International Electronic Journal of Geometry
Volume 15 No. 1 Page 69–74 (2022)
DOI: https://doi.org/10.36890/iejg.977878

On the Computation of Conjugation Classes of Elements of $\mathrm{PGL}(3, q)$

Michael Braun *

(Communicated by Levent KULA)

Abstract

In this article an explicit list of representatives of all conjugacy classes of the projective linear group $\mathrm{PGL}(3, q)$ is computed with complexity $O(q^2)$.

Keywords: *Conjugacy classes, projective linear group, group action.*
AMS Subject Classification (2020): *Primary: 05B25 ; Secondary: 20B25.*

1. Introduction

For any (multiplicatively written) group G the equivalence relation

$$x \simeq_G y :\iff \exists t \in G : txt^{-1} = y$$

is called *conjugation*. The corresponding equivalence classes are called the *conjugacy classes* of G. The set of all conjugacy classes of G will be denoted by $\mathrm{Conj}(G)$. By $\mathrm{Rep}(G)$ we denote a set of representatives of $\mathrm{Conj}(G)$. The *center* of G is defined to be the set of fixed points of all group elements, denoted by

$$\mathrm{Z}(G) := \{x \in G \mid txt^{-1} = x \,\forall t \in G\}.$$

Since $\mathrm{Z}(G)$ is a subgroup of G the set of cosets

$$\overline{G} = G/\,\mathrm{Z}(G) = \{x\,\mathrm{Z}(G) \mid x \in G\}$$

forms a group. When talking about $\overline{G}$ for sake of simplicity in the following we just write the coset representative x instead of the whole coset $x\,\mathrm{Z}(G)$.

For $x, y \in G$ we finally have the equivalence

$$x \simeq_{\overline{G}} y \iff \exists t \in G, s \in \mathrm{Z}(G) : txt^{-1}s = y.$$

Obviously, we obtain the implication for all $x, y \in G$:

$$x \simeq_G y \implies x \simeq_{\overline{G}} y.$$

Let $G = \mathrm{GL}(n, q)$ denote the general linear group of the canonical n-dimensional vector space $\mathrm{GF}(q)^n$ over the finite field with q elements, represented by full rank $n \times n$ matrices over $\mathrm{GF}(q)$. The center of $\mathrm{GL}(n, q)$ is given by

$$\mathrm{Z}(\mathrm{GL}(n, q)) = \{aU_n \mid a \in \mathrm{GF}(q)^*\}$$

where $U_n = \mathrm{diag}(1, \ldots, 1)$ denotes the $n \times n$ unit matrix. The corresponding group

$$\mathrm{PGL}(n, q) := \overline{\mathrm{GL}(n, q)} = \mathrm{GL}(n, q)/\,\mathrm{Z}(\mathrm{GL}(n, q))$$

is called the *projective linear group* of $\mathrm{GF}(q)^n$.

Conjugacy classes in projective linear groups $\mathrm{PGL}(n, q)$ are well-studied and determined [4, 5].

Received : *02–08–2021,* ***Accepted :*** *08–09–2021*
*** Corresponding author***

Theorem 1.1. *The number of conjugacy classes of* $\mathrm{PGL}(3,q)$ *satisfies*

$$|\operatorname{Conj}(\mathrm{PGL}(3,q))| = \begin{cases} q^2+q+2 & \text{if 3 divides } q-1 \\ q^2+q & \text{otherwise.} \end{cases}$$

The goal of this paper to efficiently compute and list a set of representatives of conjugacy classes of $\mathrm{PGL}(3,q)$:

$$\operatorname{Rep}(\mathrm{PGL}(3,q)).$$

The proposed set of representatives $\operatorname{Rep}(\mathrm{PGL}(3,q))$ in this work can be constructed in $O(q^2)$ which is the complexity of the number of conjugacy classes. The set $\operatorname{Rep}(\mathrm{PGL}(3,q))$ is of particular interest e.g. for the construction and characterization of combinatorial objects in the projective place $\mathrm{PG}(2,q)$ with prescribed symmetries (see [1, 2, 3]). Hence, an efficient listing of all elements of $\operatorname{Rep}(\mathrm{PGL}(3,q))$ is desired.

