2016

Polytopes of Large Rank for PSL(4,q)

Peter A. Brooksbank
Bucknell University, pbrooksb@bucknell.edu

Dimitri Leemans
University of Auckland

Journal of Algebra 452 (2016) 390–400

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Polytopes of large rank for PSL$(4, \mathbb{F}_q)$

P.A. Brooksbank [a,1], D. Leemans [b,*,2]

[a] *Department of Mathematics, Bucknell University, Lewisburg, PA 17837, USA*
[b] *Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand*

ARTICLE INFO

Article history:
Received 22 April 2015
Available online xxxx
Communicated by Gernot Stroth

Keywords:
Abstract regular polytopes
String C-groups
Projective special linear groups

ABSTRACT

This paper examines abstract regular polytopes whose automorphism group is the projective special linear group PSL$(4, \mathbb{F}_q)$. For q odd we show that polytopes of rank 4 exist by explicitly constructing PSL$(4, \mathbb{F}_q)$ as a string C-group of that rank. On the other hand, we show that no abstract regular polytope exists whose group of automorphisms is PSL$(4, \mathbb{F}_{2^k})$.

1. Introduction

Abstract polytopes are incidence structures that generalize certain discrete geometric objects, the most famous being the Platonic solids. The study of these objects has its roots in classical theory – notably in Coxeter's work [8] – but has evolved in various ways in recent years. The book of McMullen and Schulte [18] is an excellent resource for a detailed study of these structures and their history.

* Corresponding author.
E-mail addresses: pbrooksb@bucknell.edu (P.A. Brooksbank), d.leemans@auckland.ac.nz (D. Leemans).

[1] This work was partially supported by grants from the Simons Foundation (#281435 to Peter Brooksbank), and by the National Security Agency under Grant Number H98230-11-1-0146.
[2] This work was supported by Marsden Grant UOA1218 from the Royal Society of New Zealand.

http://dx.doi.org/10.1016/j.jalgebra.2015.11.051
0021-8693/

The starting point for this paper is an equivalent group-theoretic formulation of abstract regular polytopes in terms of distinguished sets of involutions that generate their automorphism groups (see sections 2B and 2D of [18]). From this viewpoint, no reference to the polytope as a combinatorial object is needed: to show that a given group G acts on an abstract regular polytope of a given rank r, one just exhibits a generating set of r involutions of G that satisfies certain properties (see Section 2 for details). It is natural, then, to consider common families of finite groups and ask which members of a particular family can be generated in this way.

In the case of rank 3 (the analogue of classical polyhedra) the relevant question was first posed for all finite simple groups by Mazurov [16]. His question was settled for simple groups of Lie type by Nuzhin [19,20], and (ultimately) by himself for sporadic simple groups [17].

Moving to rank 4 and higher, the question becomes much more difficult. The main obstacle is that a certain "intersection property" on the generating involutions becomes nontrivial to verify in higher ranks. The most significant result to date was proved by the second author in joint work with Fernandes [9]: *for $n \geqslant 4$ and every $r \in \{3, \ldots, n-1\}$ there is an abstract regular polytope of rank r whose group of automorphisms is S_n.* A similar result for alternating groups is obtained in [10].

A natural question that arises is whether or not some analogue of these results holds for families of linear groups over finite fields. Specifically, we ask:

> *For each integer $r \geqslant 4$, is there an infinite family of groups, G, satisfying $\mathrm{PSL}(d, \mathbb{F}_q) \leqslant G \leqslant \mathrm{P\Gamma L}(d, \mathbb{F}_q)$, such that G is the group of automorphisms of an abstract regular polytope of rank r?*

The groups $\mathrm{PSL}(2, \mathbb{F}_q)$ and their variants have been extensively studied [13,14], culminating in the results of [6]. In the latter work it is shown that an infinite family of abstract regular polytopes of rank 4 exists for the groups $\mathrm{PSL}(2, q^2) \rtimes \langle \tau \rangle$, where τ is a certain field automorphism (a *Baer involution*). These groups, together with S_n and A_n, are the only infinite families of (almost) simple groups that are known to act on abstract regular polytopes of rank higher than 3.

Of course, $\mathrm{PSL}(2, \mathbb{F}_q)$ is rather too small a group to expect to find large, highly constrained, generating sets of involutions. One might expect greater joy by moving up in dimension. Surprisingly, however, three-dimensional linear groups and their projective variants yield no new abstract polytopes of any rank [3].

This paper considers four-dimensional linear groups and provides a first contribution to the question above. We prove the following result.

Theorem 1.1. *If $q = p^k$ for odd p, then $\mathrm{PSL}(4, \mathbb{F}_q)$ is the group of automorphisms of an abstract regular polytope of rank 4.*

The first hints that this result may be true emerged from a computer search for very small values of q. (In fact, the data suggest that $\mathrm{PSL}(4, \mathbb{F}_q)$ likely has many non-

isomorphic abstract regular polytopes of rank 4.) Of course, the computer offers little help in proving a theorem of this type. Moreover, although exhaustive computer searches have been invaluable in earlier efforts to construct and classify polytopes [7,11,15], the groups we are now interested in are so large that machines can tell us almost nothing of value. Furthermore, unlike the situation with $\mathrm{PSL}(2,\mathbb{F}_q)$ and its variants, we have nothing like a complete description of the subgroup structure of $\mathrm{PSL}(4,\mathbb{F}_q)$. The methods of [13,14,6] are therefore simply not scalable, and new ideas are needed.

