Short presentations for three-dimensional unitary groups

Alexander Hulpke and Ákos Seress*
Department of Mathematics
The Ohio State University
231 West 18th Avenue
Columbus, OH 43202, USA

Abstract

We give a presentation of length $O\left(\log^2|G|\right)$ for the groups $G \cong \mathrm{PSU}_3(q)$. This result has applications in recent algorithms to compute the structure of permutation groups and matrix groups.

1 Introduction

A *presentation* for a group is a description by generators and relators. The *length* of a presentation is the number of symbols required to write the presentation; we count each generator as a single symbol, and allow the relators to use powers of the generators. The exponents are written in binary form, and the length of g^e is $1+\log_2(e)$.

In [BGK+97], Babai, Goodman, Kantor, Luks, and Pálfy gave presentations of length $O\left(\log^2|G|\right)$ for all finite simple groups G, except the rank one groups of Lie type $\mathrm{PSU}_3(q) = {}^2A_2(q)$, ${}^2B_2(2^{2m+1})$, and ${}^2G_2(3^{2m+1})$. This result has applications in fast computations with permutation groups and matrix groups [KS99, KS01, KS]. In order to extend these computational results to input groups which have composition factors isomorphic to the aforementioned three types of rank one groups, it is necessary to give presentations which are of polylogarithmic

*Research partially supported by the NSF.

length in the group order in these groups as well. Short presentations for these groups also would prove a conjecture of Mann [Man98] about the number of groups with a presentation of given length.

Recently, J. Thompson (personal communication to W. Kantor) observed that Suzuki's original paper [Suz62, p. 128] characterizing the groups ${}^2B_2(2^{2m+1})$ contains a presentation of length $O\left(\log^2|G|\right)$ for these groups. The purpose of this note is to prove a similar result for the groups $\mathrm{PSU}_3(q)$.

Theorem 1. *The finite simple group $G = \mathrm{PSU}_3(q)$ has a presentation of length $O\left(\log^2|G|\right)$.*

It was known already that a presentation for the Borel subgroup and q extra relations suffice to present $\mathrm{PSU}_3(q)$. We give in Lemma 13 a presentation of length $O\left(\log^2 q\right)$ for the Borel subgroup and show in Lemma 14 and Theorems 15, 16 how to reduce the q extra relations to a constant number.

We remark that the same asymptotic result can be achieved if the powers of the generators are not allowed in the presentation. For each occurrence of a power x^n in the presentation indicated in Theorem 1, let $n = \sum_{i=0}^{k} \varepsilon_i 2^i$ be the binary decomposition of n with $\varepsilon_i \in \{0,1\}$. We add new symbols $x_0, x_1, x_2, \ldots, x_k, y_{-1}, y_0, y_1, \ldots, y_k$ to the generating set and the relators $x = x_0$, $x_{i+1} = x_i \cdot x_i$ for $i = 0, 1, \ldots, k-1$ and $y_{-1} = 1$, $y_{j+1} = \begin{cases} y_j & \text{if } \varepsilon_{j+1} = 0, \\ y_j \cdot x_{j+1} & \text{if } \varepsilon_{j+1} = 1, \end{cases}$ for $j = -1, 0, \ldots, k-1$. Then x^n can be replaced by y_k in the original relators containing x^n.

2 The structure of $\mathrm{PSU}_3(q)$

Let $q = p^l$ be a prime power and take $\mathrm{GU}_3(q)$ the group of all 3×3 invertible matrices over $\mathrm{GF}(q^2)$ that preserve the hermitian form

$$\omega := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

i.e., $\mathrm{GU}_3(q) = \{A \in \mathrm{GL}_3(q^2) \mid A\omega\overline{A}^t = \omega\}$. Here $\overline{A}$ denotes the matrix obtained from A by raising each entry to the qth power. We will describe elements of $G = \mathrm{PSU}_3(q)$ via matrix representatives modulo scalars.

Our notation now follows [Suz65]: G has a maximal parabolic subgroup $\langle Q,k\rangle$ where Q and k are represented by the matrices

$$Q=\left\{u(x,y)=\begin{pmatrix}1&0&0\\ y&1&0\\ x&-y^q&1\end{pmatrix}\;\middle|\;x,y\in \mathrm{GF}(q^2), x+x^q+y^{q+1}=0\right\}$$

and

$$k=\mathrm{diag}(\rho):=\begin{pmatrix}\rho&0&0\\ 0&\rho^{q-1}&0\\ 0&0&\rho^{-q}\end{pmatrix},$$

where ρ is a generator of the multiplicative group $\mathrm{GF}(q^2)^*$ of $\mathrm{GF}(q^2)$.