Assuming that for a group G we have a transversal $\operatorname{Rep}(G)$ of conjugacy classes and we know the order $m = |\operatorname{Rep}(\overline{G})|$ we identify elements of $\operatorname{Rep}(G)$ that are equivalent with respect to $\simeq_{\overline{G}}$. We cancel out $\overline{G}$-equivalent elements from $\operatorname{Rep}(G)$ until m elements remain which finally define $\operatorname{Rep}(\overline{G})$.

2. Starting with the general linear group

Representatives of the conjugacy classes of $\mathrm{GL}(3,q)$ arise by matrices in rational canonical form for which three different types occur (folklore):

$$R_0(a,b,c) := \begin{pmatrix} 0 & 0 & -a \\ 1 & 0 & -b \\ 0 & 1 & -c \end{pmatrix},$$

$$R_1(a,b) := \begin{pmatrix} 0 & -ab & 0 \\ 1 & -(a+b) & 0 \\ 0 & 0 & -a \end{pmatrix},$$

$$R_2(a) := \begin{pmatrix} -a & 0 & 0 \\ 0 & -a & 0 \\ 0 & 0 & -a \end{pmatrix}.$$

To be precise we obtain the following result:

Lemma 2.1. *A set of representatives of conjugacy classes of* $\mathrm{GL}(3,q)$ *is given by the following set of matrices:*

$$\begin{aligned} \operatorname{Rep}(\mathrm{GL}(3,q)) = \{&R_0(a,b,c) \mid a \in \mathrm{GF}(q)^*, b,c \in \mathrm{GF}(q)\} \\ &\cup \{R_1(a,b) \mid a,b \in \mathrm{GF}(q)^*\} \\ &\cup \{R_2(a) \mid a \in \mathrm{GF}(q)^*\}. \end{aligned}$$

The three types of conjugacy classes correspond to the $\mathrm{GF}(q)[x]$ modules

$$\mathrm{GF}(q)[x]/(a+bx+cx^2+x^3),$$

$$\mathrm{GF}(q)[x]/(x+a) \oplus \mathrm{GF}(q)[x]/(x+a)(x+b),$$

$$\mathrm{GF}(q)[x]/(x+a) \oplus \mathrm{GF}(q)[x]/(x+a) \oplus \mathrm{GF}(q)[x]/(x+a).$$

Hence, the number of conjugacy classes of elements of $\mathrm{GL}(3,q)$ is given by

$$|\operatorname{Conj}(\mathrm{GL}(3,q))| = q^2(q-1)+(q-1)^2+(q-1)^3 = q^3-q.$$

When switching to the projective general linear group $\mathrm{PGL}(3,q)$, two representatives $X,Y \in \mathrm{GL}(3,q)$ of different conjugacy classes with respect to $\mathrm{GL}(3,q)$ are conjugated with respect to $\mathrm{PGL}(3,q)$, denoted by

$$X \simeq_{\mathrm{PGL}(3,q)} Y$$

if and only if they can be transformed into each other by

$$TXT^{-1}S = Y$$

with $T \in \mathrm{GL}(3,q)$ and $S \in \mathrm{Z}(\mathrm{GL}(3,q))$.

Starting with the three types $R_0(a,b,c)$, $R_1(a,b)$, and $R_2(a)$ of representatives of $\mathrm{GL}(3,q)$ we identify which of them are equivalent with respect to the relation $\simeq_{\mathrm{PGL}(3,q)}$ and determine a transversal $\mathrm{Rep}(\mathrm{PGL}(3,q)$.

Our basic tool is the following lemma:

Lemma 2.2. *The following equivalences hold:*

1. *For $a,t \in \mathrm{GF}(q)^*$ and $b,c \in \mathrm{GF}(q)$:*
$$R_0(a,b,c) \simeq_{\mathrm{PGL}(3,q)} R_0(at^3, bt^2, ct).$$
2. *For $a,b,t \in \mathrm{GF}(q)^*$:*
$$R_1(a,b) \simeq_{\mathrm{PGL}(3,q)} R_1(at, bt).$$
3. *For $a,t \in \mathrm{GF}(q)^*$:*
$$R_2(a) \simeq_{\mathrm{PGL}(3,q)} R_2(at).$$

