The complete arcs of PG(2,31)

Kris Coolsaet
Department of Applied Mathematics,
Computer Science and Statistics,
Ghent University,
Krijgslaan 281–S9, B–9000 Gent, Belgium
Kris.Coolsaet@UGent.be
March 2014

We obtained a full computer classification of all complete arcs in the Desarguesian projective plane of order 31 using essentially the same methods as for earlier results for planes of smaller order, i.e., isomorph-free backtracking using canonical augmentation.

We tabulate the resulting numbers of complete arcs according to size and automorphism group. We give explicit descriptions for all complete arcs with an automorphism group of size at least 20. In some of these cases the constructions can be generalized to other values of q. In particular, we find arcs of size $\frac{2}{3}(q + 2)$ for any field of order $q = 1 \pmod{6}$, and a 44-arc in PG(2,67) with an automorphism group of order 88.

We also correct a result by Kéi : there are 12 complete 22-arcs in PG(2,31) up to projective equivalence, and not 11.

1 Introduction

Let PG(2, q) denote the Desarguesian projective plane of order q. For a positive integer k, a $k$-arc of PG(2, q) is a set of k points of the plane no three of which are collinear. An arc is called complete if it is not strictly included in another arc. (For further information on the geometrical properties of $k$-arcs we refer to [6].)

In earlier publications [3, 4] we have reported on exhaustive computer searches for arcs in planes of order 23, 25, 27 and 29. In this paper we present the results for $q = 31$. We essentially use the same methods as before, but with one important difference : because of the sheer size of the generated data ($\approx 1800$ GBytes after compression) we had no longer the possibility to store all arcs for further processing. Instead we only stored the complete arcs of small size ($\leq 14$), of large size ($\geq 22$) and those with a non-trivial automorphism group, in the hope that all ‘interesting’ arcs would be present in this reduced collection. Although not all of them were stored, all complete arcs were still generated and counted, up to isomorphism.
The entire search took 70 years of CPU time, suggesting that the next odd case \( q = 37 \) might still stay out of reach for several years.

Some earlier (partial) results about arcs in \( \text{PG}(2,31) \) were already obtained by other authors. Bartoli et al. \[1\] found that the smallest complete arcs have size 14. Kéri \[7\] reported that there are 11 non-isomorphic complete arcs of size 22. This result is however not correct: Kéri somehow overlooked the 22-arc of Section 2.

Tables 1–2 summarize the full classification we have obtained of the complete \( k \)-arcs in \( \text{PG}(2,31) \). Each column corresponds to a different arc size \( k \). \( N_k \) denotes the number of projectively inequivalent complete arcs of size \( k \). The arcs have been listed according to the isomorphism type of their stabilizer group \( G_S \) within the projective group \( G = \text{PGL}(3,31) \). For each group type and size we print the corresponding number of arcs. We use Atlas-notation \[2\] for the groups. There are no complete \( k \)-arcs when \( k < 14, 23 \leq k \leq 31 \) or \( k > 32 \).

In subsequent sections we give an explicit description of all complete arcs with an automorphism group of size at least 20, except for the arc of size 32 which is the conic.

### 2 Arcs on two conics

Consider a field \( \text{GF}(q) \) with \( q = 1 \pmod{6} \). For \( A,B \in \text{GF}(q), A,B \neq 0 \), define \( K_3(A,B) \) to be the set of points with coordinates \( (At,1,B/t) \) such that \( t \) is a non-zero cube. For any \( k \in \text{GF}(q), k \neq 0 \), we have \( K_3(A,B) = K_3(Ak^3, Bk^{-3}) \), hence we can always choose \( A = 1, \alpha \) or \( \alpha^2 \), where \( \alpha \) is a generator of the multiplicative group of the field.