We remark that, similarly to the notation $\bar{A}$ above, it is customary to denote w^q by $\bar{w}$ for elements of $\mathrm{GF}(q^2)$. However, since we have to work with a variety of powers besides w^q, we shall use the power notation for all powers.

Note that $|k|=(q^2-1)/\gcd(3,q+1)$ in G and $|Q|=q^3$. We observe that k normalizes Q and that $\langle Q,k\rangle$ is a solvable group. The projection $\mathrm{SU}_3(q)\to\mathrm{PSU}_3(q)$ is injective on Q and we can thus identify Q with the set of matrices $u(x,y)$.

The centre of Q is

$$Z(Q)=\left\{\begin{pmatrix}1&0&0\\ 0&1&0\\ x&0&1\end{pmatrix}\;\middle|\;x\in\mathrm{GF}(q^2), x+x^q=0\right\}$$

and is therefore elementary abelian of order q. The factor group $Q/Z(Q)$ is elementary abelian of order q^2. Hence $\langle Q,k\rangle$ has a generator set $\{u_1,\dots,u_{3l},k\}$ where $Z(Q)=\langle u_1,\dots,u_l\rangle$ and it has a presentation $F=\langle\hat{u}_1,\dots,\hat{u}_{3l},\hat{k}\mid\mathcal{R}\rangle$ such that the map $\psi\colon\hat{k}\mapsto k$, $\hat{u}_i\mapsto u_i$ $(1\le i\le 3l)$ is an isomorphism between F and $\langle Q,k\rangle$. We shall prove in Lemma 13 that $u_1,\dots,u_{3l}$ can be chosen so that $F=\langle\hat{u}_1,\dots,\hat{u}_{3l},\hat{k}\mid\mathcal{R}\rangle$ has length $O\left(\log^2|\langle Q,k\rangle|\right)=O\left(\log^2|G|\right)$.

Every $u\in\langle Q,k\rangle$ can be written uniquely in the form $u=\left(\prod_{i=1}^{3l}u_i^{\alpha_i}\right)k^\alpha$ with $0\le\alpha<|k|$, $0\le\alpha_i<p$. We call the corresponding word $\mathrm{dec}(u)=\left(\prod_{i=1}^{3l}\hat{u}_i^{\alpha_i}\right)\hat{k}^\alpha$ the *decomposition* of u (with respect to the generating system $(u_1,\dots,u_{3l},k)$).

The action of G on the cosets of $\langle Q,k\rangle$ is doubly transitive. The group G is therefore generated by $\langle Q,k\rangle$ and one extra element, for which we choose

$$t=\begin{pmatrix}0&0&1\\ 0&-1&0\\ 1&0&0\end{pmatrix}.$$

We also note that the subgroup Q acts regularly on the cosets different from $\langle Q,k\rangle$. This means that every element of G is either in $\langle Q,k\rangle$, or can be written in the form $a\cdot t\cdot b$ with $a\in\langle Q,k\rangle$ and $b\in Q$. Furthermore $k^t=k^{-q}$, thus t normalizes $\langle k\rangle$. Therefore for every $u\in Q\setminus\{1\}$ there are $g(u),f(u)\in Q$ and $h(u)\in\langle k\rangle$ such that

$$u^t = g(u)\ h(u)\ t\ \ f(u). \tag{2}$$

If we take an element of $Q\setminus\{1\}$

$$u=u(x,y)=\begin{pmatrix}1&0&0\\ y&1&0\\ x&-y^q&1\end{pmatrix}$$

in matrix form, we can compute $g(u)$, $h(u)$, $f(u)$ and u^k explicitly as

$$g(u)=\begin{pmatrix}1&0&0\\ -y/x&1&0\\ 1/x&y^q/x^q&1\end{pmatrix},\qquad h(u)=\begin{pmatrix}x&0&0\\ 0&x^{q-1}&0\\ 0&0&x^{-q}\end{pmatrix},$$

$$f(u)=\begin{pmatrix}1&0&0\\ -y/x^q&1&0\\ 1/x&y^q/x&1\end{pmatrix},\qquad u^k=\begin{pmatrix}1&0&0\\ y\rho^{2-q}&1&0\\ x\rho^{q+1}&-y^q\rho^{2q-1}&1\end{pmatrix}.$$

We want to write a presentation for $\mathrm{PSU}_3(q)$ using a generating set $\{\hat{u}_1,\dots,\hat{u}_{3l},\hat{k}\}$ corresponding to the generators of $\langle Q,k\rangle$ and a generator $\hat{t}$ corresponding to t. Its relators will contain the relations $\mathcal{R}$ for $\langle Q,k\rangle$, the relations $\hat{t}^2=1$ and $\hat{t}\,\hat{k}\,\hat{t}=\hat{k}^{-q}$ as well as extra relations of the form $\mathrm{dec}\big(u\big)^{\hat{t}}=\mathrm{dec}\big(g(u)h(u)\big)\hat{t}\,\mathrm{dec}\big(f(u)\big)$ for some elements $u\in Q$. If $3\not|\,q+1$ then we will need 3 extra relations and if $3\,|\,q+1$ then we will need 7 extra relations.