Proof. The following transformations prove the equivalences

$$R_0(at^3, bt^2, ct) = TR_0(a,b,c)T^{-1}S \quad \text{with} \quad T = \mathrm{diag}(t,1,t^{-1}), \quad S = tU_3,$$
$$R_1(at, bt) = TR_1(a,b)T^{-1}S \quad \text{with} \quad T = \mathrm{diag}(t,1,1), \quad S = tU_3,$$
$$R_2(at) = TR_2(a)T^{-1}S \quad \text{with} \quad T = U_3, \quad S = tU_3.$$

□

Corollary 2.1. *The following equivalences hold:*

1. *For $a,b \in \mathrm{GF}(q)^*$:*
$$R_1(a,b) \simeq_{\mathrm{PGL}(3,q)} R_1(1, ba^{-1}).$$
2. *For $a \in \mathrm{GF}(q)^*$:*
$$R_2(a) \simeq_{\mathrm{PGL}(3,q)} R_2(-1) = U_3.$$

Proof. The result for the first equivalence follows from the previous lemma with $t := a^{-1}$ and for the second equivalence with $t := -a^{-1}$. □

3. Transversal of conjugacy classes of $\mathrm{PGL}(3,q)$

In this section we describe $\mathrm{Rep}(\mathrm{PGL}(3,q))$. Depending on how $q-1$ is divisible by 2 and 3, respectively, we obtain different versions of $\mathrm{Rep}(\mathrm{PGL}(3,q))$ in some parts.

We start with the condition $3 \nmid (q-1)$: The mapping

$$f_3 : \mathrm{GF}(q)^* \to \mathrm{GF}(q)^*, a \mapsto a^3$$

is bijective and we get

$$\mathrm{Im}(f_3) = \{f_3(a) \mid \mathrm{GF}(q)^*\} = \mathrm{GF}(q)^*.$$

Therefore, all elements $r \in \mathrm{GF}(q)^*$ have a unique preimage $s \in \mathrm{GF}(q)^*$ such that $f_3(s) = s^3 = r$. In this case we use the notation

$$\sqrt[3]{r} := s.$$

Lemma 3.1. *Let $3 \nmid (q-1)$. For $a \in \mathrm{GF}(q)^*$ and $b,c \in \mathrm{GF}(q)$ holds:*

$$R_0(a,b,c) \simeq_{\mathrm{PGL}(3,q)} R_0(1, b(\sqrt[3]{a^{-1}})^2, c\sqrt[3]{a^{-1}}).$$

Proof. In the first equivalence of Lemma 2.2 we use for t the value $t = \sqrt[3]{a^{-1}}$. Then at^3 yields 1. □

Theorem 3.1. *Let $3 \nmid (q-1)$. Then the following set of matrices is a transversal of conjugacy classes of elements of* $\mathrm{PGL}(3, q)$*:*

$$\begin{aligned} T_1(q) = \{R_0(1, a, b) \mid a, b \in \mathrm{GF}(q)\} \\ \cup \{R_1(1, a) \mid a \in \mathrm{GF}(q)^*\} \\ \cup \{R_2(-1)\}. \end{aligned}$$

Proof. According to Corollary 2.1 and Lemma 3.1 any element $A \in \mathrm{PGL}(3, q)$ is conjugated to one of the three matrices $R_0(1, a, b)$ for $a, b \in \mathrm{GF}(q)$, $R_1(1, a)$ for $a \in \mathrm{GF}(q)^*$, or $R_2(-1)$. We define $T_1(q)$ as the set of all possible combinations of the three matrices which are exactly $q^2 + (q-1) + 1 = q^2 + 2$ which is according to Theorem 1.1 exactly the number of conjugacy classes of $\mathrm{PGL}(3, q)$. Hence, $T_1(q)$ is a required transversal of $\mathrm{Conj}(\mathrm{PGL}(3, q))$. □

Example 3.1. For $q = 3$ we obtain the following transversal:

$$\begin{aligned} T_1(3) = \{ & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \\ & \begin{pmatrix} 0 & 2 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \}. \end{aligned}$$

Next, we consider the second case that $3 \mid (q-1)$. We use the following results:

Lemma 3.2. *For all $a, c \in \mathrm{GF}(q)^*$ and $b \in \mathrm{GF}(q)$ we have*

$$R_0(a, b, c) \simeq_{\mathrm{PGL}(3,q)} R_0(ac^{-3}, bc^{-2}, 1).$$

Proof. The lemma follows directly from the first item of Lemma 2.2. We just substitute $t := c^{-1}$. □

