# Black box groups and pseudofinite groups

Alexandre Borovik

Joint work with Pınar Uğurlu and Şükrü Yalçınkaya

The 5th De Brún Workshop • Gallway • 11 April 2011

# Outline

# Elementary equivalence

Let $G$ be a group

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

**Elementary equivalence**:

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

# Study of finite groups up to elementary equivalence

**Main Theorem.** It is easier than a study up to isomorphism.

# Study of finite groups up to elementary equivalence

**Main Theorem.** It is easier than a study up to isomorphism.

**Remark.** But not that easy.

# Chevalley 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)

# Special Subgroups

## Torus

An abelian connected subgroup of $\overline{G}$ consisting of semisimple elements.

$$\overline{T} \cong \overline{F}^* \times \ldots \times \overline{F}^*$$

## Borel Subgroup

A maximal closed connected solvable subgroup.

$$\overline{B} = \overline{TU}, \quad \overline{T} \cap \overline{U} = 1$$

where $\overline{U} = R_u(\overline{B})$

# Roots and Root Subgroups

Let $\overline{G}$ be a connected simple group with $\overline{T} < \overline{B} < \overline{G}$ and $\overline{B} = \overline{T}\,\overline{U}$.

Let $\overline{U}_\alpha \leqslant \overline{U}$ be a minimal $\overline{T}$-invariant subgroup. Then $\overline{U}_\alpha \cong \overline{F}^+$.

We have $\overline{T} \to Aut_{rat}(\overline{F}^+) \cong \overline{F}^*$.

This gives $\alpha \in Hom_{rat}(\overline{T}, \overline{F}^*)$.

Let $\Phi^+$ be the set of all such $\alpha$ (positive roots).

# Roots and Root Subgroups

## Fact

*There exists a unique subgroup* $\overline{B}^- = \overline{TU}^-$ *and* $\overline{B} \cap \overline{B}^- = \overline{T}$.

Similar construction in $\overline{B}^-$ gives the set $\Phi^-$ of negative roots.

## Root System

$\Phi = \Phi^+ \sqcup \Phi^-$ is called root system of $\overline{G}$.

## Root Subgroups

$\overline{U}_\alpha$, $\alpha \in \Phi$, are called $\overline{T}$-root subgroups.

## Root $\mathrm{SL}_2$-subgroups

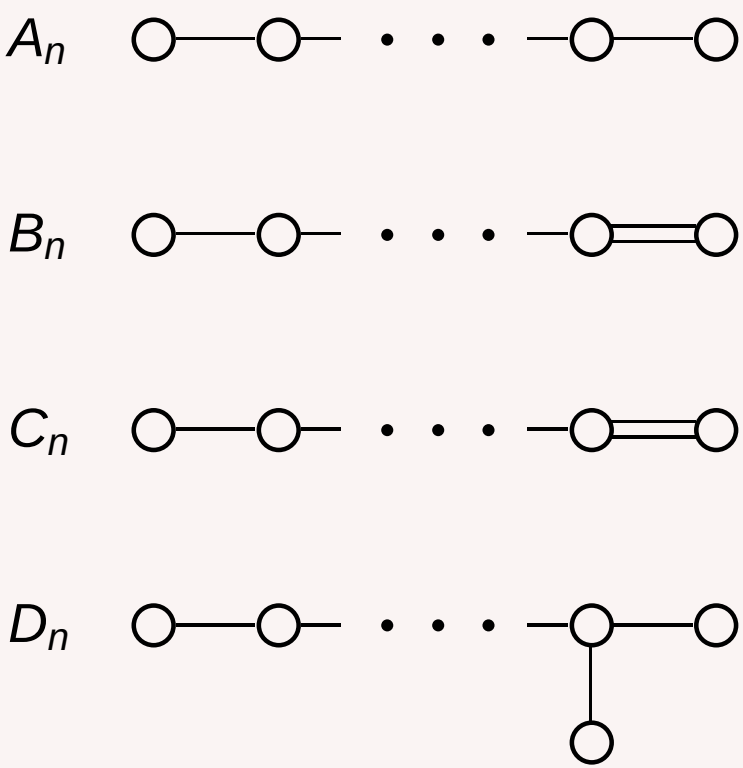
Let $\overline{K}_\alpha = \langle \overline{U}_\alpha, \overline{U}_{-\alpha} \rangle$. Then $\overline{K}_\alpha \cong (\mathrm{P})\mathrm{SL}_2(\overline{F})$.

## Fundamental Roots

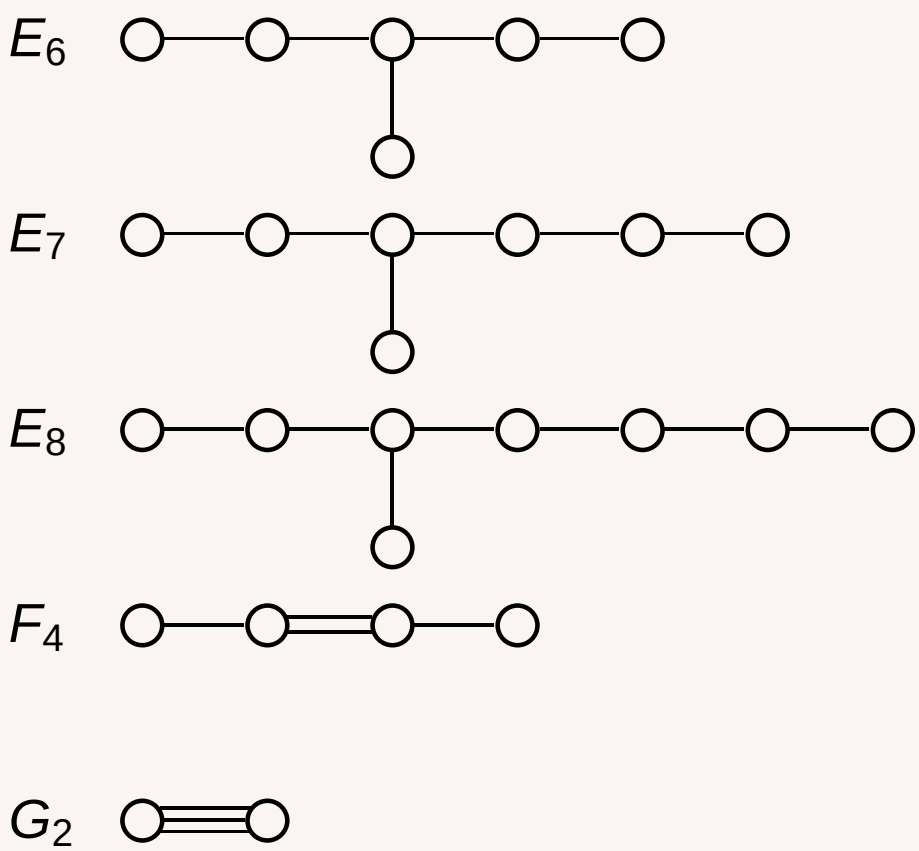
The positive roots that can not be expressed as a sum of two positive roots. They generate the root system $\Phi$.