Definition 3. For a set of elements $a_1,\dots,a_m\in Q\setminus\{1\}$, we define a finitely presented group $P(a_1,\dots,a_m)$ as follows.

$$P(a_1,\dots,a_m):=$$
$$\Big\langle \hat{k},\hat{u}_1,\dots,\hat{u}_{3l},\hat{t}\ \ \Big|\ \ \mathcal{R},\quad \hat{t}^2=1,\hat{t}\,\hat{k}\,\hat{t}=\hat{k}^{-q},$$
$$\hat{t}\,\mathrm{dec}\big(a_i\big)\hat{t}=\mathrm{dec}\big(g(a_i)h(a_i)\big)\hat{t}\,\mathrm{dec}\big(f(a_i)\big)\quad (1\le i\le m)\Big\rangle$$

Since the length of the relators of the form

$$\hat{t}\,\mathrm{dec}\big(a_i\big)\hat{t} = \mathrm{dec}\big(g(a_i)h(a_i)\big)\hat{t}\,\mathrm{dec}\big(f(a_i)\big)$$

is $O(\log q)$, Lemma 13 implies that the length of the presentation in Definition 3 is $O\big(\log^2 q + m\log q\big)$.

For a given finitely presented group $P(a_1,\dots,a_m)$ and $u \in Q\setminus\{1\}$, we consider the following condition analogous to (2):

There are $f(u), g(u) \in Q$, $h(u) \in \langle k\rangle$ such that

$$\hat{t}\,\mathrm{dec}\big(u\big)\hat{t} = \mathrm{dec}\big(g(u)\big)\mathrm{dec}\big(h(u)\big)\hat{t}\,\mathrm{dec}\big(f(u)\big) \qquad (4)$$

holds in $P(a_1,\dots,a_m)$.

The following Lemmas 5 and 7 are well known (their statement is found implicitly in [Ste81] and [BGK$^+$97]).

Lemma 5. *For every set $\{a_1,\dots,a_m\} \subset Q\setminus\{1\}$, the map $\hat{k}\mapsto k$, $\hat{u}_i \mapsto u_i$, $\hat{t}\mapsto t$ is an epimorphism from $P(a_1,\dots,a_m)$ onto* $\mathrm{PSU}_3(q)$.

If condition (4) *is fulfilled in $P(a_1,\dots,a_m)$ for every $u \in Q\setminus\{1\}$ then this epimorphism is an isomorphism and the presentation will define* $\mathrm{PSU}_3(q)$.

The proof of Lemma 5 is based on the observation that if (4) holds for every $u \in Q\setminus\{1\}$ then for any $u_1,u_2,u_3,u_4 \in Q$ and integers e, f, the product $\big(\mathrm{dec}\big(u_1\big)\hat{k}^e\hat{t}\,\mathrm{dec}\big(u_2\big)\big)\cdot\big(\mathrm{dec}\big(u_3\big)\hat{k}^f\hat{t}\,\mathrm{dec}\big(u_4\big)\big)$ can be written in $P(a_1,\dots,a_m)$ in the form $\mathrm{dec}\big(u_5\big)\hat{k}^c\hat{t}\,\mathrm{dec}\big(u_6\big)$ for suitable $u_5,u_6 \in Q$ and integer c. The precise argument is similar to the proof of Lemma 14, which we shall give in full detail.

However, to keep the presentation for $\mathrm{PSU}_3(q)$ short, we cannot add relators of the form (4) for every $u \in Q$. Instead we will use only a few relators of the form (4) and will have to show that these suffice to prove (4) for every $u \in Q$.

Definition 6. If G is a group, $g \in G$, and $U \le G$, then *the U-class of g* is the orbit of g under conjugation by U.

Lemma 7. *Suppose that* (4) *holds for some $u \in Q$ in $P(a_1,\dots,a_m)$. Then* (4) *holds for each element of the $\langle k\rangle$-class of u.*

Again, the proof is similar to the proof of Lemma 14.

