Transitive $\text{PSL}(2,11)$-invariant $k$-arcs in $\text{PG}(4,q)$

Torger Olson$^1$ · Eric Swartz$^1$

Received: 25 April 2018 / Revised: 3 October 2018 / Accepted: 14 November 2018 / Published online: 29 November 2018 © Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract

A $k$-arc in the projective space $\text{PG}(n, q)$ is a set of $k$ projective points such that no subcollection of $n + 1$ points is contained in a hyperplane. In this paper, we construct new 60-arcs and 110-arcs in $\text{PG}(4, q)$ that do not arise from rational or elliptic curves. We introduce computational methods that, when given a set $\mathcal{P}$ of projective points in the projective space of dimension $n$ over an algebraic number field $\mathbb{Q}(\xi)$, determines a complete list of primes $p$ for which the reduction modulo $p$ of $\mathcal{P}$ to the projective space $\text{PG}(n, p^h)$ may fail to be a $k$-arc. Using these methods, we prove that there are infinitely many primes $p$ such that $\text{PG}(4, p)$ contains a $\text{PSL}(2, 11)$-invariant 110-arc, where $\text{PSL}(2, 11)$ is given in one of its natural irreducible representations as a subgroup of $\text{PGL}(5, p)$. Similarly, we show that there exist $\text{PSL}(2, 11)$-invariant 110-arcs in $\text{PG}(4, p^2)$ and $\text{PSL}(2, 11)$-invariant 60-arcs in $\text{PG}(4, p)$ for infinitely many primes $p$.

Keywords Finite projective space · $k$-arc · $\text{PSL}(2, 11)$

Mathematics Subject Classification 51E20 · 20G40

1 Introduction

Let $q$ be a prime power. A $k$-arc in the projective space $\text{PG}(n, q)$ is a set of $k$ projective points such that no subcollection of $n + 1$ points is contained in a hyperplane, and such a $k$-arc is said to be complete if it is not contained in a $(k + 1)$-arc.

A motivation for studying $k$-arcs in projective spaces comes from Coding Theory and, in particular, the study of maximal distance separable codes, commonly referred to as M.D.S.
There are infinitely many primes $p$ such that there exists a transitive 60-arc and 110-arc in infinitely many 4-dimensional projective spaces and detail primes in this list, and

$$p \equiv 1 \pmod{11}.$$ 

Moreover, the automorphism group of a code can be used to decrease the computational complexity of encoding and decoding [18], so finding new examples of codes with large automorphism groups is useful in practice.

In this paper, we study $k$-arcs in 4-dimensional projective space, about which relatively little seems to be known, especially when the codes do not arise from elliptic or rational curves. In particular, we study $k$-arcs that are invariant under the action of $\text{PSL}(2, 11)$, which has a 5-dimensional irreducible representation over $\text{GF}(q)$ whenever $q^5 \equiv 1 \pmod{11}$; see Sect. 2 for details. Our main results are the following, which show the existence of $\text{PSL}(2, 11)$-transitive 60-arcs and 110-arcs in infinitely many 4-dimensional projective spaces and detail precisely when they occur.