Although the complete subgroup lattice of the almost simple linear groups is out of reach – not to mention unusable even if we had it – it is nevertheless helpful to know something about the maximal subgroups of the groups we are working with. In trying to build polytopes of rank r for a group G, the maximal subgroups of G are natural candidates to attempt to generate as polytopes of rank $r-1$. To prove Theorem 1.1, for example, we start by building a polytope of rank 3 for a subgroup $\mathrm{P}\Omega^-(4,\mathbb{F}_q)$ – close to being a maximal subgroup of $\mathrm{PSL}(4,\mathbb{F}_q)$ – where two of the chosen involutions generate a maximal dihedral subgroup. These choices make it easy for us to verify the intersection property when we extend by a suitable involution. We warmly acknowledge the considerable efforts of Bray, Holt, and Roney-Dougal in making available information on maximal subgroups of the classical groups of low rank [2].

We gain the most traction, however, by exploiting geometric properties of involutions in their action on the natural modules of $\mathrm{SL}(4,\mathbb{F}_q)$, or those of their orthogonal equivalents $\Omega^+(6,\mathbb{F}_q)$. More precisely, commutativity of involutions in these groups may be understood in terms of configurations of certain subspaces of the module, which in turn allows us to impose heavy restrictions on the putative polytopes upon which our groups can act. As an illustration of the efficacy of this approach, we can easily show that no polytopes of any rank exist for the groups $\mathrm{PSL}(4,\mathbb{F}_{2^k})$ (Corollary 4.5) by showing that any subgroup of $\Omega^+(6,\mathbb{F}_{2^k})$ arising as a quotient of a string Coxeter group necessarily acts reducibly on the natural module of $\Omega^+(6,\mathbb{F}_{2^k})$ (Theorem 4.4). Similar ideas were used in [3] and we expect them to remain useful when considering classical simple groups of higher Lie rank.

2. String C-groups

Abstract regular polytopes and string C-groups are essentially the same mathematical objects; see, for example, [18, Section 2]. For our purpose, the string C-group viewpoint is most useful. A *C-group* is a group G generated by pairwise distinct involutions $\rho_0,\ldots,\rho_{n-1}$ which satisfy the following *intersection property*:

$$\forall J,K\subseteq\{0,\ldots,n-1\},\langle\rho_j \mid j\in J\rangle\cap\langle\rho_k \mid k\in K\rangle=\langle\rho_j \mid j\in J\cap K\rangle. \tag{2.1}$$

A C-group $(G,\{\rho_0,\ldots,\rho_{n-1}\})$ is a *string C-group* if its generators also satisfy:

$$(\rho_j\rho_k)^2=1_G \text{ for all } j,k\in\{0,\ldots n-1\} \text{ with } \mid j-k\mid\geqslant 2. \tag{2.2}$$

A string C-group $(G, \{\rho_0, \ldots, \rho_{n-1}\})$ has *rank* n and its *Schläfli type* is the sequence

$$[|\rho_{i-1}\rho_i| : i \in \{1, \ldots, n-1\}]$$

where $|g|$ is the order of the element $g \in G$.

3. Linear groups and geometric spaces

The family of groups we consider here, namely the groups $\mathrm{PSL}(4, \mathbb{F}_q)$, are of course (quotients of) linear groups. We will also work with groups that act as isometries on geometric spaces equipped with certain reflexive forms. Accordingly, we now set up some standard notation for these groups that will be useful throughout; see [21, Chapter 7] for further details.

Let $\mathbb{F}_q$ be the field of q elements, and V a vector space of dimension d over $\mathbb{F}_q$. Denote by $\mathrm{GL}(V)$ or $\mathrm{GL}(d, \mathbb{F}_q)$ the group of invertible linear transformations of V. We often switch between regarding elements of $\mathrm{GL}(V)$ as linear transformations and as matrices relative to some basis. We shall make no further comment on this except to describe the basis we are using for the matrix view. We denote by $\mathrm{SL}(V)$ or $\mathrm{SL}(d, \mathbb{F}_q)$ the subgroup of elements of determinant 1.

For $g \in \mathrm{GL}(V)$, the subspace $[V, g] = \{v - vg \colon v \in V\}$ is the *support* of g. For a subgroup H of $\mathrm{GL}(V)$, we put $[V, H] = \{v - vh \colon v \in V, h \in H\}$. Observe that if H is generated by $g_1, \ldots, g_n$, then $[V, H] = [V, g_1] + \ldots + [V, g_n]$. If H acts irreducibly on V, then $[V, H] = V$.

For $g \in \mathrm{GL}(V)$, $\lambda \in \mathbb{F}_q$, $E_\lambda(g) = \{v \in V \colon vg = \lambda v\}$ is the λ-eigenspace of g.

A *quadratic form* on V is a function $\varphi \colon V \to \mathbb{F}_q$ such that:

(i) $\varphi(\alpha v) = \alpha^2 \varphi(v)$ for all $\alpha \in \mathbb{F}_q$, $v \in V$; and
(ii) $(u, v) := \varphi(u + v) - \varphi(u) - \varphi(v)$ is a nondegenerate bilinear form on V.

For a subspace $U \leqslant V$, define $U^\perp = \{v \in V \colon (u, v) = 0 \text{ for all } u \in U\}$. We say that U is *nondegenerate* if $U \cap U^\perp = 0$, and that U is *totally singular* if $\varphi(U) = 0$.