Lemma 7 implies that if $\{a_1,\dots,a_m\}$ is a set of representatives of the $\langle k\rangle$-classes in Q, then $P(a_1,\dots,a_m) \cong \mathrm{PSU}_3(q)$. However, this presentation is still too long.

3 $\langle k \rangle$-classes

To reduce the number of class representatives needed, we will investigate the $\langle k \rangle$-classes on Q in more detail. Let $S := \{s \in \mathrm{GF}(q^2) \mid s + s^q = 0\}$. Then $Z(Q) = \{u(s,0) \mid s \in S\}$, S is an additive subgroup of $\mathrm{GF}(q^2)$, and S^* is a coset of $\mathrm{GF}(q)^*$ in $\mathrm{GF}(q^2)^*$ satisfying $(S^*)^2 = \mathrm{GF}(q)^*$.

Lemma 8. *Let $0 \neq \xi \in S$. Then every nonidentity element of $Z(Q)$ is conjugate under $\langle k \rangle$ to $u(\xi,0)$.*

Proof. Let $0 \neq s \in S$. Then

$$\left(\frac{\xi}{s}\right)^q = \frac{\xi^q}{s^q} = \frac{-\xi}{-s} = \frac{\xi}{s},$$

and so $\xi/s \in \mathrm{GF}(q)$. We can thus find an exponent e such that $(\rho^e)^{q+1} = s/\xi$. Accordingly, k^e will conjugate $u(\xi,0)$ to $u(s,0)$. □

Lemma 9. *Consider elements $u(x,y), u(w,z) \in Q$ (thus $x + x^q + y^{q+1} = 0$, $w + w^q + z^{q+1} = 0$) with $x,y,w,z \neq 0$.*
(a) If $3 \not| q+1$ then $u(x,y)$ and $u(w,z)$ are conjugate under $\langle k \rangle$ if and only if $w/x \in \mathrm{GF}(q)$.
(b) If $3 \,|\, q+1$ then $u(x,y)$ and $u(w,z)$ are conjugate under $\langle k \rangle$ if and only if $w/x \in \mathrm{GF}(q)$ and $z/y = \rho^{3i}$ for some integer i.

Proof. We have $\langle k \rangle = \{\mathrm{diag}(\sigma) \mid \sigma \in \mathrm{GF}(q^2)^*\}$. Assume first that

$$u(w,z) = u(x,y)^{\mathrm{diag}(\sigma)} = u(x\,\sigma^{q+1}, y\,\sigma^{2-q}).$$

Then $w/x = \sigma^{q+1} \in \mathrm{GF}(q)$. If $3 \,|\, q+1$ then $3 \,|\, 2-q$ and so $\sigma^{2-q} = z/y$ is a third power.

Conversely, suppose that $w/x \in \mathrm{GF}(q)$ and, in the case $3 \,|\, q+1$, $z/y = \rho^{3i}$ for some integer i. First we show that there is a $\sigma \in \mathrm{GF}(q^2)^*$ with $\sigma^{2-q} = z/y$. Note that $\gcd(q^2-1, 2-q) = \gcd(3, 2-q)$. If $3 \not| q+1$, we therefore have that $\gcd(q^2-1, 2-q) = 1$ which guarantees the existence of such a σ.
If $3 \,|\, q+1$ and so $z/y = \rho^{3i}$ then let $\sigma = \rho^{i(q+2)}$. Then

$$\sigma^{2-q} = \rho^{i(q+2)(2-q)} = \rho^{i(-q^2+1+3)} = \rho^{3i} = z/y.$$

Next we claim that if $\sigma^{2-q} = z/y$, then $u(x,y)^{\mathrm{diag}(\sigma)} = u(w,z)$. We have that

$$u(x,y)^{\mathrm{diag}(\sigma)} = u(x\,\sigma^{q+1}, y\,\sigma^{2-q}) = u(x\,\sigma^{q+1}, z) \in Q.$$

Hence, denoting $w/x \in \mathrm{GF}(q)$ by a, we get:

$$\begin{aligned}(x+x^q)\sigma^{q+1} &= x\sigma^{q+1} + (x\sigma^{q+1})^q = -z^{q+1} = w + w^q \\ &= ax + (ax)^q = (x+x^q)a.\end{aligned}$$

As $x+x^q = -y^{q+1} \neq 0$, we deduce that $a = \sigma^{q+1}$. Therefore $u(x,y)^{\mathrm{diag}(\sigma)} = u(w,z)$ as claimed. □

Lemma 10. *Let $x \in \mathrm{GF}(q^2) \setminus S$ and let C be a coset of $\mathrm{GF}(q)^*$ in $\mathrm{GF}(q^2)^*$, different from S^*. Then there exists $s \in S$ such that $x+s \in C$.*