**Theorem 1** There are infinitely many primes $p$ such that there exists a $\text{PSL}(2, 11)$-transitive 110-arc in $\text{PG}(4, p)$, and a list of all primes $p$ such that $p^5 \equiv 1 \pmod{33}$ and $\text{PG}(4, p)$ may not contain a $\text{PSL}(2, 11)$-transitive 110-arc is known. Explicitly, there are exactly 2728 primes in this list, and $\text{PG}(4, p)$ contains a $\text{PSL}(2, 11)$-transitive $k$-arc whenever $p^5 \equiv 1 \pmod{33}$ and $p > 5373427$. In particular, the primes $p$ such that $3 < p < 65,000$ and $\text{PG}(4, p)$ contains a $\text{PSL}(2, 11)$-transitive 110-arc are 26029, 26437, 27127, 27481, 28081, 28759, 29401, 30259, 31069, 32257, 32803, 33247, 33301, 34159, 34543, 34747, 35797, 35869, 36061, 36217, 37339, 37579, 38239, 38281, 38317, 38371, 38449, 39301, 39439, 40093, 40099, 40357, 40423, 40771, 40903, 41023, 41143, 41221, 41299, 41737, 41809, 41911, 41959, 42013, 42397, 42409, 42463, 42751, 42901, 43399, 43759, 44203, 44383, 44797, 44851, 44983, 45433, 45631, 45841, 46171, 46399, 46663, 46861, 47221, 47287, 47389, 47491, 48409, 48541, 49339, 49393, 49417, 49603, 49921, 49999, 50671, 50821, 50989, 51439, 51613, 51859, 52177, 52453, 52501, 52561, 52567, 52783, 52837, 52957, 53047, 53089, 53101, 53161, 53551, 53593, 53617, 53857, 53881, 53887, 54037, 54151, 54367, 54499, 54547, 54679, 54829, 54949, 54979, 55201, 55213, 55411, 55639, 55807, 55837, 55903, 55933, 56101, 56167, 56269, 56467, 56629, 56809, 56827, 57601, 57667, 57847, 58129, 58237, 58243, 58369, 58567, 58573, 58789, 58921, 58963, 59119, 59167, 59233, 59557, 59779, 59863, 59887, 59929, 60223, 60589, 60679, 60901, 61099, 61141, 61381, 61417, 61561, 61603, 61681, 61933, 62011, 62131, 62533, 62617, 62683, 62701, 62731, 63127, 63277, 63331, 63361, 63391, 63409, 63463, 63559, 63853, 64381, 64513, 64579, 64663, and 64783.

The complete list of all 2767 primes $p^5 \equiv 1 \pmod{33}$ such that $p \leq 5373427$ for which there may not be a $\text{PSL}(2, 11)$-transitive 110-arc in $\text{PG}(4, p)$ can be found at http://www.math.wm.edu/~eswartz/badprimes110.

**Theorem 2** There are infinitely many primes $p$ such that there exists a $\text{PSL}(2, 11)$-transitive 110-arc in $\text{PG}(4, p^2)$ (and not in $\text{PG}(4, p)$), and a list of all primes $p$ such that $p^5 \equiv 23 \pmod{33}$ and $\text{PG}(4, p^2)$ does not contain a $\text{PSL}(2, 11)$-transitive 110-arc is known. Explicitly, $\text{PG}(4, p^2)$ (and not $\text{PG}(4, p)$) contains a $\text{PSL}(2, 11)$-transitive 110-arc if and only if $p = 311, 317, 389, 401, 419, 443, 449, 467, 509, 521, 587, 599, 617, 641, 653, 719, 773, 839, 881, 911, 947, 977, 983, 1013, 1049, 1061, 1103, 1109, 1181, 1193, 1259, 1277, 1301, 1307, 1367, 1373, 1409, 1433, 1499, 1511, 1523, 1571, 1607, 1637, 1697, 1709, 1721, 1787, 1901, 1907, 1973, 2003, 2027, 2039, 2069, 2099, 2237, 2267, 2297, 2333, 2357, 2381, 2399, 2423, 2447, 2531, 2579, 2621, 2633, 2663, 2687, 2693.
is a root of the irreducible polynomial \( c \xi_{13} \). Indeed, if \( Z \) matrix representation where each matrix has coefficients in 9857, there are infinitely many primes \( p \) such that there exists a PSL(2,11)-invariant 60-arc in PG(4, \( p \)). Explicitly, there is a PSL(2,11)-transitive 60-arc in PG(4, \( p \)) if and only if \( p = 1277, 1783, 2069, 2333, 2399, 2861, 2971, 3169, 3499, 3631, 4027, 4159, 4357, 4423, 4621, 4643, 4951, 4973, 5039, 5171, 5237, 5281, 5303, 5347, 5413, 5479, 5501, 5743, 5897, 6007, 6029, 6073, 6271, 6337, 6359, 6469, 6689, 6733, 6997, 7019, 7129, 7151, 7283, 7349, 7393, 7459, 7481, 7547, 7723, 7789, 8009, 8053, 8273, 8317, 8537, 8858, 8647, 8669, 8713, 8779, 8867, 8933, 8999, 9043, 9109, 9241, 9439, 9461, 9769, 9791, 9857, 9901, 9923, 9967, 10099, 10253, 10429, 10627, 10781, 10847, 10891, 10957, 10979, 11177, 11243, 11287, 11353, 11551, 11617, or when \( p \) is a prime such that \( p \equiv 1 \pmod{11} \) and \( p > 11903 \).