Now $d \mid (q-1)$ and if β is a primitive element of $\mathrm{GF}(q)^*$ the image of the following mapping

$$f_d : \mathrm{GF}(q)^* \mapsto \mathrm{GF}(q)^*, a \mapsto a^d$$

satisfies:

$$\begin{aligned} \mathrm{Im}(f_d) &= \{\beta^{dk \bmod q-1} \mid 0 \le k < q-1\} \\ &= \{\beta^{dk} \mid 0 \le k < \frac{q-1}{d}\}. \end{aligned}$$

From that fact together with Lemma 2.2 we obtain:

Corollary 3.1. *Let $3 \mid (q-1)$. For all $a \in \mathrm{GF}(q)^*$ and $r \in \mathrm{Im}(f_3)$ we have:*

$$R_0(a, 0, 0) \simeq_{\mathrm{PGL}(3,q)} R_0(ar, 0, 0).$$

Rewriting this equivalence with a primitive element β of $\mathrm{GF}(q)^*$ we obtain for $3 \mid (q-1)$ the equivalence

$$R_0(\beta^i, 0, 0) \simeq_{\mathrm{PGL}(3,q)} R_0(\beta^{i+3k \bmod q-1}, 0, 0)$$

for all $0 \le i, k < q-1$. On the other hand side the inequivalence

$$R_0(\beta^i, 0, 0) \not\simeq_{\mathrm{PGL}(3,q)} R_0(\beta^j, 0, 0)$$

implies that i and j must lie in different orbits of the group action

$$\langle 3 \rangle \times \mathbb{Z}_{q-1} \to \mathbb{Z}_{q-1}, (3k, i) \mapsto i + 3k \bmod q-1.$$

A set of representatives is given by
$$\{i \mid 0 \leq i < 3\}.$$

Moreover, for $2 \nmid (q-1)$, i.e. if $\mathrm{GF}(q)$ is a finite field of characteristic 2, the mapping f_2 is the Frobenius automorphism
$$f_2 : \mathrm{GF}(q)^* \to \mathrm{GF}(q)^*, a \mapsto a^2$$
with
$$\mathrm{Im}(f_2) = \mathrm{GF}(q)^*.$$
Therefore square roots exist, i.e. for each $r \in \mathrm{GF}(q)^*$ have a unique preimage $s \in \mathrm{GF}(q)^*$ such that $f_2(s) = s^2 = r$. In this case we use the notation
$$\sqrt[2]{r} := s.$$

Corollary 3.2. *Let $2 \nmid (q-1)$. For all $a, b \in \mathrm{GF}(q)^*$ we get*
$$R_0(a, b, 0) \simeq_{\mathrm{PGL}(3,q)} R_0(a(\sqrt[2]{b^{-1}})^3, 1, 0).$$

Proof. It directly follows from the first item of Lemma 2.2 by substituting $t := \sqrt[2]{b^{-1}}$ and $c := 0$. □

Putting the previous previous three lemmas and corollaries together we obtain the following inequivalent representatives

Theorem 3.2. *Let $2 \nmid (q-1)$, $3 \mid (q-1)$, and let β a primitive element of the finite field $\mathrm{GF}(q)^*$. Then the following set of matrices is a transversal of conjugacy classes of elements of $\mathrm{PGL}(3, q)$:*
$$\begin{aligned} T_2(q) = &\{R_0(a, b, 1) \mid a \in \mathrm{GF}(q)^*, b \in \mathrm{GF}(q)\} \\ &\cup \{R_0(\beta^i, 0, 0) \mid 0 \leq i < 3\} \\ &\cup \{R_0(a, 1, 0) \mid a \in \mathrm{GF}(q)^*\} \\ &\cup \{R_1(1, a) \mid a \in \mathrm{GF}(q)^*\} \\ &\cup \{R_2(-1)\}. \end{aligned}$$

Proof. Analogously to Theorem 3.1 we just have to count the elements in $T_2(q)$. Its cardinality is $q(q-1) + 3 + (q-1) + (q-1) + 1 = q^2 + q + 2$ which is exactly the required cardinality of $\mathrm{Conj}(\mathrm{PGL}(3, q))$ for the case that 3 divides $q - 1$. □