A space V equipped with a nondegenerate quadratic form is called an *orthogonal space*, and the group $\{g \in \mathrm{GL}(V) \colon \varphi(vg) = \varphi(v) \text{ for all } v \in V\}$ of isometries of φ is an *orthogonal group*. In even dimension there are, up to isometry, two types of quadratic forms, which we distinguish by $\epsilon \in \{+, -\}$, and denote the corresponding groups by $\mathrm{GO}^\epsilon(V)$. If $U \leqslant V$ is nonsingular of type ϵ and dimension n, we will often write $U = V_n^\epsilon$. We will be interested in the group $\mathrm{SO}^\epsilon(V) = \mathrm{GO}^\epsilon(V) \cap \mathrm{SL}(V)$, and especially in a particular subgroup $\Omega^\epsilon(V) \leqslant \mathrm{SO}^\epsilon(V)$, which in our case will always be the derived group of $\mathrm{SO}^\epsilon(V)$.

We shall work briefly with groups associated to *alternating* bilinear forms, where $(v, v) = 0$ for all $v \in V$. An alternating form is symmetric if, and only if, $\mathbb{F}_q$ has

characteristic 2. The isometry group $\{g \in \mathrm{GL}(V)\colon (ug, vg) = (u, v) \text{ for all } u, v \in V\}$ is called a *symplectic group* and denoted $\mathrm{Sp}(V)$.

4. The Klein correspondence

We shall occasionally exploit a correspondence first observed by Felix Klein in his PhD thesis [12] to switch to a 6-dimensional representation of $\mathrm{SL}(4, \mathbb{F}_q)$. Let $\mathcal{S}$ denote the space of skew-symmetric 4×4 matrices with entries in $\mathbb{F}_q$ of the form

$$M = \begin{bmatrix} 0 & x_{12} & x_{13} & x_{14} \\ -x_{12} & 0 & x_{23} & x_{24} \\ -x_{13} & -x_{23} & 0 & x_{34} \\ -x_{14} & -x_{24} & -x_{34} & 0 \end{bmatrix}. \tag{4.1}$$

Then the map $A \mapsto (M \mapsto A^{\mathrm{tr}} M A)$ is a homomorphism $f\colon \mathrm{GL}(4, \mathbb{F}_q) \to \mathrm{GL}(\mathcal{S})$. If $A \in \mathrm{SL}(4, \mathbb{F}_q)$, then $f(A)$ preserves the quadratic form

$$\varphi(M) = x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$$

on $\mathcal{S}$, and f restricts to a map $\mathrm{SL}(4, \mathbb{F}_q) \to \Omega^+(6, \mathbb{F}_q)$. As $|Z(\mathrm{SL}(4, \mathbb{F}_q))| = \gcd(4, q-1)$, we have $\Omega^+(6, \mathbb{F}_q) \cong \mathrm{PSL}(4, \mathbb{F}_q)$ except when $q \equiv 1 (\mathrm{mod}\ 4)$, in which case $Z(\Omega^+(6, \mathbb{F}_q)) = \{\pm I_6\}$.

We are concerned here principally with (non-central) involutions so we now describe involution classes in $\Omega^+(6, \mathbb{F}_q)$ and their relevant properties.

Let $V = V_6^+$ now denote the natural module for $G := \Omega^+(6, \mathbb{F}_q)$, $\varphi\colon V \to \mathbb{F}_q$ the quadratic form it preserves, and $(\,,\,)$ the associated symmetric form on V. We consider fields of odd and even characteristic separately.

$|\mathbb{F}_q|$ is odd. There are two classes of non-central involutions in G. Suppose that $\rho = f(A)$ is such an involution for some $A \in \mathrm{SL}(4, \mathbb{F}_q)$. Then an easy computation shows that $E_1(\rho) \oplus E_{-1}(\rho)$ is a decomposition $V = V_2 \perp V_4$ into nondegenerate subspaces of the same isometry type. If A is an involution of $\mathrm{SL}(4, \mathbb{F}_q)$, then $E_1(\rho) = V_2^+$ and $E_{-1}(\rho) = V_4^+$. Else, A has order 4, $A^2 = -1$, and $E_1(\rho) = V_4^{\pm}$ and $E_{-1}(\rho) = V_2^{\pm}$ according as $4 \mid (q \pm 1)$. In both cases $C_G(\rho)$ is the full stabilizer in G of this decomposition.

We record a property of involutions of the first type that will be useful later on.

Lemma 4.2. *If A and B are involutions of $\mathrm{SL}(4, \mathbb{F}_q)$ such that $AB = -BA$, then $E_{-1}(\rho(A))$ and $E_{-1}(\rho(B))$ intersect in a 3-dimensional subspace of V_6^+.*

Proof. As $|A| = 2$, we have a decomposition of $\mathbb{F}_q^4 = E_1(A) \oplus E_{-1}(A)$ into 2-spaces. Relative to any basis that respects this decomposition, A has matrix $\left[\begin{smallmatrix} I_2 & 0 \\ 0 & -I_2 \end{smallmatrix}\right]$. As $AB = -BA$, B interchanges $E_1(A)$ and $E_{-1}(A)$. Indeed, we can refine our basis choice so that

