Constructive Recognition of Classical Groups

supervised by Prof. Alice Niemeyer and Prof. Max Horn

Daniel Rademacher

08.09.2022









G













Leaves are (almost) simple groups.





2 Constructive Recognition



Motivation

Special Linear Group

Let $d \in \mathbb{N}$, $q = p^f$ a prime power and define SL $(d,q) := \{a \in \operatorname{GL}(d,q) \mid \det(a) = 1\}.$



Word problem

Given $\langle X \rangle = G \leq GL(d, q)$ and $a \in G$. The problem to write a as a word in the generators X is called the *word problem*.

$E_{i,j}(\alpha)$

We define $E_{i,j}(\alpha) \in \mathbb{F}^{d \times d}$ for $i, j \in \{1, \ldots, d\}$ with $i \neq j$ and $\alpha \in \mathbb{F}*$ as follows:

$$(E_{i,j}(\alpha))_{a,b} = \begin{cases} 1, & \text{if } a = b, \\ \alpha, & \text{if } i = a \text{ and } j = b, \\ 0, & \text{else.} \end{cases}$$

The matrices $E_{i,j}(\alpha)$ for $i, j \in \{1, ..., d\}$ with $i \neq j$ and $\alpha \in \mathbb{F}^*$ are transvections.



$$E_{2,5}(3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathsf{SL}(6,7)$$



Theorem

SL(d,q) is generated by transvections.







$$\begin{pmatrix} 5 & 0 & 6 & 3 \\ 5 & 5 & 2 & 0 \\ 1 & 4 & 6 & 6 \\ 5 & 5 & 2 & 2 \end{pmatrix} \in \mathsf{SL}(4,7)$$

Example



$$\begin{pmatrix} 5 & 0 & 6 & 3 \\ 5 & 5 & 2 & 0 \\ 1 & 4 & 6 & 6 \\ 5 & 5 & 2 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 5 & 6 & 3 \\ 5 & 3 & 2 & 0 \\ 1 & 5 & 6 & 6 \\ 5 & 3 & 2 & 2 \end{pmatrix} \rightarrow$$

Example



$$\begin{pmatrix} 5 & 0 & 6 & 3 \\ 5 & 5 & 2 & 0 \\ 1 & 4 & 6 & 6 \\ 5 & 5 & 2 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 5 & 6 & 3 \\ 5 & 3 & 2 & 0 \\ 1 & 5 & 6 & 6 \\ 5 & 3 & 2 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 5 & 6 & 3 \\ 5 & 3 & 2 & 0 \\ 1 & 5 & 6 & 6 \\ 5 & 3 & 2 & 2 \end{pmatrix}$$

Example



$$\begin{pmatrix} 5 & 0 & 6 & 3 \\ 5 & 5 & 2 & 0 \\ 1 & 4 & 6 & 6 \\ 5 & 5 & 2 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 5 & 5 & 6 & 3 \\ 5 & 3 & 2 & 0 \\ 1 & 5 & 6 & 6 \\ 5 & 3 & 2 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & 4 & 6 & 2 \\ 4 & 5 & 6 & 6 \\ 4 & 3 & 2 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 4 & 4 & 6 & 2 \\ 4 & 6 & 3 & 1 \\ 4 & 4 & 6 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 6 & 2 \\ 0 & 6 & 3 & 1 \\ 0 & 4 & 6 & 4 \end{pmatrix}$$

An efficient algorithm to solve the word problem returning SLPs has been designed:

- SL Straight-line programs with memory and matrix Bruhat decomposition by Alice C. Niemeyer, Tomasz Popiel and Cheryl E. Praeger, 2017
- Sp Bachelors thesis, R., 2019
- SU Bachelors thesis, R., 2019
- SO Masters thesis, R. , 2020 (except characteristic 2)