Proof. Let $c \in C$ and $v \in S^*$. As S is a $\mathrm{GF}(q)$-subspace of $\mathrm{GF}(q^2)$ and $x \notin S$, $\{v,x\}$ is a $\mathrm{GF}(q)$-basis for $\mathrm{GF}(q^2)$ and so we have $c = \alpha x + \beta v$ with $\alpha, \beta \in \mathrm{GF}(q)$. Here $\alpha \neq 0$ because $c \notin S$. Let $s := \beta v/\alpha \in S$. Then $x+s = x+\beta v/\alpha = c/\alpha \in C$. □

Lemma 11. *Assume that $3 \nmid q+1$ and $u(x,v) \in Q \setminus Z(Q)$. Then for any $\langle k \rangle$-class $K \subseteq Q \setminus Z(Q)$ there exists $u(s,0) \in Z(Q)$ such that $u(x,v) \cdot u(s,0) \in K$.*

Proof. The condition $u(x,v) \notin Z(Q)$ implies that $x + x^q = -v^{q+1} \neq 0$, so $x \notin S$. By Lemma 9 (a), the class K consists of those $u(x',y)$ for which x' belongs to the same fixed coset C of $\mathrm{GF}(q)^*$ in $\mathrm{GF}(q^2)^*$. Since $K \not\subseteq Z(Q)$, we have that $C \neq S^*$ and Lemma 10 implies that $x+s \in C$ for some $s \in S$. Then $u(x,v) \cdot u(s,0) = u(x+s,v) \in K$. □

The analogous statement for the case $3 \mid q+1$ is:

Lemma 12. *Assume that $3 \mid q+1$. Let $x \in \mathrm{GF}(q^2) \setminus S$ and let C be a coset of $\mathrm{GF}(q)^*$ in $\mathrm{GF}(q^2)^*$ different from S^*. Moreover, for $j = 0,1,2$, let $K_j = \{u(c,y_j) \mid c \in C, y_j \in \rho^j\langle\rho^3\rangle, c + c^q + y_j^{q+1} = 0\}$. (By the characterization in Lemma 9 (b), these sets are $\langle k \rangle$-classes.)*

Then there exist $v_j \in \rho^j\langle\rho^3\rangle$ for $j = 0,1,2$ such that $x + x^q + v_j^{q+1} = 0$ and, for any such v_0, v_1, v_2, there exists $u(s,0) \in Z(Q)$ such that $u(x,v_j) \cdot u(s,0) \in K_j$ for $0 \leq j \leq 2$.

Proof. Let $v \in \mathrm{GF}(q^2)$ such that $x + x^q + v^{q+1} = 0$. Then $x + x^q + (v\rho^{q-1})^{q+1} = 0$ and $x + x^q + (v\rho^{2(q-1)})^{q+1} = 0$ as well. Moreover, since $3 \nmid q-1$, the three elements $v, v\rho^{q-1}, v\rho^{2(q-1)}$ are in different cosets of $\langle\rho^3\rangle$ and so we can choose them as v_0, v_1, v_2.

The second statement of the lemma follows from the fact that, by Lemma 10, there is an $s \in S$ such that $x+s \in C$. Then $u(x,v_j) \cdot u(s,0) = u(x+s,v_j) \in K_j$. □

Every solvable group H has a power-commutator presentation of length $O\left(\log^3 |H|\right)$ [LNS84]; hence $\langle Q,k\rangle$ has a presentation of length $O\left(\log^3 q\right)$. However, for a suitable choice of generators, a subset of the commutator relations suffices and achieves a presentation for $\langle Q,k\rangle$ of length $O\left(\log^2 q\right)$.

Lemma 13. *The group $\langle Q,k\rangle$ has a presentation $F = \langle \hat{u}_1,\ldots,\hat{u}_{3l},\hat{k} \mid \mathcal{R}\rangle$ of length $O\left(\log^2 q\right)$.*

Proof. Suppose first that $3 \not| q+1$. We choose generators for a power-commutator presentation such that $u_1,\ldots,u_l$ generate $Z(Q)$ and $u_{l+1},\ldots,u_{3_l}$ generate $Q/Z(Q)$; moreover, $u_2,\ldots,u_l$ are $\langle k\rangle$-conjugate to u_1 and $u_{l+2},\ldots,u_{3l}$ are $\langle k\rangle$-conjugate to u_{l+1}. By Lemma 8 and 9(a), we can achieve this by setting $u_i := u(s_i,0)$ $(1 \le i \le l)$ for a generating set $\{s_1,\ldots,s_l\}$ of the additive subgroup S of $\mathrm{GF}(q^2)$, and setting $u_i = u(x_i,\rho^{i-l})$ $(i > l)$ for suitable x_i.