# Dynkin diagrams of simple algebraic groups

## Classical Groups




## Exceptional Groups



# Curtis–Tits Theorem

Let $\Phi$ be an irreducible root system of rank at least 3 with fundamental system $\Pi$ and Dynkin diagram $\Delta$. Let $G$ be a group and assume the following

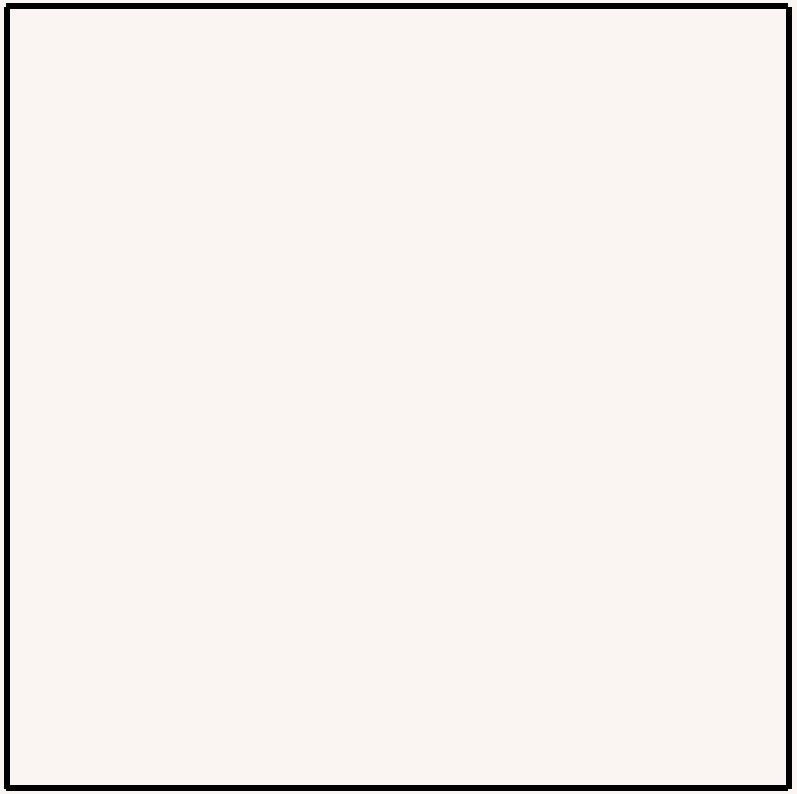
- $G = \langle K_\alpha \mid \alpha \in \Pi \rangle$, $K_\alpha = \langle U_\alpha, U_{-\alpha} \rangle = (\mathrm{P})\mathrm{SL}_2(F)$.
- $H_\alpha = N_{K_\alpha}(U_\alpha) \cap N_{K_\alpha}(U_{-\alpha}) \leqslant N_G(U_\beta)$ for all $\alpha, \beta \in \Pi$.
- $[K_\alpha, K_\beta] = 1$ if $\alpha$ and $\beta$ are not connected in $\Delta$.
- $\langle K_\alpha, K_\beta \rangle = (\mathrm{P})\mathrm{SL}_3(F)$ if $\alpha$ and $\beta$ are connected with a single bond.
- $\langle K_\alpha, K_\beta \rangle = (\mathrm{P})\mathrm{Sp}_4(F)$ if $\alpha$ and $\beta$ are connected with a double bond.

Then there exists a group of Lie type $\widetilde{G}$ with a root system $\Phi$ and fundamental system $\Pi$, and a surjective homomorphism $\varphi : G \to \widetilde{G}$ mapping the $K_\alpha$ onto the corresponding fundamental root $(\mathrm{P})\mathrm{SL}_2$-subgroups of $\widetilde{G}$.

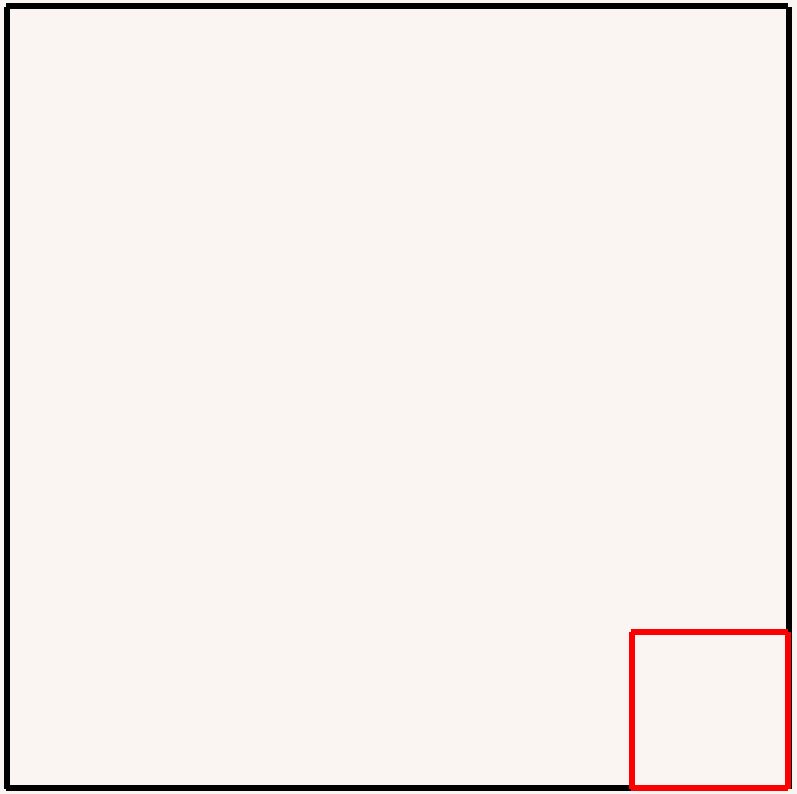
## Definition

Assume that the subgroups $\overline{K}_\alpha$, $\alpha \in \Pi$ and $\overline{T}$ satisfies the conditions in the Curtis-Tits theorem.
Then we call the set $(\{\overline{K}_\alpha \mid \alpha \in \Pi\}; \overline{T})$ a Curtis-Tits system for $\overline{G}$.