The complete code for the calculations done in GAP [17], many with the aid of the package FinInG, are included in the arXiv version of this paper [11].

In general, the arcs constructed here are not complete arcs. Interestingly, calculations in GAP show that, for large enough primes \( p \) such that \( p \equiv 1 \pmod{33} \), the union of a PSL(2,11)-transitive 110-arc and a PSL(2,11)-transitive 60-arc is actually a 170-arc in PG(4, \( p \)); see [11, Calculation A.13]. On the other hand, while it is clear that the arcs constructed here are not complete for sufficiently large values of \( p \), it is unclear whether or not the arcs are complete in some of the “small” spaces. However, the smallest space in which an arc is constructed in this paper is PG(4, 1277), which contains 2661361144381 points, making the problem intractable computationally.

This paper is organized as follows. In Sect. 2, we give the details of an irreducible 5-dimensional representation of PSL(2,11) over the complex numbers. In Sect. 3, we make explicit our method for verifying that a set of projective points is a \( k \)-arc. We discuss the 110-arcs in Sect. 4, and we discuss the 60-arcs in Sect. 5.

### 2 A 5-dimensional irreducible representation of PSL(2,11)

From the Atlas [5], the group PSL(2,11) has a 5-dimensional irreducible representation over \( \mathbb{C} \), and generators for this representation in GAP [17] can be found at [1]; see [11, Remark 13]. Indeed, if \( \xi \) is a primitive 11th root of unity, \( c := \xi + \xi^3 + \xi^4 + \xi^5 + \xi^9 = (-1 + i \sqrt{11})/2 \), and

\[
A := \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
1 & -1 & c & 1 & -c \\
0 & 0 & 1 & 0 & 0
\end{pmatrix},
B := \begin{pmatrix}
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & -1 & -1 & 0 & 0 \\
c + 1 & 0 & 0 & -1 & c + 2 \\
1 & 0 & 0 & -1 & 1
\end{pmatrix},
\]

then \( (A, B) \cong PSL(2, 11) \). This irreducible representation of PSL(2,11) may be viewed as a matrix representation where each matrix has coefficients in \( \mathbb{Z}[c] \), where \( c \) (as defined above) is a root of the irreducible polynomial \( c^5 + c + 3 \). We could also view these as matrices in \( \mathbb{Z}[\xi] \). Indeed, by [4, Table 8.19], we see that PSL(2,11) is a maximal subgroup of PGL(5, \( q \)) whenever \( q^5 \equiv 1 \pmod{11} \), \( q \neq 3 \). (The group PGL(5, 3) contains a maximal subgroup
3 Verifying that a set of projective points is an arc

The purpose of this section is to provide a computationally effective method for determining whether the reduction modulo \( p \) of a set of points \( \mathcal{P} \) contained in \( n \)-dimensional projective space over a number field \( \mathbb{Q}(\xi) \) to \( \text{PG}(n, q) \), where \( q \) is some power of \( p \), is an arc.

The lemma that follows gives a sufficient condition for a set of points to be a \( k \)-arc. This condition is well-known, and its proof is omitted here.

**Definition 4** Given a field \( \mathbb{K} \), a subset \( J \) of size five of \( \mathbb{K}^5 \), and an ordering \( \sigma = (v_1, v_2, v_3, v_4, v_5) \) of the elements of \( J \), define \( X_{J,\sigma} \) to be the matrix whose \( i \)-th row is \( v_i \), and define \( [J] \) to be the set of all matrices \( X_{J,\sigma} \) for a fixed subset \( J \) of \( \mathbb{K}^5 \). If \( K := \{ P_1, \ldots, P_5 \} \) are projective points in \( \text{PG}(4, \mathbb{K}) \), define \( [K] \) to be the set of all \( X_{J,\sigma} \), where \( P_i \) is associated to the linear subspace \( \langle v_i \rangle \) of \( \mathbb{K}^5 \) and \( J := \{ v_1, v_2, v_3, v_4, v_5 \} \) with an ordering \( \sigma = (v_1, v_2, v_3, v_4, v_5) \).

