The Hrushovski Programme

Alexandre Borovik
(Unfinished) joint projects with
Omaima Alshanqiti, Pınar Uğurlu, and Şükrü Yalçınkaya

Antalya Algebra Days XIV

16 May 2012

Outline

Simple algebraic groups

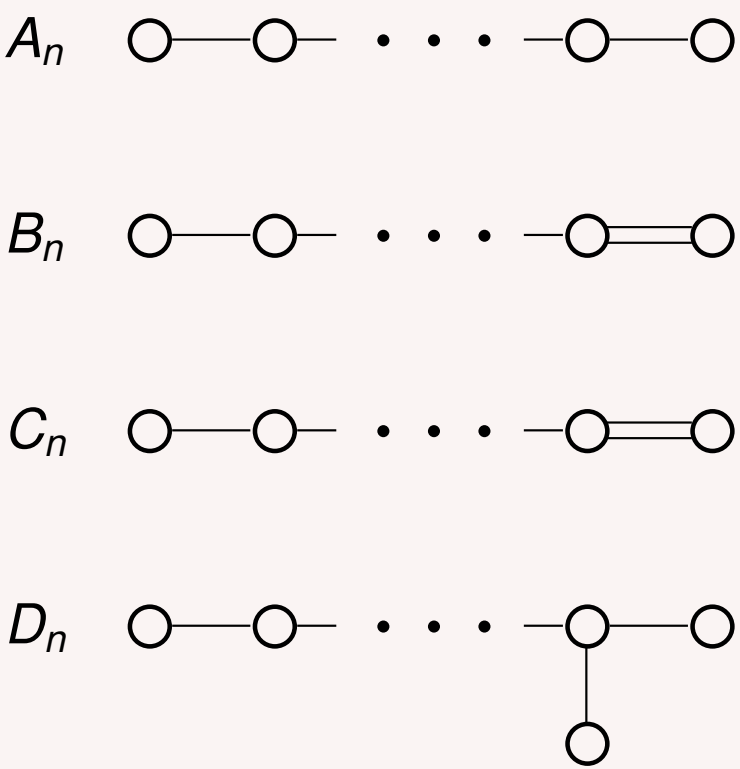
Chevalley:

A simple algebraic group is one of the following types:

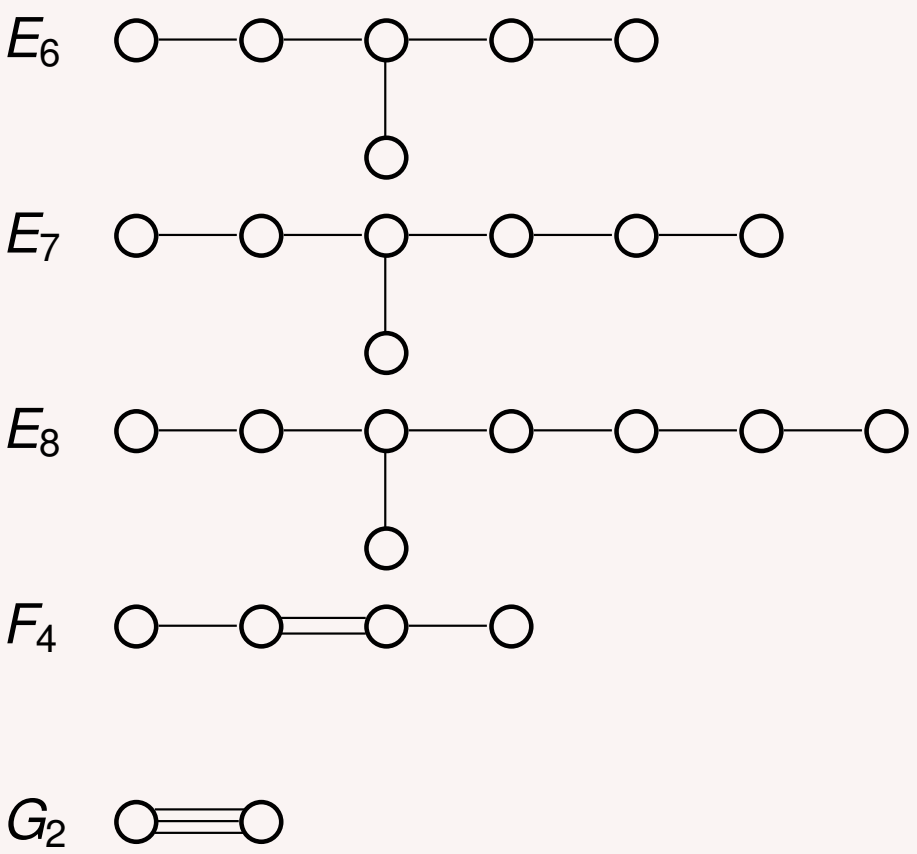
A_n, B_n, C_n, D_n (classical groups)
E_6, E_7, E_8, F_4, G_2 (exceptional groups)