The subgroups $\langle u_1,\ldots,u_i\rangle$ $(1 \le i \le 3l)$ form a subnormal series of Q. We write a presentation for $\langle Q,k\rangle$ in a generator set $\{\hat{u}_1,\ldots\hat{u}_{3l},\hat{k}\}$ corresponding to the generators $\{u_1,\ldots,u_{3l},k\}$. Let $\hat{Q} = \langle \hat{u}_1,\ldots,\hat{u}_{3l}\rangle$.

The relation set $\mathcal{R}$ for this presentation consists of the power relations $\hat{u}_i^p = 1$ $(1 \le i \le 3l)$ and $k^{q^2-1} = 1$; commutator relations $[\hat{u}_1,\hat{u}_i] = 1$ $(2 \le i \le 3l)$, $[\hat{u}_{l+1},\hat{u}_i] = \mathrm{dec}\left([u_{l+1},u_i]\right)$ $(l+2 \le i \le 3l)$, and $[\hat{u}_i,\hat{k}] = \mathrm{dec}\left([u_i,k]\right])$ $(1 \le i \le 3l)$; as well as relations $\hat{u}_1 = \hat{u}_i^{\hat{k}^{e_i}}$ $(2 \le i \le l)$ and $\hat{u}_{l+1} = \hat{u}_i^{\hat{k}^{e_i}}$ $(l+2 \le i \le 3l)$ that show that the generators u_i lie in two $\langle k\rangle$-orbits.

The relations imply that $\hat{u}_1 \in Z(\hat{Q})$. In particular, $\hat{u}_1$ commutes with $\hat{u}_j^{\hat{k}^{-e_i}}$ for $2 \le i \le l$ and $1 \le j \le 3l$; conjugating by $\hat{k}^{e_i}$, we obtain that $\hat{u}_i \in Z(\hat{Q})$ for $2 \le i \le l$. Similarly, using the commutator identity $[a,bc] = [a,c][a,b]^c$, we can deduce the relation $[\hat{u}_{l+1},\mathrm{dec}\left(u_j^{k^{-e_i}}\right)] = \mathrm{dec}\left([u_{l+1},u_j^{k^{-e_i}}]\right)$ for $l+2 \le i \le 3l$ and $l+1 \le j \le 3l$. Conjugating by $\hat{k}^{e_i}$, we obtain the remaining commutator relations among the $\hat{u}_i$. Thus $\mathcal{R}$ implies a full power-commutator presentation.

If $3 \mid q+1$ then $u_1,\ldots,u_l$ are defined as above, but for $l+1 \le i \le 3l$ we require that $u_i = u(x_i,\rho^{i-l})$ is conjugate under $\langle k\rangle$ to one of u_{l+1}, u_{l+2}, u_{l+3}. In the presentation $\mathcal{R}$, the commutator relators $[\hat{u}_{l+2},\hat{u}_i] = \mathrm{dec}\left([u_{l+2},u_i]\right)$ and $[\hat{u}_{l+3},\hat{u}_i] = \mathrm{dec}\left([u_{l+2},u_i]\right)$ are added for $l+1 \le i \le 3l$ and the order relation for $\hat{k}$ is replaced by $\hat{k}^{(q^2-1)/3} = 1$. The same proof as in the case $3 \not| q+1$ gives that $\mathcal{R}$ implies all relations in the power-commutator presentation of $\langle Q,k\rangle$.

Clearly, in both of the cases $3 \not| q+1$ and $3 \mid q+1$ the presentation $\mathcal{R}$ consists of $O(l)$ relators of total length $O\left(l^2 \log p\right) = O\left(\log^2 q\right)$. □

4 A presentation for $\mathrm{PSU}_3(q)$

In proving that a presentation defines $\mathrm{PSU}_3(q)$ we will have to show that (4) holds for representatives u from all $\langle k\rangle$-classes.

The key observation for this is the following lemma that permits us to deduce conjugation relations for new $\langle k\rangle$-classes.