**Lemma 5** If \( \mathcal{A} \) is a set of \( k \) projective points in \( \text{PG}(4, \mathbb{K}) \), where \( \mathbb{K} \) is a field, and, for all subsets \( K \) of \( \mathcal{A} \) of size five, \( \det(X) \neq 0 \) for some \( X \in [K] \), then \( \mathcal{A} \) is a \( k \)-arc of \( \text{PG}(4, \mathbb{K}) \).

It is easy to see that an analogous result holds for \( \text{PG}(n, \mathbb{K}) \), where \( n \neq 4 \). Moreover, Lemma 5 provides us with the following method to find an arc in \( \text{PG}(4, q) \). Assume that we find a \( k \)-arc \( \mathcal{P} \) in \( \text{PG}(4, \mathbb{Q}(\xi)) \), where \( \mathbb{Q}(\xi) \) is a number field. Lemma 5 implies that, given any subset \( K \) of \( \mathcal{P} \) of size five, we know that \( \det(X) \neq 0 \) for some \( X \in [K] \). Roughly speaking, if each of these determinants is nonzero in the reduction modulo \( p \), then the image of \( \mathcal{P} \) will be a \( k \)-arc in the reduction modulo \( p \). In fact, there can only be a finite number of primes \( p \) for which the reduction of \( \mathcal{P} \) modulo \( p \) fails to be a \( k \)-arc. The remainder of this section is dedicated to first formalizing this idea (Proposition 6) and then finding an effective method for computing a finite list of primes for which there may fail to be a \( k \)-arc in the reduction (Lemma 8).

Henceforth in this section, let \( f(x) \) be an irreducible polynomial over \( \mathbb{Z} \), and let \( R := \mathbb{Z}[\xi] \), where \( \xi \) is a root of \( f \). By abuse of notation, we identify \( R \) with the field \( \mathbb{Z}[x]/(f(x)) \). Let \( \phi_{f(x)} \) be the homomorphism

\[
\phi_{f(x)} : \mathbb{Z}[x] \to \mathbb{Z}[x]/(f(x)) \cong R.
\]

For a prime \( p \) such that \( f(x) \) is still irreducible modulo \( p \), let \( \phi_p \) be the homomorphism

\[
\phi_p : R \cong \mathbb{Z}[x]/(f(x)) \to \mathbb{Z}/p\mathbb{Z}[x]/(f(x)).
\]

Thus

\[
\phi_{f(x)}\phi_p : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]/(f(x)),
\]

and, since \( \text{Ker}(\phi_{f(x)}\phi_p) = \{ p \cdot f(x) \} \) is a maximal ideal of \( \mathbb{Z}[x] \), the image of \( R \) under \( \phi_p \) is a field, and we let \( \text{GF}(q) \) be the finite field \( R^{\phi_p} \).
In the following proposition, note that \( \mathcal{P} \) corresponds to a \( k \)-arc in \( PG(4, \mathbb{Q}(\zeta)) \), and so what we are really doing is verifying that, for infinitely many primes \( p \), the reduction of this \( k \)-arc modulo \( p \) is still a \( k \)-arc in the associated finite projective space.

**Proposition 6** Let \( \mathcal{P} \) be a subset of \( R^5 \) of size \( k \), and suppose for each subset \( J \) of \( \mathcal{P} \) of size five that \( \det(X) \neq 0 \) for some \( X \in [J] \). Let \( Q \) be an infinite set of prime powers such that, if \( q \in Q \), then \( GF(q) \cong R^{\phi_p} \) for some prime \( p \). Then, there exist infinitely many \( q \in Q \) such that \( \mathcal{P}_q := \mathcal{P}^{\phi_q} \) is a \( k \)-arc in \( PG(4, q) \).