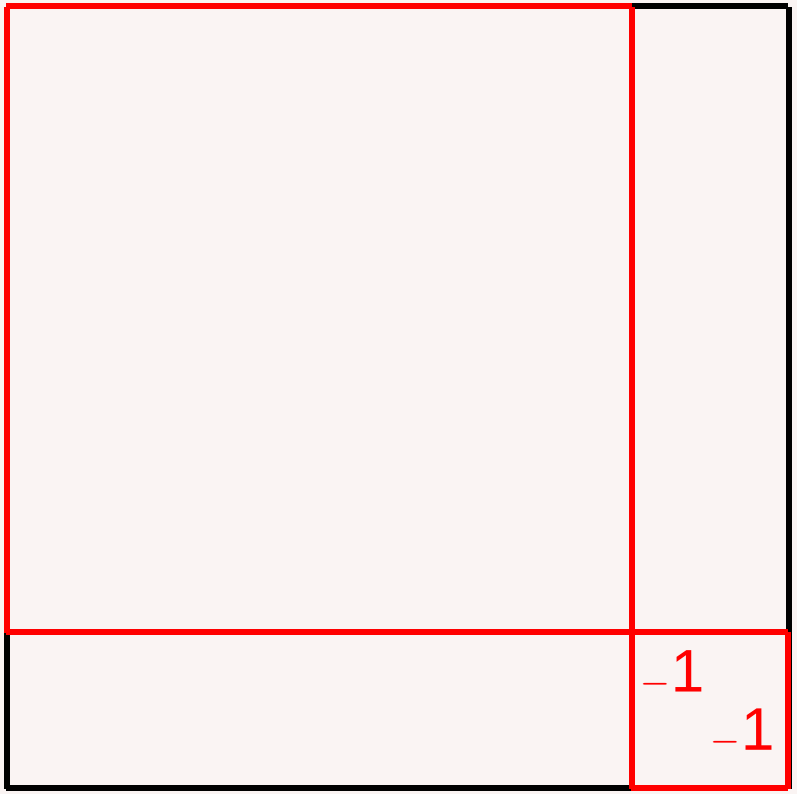
# Curtis-Tits system for $\mathrm{SL}_n(q)$:



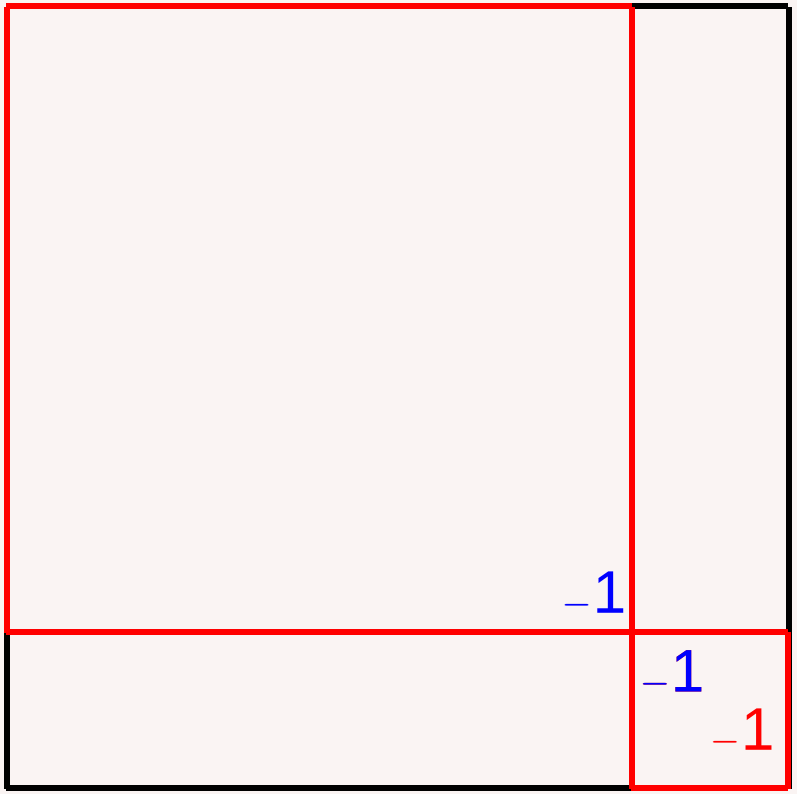
# Curtis-Tits system for $\mathrm{SL}_n(q)$:



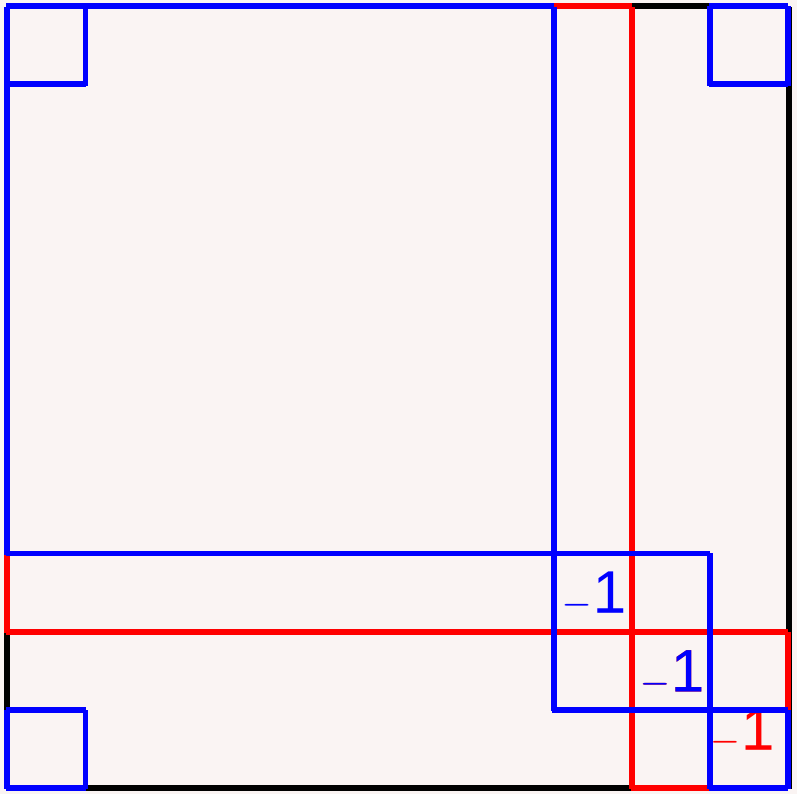
# Curtis-Tits system for $\mathrm{SL}_n(q)$:



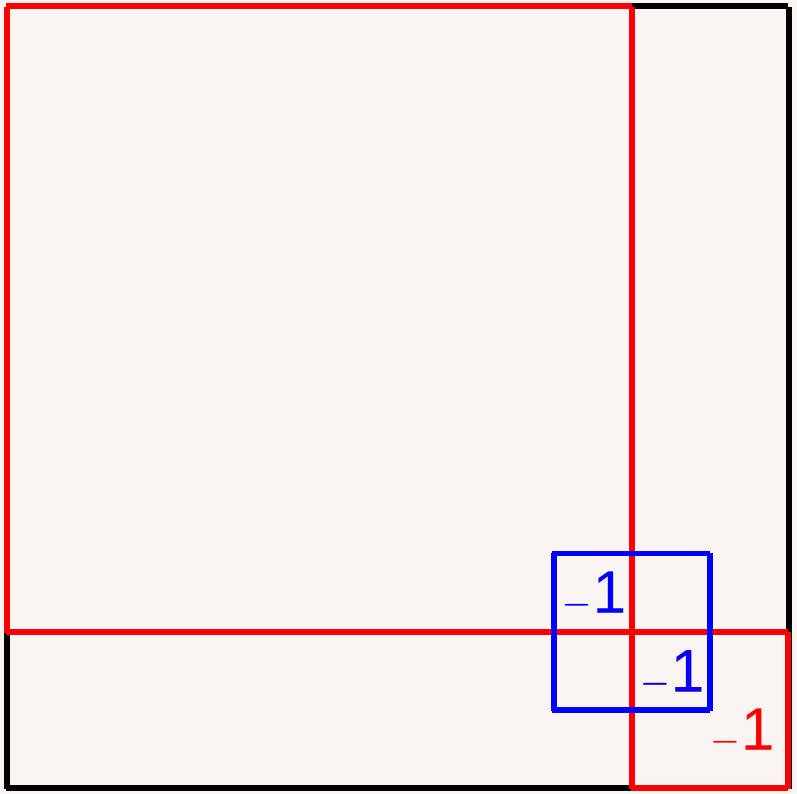

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



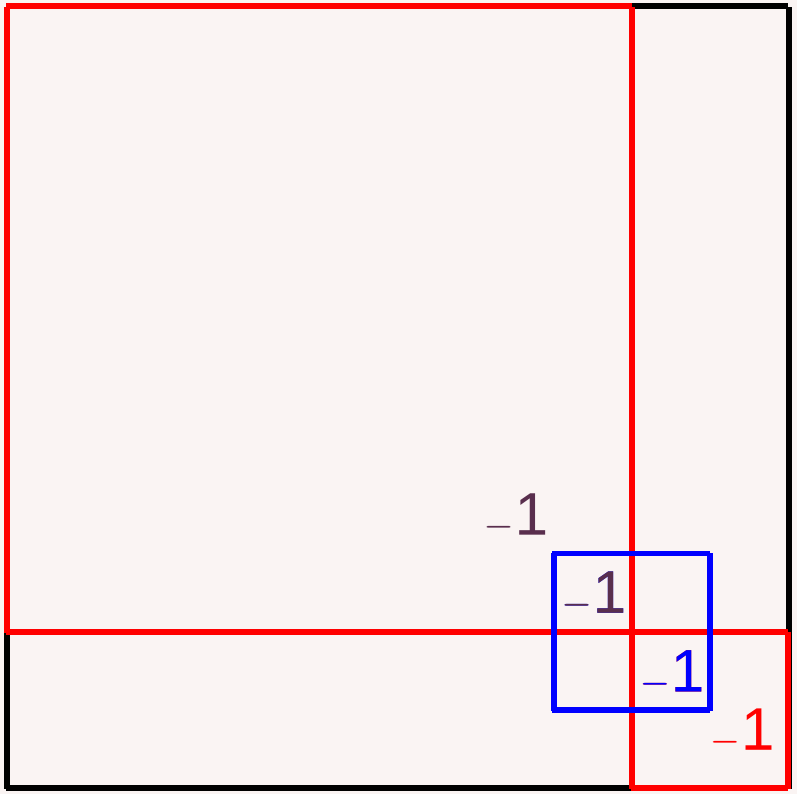

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



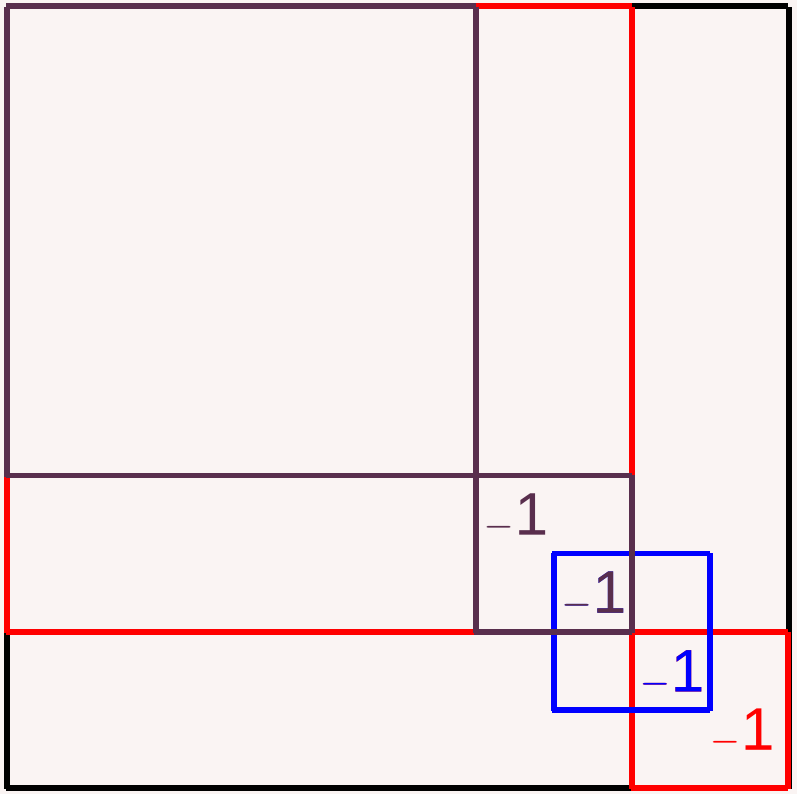

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



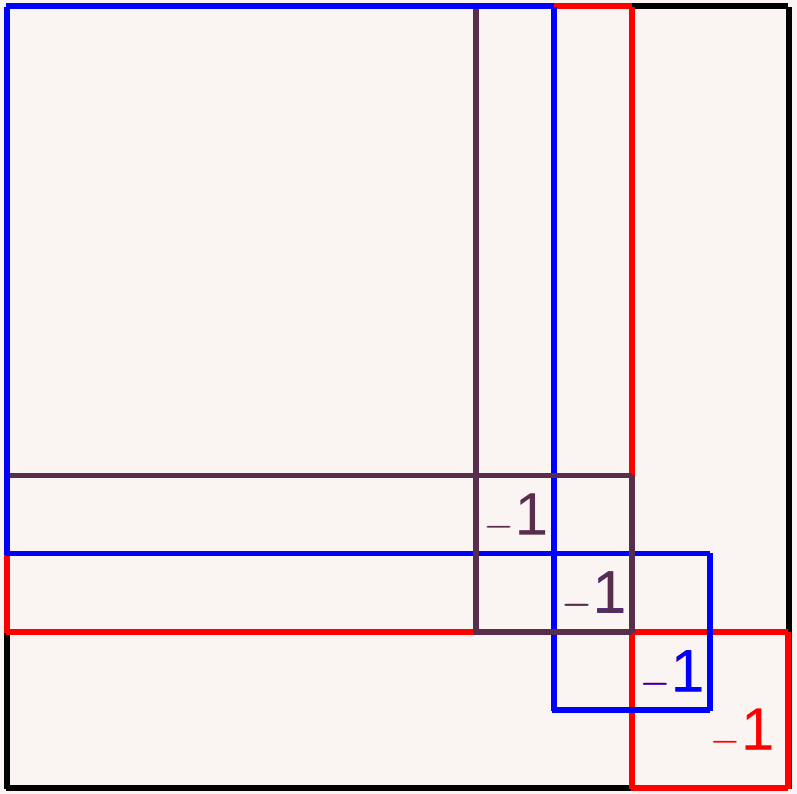

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



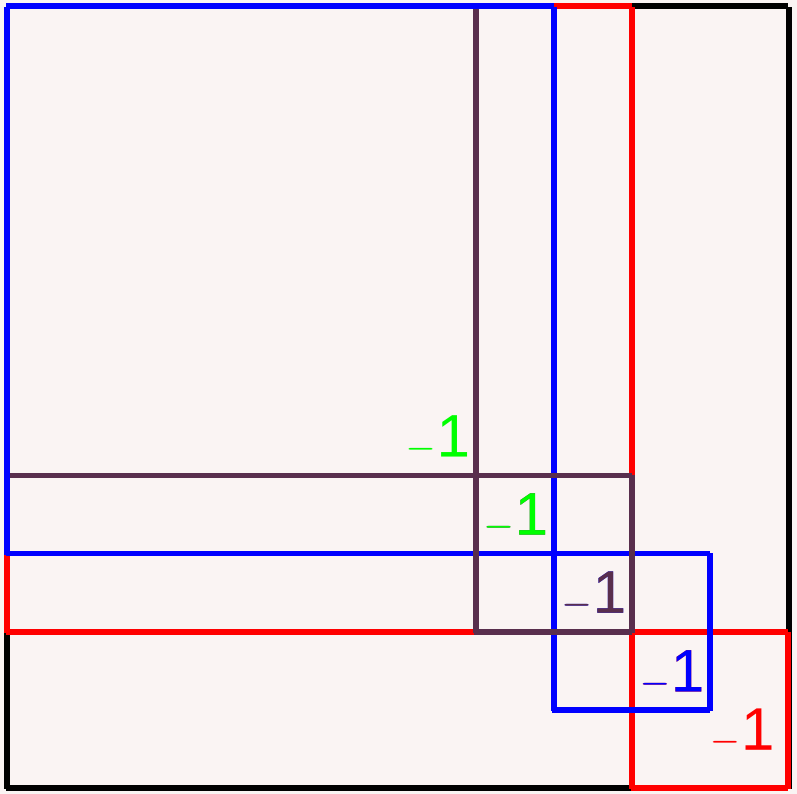

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



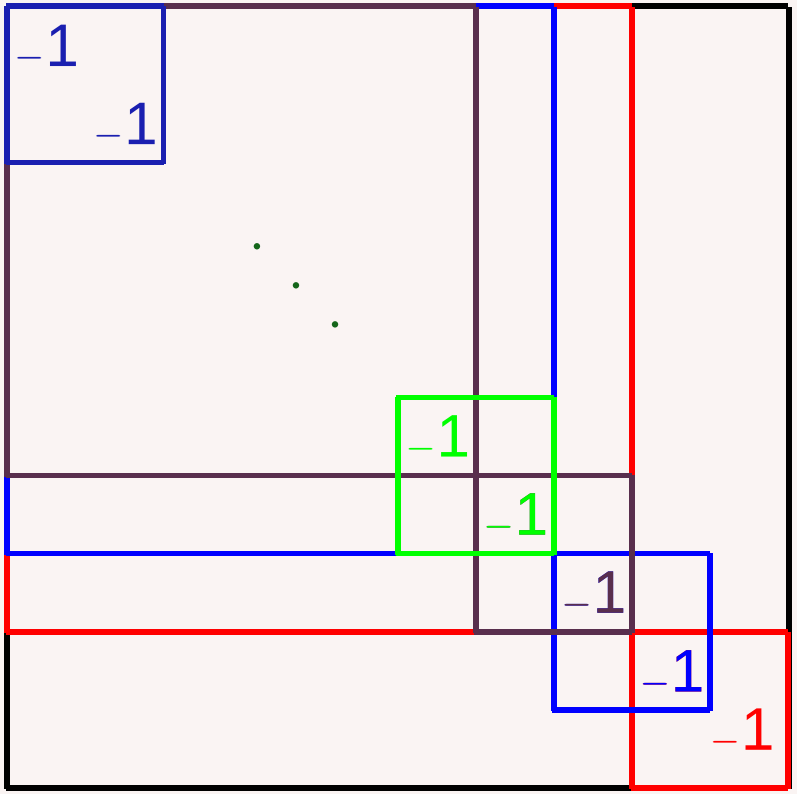

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



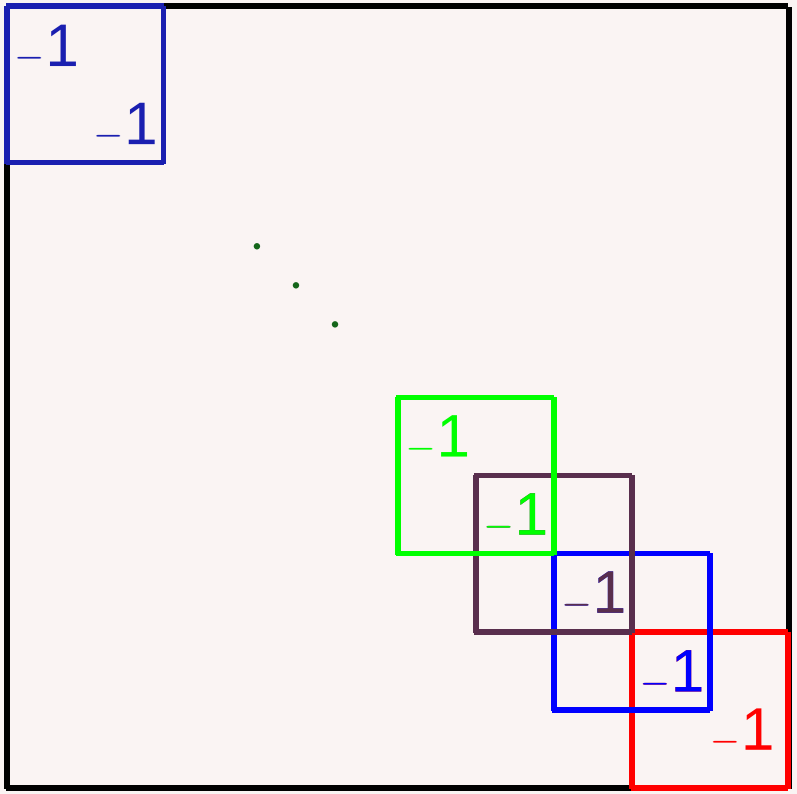

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



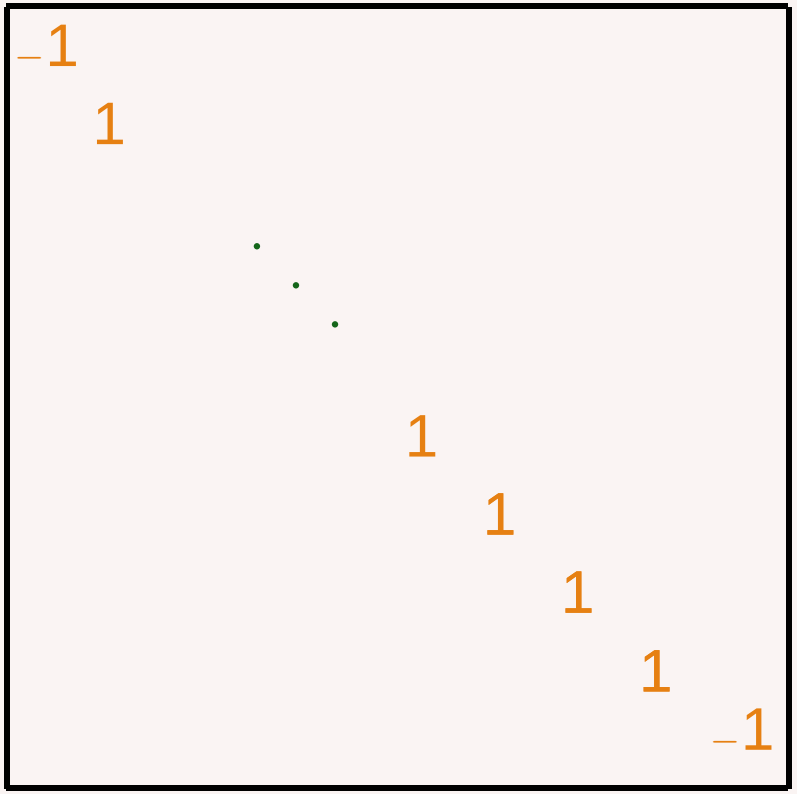

# Curtis-Tits system for $\mathrm{SL}_n(q)$:

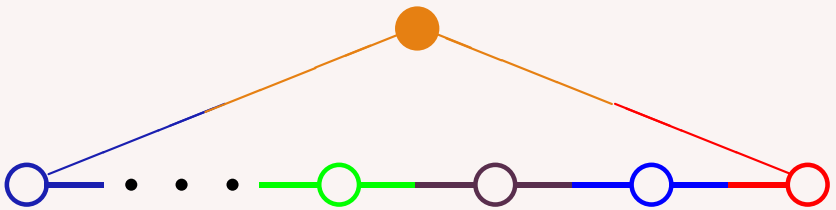



# Curtis-Tits system for $\mathrm{SL}_n(q)$:

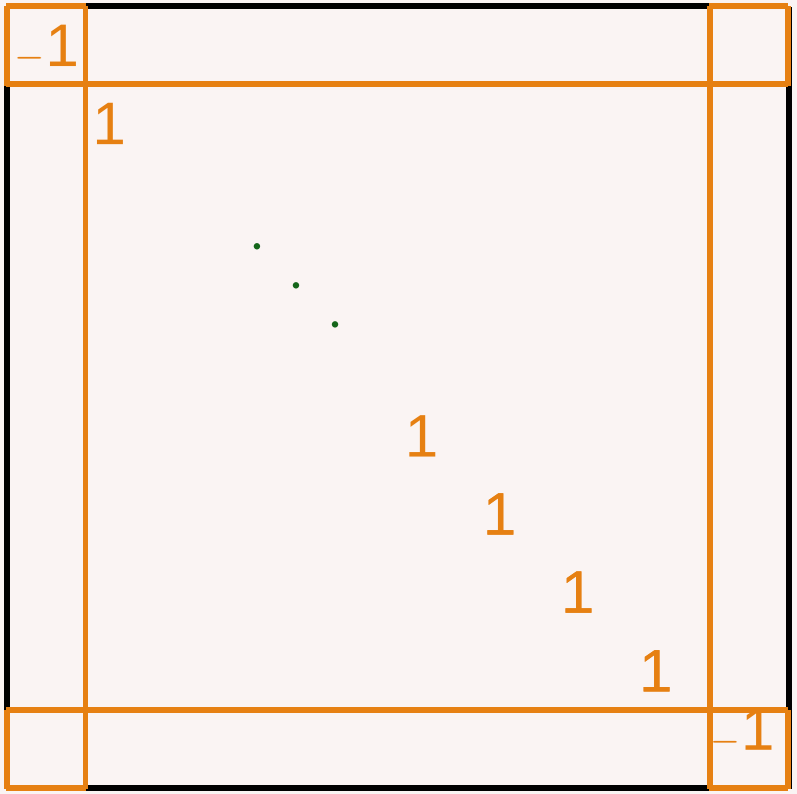


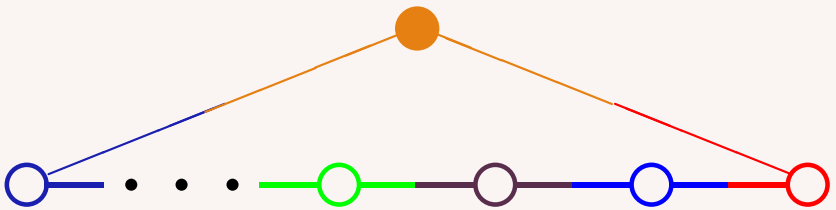

# Curtis-Tits system for $\mathrm{SL}_n(q)$:



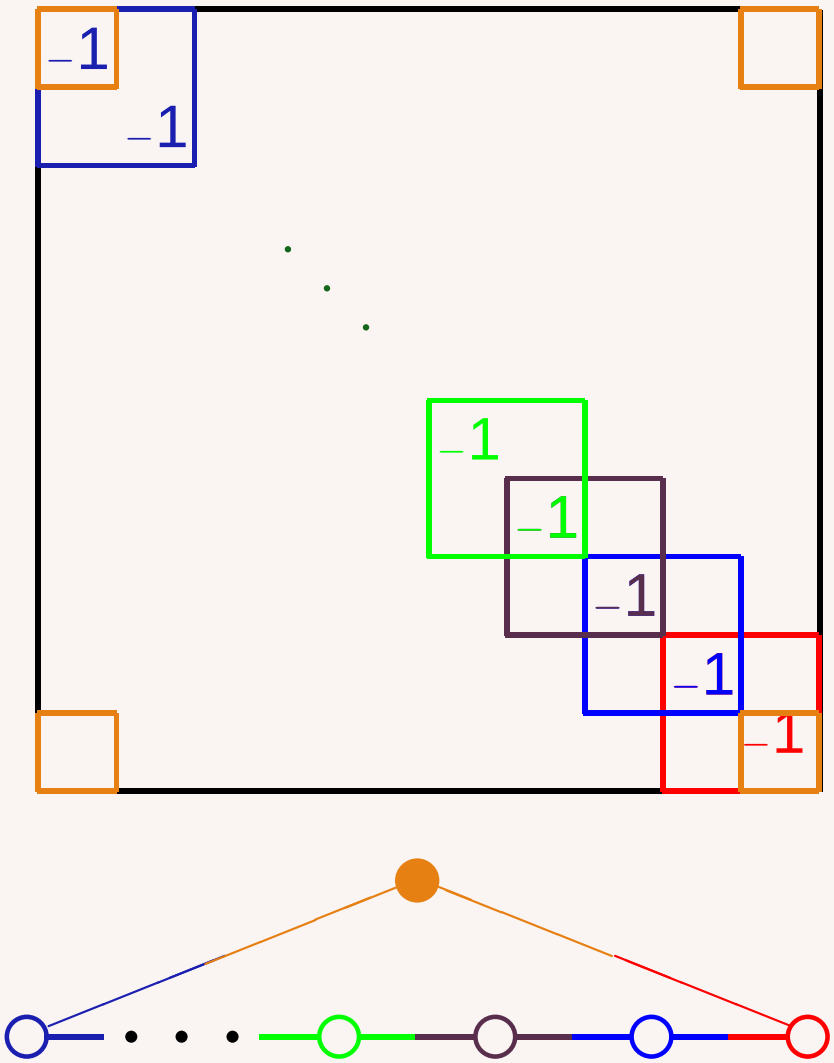



# Curtis-Tits for $\mathrm{SL}_n(q)$:

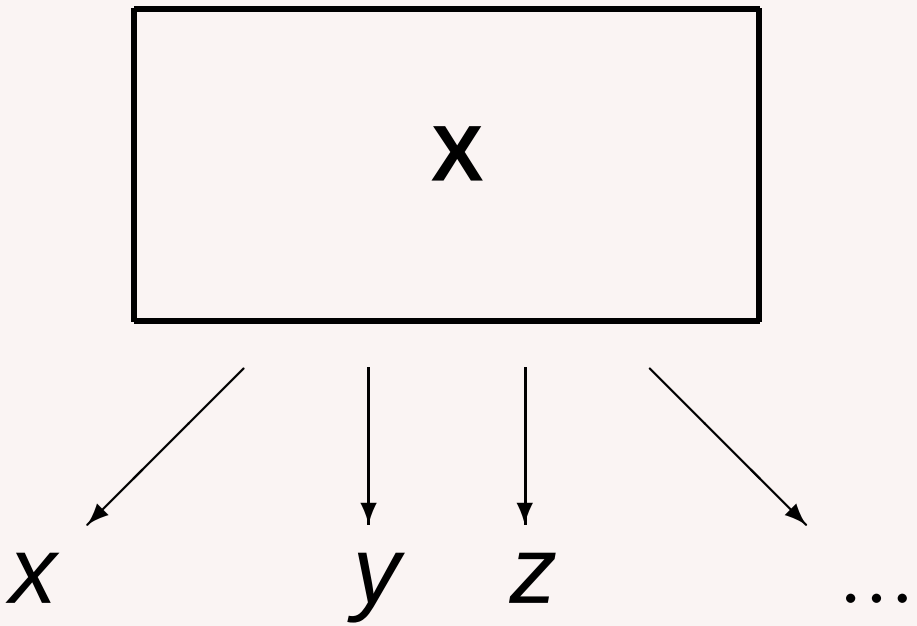


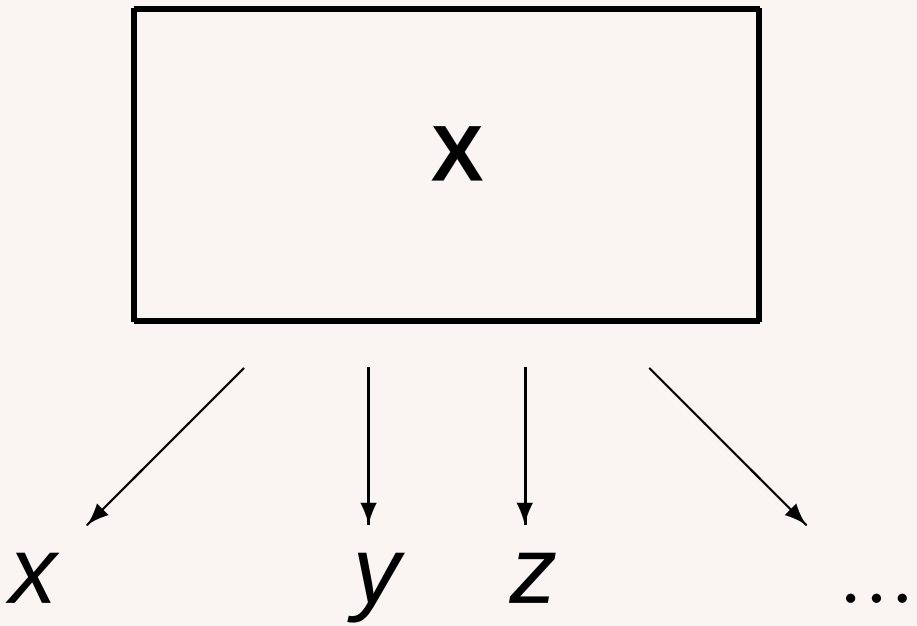
# Curtis-Tits for $\mathrm{SL}_n(q)$:



# 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: $|S| n^2 \log q$

Recognition of black box is highly technical and uses CFSG.

