lie Theory Programme
29 January 2009

Uncountable categoricity.

Let G be a group

$Th(G)$ the set of first order formulae true in G

Elementary equivalence:

$$G \equiv H \Longleftrightarrow Th(G) = Th(H)$$

G is $\aleph_1$-**categorical**

$$\Longleftrightarrow \exists! \text{ group } \widetilde{G} \equiv G \text{ of cardinality } \aleph_1$$

Example

$\mathbb{Q}^+$ is torsion-free divisible abelian:

$$\left.\begin{array}{l} \forall x \forall y\ xy = yx \\ \forall x\ (x^2 = 1 \to x = 1) \\ \forall x\ (x^3 = 1 \to x = 1) \\ \quad \vdots \\ \forall x \exists y\ y^2 = x \\ \forall x \exists y\ y^3 = x \\ \quad \vdots \end{array}\right\} \text{ infinite list of axioms}$$

$H \equiv \mathbb{Q}^+ \Longrightarrow H \simeq \bigoplus \mathbb{Q}^+$

Only one such group of cardinality $\aleph_1$ (for example, $\mathbb{R}^\times_{>0}$).

Hence $\mathbb{Q}^+$ is $\aleph_1$-categorical.

$\aleph_1$-categorical:

- Algebraically closed fields
- Simple algebraic groups over a.c. fields

Macintyre 1970:

$\aleph_1$-categorical fields are algebraically closed

Zilber's Conjecture (c. 1975)

Simple $\aleph_1$-categorical groups are simple algebraic groups over a.c. fields.

Altınel, B, Cherlin:

If a simple $\aleph_1$-categorical group G contains an infinite elementary abelian 2-group,

then G is a Chevalley group over a.c. field of characterisitic 2.

Corollary: classification of simple algebraic groups in characteristic 2.

So, simple algebraic groups over a.c. fields appear

- to have exceptionally nice description by first order formulae;
- are characterised by the very existence of a good description.

What is this description?

Is there an "optimal" short axiomatization?

Exercise for the audience:

find formulae which define $PSL_2(q)$, q odd, $q > 3$, in the class of finite groups.

Exercise for the audience:

find formulae which define $PSL_2(q)$, $q > 3$, in the class of finite groups. Will the following suffice?

- G has no abelian normal subgroups:

$$\forall x(x \neq 1 \rightarrow \exists y([x, x^y] \neq 1))$$

- Every element is a commutator:

$$\forall x \exists y \exists z(x = [y, z])$$

- centralisers of elements of order bigger than 3 are abelian:

$$\forall x((x^2 \neq 1 \wedge x^3 \neq 1) \rightarrow \forall y \forall z(([x, y] = 1 \wedge [x, z] = 1) \rightarrow [y, z] = 1))$$

- centralisers are abelian-by-2-elementary:

$$\forall x(x^2 \neq 1 \rightarrow \forall y \forall z(([x, y] = 1 \wedge [x, z] = 1) \rightarrow [y^2, z^2] = 1))$$

Exercise for the audience:

find formulae which define $PSL_2(q)$, $q > 3$, in the class of finite groups. Will the following suffice?

- G has no abelian normal subgroups:

$$\forall x(x \neq 1 \rightarrow \exists y([x, x^y] \neq 1))$$

- Every element is a commutator:

$$\forall x \exists y \exists z(x = [y, z])$$

- centralisers of elements of order bigger than 3 are abelian:

$$\forall x((x^2 \neq 1 \wedge x^3 \neq 1) \rightarrow \forall y \forall z(([x, y] = 1 \wedge [x, z] = 1) \rightarrow [y, z] = 1))$$

- centralisers are abelian-by-2-elementary:

$$\forall x(x^2 \neq 1 \rightarrow \forall y \forall z(([x, y] = 1 \wedge [x, z] = 1) \rightarrow [y^2, z^2] = 1))$$

No: Alt_7 satisfies the above three properties.

Plato defined man thus:

Man is a two-legged animal without feathers;

and was much praised for the definition; so Diogenes plucked a cock and brought it into his school, and said,

This is Plato's man. ⇓

Plato defined man thus:

Man is a two-legged animal without feathers;

and was much praised for the definition; so Diogenes plucked a cock and brought it into his school, and said,

This is Plato's man.