Dynkin diagrams of simple algebraic groups

Classical Groups



Exceptional Groups



The Steinberg Endomorphisms

G simple algebraic group defined over $\mathbb{F}_p$

σ rational endomorphism of G with finite group of fixed points

G_σ group of fixed points of σ

Example: Frobenius map induced by $x \mapsto x^q$, $q = p^k$.

Classification of Finite Simple Groups

Every non-abelian finite simple group is one of:

- 26 sporadic groups;
- alternating groups;
- $O^{p'}(G_\sigma)$ (generated in G_σ by p-elements): **groups of Lie type**.

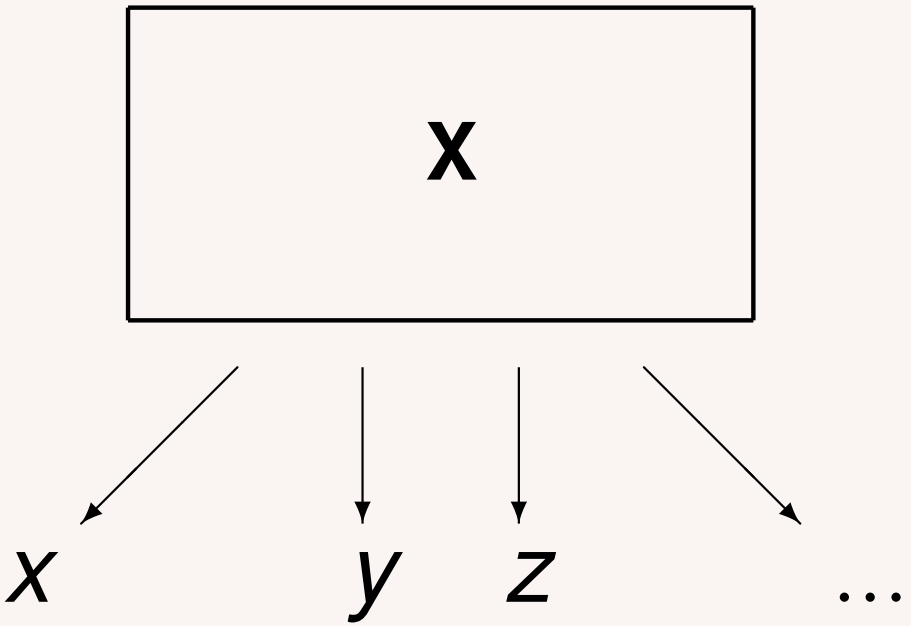
Uniform description of finite groups of Lie type

- for T σ-invariant torus (Borel) in G form T_σ,
- for B σ-invariant Borel subgroup in G form B_σ, etc.