Note that the points of \( K_3(A,B) \) lie on the conic with equation \( XZ = ABY^2 \). In fact, the conic with equation \( XZ = CY^2 \) with \( C \in \text{GF}(q), C \neq 0 \), can be written as the disjoint union of the following sets:

\[
\{(1,0,0),(0,0,1)\}, \quad K_3(1,C), \quad K_3(\alpha, C/\alpha), \quad K_3(\alpha^2, C/\alpha^2).
\]
<table>
<thead>
<tr>
<th>$k$</th>
<th>$N_k$</th>
<th>$G_S$</th>
<th>#</th>
<th>$k$</th>
<th>$N_k$</th>
<th>$G_S$</th>
<th>#</th>
<th>$k$</th>
<th>$N_k$</th>
<th>$G_S$</th>
<th>#</th>
<th>$k$</th>
<th>$N_k$</th>
<th>$G_S$</th>
<th>#</th>
<th>$k$</th>
<th>$N_k$</th>
<th>$G_S$</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>1014806907</td>
<td>1</td>
<td>1014134408</td>
<td>1</td>
<td>5992950</td>
<td>2</td>
<td>665004</td>
<td>2</td>
<td>8933</td>
<td>3</td>
<td>2312</td>
<td>2</td>
<td>590</td>
<td>3</td>
<td>134</td>
<td>2</td>
<td>13</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>5992950</td>
<td>2</td>
<td>19481</td>
<td>3</td>
<td>134</td>
<td>3</td>
<td>7</td>
<td>S3</td>
<td>6</td>
<td>S3</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>8933</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>PGL(2, 31)</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>28</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>17</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>12</td>
<td>3</td>
<td>2</td>
<td>17</td>
<td>4</td>
<td>2</td>
<td>17</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Complete $k$-arcs in PG(2, 31) for $k = 18, \ldots, 22, 32$.

The set $K_3(1, 1)$ is left invariant by the following projectivities:

$$
\phi_1: (x, y, z) \mapsto (\alpha^3 x, y, \alpha^{-3} z), \\
\phi_2: (x, y, z) \mapsto (z, y, x).
$$

$\phi_1$ has order $\frac{1}{3}(q - 1)$, $\phi_2$ has order 2 and together they generate the dihedral group $D_{2(q - 1)}$.

Note that $\phi_1$ leaves invariant all sets $K_3(A, B)$ while $\phi_2$ leaves invariant all sets $K_3(A, B)$ for which $B/A$ is a cube.

In this section, a pair $(A, B)$ with $A, B \neq 0$ will be called special if and only if neither of the following equations has a solution $x, y \in GF(q) - \{0\}$.

$$
(x^3 - A)(y^3 - B) = AB - 1, \quad (Ax^3 - 1)(By^3 - 1) = 1 - AB.
$$

(The second equation is obtained from the first by substituting $1/A$ for $A$ and $1/B$ for $B$.)

**Theorem 1.** Let $A, B \in GF(q)$, $A, B \neq 0$, $AB \neq 1$, with $q = 1 \pmod{6}$. Then

$$
S(A, B) \overset{\text{def}}{=} K_3(1, 1) \cup K_3(A, B)
$$

is an arc if and only if $(A, B)$ is special.

In that case, the arc $S(A, B)$ can be extended to

- an arc $S_1(A, B) \overset{\text{def}}{=} S(A, B) \cup \{(0, 0, 1)\}$, if and only if $A$ is not a cube,
- an arc $S_2(A, B) \overset{\text{def}}{=} S(A, B) \cup \{(1, 0, 0)\}$, if and only if $B$ is not a cube, and
- an arc $S_{12}(A, B) \overset{\text{def}}{=} S(A, B) \cup \{(1, 0, 0), (0, 0, 1)\}$, if and only if neither $A$ nor $B$ is a cube.
We have \( |S(A, B)| = \frac{2}{3}(q - 1) \), \( |S_1(A, B)| = |S_2(A, B)| = \frac{1}{3}(2q + 1) \) and \( |S_{12}(A, B)| = \frac{2}{3}(q + 2) \).

**Proof.** Because \( K_3(1, 1) \) and \( K_3(A, B) \) are parts of conics, any line that intersects \( S(A, B) \) in more than two points must contain at least one point of \( K_3(1, 1) \) and at least one point of \( K_3(A, B) \). Because of the action of \( \phi_1 \) we may assume without loss of generality that the point of \( K_3(1, 1) \) corresponds to \( t = 1 \).