On which account this addition was made to the definition,

With broad flat nails.

[From *Lives of the Philosophers* by Diogenes Laërtius]

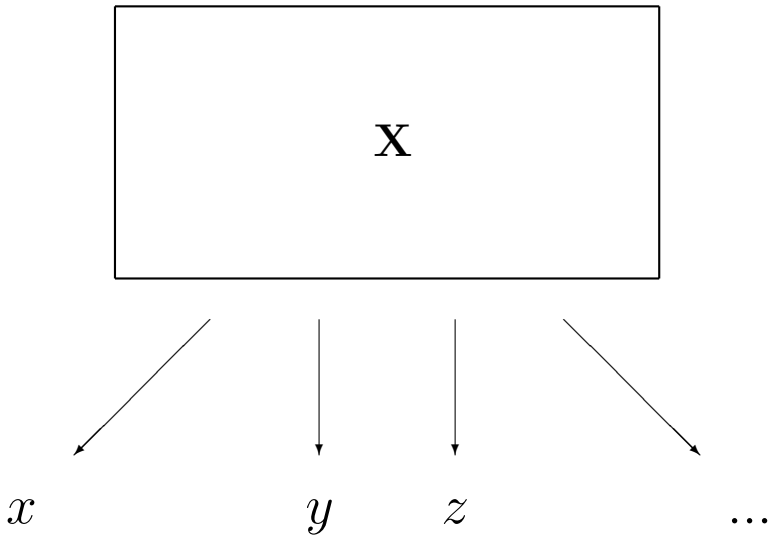
Core of the matter: Curtis-Tits Theorem.

- $L_i \simeq (P)SL_2$ assigned to nodes of a Dynkin diagram
- $\langle L_i, L_j \rangle \simeq (P)SL_2 * (P)SL_2, \ \ (P)SL_3, \ \ (P)Sp_4$
  depending on the number of edges between nodes i and j:
  nil, one, two;
- a few a bit more accurate details ...

Then $G = \langle L_1, \ldots, L_n \rangle$ is a Chevalley group with the corresponding Dynkin diagram.

(Extended) Dynkin diagram is a first order property!

Black Box Group



random, independent, uniformly distributed elements

Aim: determine $\mathbf{X}$

Recognition of black box groups is highly technical and uses CFSG.

Classical example: Miller-Rabin primality test

An odd integer n is prime **iff**

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/(n-1)\mathbb{Z})^+;$$

treat the group on LHS as a black box and on RHS as a "target" group.

"Verification problem":

given bb group $\mathbf{X}$ and a known target group $\mathbb{G}$, check whether they are isomorphic.

Typical Example: Matrix Groups

$\mathbf{X} = \langle x_1, \ldots, x_k \rangle \leqslant GL_d(\mathbb{F}_q)$

is a matrix group of big dimension, so that $|\mathbf{X}|$ is astronomical.

- Statistical study of 'random' products (Leedham-Green et al.) of

  $$x_1, \ldots, x_k$$

  is the only known approach to identification of $\mathbf{X}$.

- Basically, we are looking for a

  "short" and "easy to check by random testing" first order formula which identifies $\mathbf{X}$.

- **Existence /non-existence of elements of particular orders** is an example.

"Orders of elements" approach fails for recognising

$$B_n(q) = \Omega_{2n+1}(q),$$

$$C_n(q) = PSp_{2n}(q),$$

q odd:

they have virtually the same statistics of orders of elements.

Here,

$\Omega_{2n+1}(q)$ is the subgroup of index 2 in the orthogonal group $SO_{2n+1}(q)$,

$PSp_{2n}(q)$ is the projective symplectic group.

Why does statistics fail?

- For large p, unipotent and non-semisimple elements occur with probability $\sim 1/p$ and are "invisible": a random element is semisimple.

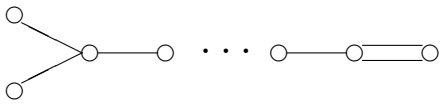
Why does statistics fail?

