Presentations On Standard Generators For Some Classical Groups

Bachelor Project

Emma Ahrens
Supervisors: D. Bernhardt Prof. Dr. A. Niemeyer

Lehrstuhl B für Mathematik, RWTH Aachen University

10 October 2019

Contents

Matrix Group Recognition Project

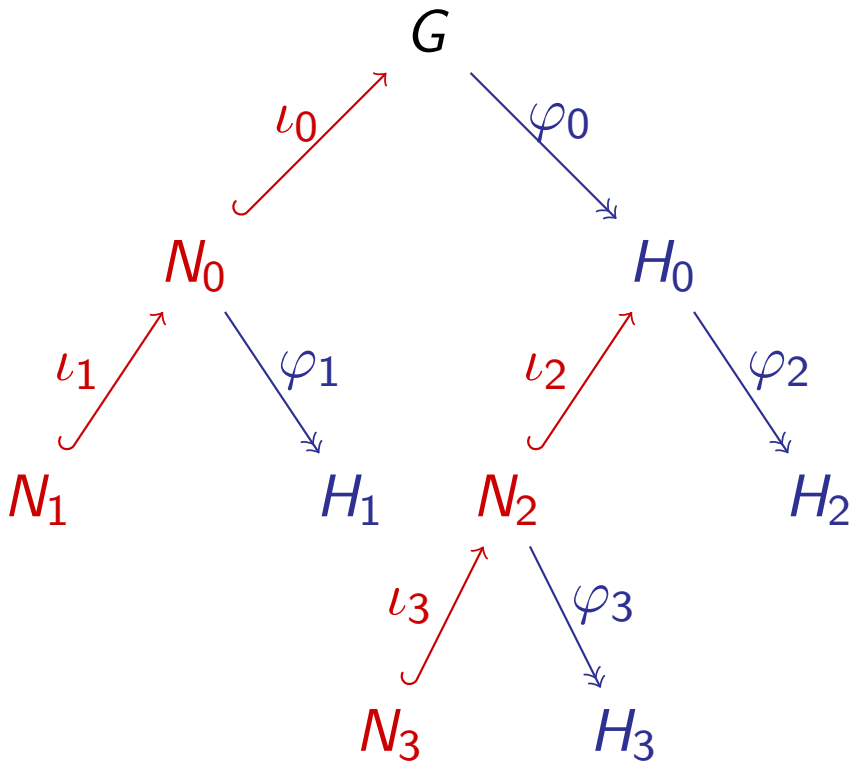
$$G := \langle M_1, \ldots, M_k \rangle \leq GL(n, q)$$

Objectives:

- Size of G?
- Isomorphism types?
- Membership Test
- Word Problem

Composition Tree

A composition tree is constructed such that the leafs of this tree can be recognised constructively. The algorithms for that task are randomised.



My Bachelor Project

Implement and prove the correctness of the presentations of

- the symmetric group S_n,
- the group of signed permutation matrices SH_n,
- the special linear group $\mathsf{SL}(2, q)$
- and the special unitary group $\mathsf{SU}(3, q)$.

and the corresponding projective groups.

Mathematical Background

Definition (Presentation of a Group)

Let X be a set, F_X the free group on X and $R \subseteq F_X$. Then we define $\{X \mid R\}$ to be the presentation of the group $G := F_X/N$, where $N = \langle R \rangle_{F_X}$ is the normal closure of R in F_X.
We write $G = \langle X \mid R \rangle$.

Definition (Length of a Presentation)

The *bit-length* of a presentation $\{X \mid R\}$ is defined as $|X|$ plus the total number of bits required to encode the words in R as strings over the alphabet $X \cup X^{-1}$ where all exponents are encoded as binary strings.

Mathematical Background

We build presentations on the *standard generators* as defined in [LGOB09].

Theorem ([LGOB19])

Every classical group of rank r defined over $GF(q)$ has a presentation on its standard generators with $O(r)$ relations and total bit-length $O(r + \log q)$.

Those presentations are called *short*.

Symmetric Group S_n

Theorem

The symmetric group S_n has the presentations

$$\{X_1 \mid R_1\} = \{\, \tau_1, \ldots, \tau_{n-1} \mid \tau_i^2 = (\tau_i\tau_{i+1})^3 = (\tau_i\tau_j)^2 = 1 \ \forall j > i+1 \,\}$$

and

$$\begin{aligned}\{X_2 \mid R_2\} = \{\, U, V \mid U^2 = V^n = (UV)^{n-1} = (UU^V)^3 \\ = (UU^{V^j})^2 = 1 \text{ for } 2 \leq j \leq n/2 \,\}\end{aligned}$$

for $n > 2$.