**Proof** Assume that \( p \) is a prime such that \( \mathcal{P}_p \) is not a \( k \)-arc of \( PG(4, R^{\phi_p}) = PG(4, q) \). This implies that there is a set of five projective points \( K = \{P_1, P_2, P_3, P_4, P_5\} \) of \( \mathcal{P}_p \) contained in a hyperplane, which implies that \( \det(X) = 0 \) for every matrix \( X \in [K] \). Let each \( P_i \) correspond to the vector \( v_i \in \mathcal{P} \) and \( J = \{v_1, v_2, v_3, v_4, v_5\} \). Since \( \det(Y) \neq 0 \) for some \( Y \in [J] \) by assumption and the matrices of \( [J] \) differ by elementary row operations, this implies that no matrix in \( [J] \) has zero determinant in \( R \). Hence, for some matrix \( Y \in [J] \), \( \det(Y) \) is nonzero in \( R \), but the corresponding determinant is zero in \( GF(q) \).

On the other hand, there are only finitely many subsets of size five of \( \mathcal{P} \), namely \( \binom{k}{5} \). For each subset \( J \) of size five, there are only finitely many different matrices in \( [J] \), which means there are only finitely many different values of \( \det(X) \), where \( X \in [J] \). Since each such determinant is nonzero, for each \( X \in [J] \), there are only finitely many different primes \( p \) such that \( \det(X^{\phi_p}) = 0 \) in \( GF(q) \), where \( q \) is a power of \( p \). Therefore, there are only finitely many primes such that \( \mathcal{P}_p \) is not a \( k \)-arc in \( PG(4, q) \). The result follows.

More practically, we want to be able to determine in an efficient manner precisely which primes will yield a \( k \)-arc. We first define notation that will be useful.

**Definition 7** Let \( \mathcal{P} \) be a subset of \( R^5 \) of size \( k \), and suppose for each subset \( J \) of \( \mathcal{P} \) of size five that \( \det(X) \neq 0 \) for some \( X \in [J] \). Let \( X_p \) be a set of representatives of \( [J] \) as \( J \) runs over the subsets of size five of \( \mathcal{P} \). Let \( D_p := \{\det(X) : X \in X_p\} \), let \( E_p \) be set of all minimal polynomials of the elements of \( D_p \) over \( \mathbb{Q} \), and let \( F_p \) be the set of all polynomials in \( E_p \) rationalized such that all coefficients are in \( \mathbb{Z} \) (and the coefficients of polynomials in \( F_p \) have greatest common divisor 1). We define \( C_p \) to be the set of prime factors of the constant terms of the polynomials in \( F_p \).

The following lemma provides a method for finding every prime such that \( \mathcal{P}^{\phi_p} \) is not a \( k \)-arc.

**Lemma 8** If \( p \) is a prime such that \( f(x) \) is irreducible modulo \( p \) and \( p \notin C_p \), then \( \mathcal{P}_p := \mathcal{P}^{\phi_p} \) is a \( k \)-arc in \( PG(4, q) \), where \( GF(q) \cong R^{\phi_p} \).

**Proof** We first make an observation. Fix \( J \subset \mathcal{P}, |J| = 5 \), and let \( X, Y \in [J] \). Since \( X \) and \( Y \) differ only in the order in which the rows appear in each matrix, \( \det(Y) = \pm \det(X) \), and so \( \det(X^{\phi_p}) = 0 \) if and only if \( \det(Y^{\phi_p}) = 0 \). It thus suffices to consider a representative of each class \( [J] \).

Assume that \( p \) is a prime but that \( \mathcal{P}_p := \mathcal{P}^{\phi_p} \) is not a \( k \)-arc in \( PG(4, q) \), where \( GF(q) \cong R^{\phi_p} \). This means that there exists some subset \( J \) of \( \mathcal{P} \) such that \( \det(X^{\phi_p}) = 0 \) for all \( X \in [J] \). Let \( d := \det(X) \) for some \( X \in [J] \), and define \( f_d(x) \) to be the minimal polynomial of \( d \) over \( \mathbb{Q} \). There exists \( N \in \mathbb{N} \) such that \( g_d(x) := N \cdot f_d(x) \in \mathbb{Z}[x] \) and the coefficients of \( g_d(x) \) have greatest common divisor 1. Since \( f_d(d) = 0 \in \mathbb{Q} \), \( g_d(d)^{\phi_p} = 0 \in GF(q) \). On the other hand \( d^{\phi_p} = 0 \in GF(q) \), and so

\[
g_d(d)^{\phi_p} = c_d^{\phi_p},
\]
where \( c_d \) is the constant term of \( g_d(x) \), which implies that \( p \mid c_d \), i.e., \( p \in \mathbb{C}_P \). The result follows. \( \square \)

Indeed, in practice the hypotheses of Lemma 8 can be checked relatively quickly in GAP for \( k \)-arcs of moderate size.