**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.

# 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 $p$, 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.

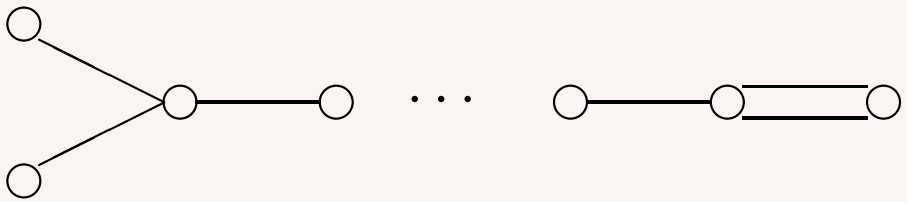
- regular semisimple elements form an open subset of $G$
- statistics of orders of regular semisimple elements is determined by the **Dynkin diagram** of $G$, which is the same in the case of groups $B_n$ and $C_n$, $n \geqslant 3$:

$BC_n, \ n \geq 2$

# How one can fix the failure of statistics?

- But the conjugacy classes and the structure of centralisers of $\mathrm{SL}$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?

**Şükrü Yalçınkaya:**

In odd characteristic, reads the (extended) Dynkin diagram from the centralisers of involutions

# Black-Box Curtis-Phan-Tits Theorem (Yalçinkaya)

## Theorem (arXiv:1008.2823v1)

*Let G be a (quasi)-simple black box group of (unknown) Lie type over a field of odd characteristic and known global exponent.*

*There is an probabilistic polynomial time algorithm which constructs a Curtis–Phan–Tits system for G.*

# 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!**

# The key to structure of Chevalley groups: centralisers of involutions

If $t$ is an involution, we have a partial map

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