$$\mathsf{SL}(4,7) \cong \langle \begin{pmatrix} 6 & 2 & 3 & 5 & 5 & 1 \\ 5 & 3 & 2 & 3 & 6 & 1 \\ 0 & 0 & 5 & 1 & 3 & 0 \\ 6 & 1 & 0 & 4 & 4 & 4 \\ 2 & 5 & 1 & 3 & 6 & 6 \\ 5 & 2 & 5 & 2 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 5 & 2 & 0 & 1 & 3 \\ 5 & 2 & 3 & 3 & 1 & 4 \\ 2 & 4 & 2 & 4 & 4 & 5 \\ 5 & 2 & 1 & 6 & 4 & 5 \\ 6 & 3 & 4 & 2 & 3 & 6 \\ 1 & 1 & 5 & 3 & 5 & 4 \end{pmatrix} \rangle =: \hat{G} \leq \mathsf{SL}(6,7)$$

$$\begin{pmatrix} 5 & 0 & 6 & 3 \\ 5 & 5 & 2 & 0 \\ 1 & 4 & 6 & 6 \\ 5 & 5 & 2 & 2 \end{pmatrix} \leftrightarrow \begin{pmatrix} 2 & 3 & 5 & 1 & 0 & 5 \\ 1 & 1 & 2 & 2 & 4 & 6 \\ 4 & 4 & 5 & 2 & 2 & 6 \\ 0 & 4 & 0 & 4 & 4 & 4 \\ 0 & 3 & 2 & 0 & 1 & 2 \\ 5 & 1 & 3 & 5 & 3 & 0 \end{pmatrix} \in \hat{G}$$

$$E_{1,2}(1) \leftrightarrow \begin{pmatrix} 2 & 6 & 5 & 0 & 5 & 3 \\ 2 & 6 & 3 & 0 & 3 & 6 \\ 3 & 4 & 2 & 0 & 1 & 2 \\ 2 & 5 & 3 & 1 & 3 & 6 \\ 2 & 5 & 3 & 0 & 4 & 6 \\ 6 & 1 & 2 & 0 & 2 & 5 \end{pmatrix}$$

$$E_{1,2}(1) \leftrightarrow \begin{pmatrix} 2 & 6 & 5 & 0 & 5 & 3 \\ 2 & 6 & 3 & 0 & 3 & 6 \\ 3 & 4 & 2 & 0 & 1 & 2 \\ 2 & 5 & 3 & 1 & 3 & 6 \\ 2 & 5 & 3 & 0 & 4 & 6 \\ 6 & 1 & 2 & 0 & 2 & 5 \end{pmatrix} \quad E_{5,2}(3) \leftrightarrow \begin{pmatrix} 4 & 4 & 1 & 0 & 1 & 2 \\ 6 & 2 & 2 & 0 & 2 & 4 \\ 1 & 6 & 6 & 0 & 5 & 3 \\ 3 & 4 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 4 & 3 & 6 & 0 & 6 & 6 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 5 & 6 & 3 \\ 5 & 3 & 2 & 0 \\ 1 & 5 & 6 & 6 \\ 5 & 3 & 2 & 2 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 4 & 0 & 1 & 2 & 2 \\ 2 & 0 & 0 & 2 & 2 & 2 \\ 5 & 3 & 3 & 2 & 0 & 2 \\ 6 & 5 & 2 & 4 & 6 & 1 \\ 5 & 5 & 6 & 0 & 5 & 3 \\ 2 & 4 & 2 & 5 & 2 & 5 \end{pmatrix} \in \hat{G}$$

Motivation 00000 **RNTHAACHEN**



RNTHAACHEN

Constructive Recognition



Let $G = \langle X \rangle \leq \mathsf{GL}(d,q)$ be a a classical group.

Let $G = \langle X
angle \leq \mathsf{GL}(d,q)$ be a a classical group.

The goal of constructive recognition is to construct an isomorphism

$$\varphi\colon G\to \hat{G}$$

where \hat{G} is the standard copy of G such that $\varphi(g)$ and $\varphi^{-1}(\hat{g})$ can be computed efficiently for each $g \in G$ and $\hat{g} \in \hat{G}$.

Let $G = \langle X \rangle \leq \operatorname{GL}(d,q)$ be a classical group.