Let $G = G(\overline{\mathbb{F}}_q)$ be a simple algebraic group

- regular semisimple elements form an open subset of G
- statistics of orders of regular semisimple elements is determined by the **Dynkin diagram** of G, which is the same in the case of groups B_n and C_n, $n \geqslant 3$:

$BC_n,\ n \geq 2$ 

- But the conjugacy classes and the structure of centralisers of *involutions* (elements of order 2) are determined by the **extended Dynkin diagrams** which are different:

$\widetilde{B}_n, \quad n \geq 3$ 

$\widetilde{C}_n, \ n \geq 3$ 

- **Şükrü Yalçınkaya:**

  Reads the (extended) Dynkin diagram from the centralisers of involutions

Construction of involutions:

Assume that we know a computationally feasible E such that $x^E = 1$ for all $x \in \mathbf{X}$.

Factorise

$$E = 2^l \cdot m \ \ , m \text{ odd.}$$

$$\begin{aligned} E &= 2^l \cdot m \ \ , m \text{ odd} \\ x &\mapsto x^m, (x^m)^2, \ldots, (x^m)^{2^r} \neq 1, 1 \\ \mathrm{i}(x) &:= (x^m)^{2^r} \quad \text{is an involution} \end{aligned}$$

Centralisers of involutions:

If t is an involution, we have a **Cartan map**

$$\begin{aligned} \zeta : \mathbf{X} &\longrightarrow C_{\mathbf{X}}(t) \\ x &\mapsto (t \cdot t^x)^{(m+1)/2} \cdot x^{-1}, \quad |t \cdot t^x| \text{ odd} \\ &= \sqrt{tt^x} \cdot x^{-1} \end{aligned}$$

It remains usable in $\aleph_1$-categorical groups.

Was invented by E. Cartan: map

$$\zeta : \mathrm{SL}_n(\mathbb{R}) \longrightarrow \mathrm{SO}_n(\mathbb{R})$$

for t the inverse-transpose automorphism.

Why does Cartan map ζ work?

If $c \in C_{\mathbf{X}}(t)$,

$$\begin{aligned} \zeta(cx) &= \sqrt{tt^{cx}} \cdot x^{-1} \cdot c^{-1} \\ &= \sqrt{tt^{x}} \cdot x^{-1} \cdot c^{-1} \\ &= \zeta(x) \cdot c^{-1} \end{aligned}$$

If $x \in \mathbf{X}$ are uniformly distributed and independent,

then $\zeta(x)$ are uniformly distributed and independent in $C_{\mathbf{X}}(t)$

Black box in $\mathbf{X}$ generates a black box in $C_{\mathbf{X}}(t)$.

Parker and Wilson:

Black Box algorithm for computation of $O_p(\mathbf{X})$ for matrix black box groups $\mathbf{X}$ in characteristic $p > 2$.

Şükrü Yalçınkaya:

Black Box algorithm for computation of both

$O_p(\mathbf{X})$ and $\mathbf{X}/O_p(\mathbf{X})$

for matrix black box groups $\mathbf{X}$ in characteristic $p > 2$.

Şükrü Yalçınkaya:

Reads the (extended) Dynkin diagram of $\mathbf{X}/O_p(\mathbf{X})$ from the centralisers of involutions

ignoring $O_p(\mathbf{X})$ at the first stage:

$$\mathbf{X} = \langle \mathbf{L}_1, \ldots, \mathbf{L}_n \rangle$$

where

$$\mathbf{L}_i/O_p(\mathbf{L}_i) \simeq (P)SL_2$$

(root SL_2-subgroups)

Şükrü Yalçınkaya:

- First finds a classical SL_2 (long root SL_2)

$$\mathbf{J} \lhd C_{\mathbf{X}}(z), \quad \mathbf{J}/O_p(\mathbf{J}) \simeq SL_2, \quad \mathbf{J}' = \mathbf{J}, \quad z \in \mathbf{J}$$

- Ability to build such $\mathbf{J}$ suffices for testing $O_p(\mathbf{X}) \neq 1$.
- Then builds around $\mathbf{J}$ a Curtis-Tits system for **extended** Dynkin diagram for $\mathbf{X}/O_p(\mathbf{X})$.
- This is a black box analogue of Aschbacher's Classical Involution Theorem.