4 Transitive PSL(2,11)-invariant 110-arcs in PG(4,q)

4.1 Existence

We recall from Sect. 2 that there is a 5-dimensional representation of PSL(2, 11) over \( \mathbb{Z}[\xi] \) with generators

\[
A := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 1 & -c & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad B := \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 \\ c + 1 & 0 & 0 & -1 & c + 2 \\ 1 & 0 & 0 & -1 & 1 \end{pmatrix},
\]

where \( c = \xi + \xi^3 + \xi^4 + \xi^5 + \xi^9 = (-1 + i\sqrt{11})/2 \) for a primitive 11th root of unity \( \xi \).

By [1], \( M := ABABABABB \) has order 6 in \( G := \langle A, B \rangle \cong \text{PSL}(2, 11) \). Suppose \( v \) is an eigenvector of \( M \). This means \( vM \in \langle v \rangle \), and so \( \langle v \rangle \) is fixed by \( H := \langle M \rangle \). If \( T_1, \ldots, T_{110} \) are representatives of the distinct cosets of \( \langle M \rangle \), then we will see that the 110-arc we are looking for comes from the projective points associated to the linear subspaces \( \langle vT_1 \rangle, \ldots, \langle vT_{110} \rangle \). Note that, in order to get a suitable eigenvector \( v \), there need eventually to exist third roots of unity in the finite field, and so we work in \( \mathbb{Z}[\xi_{33}] \), where \( \xi_{33} \) is a primitive 33rd root of unity.

**Proposition 9** Let \( G = \langle A, B \rangle \) and \( H := \langle M \rangle \), as above. Let \( T_1 = I, \ldots, T_{110} \) be a set of representatives of the distinct cosets of \( H \) in \( G \). Then, there exists an eigenvector \( v \) of \( H \) such that any subset \( J \) of size five of the set \( \mathcal{P} := \{ v, vT_2, \ldots, vT_{110} \} \) has the property that \( \det(X) \neq 0 \) for some \( X \in [J] \).

**Proof** This follows by [11, Calculation A.2]. We note that it took approximately 6.8 GB of RAM to complete this calculation. \( \square \)

**Theorem 10** There are infinitely many primes \( p \) such that, if \( GF(q) = \mathbb{Z}[\xi_{33}]^{\phi_p} \), then there exists a PSL(2, 11)-transitive 110-arc in PG(4, q).

**Proof** This follows from Propositions 9 and 6. \( \square \)

4.2 Examples

With the aid of GAP and the package FinInG [2], we are able to calculate specific primes and prime powers \( q \) such that there is a PSL(2, 11)-transitive 110-arc in PG(4, q).

Assume that \( p \) is a prime and that there exists a faithful representation of PSL(2, 11) over GF(p). In this case, we need both primitive 11th and primitive 3rd roots of unity to exist in GF(p); hence, we assume that \( p^5 \equiv 1 \) (mod 11) and \( p \equiv 1 \) (mod 3). We are now ready to prove Theorem 1.
Proof of Theorem 1  That there are infinitely many such primes follows from the fact that \( \text{GF}(p) = \mathbb{Z}[\xi_{33}]^{\phi\varphi} \) whenever \( p \equiv 1 \pmod{33} \) by the above discussion, Propositions 9, and 6.

By Lemma 8 and [11, Calculation A.4], the possible primes \( p \) for which PG(4, \( p \)) does not contain a 110-arc are explicitly known. These calculations have further been verified for all primes \( p \) such that \( p^5 \equiv 1 \pmod{33} \) and \( p < 65,000 \) using [11, Functions A.7, A.8]. Moreover, we have verified all of these calculations for both irreducible 5-dimensional representations of PSL(2, 11) over \( \mathbb{C} \), although these calculations are omitted since they are analogous to the ones listed.

There are many prime powers such that \( \text{GF}(p) \) contains a primitive 11th root of unity but not a primitive 3rd root of unity. In this case, \( p^5 \equiv 1 \pmod{11} \) and \( p \equiv 2 \pmod{3} \). In this case, we need to adjoin a primitive third root of unity to \( \text{GF}(p) \), and so we examine \( \text{GF}(p^2) \).