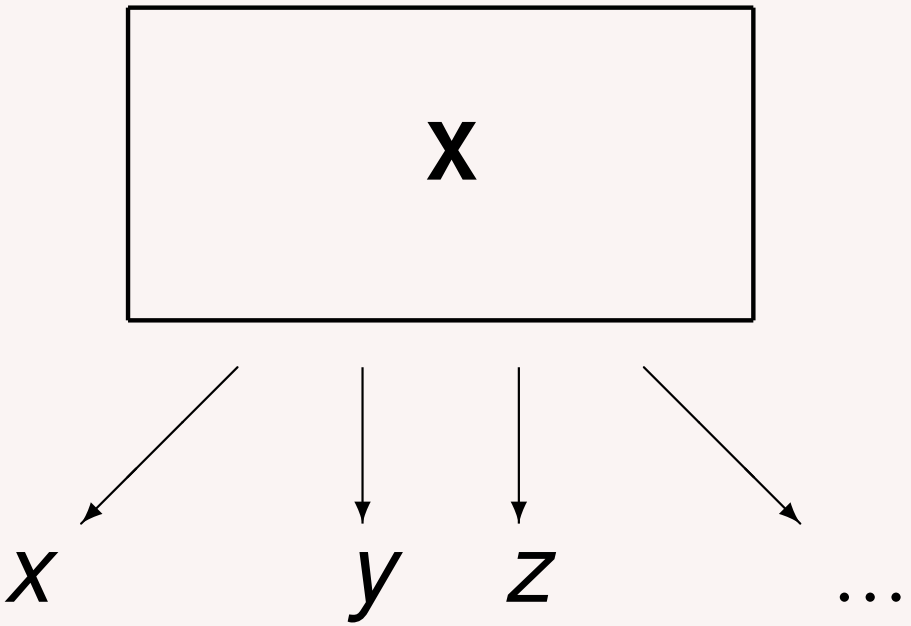
Lang-Steinberg: σ-invariant Borel subgroups do exist, etc.

This is **THE** correct way to look at finite simple groups.

Black box groups



Black box groups



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

Example

- Matrix groups over finite fields
  - S a small set of invertible matrices over a finite field
  - $X = \langle S \rangle \leqslant \mathrm{GL}_n(q)$
  - Input length: $|S| n^2 \log q$

Matrix Groups

Let $X = \langle x_1, \ldots, x_n \rangle \leqslant \mathrm{GL}_n(q)$ be a **big** matrix group so that $|X|$ is astronomical.

- Statistical study of random products of $x_1, \ldots, x_n$ is the only known approach to identification of X.
- Determination of orders involves either
  - Factorization of integers into primes, or
  - Discrete logarithm problem over finite fields.

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

$$x_1, \ldots, x_k$$

  is the only known approach to identification of **X**.
- Basically, we are looking for a **“short" and “easy to check by random testing" first order formula which identifies X.**
- **Existence /non-existence of elements of particular orders** is an example.

Limits of crude statistical approach

"Order 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 q, unipotent and non-semisimple elements occur with probability $\sim 1/q$ 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, $n \geqslant 3$:

$BC_n, \ n \geq 2$

How one can fix the failure of statistics?

- 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:

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

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

How one can fix the failure of statistics?

(Extended) Dynkin diagrams are first order properties in the language of groups!

Black-Box Curtis–Tits Theorem (Yalçinkaya)

Theorem

Let G be a (quasi)-simple black box group of (unknown) Lie type over a field of odd characteristic and known "global exponent" N: $g^N = 1$ for all $g \in G$.

There is a polynomial in $\log N$ *algorithm which constructs the extended Dynkin diagram of G . . .*

. . . which also allows to construct "subgiagram" subgroups, etc.—in sort, to do a lot of fascinating stuff.

The moral of the story so far

Black box theory works much better . . .

. . . if groups are studied up to elementary equivalence—rather than up to isomorphism

Elementary theory and elementary equiavalence

Let G be a group

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

Elementary equivalence:

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

Pseudofinite groups

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.

This is not a 0-1 measure!

There are **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”.

Uncountable categoricity

$$G \text{ is } \aleph_1\textbf{-categorical} \iff \exists!\ \widetilde{G} \equiv G \text{ of cardinality } \aleph_1$$

Definable set

Definable set: defined by a first order formula

$$\begin{aligned} C_G(a) &= \{ x : ax = xa \}, \\ a^G &= \{ x : \exists y\, x = a^y \}. \end{aligned}$$

Groups of finite Morley rank:

- have a rank function

$$\{ \text{Definable sets in } G^n \} \xrightarrow{rk} \mathbb{N} \cup \{0\}$$

- behaves like dimension of Zariski closed sets
- axiomatised by natural axioms

In the case of simple groups:

$\aleph_1$-categorical $\iff$ of finite Morley rank

The Cherlin-Zilber Conjecture (c. 1980):

A simple infinite group of finite Morley rank is isomorphic as an abstract group to an algebraic group over an algebraically closed field.

The Hrushovski Programme

The Hrushovski Programme
G simple group of finite Morley rank
ψ a generic automorphism
Then $G_0 = C_G(\psi)$ **is pseudofinite or at least behaves like 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 the group of points of G over a pseudofinite field.