B has matrix $\left[\begin{smallmatrix} 0 & I_2 \\ I_2 & 0 \end{smallmatrix}\right]$. One now checks by direct calculation that the intersection of the -1-eigenspaces of A and B in their action on $\mathcal{S}$ is

$$\left\{ \begin{bmatrix} 0 & 0 & \alpha & \beta \\ 0 & 0 & \beta & \gamma \\ -\alpha & -\beta & 0 & 0 \\ -\beta & -\gamma & 0 & 0 \end{bmatrix} : \alpha, \beta, \gamma \in \mathbb{F}_q \right\},$$

and the result follows. □

$|\mathbb{F}_q|$ is even. In fields of characteristic 2, involutions of $\Omega^+(6, \mathbb{F}_q)$ occur within "pseudo-transvection groups", which in turn correspond to certain lines in the projective geometry. Specifically, let $\ell = \langle e, b \rangle$ with $\varphi(e) = 0 = (e, b)$, and define

$$R_\ell = \{ v \mapsto v + \alpha[(v \cdot b)e - (v \cdot e)b] + \alpha^2 \varphi(b)(v \cdot e)e \colon \alpha \in \mathbb{F}_q \}. \tag{4.3}$$

Then $[V, R_\ell] = \ell$ and $R_\ell \cong \mathbb{F}_q^+$ is the subgroup of G that induces the identity on $\ell^\perp$ and on V/ℓ. All involutions occur within these groups and there are again two involution classes: elements of the first class belong to some $R_{\langle e,b \rangle}$ with $\varphi(b) = 0$ (so $\ell = \langle e, b \rangle$ is totally singular), and those of the second class to $R_{\langle e,b \rangle}$ with $\varphi(b) \neq 0$.

The following relations are easily verified for $\rho \in R_\ell$ and $\sigma \in R_m$:

- If $[\rho, \sigma] = 1$, then ℓ meets m; and
- If $[\rho, \sigma] \neq 1$, then either ℓ and m are skew, or $\ell = \langle e, b \rangle$, $m = \langle f, b \rangle$, with $\varphi(e) = \varphi(f) = 0$, $\varphi(b) \neq 0$, and $(e, f) \neq 0$.

We now use this geometric interpretation of involutions in to establish a heavy constraint on string C-subgroups of $\mathrm{PSL}(4, \mathbb{F}_{2^k})$.

Theorem 4.4. *If $\rho_0, \rho_1, \ldots, \rho_{r-1}$ is a sequence of involutions in $\Omega^+(6, \mathbb{F}_{2^k})$ satisfying condition (2.2), then $H := \langle \rho_0, \ldots, \rho_{r-1} \rangle$ acts reducibly on the module V_6^+.*

Proof. The result is clear for $r < 3$. If $r = 3$, then ρ_0 and ρ_2 commute, so $[V, \rho_0] \cap [V, \rho_2] \neq 0$. It follows that $[V, H] = [V, \rho_0] + [V, \rho_1] + [V, \rho_2]$ is at most 5-dimensional. If $r = 4$, then $[V, \rho_0] + [V, \rho_2]$ and $[V, \rho_1] + [V, \rho_3]$ are both 3-dimensional. Also, $[V, \rho_3] \cap [V, \rho_0] \neq 0$, so $[V, H]$ is again at most 5-dimensional.

We may therefore assume that $r > 4$. For $i = 0, \ldots, r-1$, let $\ell_i = [V, \rho_i]$. If ℓ_0 and ℓ_1 are skew then, since ℓ_j meets both of these lines for all $j \geqslant 3$, it follows that ℓ_j lies within $\langle \ell_0, \ell_1 \rangle$, and hence that $[V, H]$ is at most 5-dimensional. Thus, we may assume that ℓ_0 meets ℓ_1 at a point $\langle b \rangle$ with $\varphi(b) \neq 0$; note that $\langle \ell_0, \ell_1 \rangle \leqslant \langle b \rangle^\perp$. Similarly, if ℓ_1 and ℓ_2 are skew, then ℓ_j lies within $\langle \ell_1, \ell_2 \rangle$ for each $j \geqslant 4$, so once again $[V, H]$ is at most 5-dimensional. We may therefore assume that ℓ_2 meets ℓ_1 at $\langle c \rangle$ with $\varphi(c) \neq 0$. As ℓ_2 meets ℓ_0 as well, there are two possibilities: first that $\langle c \rangle = \langle b \rangle$, and secondly that

$\langle c\rangle \neq \langle b\rangle$ in which case ℓ_2 lies within $\langle \ell_0, \ell_1\rangle \leqslant \langle b\rangle^\perp$. In either case, $\langle \rho_0, \rho_1, \rho_2\rangle$ fixes $\langle b\rangle$. Now, if ρ is any involution commuting with both ρ_0 and ρ_1, and $\ell = [V, \rho]$, then either $\langle b\rangle$ lies on ℓ, or ℓ lies within $\langle \ell_0, \ell_1\rangle$. Again, in either case, ρ fixes $\langle b\rangle$ and the result follows. □

Nuzhin noted in [19, Proposition 4] that there are no string C-groups of rank 3 for $\mathrm{PSL}(4, \mathbb{F}_{2^k})$. The following extension to higher ranks follows immediately from Theorem 4.4.