The line \( \ell \) connecting \((1, 1, 1)\) with \((At, 1, B/t)\) has equation

\[
(B - t)X + (At^2 - B)Y + (t - At^2)Z = 0. \tag{2}
\]

This line has a third point in \( K_3(1, 1) \), say \((u, 1, 1/u)\), if and only if

\[
0 = (B - t)u + (At^2 - B) + (t - At^2)/u \\
= Bu - tu + At^2 - B + t/u - At^2/u \\
= (u - 1)(B + At^2/u - t - t/u) = (u - 1)t(AB - 1 - (A - 1/t)(B - t/u)].
\]

Similarly, \( \ell \) has a third point in \( K_3(A, B) \), say \((Au, 1, B/u)\), if and only if

\[
0 = (B - t)Au + (At^2 - B) + (t - At^2)B/u \\
= ABu - Atu + At^2 - B + Bt/u - ABt^2/u \\
= (u - t)(AB + ABt/u - At - B/u) = (u - t)[AB - 1 + (A - 1)(B - t/u)].
\]

Because \((1/t, t/u)\) and \((t, 1/u)\) range over all pairs of non-zero cubes when \((t, u)\) does, it follows that \( S(A, B) \) is an arc if and only if \((A, B)\) is special.

To check whether \( S_1(A, B) \) is an arc, we must check additional lines through \((0, 0, 1)\). Because this point lies on both conics, it is again sufficient to check that it does not lie on any line of the form (2). This will be true if and only if \( t - At^2 \neq 0 \), i.e., \( A \neq 1/t \) for any non-zero cube \( t \). In other words, if \( A \) is not a cube. By symmetry (e.g., applying \( \phi_2 \)), \( S_2(A, B) \) is an arc if an only if \( B \) is not a cube. And because both arguments can be applied independently, \( S_{12}(A, B) \) will be an arc if and only if neither \( A \) nor \( B \) is a cube. \( \square \)

Unfortunately, there seem to be only few pairs \((A, B)\) (with \( A, B \neq 0 \), \( AB \neq 1 \)) that are special. A small computer program yields the following pairs for all fields of order \( q = 1 \) (mod 6), \( q < 256 \), and for \( q < 32768 \) with \( q \) prime.

<table>
<thead>
<tr>
<th>( q )</th>
<th>((A, B))</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>13</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>19</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>25</td>
<td>(1, ±(\sqrt{2}))</td>
</tr>
<tr>
<td>31</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>37</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>43</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>67</td>
<td>(1, 1)</td>
</tr>
</tbody>
</table>

Pairs are only listed up to the following equivalence:

\[
(A, B) \simeq (At^3, Bk^{-3}), \quad (A, B) \simeq (B, A) \simeq (1/A, 1/B) \simeq (1/B, 1/A).
\]

(Equivalent pairs yield equivalent arcs.)
The case \((A, B) = (1, -1)\) yields arcs of size \(\frac{2}{3}(q - 1)\) with an additional automorphism \(\phi_3 : (x, y, z) \mapsto (x, y, -z)\) which interchanges \(K_3(1, 1)\) and \(K_3(1, -1)\). For \(q = 31\) we find the unique complete arc of size 20 with \(G_S \simeq D_{20}\).2 and for \(q = 67\) we find an arc of size 44 with \(G_S \simeq D_{44.2}\).

For \(q = 31\) the case \((A, B) = (3, -12)\), or equivalently \((A, B) = (5, -5)\), produces the unique complete arc of size 22 with \(G_S \simeq D_{20}\).

Finally, note that the recipe (and the arguments) of this section can be extended to \(k\)-th powers instead of cubes, yielding arcs of sizes \(\frac{2}{3}(q - 1), \frac{2}{3}(q - 1) + 1\) and \(\frac{2}{3}(q - 1) + 2\). Unfortunately, for \(k > 3\), the resulting arcs are rather small.

For \(k = 2\) special pairs \((A, B)\) are very scarce. We find \((A, B) = (1, -1)\) for \(q = 5\), yielding a trivial arc of size 4, and for \(q = 13\), yielding the exceptional complete 12-arc in \(PG(2, 13)\). For \(q = 9\) we have the special pair \((A, B) = (1, \sqrt{-1})\), producing the exceptional complete 8-arc in \(PG(2, 9)\). In [5] we combined three sets of the form \(K_2(A, B)\) (‘half conics’) to produce several large \((k, 3)\)-arcs.