Used in black box groups and in **Model Theory**: groups of finite

# Élie Cartan

$$z = \sqrt{(x^{-1})^t \cdot x} \cdot x^{-1} \in C_{\mathbf{X}}(t)$$

If $t$ is an inverse-transpose automorphism of $\mathbf{X} = \mathrm{GL}_n(\mathbb{R})$, we get a canonical decomposition

$$x = z^{-1} \cdot \sqrt{x^T \cdot x}$$

of a real matrix $x$ into product of an orthogonal $z^{-1}$ and symmetric $\sqrt{x^T \cdot x}$ matrices, due to Élie Cartan: he used the map

$$\zeta : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{SO}_n(\mathbb{R})$$

to compute homotopy of $\mathrm{SO}_n(\mathbb{R})$.

# 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:
  **if** a finite simple group $G$ contains a classical $SL_2$
  **then**,
  with known exceptions, $G$ is a Chevalley group or a twisted analogue of a Chevalley group over aa field of odd order.

# 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 (that is, can be computed) with positive probability*
$\forall^* =$ *for almost all (outputs) with probability* 1.

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

# 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!

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”.*

# CFSG contains a large “robust” fragment

The Classification of Finite Simple Groups contains large “robust” fragments, for example:

- Component analysis in groups of odd type.
- Signalizer functor theory.

# “Balance” in the sense of Gorenstein and Walter

One of the most curious cross-disciplinary interactions in the whole mathematics:

- “Obstructions” to balance as they reappear in the theory of groups of finite Morley rank are so-called “bad fields”;
- “Bad fields”, by their intrinsic nature, are non-commutative tori in the sense of Alain Connes.

Gorenstein and Walter published hundreds of pages of mind-wrecking proofs fighting the shadows cast over finite groups by objects of non-commutative geometry.

# 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.

# Larsen and Pink vs black box groups:

In characteristic $\neq 2$, the theorem

> *An infinite definably simple pseudofinite subgroup of $GL_n$ is a Chevalley group over a pseudofinite field*

can be proven by methods of the “Odd Programme” for classification of groups of finite Morley rank and odd type (which is, basically, the same as black box group theory in odd characteristic).

**And without use of the Classification of Finite Simple Groups!**

# Periodic linear groups, ca. 1980

Simple infinite periodic linear groups of odd characterisitic are Chevalley groups over locally finite fields.

**Proved without use of the Classification of Finite Simple Groups!**

# Periodic linear groups

**Proof of their classification:**

- Centralisers of involutions.
- No use of CFSG.

# Why does it work?

- We have the concept of unipotent and semisimple elements.
- A pseudofinite linear group without involutions is solvable (**Feit-Thompson**).
- A pseudofinite linear group without unipotent elements is abelian-by-finite.

# Why does it work?

- **Brouwer-Fowler**: An infinite definably simple pseudofinite group has an involution with infinite centraliser.
- **Brauer's Lemma**: Two involutions in a pseudofinite group either commute with a third involution, or are conjugate.
- More results of that kind are directly transferable from finite to pseudofinite groups . . .
- In particular, we have a working theory of signaliser functors.

**Induction:** Descending chain condition for centralisers and Zariski dimension of $\bar{G}$.

**Basis of induction**: description of finite subgroups in $GL_2$ (L. Dixon, ca. 1920), $GL_3$, $GL_4$.

# What is in common with Larsen and Pink?

Let $\bar{G}$ be the Zariski closure of $G$ in $GL_n$.
We can make $\bar{G}$ being a simple algebraic group.
Our aim is to construct a Curtis-Tits system in $G$ that "matches" a Curtis-Tits sytem in $\bar{G}$.
Unipotent elements from $SL_2$ appearing in Curtis-tits systems are "minimal unipotent elements" of Larsen and Pink.