Corollary 4.5. $\mathrm{PSL}(4, \mathbb{F}_{2^k})$ *is not the group of automorphisms of an abstract regular polytope of any rank.*

5. Proof of Theorem 1.1

We restrict now to fields $\mathbb{F}_q$ of odd characteristic, and describe an explicit construction of $\mathrm{PSL}(4, \mathbb{F}_q)$ as a string C-group of rank four, thereby establishing Theorem 1.1. More precisely, we prove the following result, which also describes the Schläfli types of the corresponding abstract regular polytopes.

Theorem 5.1. *For each odd prime power $q \geqslant 5$, the group $\mathrm{PSL}(4, \mathbb{F}_q)$ has a string C-generating sequence $\rho_0, \rho_1, \rho_2, \rho_3$ such that:*

(i) $|\rho_0\rho_1| = q-1$, $|\rho_1\rho_2| = \frac{q^2+1}{2}$, *and* $|\rho_2\rho_3| = e$, *where $e = p$, or e divides $q \pm 1$, i.e. the string C-group has Schläfli type* $[q-1, \frac{q^2+1}{2}, e]$;
(ii) $\langle \rho_0, \rho_1, \rho_2\rangle \cong \Omega^-(4, \mathbb{F}_q) \cong \mathrm{PSL}(2, \mathbb{F}_{q^2})$; *and*
(iii) $\langle \rho_1, \rho_2, \rho_3\rangle$ *is isomorphic to a subgroup* $\mathrm{PSp}(4, \mathbb{F}_q).2$.

Remark 5.2. One readily sees that no such generating sequence of this type may exist for $\mathrm{PSL}(4, 3)$ as in that case $q - 1 = 2$ which implies that ρ_0 commutes with all the other generators and hence the generated group is not simple. However, the online version[3] of the Atlas of abstract regular polytopes [15] gives several examples of rank 4 abstract regular polytopes for that group.

A polyhedron of type $[q-1, \frac{q^2+1}{2}]$ for $\mathrm{PSL}(2, \mathbb{F}_{q^2})$. For q an odd prime power, we work with a tower of fields $\mathbb{F}_q \subset \mathbb{F}_{q^2} \subset \mathbb{F}_{q^4}$. Put $m = \frac{q^2+1}{2}$. We first use the construction in [5, Proposition 2.3] to obtain matrices $R, S \in \mathrm{SL}(2, \mathbb{F}_{q^2})$ of orders $2(q-1)$ and $2m$, respectively, such that $RS = -1$. Following [5], for *projective orders* $(q-1, m, 2)$ we build a representative triple $(R, S, T = RS)$ having *representative orders* $(2(q-1), 2m, 4)$.

Fix elements a and b of $\mathbb{F}_{q^4}$ of orders $2(q-1)$ and $2m$, respectively. Let $t\colon \mathbb{F}_{q^4} \to \mathbb{F}_{q^4}$ be the map sending $x \mapsto x + 1/x$. Since

[3] See http://www.math.auckland.ac.nz/~dleemans/polytopes.

$$t(x) = t(y) \iff (x-y)(1-1/(xy)) = 0 \iff y = x \text{ or } y = x^{-1},$$

clearly t is a 2-to-1 function. Also, $b^{q^2} = 1/b$, so $t(b) = b + b^{q^2}$ is the usual trace map from $\mathbb{F}_{q^4}$ to $\mathbb{F}_{q^2}$, whence $t(b) \in \mathbb{F}_{q^2}$. Following [5, Proposition 2.3], put

$$R = R(a) = \begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix} \quad \text{and} \quad S = S(a,b) = \begin{bmatrix} -ct(b)/a & -cD \\ c & ca\,t(b) \end{bmatrix},$$

where $D = t(a)^2 + t(b)^2 - 4 = t(a^2) + t(b^2) \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and $c = 1/(a - 1/a)$. Clearly $R, S \in \mathrm{SL}(2, \mathbb{F}_{q^2})$, and by construction $|R| = 2(q-1)$, $|S| = q^2 + 1$, and $RS = -1$.

Next, in [5, Proposition 3.2], it is shown that there is a unique $Z \in \mathrm{SL}(2, \overline{\mathbb{F}}_q)$ inverting both R and S (here, $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$), and in fact

$$Z = Z(a,b) = \begin{bmatrix} 0 & \delta D \\ \delta & 0 \end{bmatrix},$$

where $\delta = -1/\sqrt{-D} \in \mathbb{F}_{q^4}$. Since -1 is a square in $\mathbb{F}_{q^2}$, evidently $Z \in \mathrm{SL}(2, \mathbb{F}_{q^2})$ if, and only if, D has a square root in $\mathbb{F}_{q^2}$. As one might expect, this seems to occur about half of the time for an arbitrary choice of a and b. To be certain that a suitable choice of a and b is always available, however, we use the following special case of [4, Corollary 4.1].

Theorem 5.3. *Let K be a finite field, and $A, B \subseteq K$. The number of solutions of*

$$x + y = z^2 \qquad (x \in A,\ y \in B,\ z \in K)$$

is $|A||B| + \theta\sqrt{|A||B||K|}$ for some θ with $|\theta| \leqslant 1$.

Applying this result to our situation, we can show that good choices of a and b do indeed exist.

Corollary 5.4. *Let $q > 3$ be an odd prime power. Let A_0 and B_0 be the subsets of $\mathbb{F}_{q^4}^*$ consisting, respectively, of elements of order $(q-1)$ and $m = \frac{q^2+1}{2}$. Then*

$$t(A_0) + t(B_0) = \{t(x_0) + t(y_0) \colon x_0 \in A_0,\ y_0 \in B_0\} \subseteq \mathbb{F}_{q^2}$$

contains an element whose square roots also lie in $\mathbb{F}_{q^2}$.