Special Unitary Group $SU(3, q)$

Definition

We define

$$\mathrm{GU}(3, q) := \{M \in \mathrm{GF}(q^2)^{3\times 3} \mid \phi(Mv, Mw) = \phi(v, w) \quad \forall v, w \in \mathrm{GF}(q^2)^3\}$$

and call it the *unitary group of degree* 3 *over the field* $\mathrm{GF}(q^2)$. Furthermore we define

$$\mathrm{SU}(3, q) := \mathrm{GU}(3, q) \cap \mathrm{SL}(3, q^2)$$

and call it the *special unitary group of degree* 3 *over the field* $\mathrm{GF}(q^2)$.

Special Unitary Group SU(3, q)

Lemma

$$\nu(\alpha, \beta) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \alpha^{q+1} = \beta + \beta^q$$

$$\text{and} \quad \Delta(\gamma) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \gamma \neq 0.$$

Special Unitary Group SU(3, q)

Lemma

$$\nu(\alpha, \beta) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \alpha^{q+1} = \beta + \beta^q$$

$$\text{and} \quad \Delta(\gamma) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \gamma \neq 0.$$

Theorem

$$\langle \nu, \tau, \Delta, A \rangle = \mathsf{SU}(3, q)$$

Special Unitary Group SU(3, q)

Lemma

$$\nu(\alpha, \beta) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \alpha^{q+1} = \beta + \beta^q$$

$$\text{and} \quad \Delta(\gamma) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \gamma \neq 0.$$

Theorem

$$\langle \nu, \tau, \Delta, A \rangle = \mathsf{SU}(3, q)$$

Theorem

$$|H| = (q^2 - 1)q^3$$

Special Unitary Group SU(3, q)

Lemma

$$\nu(\alpha, \beta) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \alpha^{q+1} = \beta + \beta^q$$

$$\text{and} \quad \Delta(\gamma) \in \mathsf{SU}(3, q) \quad \Leftrightarrow \quad \gamma \neq 0.$$

Theorem

$$\langle \nu, \tau, \Delta, A \rangle = \mathsf{SU}(3, q)$$

Theorem

$$|H| = (q^2 - 1)q^3$$

Theorem

$$H \dot{\cup} UDLU = \mathsf{SU}(3, q)$$

Presentation of SU(3, q)

Lemma

Let $\nu(\alpha, \beta) = u \in U$ be an upper unitriangular matrix in SU(3, q). *Then the matrices*

$$u_L := \nu(-\alpha, \beta^{-q}, \beta^{-1}) \in U,$$
$$u_R := \nu(-\alpha\beta^{-1}, \beta^{-1}) \in U$$
$$\text{and } \ d := \operatorname{diag}(\beta^{-q}, \beta^{q-1}, \beta) \in \langle \Delta \rangle =: D$$

fulfil the relation $u^A = u_L d A u_R$.

Presentation of $\mathrm{SU}(3, q)$

Definition

We define the group

$$G := \langle \nu, \tau, \Delta, A \mid R(1), R(2), \Delta^A = \Delta^{-q}, A^2 = 1 \rangle,$$

where $R(2) \subseteq \{P(u) \mid u \in U\}$.

Definition

We define $V := \{u \in U \mid P(u) \in N\}$, where N is the normal closure of $R(2)$ in the free group over ν, τ, Δ, A.

Theorem

If $V = U \backslash \{1\}$, then G is isomorphic to $\mathrm{SU}(3, q)$.

Presentation of $\mathrm{SU}(3,q)$ for $q \not\equiv 2 \bmod 3$

Theorem

Suppose that $q \not\equiv 2$ *mod* 3. *Then there exist* $\alpha_0, \beta_0, \gamma_0 \in \mathrm{GF}(q^2)$ *such that the following holds:*
Let $\nu_0 = \nu(\alpha_0, \beta_0), \tau_0 = \nu(0, \gamma_0)$, $\hat{U} = \{\nu_0, \tau_0, \nu_0\tau_0\}$ *and* $R(2) = \{P(u) \mid u \in \hat{U}\}$. *Then* G *is isomorphic to* $\mathrm{SU}(3,q)$.

Evaluation of the Implementation

Runtime Optimisation

A minimised number of matrix multiplications is obtained through the usage of *short* presentations and adapations of the *Square-And-Multiply* Algorithm.

Memory Consumption

Efficient memory consumption is obtained through carefully choosing the order of the verification of the relations.
The programs store at most 12 matrices simultaneously.

Future Work

- Implement presentations of other finite classical and related groups in order to ensure verification in the *matrix group recognition project*.
- Integrate into the GAP package `recog`.

Bibliography

The GAP Group. *GAP - Groups, Algorithms and Programming*. Version 4.10. 2019.

C. R. Leedham-Green and E. A. O'Brien. "Constructive recognition of classical groups in odd characteristic". In: *Journal of Algebra* 322 (2009).

C. R. Leedham-Green and E. A. O'Brien. "Presentations on standard generators for classical groups". 2019.