Lemma 14. *Let $a,b \in Q$ and assume that in a group $P(a_1,\ldots,a_m)$ the relation (4) holds for the $\langle k\rangle$-classes of a, b, and ab. Then (4) must hold for the class of $f(a)g(b)$ as well.*

Proof. Using the relations in $P(a_1,\ldots,a_m)$ and using that (4) holds for the denoted classes, we get:

$$\begin{aligned}
& \mathrm{dec}\big(g(ab)\big)\mathrm{dec}\big(h(ab)\big)\hat{t}\ \mathrm{dec}\big(f(ab)\big)\\
= \ & \hat{t}\ \mathrm{dec}\big(ab\big)\hat{t} = \hat{t}\ \mathrm{dec}\big(a\big)\hat{t}\ \hat{t}\ \mathrm{dec}\big(b\big)\hat{t}\\
= \ & \mathrm{dec}\big(g(a)h(a)\big)\hat{t}\ \mathrm{dec}\big(f(a)\big)\mathrm{dec}\big(g(b)h(b)\big)\hat{t}\ \mathrm{dec}\big(f(b)\big)\\
= \ & \mathrm{dec}\big(g(a)h(a)\big)\hat{t}\ \mathrm{dec}\big(f(a)g(b)\big)\hat{t}\ \mathrm{dec}\big(h(b)\big)^{\hat{t}}\ \mathrm{dec}\big(f(b)\big)\\
= \ & \mathrm{dec}\big(g(a)h(a)\big)\hat{t}\ \mathrm{dec}\big(f(a)g(b)\big)\hat{t}\ \mathrm{dec}\big(h(b)^t f(b)\big)
\end{aligned}$$

with $\mathrm{dec}\big(h(b)^t\big) \in \langle\hat{k}\rangle$. Therefore

$$\hat{t}\ \mathrm{dec}\big(f(a)g(b)\big)\ \hat{t} = \mathrm{dec}\big((g(a)h(a))^{-1}g(ab)h(ab)\big)\hat{t}\ \mathrm{dec}\big(f(ab)f(b)^{-1}(h(b)^t)^{-1}\big).$$

As k normalizes Q and is normalized by t, we have that

$$f(ab)f(b)^{-1}(h(b)^t)^{-1} = k^n f(u)$$

for some integer n and $f(u) \in Q$. Hence

$$\begin{aligned}
\hat{t}\ \mathrm{dec}\big(f(a)g(b)\big)\hat{t} \ &= \ \mathrm{dec}\big((g(a)h(a))^{-1}g(ab)h(ab)\big)\hat{t}\ \mathrm{dec}\big(k^n\big)\mathrm{dec}\big(f(u)\big)\\
&= \ \mathrm{dec}\big((g(a)h(a))^{-1}g(ab)h(ab)\big)\mathrm{dec}\big(k^{-nq}\big)\hat{t}\ \mathrm{dec}\big(f(u)\big)\\
&= \ \mathrm{dec}\big((g(a)h(a))^{-1}g(ab)h(ab)\ k^{-nq}\big)\hat{t}\ \mathrm{dec}\big(f(u)\big)
\end{aligned}$$

with $(g(a)h(a))^{-1}g(ab)h(ab)\ k^{-nq} \in \langle Q,k\rangle$ and $f(u) \in Q$. □

We now fix a field element $x \in \rho\ S^*$ and then $s \in S$ such that $x+s \in S^*/\rho$. (By Lemma 10 such s exists.)

Theorem 15. *Assume that* $3 \nmid q+1$ *and choose* $v \in \mathrm{GF}(q^2)^*$ *such that* $x + x^q + v^{q+1} = 0$. *Let* $a = u(x,v)$ *and* $b = u(s,0)$. *Then*

$$P = P(a,b,ab) \cong \mathrm{PSU}_3(q).$$

Proof. By Lemmas 5 and 7, it is enough to prove that (4) holds in P for representatives of all $\langle k \rangle$-classes in $Q \setminus \{1\}$. Since $b \in Z(Q) \setminus \{1\}$, condition (4) holds for all nonidentity elements of $Z(Q)$.

Let $K_1, \ldots, K_q$ be the $\langle k \rangle$-classes in $Q \setminus Z(Q)$, where $K_i = \{u(y,z) \in Q \mid y \in S^*/\rho^i\}$. By induction on $i = 1, \ldots, q$, we show that (4) holds in P for a representative of K_i (and so for the whole of K_i).