Proof. We apply Theorem 5.3 to $A = t(A_0)$ and $B = t(B_0)$ and $K = \mathbb{F}_{q^2}$. Put $n = |A||B|$. As we require only *one* triple (x, y, z) with $x = t(x_0) \in A$, $y = t(y_0) \in B$ and $z \in \mathbb{F}_{q^2}$ such that $x + y = z^2$, it suffices to show that $n > q^2$. Note, $|A_0| = \varphi((q^2+1)/2) > q^2/6 \log\log q$, while $|B_0| = \varphi(q-1) > q/3 \log\log q$. Thus, $n = |A||B| = |A_0||B_0|/4 > q^3/72(\log\log q)^2$, so n certainly exceeds q^2 provided that $q > 200$. The existence of suitable triples (x, y, z) for smaller values of q can easily be verified using Magma [1]. □

We can now prove the result that we need.

Proposition 5.5. *For $q > 3$, there are involutions $t_0, t_1, t_2 \in \mathrm{PSL}(2, \mathbb{F}_{q^2})$ with $[t_0, t_2] = 1$, $|t_0 t_1| = q - 1$, $|t_1 t_2| = (q^2+1)/2$, and $\langle t_0, t_1, t_2 \rangle = \mathrm{PSL}(2, \mathbb{F}_{q^2})$.*

Proof. Choose elements a_0 and b_0 of $\mathbb{F}_{q^4}$ of order $q-1$ and $\frac{q^2+1}{2}$, respectively, such that $t(a_0) + t(b_0)$ has a square root in $\mathbb{F}_{q^2}$. Let a be a square root of a_0 of order $2(q-1)$, and let b be a square root of b_0 of order q^2+1. The reckoning above ensures that the elements $R(a), S(a,b)$ and $Z(a,b)$ all lie in $\mathrm{SL}(2, \mathbb{F}_{q^2})$. Then the elements $T_0 = RZ$, $T_1 = Z$ and $T_2 = ZS$ project onto elements t_0, t_1 and t_2 of the stated type. The order properties follow immediately from the foregoing discussion, and the fact that $q-1$ and $(q^2+1)/2$ are coprime ensures that the triple generates $\mathrm{PSL}(2, \mathbb{F}_{q^2})$. □

From $\mathrm{PSL}(2, \mathbb{F}_{q^2})$ to $\Omega^-(4, \mathbb{F}_q)$. We next use a well-known construction to embed $\mathrm{PSL}(2, \mathbb{F}_{q^2})$ in $\mathrm{SL}(4, \mathbb{F}_q)$ as the group $\Omega^-(4, \mathbb{F}_q)$. Let $\mathcal{H}$ denote the $\mathbb{F}_q$-space of 2×2 Hermitian matrices with entries in $\mathbb{F}_{q^2}$, namely all $M \in \mathbb{M}_2(\mathbb{F}_{q^2})$ such that $\overline{M} = M^{\mathrm{tr}}$, where $\overline{M}$ denotes the image of M under the Frobenius automorphism $\alpha \mapsto \alpha^q$ applied to the entries of M. The map $A \mapsto (M \mapsto \overline{A}^{\mathrm{tr}} M A)$ is a homomorphism $g\colon \mathrm{GL}(2, \mathbb{F}_{q^2}) \to \mathrm{GL}_{\mathbb{F}_q}(\mathcal{H})$. Furthermore, $\mathcal{H}$ is an orthogonal space of type V_4^- – with quadratic form given by the determinant map – and g restricts to an epimorphism $SL(2, \mathbb{F}_{q^2}) \to \Omega^-(4, \mathbb{F}_q)$ with kernel $\{\pm 1\}$.

Thus, if T_0, T_1, T_2 are the elements of $\mathrm{SL}(2, \mathbb{F}_{q^2})$ constructed in the proof of Proposition 5.5, and $\rho_i = g(T_i)$ for $i = 0, 1, 2$, then $H := \langle \rho_0, \rho_1, \rho_2 \rangle$ is a subgroup of $\mathrm{SL}(4, \mathbb{F}_q)$ isomorphic to $\Omega^-(4, \mathbb{F}_q) \cong \mathrm{PSL}(2, \mathbb{F}_{q^2})$. Furthermore $[\rho_0, \rho_2] = 1$, $|\rho_0 \rho_1| = q - 1$, and $|\rho_1 \rho_2| = (q^2+1)/2$, as required.

Constructing ρ_3. We have built, for each $q > 3$, a polyhedron $H = \langle \rho_0, \rho_1, \rho_2 \rangle$ of $G = \mathrm{SL}(4, \mathbb{F}_q)$ isomorphic to $\Omega^-(4, \mathbb{F}_q)$. It remains to construct an involution $\rho_3 \in G$ behaving as in Theorem 5.1.

We continue to work with $V = \mathbb{F}_q^4$ as an orthogonal space of Witt index 1 equipped with the quadratic form φ preserved by H. As $h := \rho_0 \rho_1 \in \Omega^-(4, \mathbb{F}_q)$ has order $q-1$, it preserves a decomposition $V = V_2^+ \perp V_2^-$, where V_2^+ is a nondegenerate hyperbolic line upon which h induces an element of order $q-1$, and V_2^- is an anisotropic line upon which h induces ± 1. Observe that neither V_2^+ nor V_2^- is an eigenspace of ρ_0 or ρ_1; otherwise both subspaces would necessarily be eigenspaces for both involutions, in which case $\rho_0 = \pm \rho_1$.