Finally, we consider the remaining case $2 \mid (q-1)$, $3 \mid (q-1)$. Again from Lemma 2.2 we get
$$R_0(a, b, 0) \simeq_{\mathrm{PGL}(3,q)} R_0(at^3, bt^2, 0)$$
for all $a, b, t \in \mathrm{GF}(q)^*$. In terms of a primitive element β of $\mathrm{GF}(q)^*$ this equivalence can be reformulated as
$$R_0(\beta^i, \beta^j, 0) \simeq_{\mathrm{PGL}(3,q)} R_0(\beta^{i+3k \bmod q-1}, \beta^{j+2k \bmod q-1}, 0)$$
for $0 \leq i, j, k < q - 1$. Therefore the inequivalence
$$R_0(\beta^i, \beta^j, 0) \simeq_{\mathrm{PGL}(3,q)} R_0(\beta^s, \beta^t, 0)$$
implies that the pairs (i, j) and (s, t) must be contained in different orbits of the action group action
$$\langle(3, 2)\rangle \times \mathbb{Z}_{q-1}^2 \to \mathbb{Z}_{q-1}, ((3k, 2k), (i, j)) \mapsto (i + 3k \bmod q - 1, j + 2k \bmod q - 1)$$
A set of representatives of the orbits of this group action is given by
$$\{(i, j) \mid 0 \leq i < 3, 0 \leq j < \frac{q-1}{3}\}.$$

Hence we obtain:

Theorem 3.3. *Let $2 \mid (q-1)$, $3 \mid (q-1)$, and let β a primitive element of the finite field $\mathrm{GF}(q)^*$. Then the following set of matrices is a transversal of conjugacy classes of elements of $\mathrm{PGL}(3,q)$:*

$$\begin{aligned} T_3(q) = &\{R_0(a,b,1) \mid a \in \mathrm{GF}(q)^*, b \in \mathrm{GF}(q)\} \\ &\cup \{R_0(\beta^i,\beta^j,0) \mid 0 \le i < 3, 0 \le j < \frac{q-1}{3}\} \\ &\cup \{R_0(\beta^i,0,0) \mid i \in 0 \le i < 3\} \\ &\cup \{R_1(1,a) \mid a \in \mathrm{GF}(q)^*\} \\ &\cup \{R_2(-1)\}. \end{aligned}$$

Proof. Again we only have to show that the cardinalities fit: $T_3(q)$ contains exactly $q(q-1) + 3 \cdot \frac{q-1}{3} + 3 + (q-1) + 1 = q^2 + q + 2$ elements. □

In order to summarize the results we obtain the final corollary:

Corollary 3.3. *For any prime power q the set*

$$T(q) = \begin{cases} T_1(q) & \text{if } 3 \nmid (q-1) \\ \begin{cases} T_2(q) & \text{if } 2 \nmid (q-1) \\ T_3(q) & \text{otherwise} \end{cases} & \text{otherwise} \end{cases}$$

defines a transversal of conjugacy classes of elements of $\mathrm{PGL}(3,q)$ that can be obtained in $O(q^2)$.

Acknowledgements

The authors would like to express their sincere thanks to the editor and the anonymous reviewers for their helpful comments and suggestions.

Funding

There is no funding for this work.

Competing interests

The authors declare that they have no competing interests.

References

[1] Ball, S., Hirschfeld, J.W.P.: *Bounds on (n,r)-Arcs and their Application to Linear Codes*. Finite Fields and Their Applications. **3**, 326–336 (2005).
[2] Braun, M.: *New Lower Bounds on the Size of (n,r)-Arcs in $PG(2,q)$*. Journal of Combinatorial Designs. **27**, 682-687 (2019).
[3] Hirschfeld, J.W.P., Storme, L.: The Packing Problem in Statistics, Coding Theory and Finite Projective Spaces: Update 2001, pages 201–246. Springer US, Boston, MA. (2001).
[4] MacDonald, I.G.: *Numbers of Conjugacy Classes in Some Finite Classical Groups*. Bulletin of the Australian Mathematical Society. **23**, 23–48 (1981).
[5] Wall, G.E.: *Conjugacy Classes in Projective and Special Linear Groups*. Bulletin of the Australian Mathematical Society. **22**, 339–364 (1980).

Affiliations

MICHAEL BRAUN
ADDRESS: Faculty of Computer Science, University of Applied Sciences, Darmstadt, Germany
E-MAIL: michael.braun@h-da.de
ORCID ID: 0000-0001-9816-2216