We are now ready to prove Theorem 2.

Proof of Theorem 2  That there are infinitely many such primes follows from the fact that \( \text{GF}(p^2) = \mathbb{Z}[\xi_{33}]^{\phi\varphi} \) whenever \( p^5 \equiv 23 \pmod{33} \) and \( p \) by the above discussion, Propositions 9, and 6.

By Lemma 8 and [11, Calculation A.4], the possible primes \( p \) for which PG(4, \( p^2 \)) does not contain a 110-arc are explicitly known. These calculations have further been verified for all primes \( p \) such that \( p^5 \equiv 23 \pmod{33} \) and \( p < 65,000 \) using [11, Functions A.9, A.10]. Moreover, we have verified all of these calculations for both irreducible 5-dimensional representations of PSL(2, 11) over \( \mathbb{C} \), although these are omitted since they are analogous to the ones listed.

5 Transitive PSL(2,11)-invariant 60-arcs in PG(4,q)

5.1 Existence

We recall from Sect. 2 that there is a 5-dimensional representation of PSL(2, 11) over \( \mathbb{Z}[\xi] \) with generators

\[
A := \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
1 & -1 & c & 1 & -c \\
0 & 0 & 1 & 0 & 0
\end{pmatrix},
B := \begin{pmatrix}
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & -1 & -1 & 0 & 0 \\
c + 1 & 0 & 0 & -1 & c + 2 \\
1 & 0 & 0 & -1 & 1
\end{pmatrix},
\]

where \( c = \xi + \xi^3 + \xi^4 + \xi^5 + \xi^9 = (-1 + i \sqrt{11})/2 \) for a primitive 11th root of unity \( \xi \).

By [1], \( M := AB \) is an element of order 11 in \( \langle A, B \rangle \cong \text{PSL}(2, 11) \). Suppose \( v \) is an eigenvector of \( M \). This means \( vM \in \langle v \rangle \), and so \( \langle v \rangle \) is fixed by \( H := \langle M \rangle \). If \( T_1, \ldots, T_{60} \) are representatives of the distinct cosets of \( \langle M \rangle \), then we will see that the 60-arc we are looking for comes from the projective points associated to the linear subspaces \( \langle vT_1 \rangle, \ldots, \langle vT_{60} \rangle \).

Proposition 11  Let \( G = \langle A, B \rangle \) and \( H := \langle M \rangle \), as above. Let \( T_1 = I, \ldots, T_{60} \) be a set of representatives of the distinct cosets of \( H \) in \( G \). Then, there exists an eigenvector \( v \) of \( H \) such that any subset \( J \) of size five of the set \( \mathcal{P} := \{v, vT_2, \ldots, vT_{60}\} \) has the property that \( \det(X) \neq 0 \) for some \( X \in [J] \).

Proof  This follows by [11, Calculation A.3].
Theorem 12 There are infinitely many primes \( p \) such that, if \( GF(q) = \mathbb{Z}[[\xi]]^{\Phi_p} \), then there exists a \( \text{PSL}(2, 11) \)-transitive 60-arc in \( PG(4, q) \).

Proof This follows from Propositions 11 and 6.

5.2 Examples

With the aid of GAP and the package FinInG [2], we are able to calculate specific primes and prime powers \( q \) such that there is a \( \text{PSL}(2, 11) \)-transitive 60-arc in \( PG(4, q) \).

Assume that \( p \) is a prime and that there exists a faithful representation of \( \text{PSL}(2, 11) \) over \( GF(p) \). In this case, we need the constant \( c \) to exist in \( GF(p) \); hence, we assume that \( p^5 \equiv 1 \pmod{11} \). Moreover, the eigenvalue we choose is actually a primitive 11th root of unity, so we assume further that \( p \equiv 1 \pmod{11} \). We are now ready to prove Theorem 3.

Proof of Theorem 3 That there are infinitely many such primes follows from the fact that \( GF(p) = \mathbb{Z}[[\xi]]^{\Phi_p} \) whenever \( p \equiv 1 \pmod{11} \) by the above discussion, Propositions 11 and 6.