The goal of constructive recognition is to construct an isomorphism

$$\varphi\colon G\to \hat{G}$$

where \hat{G} is the standard copy of G such that $\varphi(g)$ and $\varphi^{-1}(\hat{g})$ can be computed efficiently for each $g \in G$ and $\hat{g} \in \hat{G}$.

• Define a set of *standard generators* \hat{S} for each classical group in the standard copy.

Let $G = \langle X \rangle \leq \operatorname{GL}(d,q)$ be a classical group.

The goal of constructive recognition is to construct an isomorphism

$$\varphi\colon G\to \hat{G}$$

where \hat{G} is the standard copy of G such that $\varphi(g)$ and $\varphi^{-1}(\hat{g})$ can be computed efficiently for each $g \in G$ and $\hat{g} \in \hat{G}$.

• Define a set of *standard generators* \hat{S} for each classical group in the standard copy.

• Express
$$S = \varphi(\hat{S})^{-1}$$
 as words in terms of X.

Let $G = \langle X \rangle \leq \operatorname{GL}(d,q)$ be a classical group.

The goal of constructive recognition is to construct an isomorphism

$$\varphi\colon G\to \hat{G}$$

where \hat{G} is the standard copy of G such that $\varphi(g)$ and $\varphi^{-1}(\hat{g})$ can be computed efficiently for each $g \in G$ and $\hat{g} \in \hat{G}$.

- Define a set of *standard generators* \hat{S} for each classical group in the standard copy.
- Express $S = \varphi(\hat{S})^{-1}$ as words in terms of X.
- Express g in terms of S and \hat{g} in terms of \hat{S} as words.







1) GoingDown Algorithm: Reduce the problem to a smaller classical group until a base case.



- 1) GoingDown Algorithm: Reduce the problem to a smaller classical group until a base case.
- 2) Base Case Algorithm: Use a constructive recognition algorithm for the base case.



- 1) GoingDown Algorithm: Reduce the problem to a smaller classical group until a base case.
- 2) Base Case Algorithm: Use a constructive recognition algorithm for the base case.
- GoingUp Algorithm: Use the knowledge of standard generators for a smaller classical group to construct standard generators for a larger one.



- 1) GoingDown Algorithm: Reduce the problem to a smaller SL until a SL(2, q) is found.
- Base Case Algorithm: Constructive recognition algorithm for SL(2, q) by Conder, Leedham-Green and O'Brien.
- GoingUp Algorithm: Use the knowledge of standard generators for a smaller SL to construct standard generators for a larger SL.



- 1) GoingDown Algorithm: Reduce the problem to a smaller SL until a SL(2, q) is found.
- Base Case Algorithm: Constructive recognition algorithm for SL(2, q) by Conder, Leedham-Green and O'Brien.
- GoingUp Algorithm: Use the knowledge of standard generators for a smaller SL to construct standard generators for a larger SL.



Let $G \leq GL(d, q)$ with $G \cong SL(d, q)$. We search for certain elements in the special linear groups called stingray elements to compute a chain

 $\mathsf{SL}(4,q) \cong U \leq U_k \cong \mathsf{SL}(d_k,q) \leq \ldots \leq U_1 \cong \mathsf{SL}(d_1,q) \leq G$ where $d_i \leq 2 \cdot \log_2(d_{i-1})$.

Stingray element

Let $G \leq GL(d, q)$. An element $s \in G$ is called *stingray element*, if s acts irreducibly on a subspace of dimension m, that is it does not leave invariant a subspace of the m-dimensional space, with m small relative to d, and fixes a complementary subspace pointwise.

Example of a Stingray Element

$$\begin{pmatrix} 4 & 1 & 3 & 3 & 2 & 1 & 2 & 4 & 0 & 4 \\ 3 & 3 & 4 & 4 & 3 & 4 & 1 & 0 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 & 1 & 1 & 2 & 0 & 3 \\ 3 & 1 & 3 & 4 & 4 & 0 & 2 & 0 & 1 & 3 \\ 3 & 4 & 1 & 1 & 0 & 3 & 4 & 4 & 1 & 1 \\ 1 & 0 & 4 & 4 & 2 & 2 & 1 & 1 & 4 & 2 \\ 2 & 4 & 2 & 2 & 0 & 3 & 4 & 2 & 1 & 0 \\ 0 & 2 & 2 & 2 & 2 & 4 & 0 & 3 & 4 & 2 & 1 \\ 0 & 2 & 2 & 2 & 2 & 2 & 1 & 3 & 2 & 1 & 2 \end{pmatrix} \in SL(10,5)$$