Since $ab \in K_1$, this statement is true for $i = 1$. Suppose now that (4) holds for the elements of K_i. By Lemma 11, there exists $w \in S^*$ such that $u(x,v)\ u(w,0) \in K_i$. Then, by Lemma 14, (4) holds in P for

$$f(u(x,v))\ g(u(w,0)) = \begin{pmatrix} 1 & & \\ -\frac{v}{x^q} & 1 & \\ \frac{1}{x} & \frac{v^q}{x} & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ 0 & 1 & \\ \frac{1}{w} & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ -\frac{v}{x^q} & 1 & \\ \frac{x+w}{x\,w} & \frac{v^q}{x} & 1 \end{pmatrix}.$$

Since $x + w \in S^*/\rho^i$ and $xw \in (\rho S^*)(S^*) = \rho\ \mathrm{GF}(q)^*$, we have that $(x+w)/xw \in S^*/\rho^{i+1}$ and thus $f(u(x,v))\ g(u(w,0)) \in K_{i+1}$. □

Theorem 16. *Assume that* $3 \mid q+1$ *and choose* $v_0 \in \langle \rho^3 \rangle$, $v_1 \in \langle \rho^3 \rangle \rho$, $v_2 \in \langle \rho^3 \rangle \rho^2$ *such that* $x + x^q + v_j^{q+1} = 0$ *for* $j \in \{0,1,2\}$. (*By Lemma* 12, *such* v_j *exist.*) *Let* $a_j = u(x,v_j)$ *and* $b = u(s,0)$. *Then*

$$P = P(a_1, a_2, a_3, b, a_1 b, a_2 b, a_3 b) \cong \mathrm{PSU}_3(q).$$

Proof. As in the proof of Theorem 15, it is enough to show that (4) holds in P for a representative of each $\langle k \rangle$-class in $Q \setminus Z(Q)$. For $0 \le j \le 2$ and $1 \le i \le q$, let $K_{i,j}$ be the $\langle k \rangle$-class in $Q \setminus Z(Q)$ given by

$$K_{i,j} = \left\{ u(y,z) \in Q \mid y \in S^*/\rho^i \text{ and } z \in \rho^j \langle \rho^3 \rangle \right\}.$$

By induction on $i = 1, \ldots, q$, we show that (4) holds in P for a representative of $K_{i,j}$ for $0 \le j \le 2$.

Since $a_j b \in K_{1,j}$, this statement is true for $i = 1$. Suppose that (4) holds for the elements of $K_{i,j}$ for $0 \le j \le 2$. By Lemma 12, there exists $w \in S^*$ such that $u(x,v_j)\ u(w,0) \in K_{i,j}$ for $0 \le j \le 2$. Then by Lemma 14, (4) holds in P for

$$f(u(x,v_j))\ g(u(w,0)) = \begin{pmatrix} 1 & & \\ -\frac{v_j}{x^q} & 1 & \\ \frac{x+w}{x\,w} & \frac{v_j^q}{x} & 1 \end{pmatrix}.$$

As in the proof of Theorem 15, $(x+w)/xw \in S^*/\rho^{i+1}$. Moreover, for $j = 0,1,2$, the field elements $-v_j/x^q$ are in different cosets of $\langle\rho^3\rangle$ in $\mathrm{GF}(q^2)^*$, so (4) holds in P for all three $\langle k\rangle$-classes $K_{i+1,0}$, $K_{i+1,1}$, $K_{i+1,2}$. □

Acknowledgement We are indebted to Bill Kantor for many helpful comments.

References

[BGK+97] László Babai, Albert J. Goodman, William M. Kantor, Eugene M. Luks, and Péter P. Pálfy, *Short presentations for finite groups*, J. Algebra **194** (1997), 97–112.

[KS] William M. Kantor and Ákos Seress, *Algorithms for finite linear groups*, in preparation.

[KS99] William M. Kantor and Ákos Seress, *Permutation group algorithms via black box recognition algorithms*, Groups St Andrews 1997 in Bath (C. M. Campbell, E. F. Robertson, N. Ruskuc, and G. C. Smith, eds.), London Mathematical Society Lecture Note Series, vol. 260/261, Cambridge University Press, 1999, pp. 436–446.

[KS01] William M. Kantor and Ákos Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708.

[LNS84] Reinhard Laue, Joachim Neubüser, and Ulrich Schoenwaelder, *Algorithms for finite soluble groups and the SOGOS system*, Computational Group theory (M. D. Atkinson, ed.), Academic Press, 1984, pp. 105–135.

[Man98] Avinoam Mann, *Enumerating finite groups and their defining relations*, J. Group Theory, **1** (1998), no. 1, 59–64.

[Ste81] Robert Steinberg, *Generators, relations and coverings of algebraic groups. II*, J. Algebra **71** (1981), no. 2, 527–543.

[Suz62] Michio Suzuki, *On a class of doubly transitive groups*, Ann. of Math. (2) **75** (1962), 105–145.

[Suz65] Michio Suzuki, *A characterization of the* 3*-dimensional projective unitary group over a finite field of odd characteristic,* J. Algebra **2** (1965), 1–14.