By Lemma 8 and [11, Calculation A.5], the possible primes \( p \) for which \( PG(4, p) \) does not contain a 60-arc are explicitly known. These calculations have further been verified for all primes \( p \) such that \( p^5 \equiv 1 \pmod{11} \) and \( p < 65,000 \) using [11, Functions A.11, A.12]. Moreover, we have verified all of these calculations for both irreducible 5-dimensional representations of \( \text{PSL}(2, 11) \) over \( \mathbb{C} \), although these are omitted since they are analogous to the ones listed.

Acknowledgements The authors would like to thank John Bamberg for helpful discussions about the GAP package FinInG and Jan De Beule for GAP code that allows for calculations using FinInG beyond what is normally possible in GAP. The authors would also like to thank the anonymous referees for many useful suggestions that improved the readability of this paper.

References

1. Abbott R., Bray J., Linton S., Nickerson S., Norton S., Parker R., Suleiman I., Tripp J., Walsh P., Wilson R.: Atlas of finite group representations—version 3. http://brauer.maths.qmul.ac.uk/Atlas/v3/.
2. Bamberg J., Betten A., Cara Ph, De Beule J., Lavrauw M., Neunhöffer M.: Finite incidence geometry. FinInG—a GAP package, version 1(4) (2017).
3. Bartoli D., Giulietti M., Platoni I.: On the covering radius of MDS codes. IEEE Trans. Inf. Theory 61(2), 801–811 (2015).
4. Bray J.N., Holt D.F., Roney-Dougal C.M.: The maximal subgroups of the low-dimensional finite classical groups. With a foreword by M. Liebeck. London Mathematical Society Lecture Note Series, 407. Cambridge University Press, Cambridge (2013).
5. Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson R.A.: Atlas of finite groups. Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G, Thackray (1985).
6. Giulietti M., Korchmáros G., Marcugini S., Pambianco F.: Transitive \( A_6 \)-invariant \( k \)-arcs in \( PG(2, q) \). Des. Codes Cryptogr. 68, 73–79 (2013).
7. Indaco L., Korchmáros G.: 42-arcs in \( PG(2, q) \) left invariant by \( \text{PSL}(2, 7) \). Des. Codes Cryptogr. 64, 33–46 (2012).
8. Jackson W.-A., Martin K.M., O’Keefe C.M.: Geometrical contributions to secret sharing theory. J. Geom. 79(1–2), 102–133 (2004).
9. Korchmáros G., Pace N.: Infinite family of large complete arcs in \( PG(2, q^n) \) with \( q \) odd and \( n > 1 \) odd. Des. Codes Cryptogr. 55, 285–296 (2010).
10. Korchmáros G., Lanzone V., Sonnino A.: Projective \( k \)-arcs and 2-level secret-sharing schemes. Des. Codes Cryptogr. 64(1–2), 3–15 (2012).
11. Olson T., Swartz E.: Transitive PSL(2, 11)-invariant $k$-arcs in $\text{PG}(4, q)$ (including supporting GAP code). arXiv:1804.09707.
12. Pace N.: On small complete arcs and transitive $A_5$-invariant arcs in the projective plane $\text{PG}(2, q)$. J. Comb. Des. 22(10), 425–434 (2014).
13. Pace N., Sonnino A.: On linear codes admitting large automorphism groups. Des. Codes Cryptogr. 83(1), 115–143 (2017).
14. Simmons G.J., Jackson W.-A., Martin K.M.: The geometry of shared secret schemes. Bull. Inst. Comb. Appl. 1, 71–87 (1991).
15. Sonnino A.: Transitive PSL(2, 7)-invariant 42-arcs in 3-dimensional projective spaces. Des. Codes Cryptogr. 72, 455–463 (2014).
16. Thas J.A.: M.D.S. codes and arcs in projective spaces: a survey. Mathematiche (Catania) 47(2), 315–328 (1993).
17. The GAP Group. GAP—Groups, Algorithms, and Programming, Version 4.8.9 (2017). https://www.gap-system.org.
18. Tolhuizen L.M.G.M., van Gils W.J.: A large automorphism group decreases the computations in the construction of an optimal encoder/decoder pair for a linear block code. IEEE Trans. Inf. Theory 34(2), 333–338 (1988).

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.