RWTHAACHEN UNIVERSITY



RWITHAACHEN

LINIVERSITY



GoingDown Algorithm

RNTHAACHEN



$$s_1 = \left(\boxed{*} \right) \in \operatorname{GL}(d,q)$$

$$s_2 = \left(\boxed{ * } \right) \in \operatorname{GL}(d, q)$$



















		~				
$\left(\right)$	SL(<i>n</i> , <i>q</i>)			0		
			1		0	
	0		: : 0	÷.	: : 1)

Stingray candidate

Let $G \leq GL(d, q)$. An element $s' \in G$ is called *stingray candidate*, if s' acts on a subspace of dimension m with m small relative to d, and fixes a complementary subspace pointwise.

Stingray candidate

Let $G \leq GL(d, q)$. An element $s' \in G$ is called *stingray candidate*, if s' acts on a subspace of dimension m with m small relative to d, and fixes a complementary subspace pointwise.

Pre-stingray candidate

Let $G \leq GL(d, q)$. An element $\tilde{s} \in G$ is called *pre-stingray* candidate, if the characteristic polynomial $\chi_{\tilde{s}}(x)$ has an irreducible factor $P(x) \in \mathbb{F}_q[x]$ of degree k over \mathbb{F}_q and no other irreducible factors of degree divisible by k.

Theorem

Let $G \leq GL(d, q)$ and $\tilde{s} \in G$ a pre-stingray candidate. Then \tilde{s}^{ℓ} is a stingray candidate where $\ell \in \mathbb{N}$ can easily be computed with information from $\chi_{\tilde{s}}(x)$.

Algorithm 1 FindStingrayCandidate				
1:	<pre>procedure FindStingrayCandidate(H, n)</pre>			
2:	while true do			
3:	$h := (pseudo)random(H); \chi_h(x) := characteristic polynomial of h;$			
4:	$\{P_i(x)\} :=$ irreducible factors of $\chi_h(x)$;			
5:	if $\exists P_i(x), k := \deg(P_i(x))$ does not divide $\deg(P_j(x)), j \neq i$ then			

- 6: Compute $\ell \in \mathbb{N}$ according to theorem
- 7: Return h^{ℓ} ;
- 8: end if
- 9: end do



Let $s_1, s_2 \in G \leq GL(d, q)$ with $G \cong SL(d, q)$ and s_1, s_2 stingray elements where s_i acts irreducibly on $W_i \leq \mathbb{F}_q^d$ and $W_1 \cap W_2 = \{0\}$. With some probability

$$\langle s_1, s_2 \rangle \cong \mathsf{SL}(m_1 + m_2, q)$$

where m_i is the dimension of W_i .





1) What is the probability to find a pre-stingray candidate?





 What is the probability to find a pre-stingray candidate? *Elements in finite classical groups whose powers have large 1-Eigenspaces* by Alice C. Niemeyer and Cheryl E. Praeger, 2018



- What is the probability to find a pre-stingray candidate? *Elements in finite classical groups whose powers have large 1-Eigenspaces* by Alice C. Niemeyer and Cheryl E. Praeger, 2018
- 2) What is the probability that two stingray elements generate a special linear group?



- What is the probability to find a pre-stingray candidate? Elements in finite classical groups whose powers have large 1-Eigenspaces by Alice C. Niemeyer and Cheryl E. Praeger, 2018
- 2) What is the probability that two stingray elements generate a special linear group? The probability of spanning a classical space by two non-degenerate subspaces of complementary dimensions by S.P. Glasby, Alice C. Niemeyer and Cheryl E. Praeger Random generation of direct sums of finite non-degenerate subspaces by S.P. Glasby, Alice C. Niemeyer and Cheryl E. Praeger

Second item is not completely solved yet.

Thank you for your attention!