Let $0 \neq e \in V_2^+$ with $\varphi(e) = 0$. Then $\langle e\rho_0 \rangle \neq \langle e \rangle$, and both ρ_0 and ρ_1 interchange $\langle e \rangle$ and $\langle e\rho_0 \rangle$. Next, choose any $u \in V_2^-$ such that $u\rho_0 \notin \langle u \rangle$. Let ρ_3 be the involution whose 1-eigenspace is $\langle e, u \rangle$, and whose -1-eigenspace is $\langle e, u \rangle \rho_0$. Then, by construction, both ρ_0 and ρ_1 interchange the eigenspaces of ρ_3, so that $[\rho_0, \rho_3] = -1 = [\rho_1, \rho_3]$. Note, $\varphi(u\rho_3) = \varphi(u) \neq 0$, but $\varphi(e + e\rho_0) = (e, e\rho_0) \neq 0$ and $\varphi((e + e\rho_0)\rho_3) = \varphi(e - e\rho_0) = -(e, e\rho_0)$, so

ρ_3 does not preserve φ even up to scalar multiple. Since the extension of $\mathrm{SO}^-(4,\mathbb{F}_q)$ by scalars is maximal in $\mathrm{SL}(4,\mathbb{F}_q)$ [2, Table 8.8], it follows that $\langle \rho_0,\rho_1,\rho_2,\rho_3\rangle = \mathrm{SL}(4,\mathbb{F}_q)$.

We record one last consequence of our construction. The element $\rho_2\rho_3$ skew-commutes with ρ_0. Therefore, $\rho_2\rho_3$ interchanges the eigenspaces of ρ_0, and hence lies inside a subgroup of $\mathrm{GL}(4,\mathbb{F}_q)$ isomorphic to $(\mathrm{GL}(2,\mathbb{F}_q)\times\mathrm{GL}(2,\mathbb{F}_q))\rtimes C_2$. It follows that $\gcd(|\rho_1\rho_2|,|\rho_2\rho_3|)=1$.

Lemma 5.6. *There is a nondegenerate alternating form on $\mathbb{F}_q^4$ such that*

$$(u\rho_i, v\rho_i) = -(u,v) \text{ for all } u,v\in\mathbb{F}_q^4 \text{ and for all } i\in\{1,2,3\}.$$

In particular, $\langle\rho_1,\rho_2,\rho_3\rangle$ is a subgroup of $\mathrm{Sp}(4,\mathbb{F}_q).2$.

Proof. As in Section 4, consider the action on $\mathcal{S}$, the $\mathbb{F}_q$-space of skew-symmetric matrices, via the Klein correspondence $f\colon \mathrm{SL}(4,\mathbb{F}_q)\to\Omega^+(\mathcal{S})$. As ρ_i is an involution of $\mathrm{SL}(4,\mathbb{F}_q)$, each eigenspace $E_{-1}(f(\rho_i))$ has dimension 4 in $\mathcal{S}$. Furthermore, by Lemma 4.2, $E_{-1}(f(\rho_0))\cap E_{-1}(f(\rho_2))$ has dimension 3. Hence, $\bigcap_{i=0}^{2} E_{-1}(f(\rho_i))$ has dimension at least 1, so there exists $0\neq M\in\mathcal{S}$ such that $\rho_i^{\mathrm{tr}} M\rho_i = -M$ for $i\in\{0,1,2\}$. The alternating form represented by any such M is nondegenerate (i.e. M is nonsingular) for, otherwise, it has a (necessarily 2-dimensional) radical, and so its group of isometries acts reducibly on $\mathbb{F}_q^4$ and hence contains no element of order $|\rho_1\rho_2| = (q^2+1)/2$. □

We now have all of the ingredients we need to complete the proof of our main theorem.

Proof of Theorem 5.1. Let $G=\mathrm{SL}(4,\mathbb{F}_q)$ and $\overline{G}=G/Z(G)=\mathrm{PSL}(4,\mathbb{F}_q)$. For $g\in G$, put $\overline{g}:=gZ(G)\in\overline{G}$. Let ρ_0, ρ_1, ρ_2, ρ_3 the involutions of G constructed above. We have already shown that $G=\langle\rho_0,\rho_1,\rho_2,\rho_3\rangle$. It remains to show that $(\overline{G},\{\overline{\rho_0},\overline{\rho_1},\overline{\rho_2},\overline{\rho_3}\})$ is a string C-group with properties listed in Theorem 5.1.