Şükrü Yalçınkaya, subtler points:

- His method works with root $(P)SL_2$'s around maximal tori of both types $(q-1)^n$ and $(q+1)^n$, with some beautiful configurations arising.
- A Curtis-Tits system for extended Dynkin diagram allows to build reductive subsystem subgroups, involutions and other semisimple elements from given conjugacy classes, etc. in groups over very large fieds.
- His method is developed and justified for classical groups but works for exceptional groups as well.

Back to uncountably categorical groups

A version of Curtis-Tits Theorem is the principal identification took in the classification of simple uncountably categorical groups (**Berkman, B, Burdges, Cherlin**).

Why?

Because it can be written by a relatively simple first-order formula.

Why does Curtis-Tits Theorem appear in Black Box Group Theory?

Because the formula is *robust*, it remains true in a version of probabilistic logic with quantifiers

$\exists^* =$ exists with positive probability

$\forall^* =$ for almost all with probability 1.

The actual calculations take place in a (infinite) pseudofinite group with a superreal measure.

G is **pseudofinite** if

- every formula which is true on G is true on some finite group.

One may think of pseudofinite groups as ultraproducts of finite groups

$$G \simeq \prod_{i \in I} G_i / \mathcal{F}.$$

Measure on G is the ultraproduct of canonical finite measures on G_i.

A pseudofinite field could be of characteristic 0!

A field F is pseudofinite **iff**

- it is perfect,
- has exactly one extension of degree n for each $n > 1$, and
- every absolutely irreducible variety defined over F has an F-rational point.

Intermediate steps involve **sets of probability different from** 0 **and** 1**:**

In PSL_2 over a field of odd order, formula

$$\text{“}Z(C_G(x)) \text{ contains an involution }\text{”}$$

holds with probability $\approx 1/2$ (or $1/2 +$ infinitesimal).

Formulae like that make a decent approximation to the property

“x has even order”.

Brave bright future

The Cherlin-Hrushovski Conjecture

G simple uncountably categorical group

ψ a generic automorphism

Then $G_0 = C_G(\psi)$ is pseudofinite.

In "real life", due to a theorem by Hrushovski:

If G is algebraic over an a.c. field **then**

- ϕ is generalised Frobenius, and
- $G_0 = C_G(\phi)$ is group of points of G over a pseudofinite field.

Hrushovski's Intermediate Conjecture:

G simple uncountably categorical group

ψ a generic automorphism

Then $G_0 = C_G(\psi)$ has a "good" probabilistic measure.

Towards Cherlin-Hrushovski

Pinar Ugurlu:

Let G be a $\aleph_1$-categorical simple group and α be a tight automorphism of G.

Assume that $C_G(\alpha)$ is pseudofinite.

Then G is a simple algebraic group over an algebraically closed field.

Tight automorphisms.

Let G be a $\aleph_1$-categorical group. An automorphism α is called **tight** if:

- If $H < G$ is a connected definable α-invariant subgroup of G, then $d(C_H(\alpha)) = H$.

Two results modulo Classification of Finite Simple Groups

John Wilson: A simple pseudofinite group is elementarily equivalent to a Chevalley or twisted Chevalley group over a pseudofinite field.

Pinar Ugurlu:

Let G be a definably simple pseudofinite group with descending chain condition on centralizers.

Then G is elementarily equivalent to a Chevalley or twisted Chevalley group over a pseudofinite field.

Pinar Ugurlu:

Let G be a simple $\aleph_1$-categorical group and α a tight automorphism of G. Assume that $C_G(\alpha) = P$ is pseudofinite.

Then there is a definable (in P) normal subgroup S of P such that

$$S \lhd P \lhd Aut(S)$$

and S is a Chevalley group over a peseudofinite field.

A bold observation:

this results can be proven *without* use of Classification of Finite Simple Groups.

The Cherlin-Hrushovski Programme fits incredibly well with the finite group theory.

B-Ugurlu (without CFSG); work in progress. Let G be a $\aleph_1$-categorical simple group, α an automorphism.

Assume

- For all $n \in \mathbb{N}$, α^n is tight.
- For all $n \in \mathbb{N}$, $C_G\alpha^n$ is pseudofinite.

Then G is a simple algebraic group.