Pınar Uğurlu:

G simple group of finite Morley rank

α automorphism of G

$d(C_H(\alpha^{km})) = H$ for every connected α^k-invariant $H \leq G$ and every $k, m \in \mathbb{N}$.

$C_G(\alpha^k)$ is pseudofinite for all $k \in \mathbb{N}$.

Then G is algebraic.

Proof does not use CFSG (the Classification of Finite Simple Groups).

Why CFSG has to be eliminated?

There is a good algebraic characterisation of pseudofinite fields:

- perfect
- exactly one extension of every degree
- pseudo algebraically closed

but nothing of this kind is known for groups.

Larsen and Pink, 1998

For every n there exists a constant J depending only on n such that for any finite simple group X possessing a faithful linear or projective representation of dimension n over a field k we have either

(a) $|X| < J(n)$, or

(b) $p := char(k)$ is positive and X is a group of Lie type in characteristic p.

Larsen and Pink, equivalent statement:

A definably simple infinite pseudofinite subgroup $G \leqslant GL_n$ is a Chevalley group over a pseudofinite field.

Proof in odd characteristic

- Work in the pair $G < \overline{G}$, where G is pseudofinite and $\overline{G}$ is its Zariski closure (in GL_n).
- No use of CFSG.
- Use of large "definable" fragments of CFSG, for example:
  - Component analysis in groups of odd type.
  - Signalizer functor theory.

Count functions: motivation

- An attempt to replace both “finite” and “pseudofinite” by an unifying algebraic concept.
- We need to balance:
  - **feasibility**: the property needs to be verifiable in the context of the Hrushovski Programme
  - **power**: has to be strong enough to allow classification of definably simple groups with this property.

What follows is just a first try to achieve *power*; the feasibility was not even considered.

Count functions, after Krajíček and Scanlon

Let A be an algebraic structure and $\mathcal{D}$ the set of definable subsets in all A^n, $n = 1, 2, \ldots$.

Let R be a linearly ordered unital commutative ring. A function

$$\mu : \mathcal{D} \to R$$

is *a count function* on A over R if and only if it satisfies the following conditions.

Count functions, continued

1. $\mu(\{a\}) = 1$ for any $a \in A^k$.
2. $\mu(X \cup Y) = \mu(X) + \mu(Y)$, whenever $X, Y \in \mathcal{D}$ and X, Y are disjoint.
3. $\mu(X \times Y) = \mu(X) \times \mu(Y)$, whenever $X, Y, X \times Y \in \mathcal{D}$.
4. $\mu(X) = \mu(Y)$, whenever $X, Y \in \mathcal{D}$ and there is a definable bijection between X, Y.
5. $\mu(X) = c \cdot \mu(Y)$, whenever $c \in R, X, Y \in \mathcal{D}$, and there is a definable map $f : X \longrightarrow Y$ such that each of its fibers $f^{(-1)}(y)$, where $y \in Y$, has count $\mu(f^{(-1)}(y)) = c$.
6. $\mu(X) \geq 0$ for all $X \in \mathcal{D}$.

A count function is *nontrivial* if $0 < 1$ and the image of μ is not just $\{0\}$.

Tallied structures

For brevity, a structure with a nontrivial count function is called **tallied**.

Krajíček: Let A_i, for $i \in I$, be structures of the same languages, and assume that A is an ultraproduct of A_i. Assume that all A_i are tallied. Then A is tallied.

Tallied fields

A field F is *quasi-finite* if F is perfect and has precisely one extension of each degree (in a fixed algebraic closure $\tilde{F}$).

Scanlon: Any field admitting a non-trivial count function is quasi-finite.

Frobenious groups

A group G is called *Frobenius* if it contains a non-trivial proper subgroup H such that

$$H \cap H^g = 1 \text{ for all } g \in G \setminus H;$$

H is called *a Frobenius complement* of G. The set

$$K = \left\{ G \setminus \bigcup_{g \in G \setminus H} H^g \right\} \cup \{1\}.$$

is called *the Frobenius kernel* of G.

A version of the Frobenius Complement Theorem

B-Alshanqiti: Assume G is a tallied Frobenius group with a definable Frobenius complement H and the Frobenius kernel K. In addition, assume that H contains an involution.Then

- K is a definable normal subgroup of G.
- K is an abelian group.
- H contains exactly one involution.

Counting arguments work!