The group $\langle\overline{\rho_0},\overline{\rho_1},\overline{\rho_2}\rangle\cong\mathrm{PSL}(2,\mathbb{F}_{q^2})$ was built as a polyhedron. We have also shown that $\langle\overline{\rho_1},\overline{\rho_2},\overline{\rho_3}\rangle$ is isomorphic to a subgroup of $\mathrm{PSp}(4,\mathbb{F}_q).2$, as stated. Furthermore, since $|\rho_1\rho_2|$ and $|\rho_2\rho_3|$ are coprime, $\langle\rho_1,\rho_2\rangle\cap\langle\rho_2,\rho_3\rangle=\langle\rho_2\rangle$. Hence, $\langle\overline{\rho_1},\overline{\rho_2},\overline{\rho_3}\rangle$ satisfies the intersection condition and is therefore a polyhedron. Finally, since $\langle\rho_1,\rho_2\rangle\cong D_{q^2+1}$ is maximal in $\langle\rho_0,\rho_1,\rho_2\rangle\cong\mathrm{PSL}(2,q^2)$, it follows that $\langle\rho_0,\rho_1,\rho_2\rangle\cap\langle\rho_1,\rho_2,\rho_3\rangle=\langle\rho_1,\rho_2\rangle$. Thus, by [18, Proposition 2E16], the intersection condition holds for $(\overline{G},\{\overline{\rho_0},\overline{\rho_1},\overline{\rho_2},\overline{\rho_3}\})$. It follows that $(\overline{G},\{\overline{\rho_0},\overline{\rho_1},\overline{\rho_2},\overline{\rho_3}\})$ is a string C-group of rank 4, as required. □

Remark 5.7. Magma functions that construct the family of string C-groups described in Theorem 5.1 are available upon request from either author.

Acknowledgments

The authors are indebted to Alex Rice for bringing their attention to the results in [4]. They also thank Marston Conder for helpful discussions on polyhedra for $\mathrm{PSL}(2,q)$. The

first author thanks the University of Auckland for its generous hospitality during the conclusion of this work. Finally the authors would like to thank an anonymous referee for useful comments.

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265, MR1484478.
[2] J.N. Bray, D.F. Holt, C.M. Roney-Dougal, The Maximal Subgroups of the Low-Dimensional Finite Classical Groups, London Math. Soc. Lecture Note Ser., vol. 407, Cambridge University Press, Cambridge, 2013, MR3098485.
[3] P.A. Brooksbank, D.A. Vicinsky, Three-dimensional classical groups acting on polytopes, Discrete Comput. Geom. 44 (3) (2010) 654–659, MR2679061 (2011g:52020).
[4] J. Cilleruelo, Combinatorial problems in finite fields and Sidon sets, Combinatorica 32 (5) (2012) 497–511, MR3004806.
[5] M. Conder, P. Potočink, J. Širáň, Regular hypermaps over projective linear groups, J. Aust. Math. Soc. 85 (2) (2008) 155–175, MR2470535 (2010f:57005).
[6] T. Connor, J. De Saedeleer, D. Leemans, Almost simple groups with socle $PSL(2, q)$ acting on abstract regular polytopes, J. Algebra 423 (2015) 550–558, MR3283730.
[7] T. Connor, D. Leemans, M. Mixer, Abstract regular polytopes for the O′Nan group, Internat. J. Algebra Comput. 24 (1) (2014) 59–68, MR3189666.
[8] H.S.M. Coxeter, Regular Polytopes, third edition, Dover Publications, New York, 1973, MR0370327 (51 #6554).
[9] M.E. Fernandes, D. Leemans, Polytopes of high rank for the symmetric groups, Adv. Math. 228 (2011) 3207–3222, MR2844941 (2012j:52025).
[10] M.E. Fernandes, D. Leemans, M. Mixer, Polytopes of high rank for the alternating groups, J. Combin. Theory Ser. A 119 (2012) 42–56, MR2844081 (2012h:52026).
[11] M.I. Hartley, An atlas of small regular abstract polytopes, Period. Math. Hungar. 53 (1–2) (2006) 149–156, MR2286467 (2007i:51027).
[12] F. Klein, Über die Transformation der allgemeinen Gleichung des zweiten Grades zwischen Linien-Koordinaten auf eine kanonische Form, Rheinische Friedrich-Wilhelms-Universität Bonn, 1868.
[13] D. Leemans, E. Schulte, Groups of type $L_2(q)$ acting on polytopes, Adv. Geom. 7 (4) (2007) 529–539, MR2360900 (2008i:20003).
[14] D. Leemans, E. Schulte, Polytopes with groups of type $\mathrm{PGL}_2(q)$, Ars Math. Contemp. 2 (2) (2009) 163–171, MR2550963 (2010k:52014).
[15] D. Leemans, L. Vauthier, An atlas of abstract regular polytopes for small groups, Aequationes Math. 72 (2006) 313–320, MR2282877 (2007i:51028).
[16] V.D. Mazurov, Unsolved Problems in Group Theory, The Kourovka Notebook, vol. 10, 1986.
[17] V.D. Mazurov, Generation of sporadic simple groups by three involutions, two of which commute, Sibirsk. Mat. Zh. 44 (1) (2003) 193–198, MR1967616 (2004g:20023).
[18] P. McMullen, E. Schulte, Abstract Regular Polytopes, Encyclopedia Math. Appl., vol. 92, 2002, xiv+551, MR1965665 (2004a:52020).
[19] Ya.N. Nuzhin, Generating triples of involutions of Chevalley groups over a finite field of characteristic 2, Algebra Logic 29 (1990) 134–143, MR1131150 (92j:20046).
[20] Ya.N. Nuzhin, Generating triples of involutions for Lie-type groups over a finite field of odd characteristic, II, Algebra Logic 36 (1997) 245–256, MR1601503 (98m:20021).
[21] D.E. Taylor, The Geometry of the Classical Groups, Sigma Ser. Pure Math., vol. 9, Heldermann Verlag, Berlin, 1992, MR1189139 (94d:20028).