3 The unique complete arc of size 18 and \(G_S \simeq A_5\)

**Theorem 2.** Let \(K\) be a field with characteristic different from 2, 5 and 11 such that there exists \(\sigma \in K\) with \(\sigma^4 + 5\sigma^2 + 5 = 0\). Let \(\tau = -\sigma^2 - 2\). Consider the following sets of points:

\[
R = \{(1, \pm \tau, 0), (0, 1, \pm \tau), (\pm \tau, 0, 1)\},
\]

\[
S = \{((\pm \tau, 1, \pm \sigma), (\pm \sigma, \pm \tau, 1), (1, \pm \sigma, \pm \tau)\}.
\]

Then \(R \cup S\) is an 18-arc of \(PG(2, q)\) and the alternating group \(A_5\) of 60 elements, generated by

\[
\phi_2 : (x, y, z) \mapsto (x - y, z)
\]

\[
\phi_3 : (x, y, z) \mapsto (y, z, x)
\]

\[
\phi_5 : (x, y, z) \mapsto \frac{1}{2}(x, y, z) \begin{pmatrix}
1 & -\tau^{-1} & \tau \\
-\tau & \tau & 1 \\
-\tau^{-1} & 1 & \tau^{-1}
\end{pmatrix},
\]

stabilizes both \(R\) and \(S\), and hence the entire 18-arc.

**Proof.** Note that \(\tau^2 = \sigma^4 + 4\sigma^2 + 4 = -\sigma^2 - 1 = \tau + 1\). (Hence \(\tau\) is the ‘golden ratio’.) It follows that \(\tau^{-1} = \tau - 1 = -\sigma^2 - 3\).

Also note that \(|R| = 6\) unless \(2\tau = 0\), which cannot happen in odd characteristic. Similarly, in odd characteristic, \(|S| = 12\) unless \(\tau = 0\) or \(\sigma = 0\), which is only possible when the characteristic is 5.

It is fairly easily computed that \(R\) and \(S\) are both orbits of \(A_5\) (and hence must be disjoint). In fact, \(A_5\) acts doubly transitive on \(R\). Hence the lines connecting two different points of \(R\) must form an orbit of \(A_5\). One such line is the line with equation \(Z = 0\). This line intersects \(R\) in exactly two points, and therefore this must be true of all such lines. This proves that \(R\) is an arc.

The points of \(S\) lie on the conic with equation \(X^2 + Y^2 + Z^2 = 0\). Hence \(S\) is an arc. The secant \(Z = 0\) of \(R\) does not intersect \(S\), and therefore, because of the action of \(A_5\), none of the 15 secants of \(R\) intersects \(S\). To prove that \(R \cup S\) is an arc it remains to show that no secant of \(S\) intersects \(R\).
Consider a secant of $S$. $A_5$ acts transitively on the points of $S$ and therefore we may as well choose one point of this secant to have coordinates $(τ, 1, σ)$. The stabilizer in $A_5$ of that point is the group of order 5 generated by $φ_5$. Its orbits on the remaining points of $S$ are of size 1, 5 and 5, as follows

$$(τ, 1, −σ) \quad (1, σ, τ) \quad (1, −σ, −τ) \quad (σ, τ, 1) \quad (−τ, 1, σ) \quad (σ, −τ, 1) \quad (1, −σ, τ) \quad (1, σ, −τ) \quad (−σ, τ, 1) \quad (−τ, 1, −σ) \quad (−σ, −τ, 1)$$

For the second point on the secant we need only consider one point for each of these orbits.

- The line connecting $(τ, 1, σ)$ with $(τ, 1, −σ)$ has equation $X = τY$, and would intersect $R$ only if $τ = 0$ or $τ^2 = ±1$, which is not possible when the characteristic is different from 5.
- The line connecting $(τ, 1, σ)$ with $(-τ, 1, σ)$ has equation $Z = σY$. This line intersects $R$ only if $σ = 0$, $τ = 0$ or $τ = ±σ$. The last equality implies $1 + τ = τ^2 = σ^2 = −τ − 2$ and hence $τ = −3/2$, and therefore $9/4 = 3/2 + 1$, a contradiction.
- The line connecting $(τ, 1, σ)$ with $(−τ, 1, −σ)$ has equation $σX = τZ$. This line intersects $R$ only if $σ = 0$, $τ = 0$ or $σ = ±1$. The last equality implies $0 = σ^4 + 5σ^2 + 5 = 11$. □

For $q = 31$ the theorem yields an arc with $σ = ±4, ±14$. Other examples occur for $q = 41$ with $σ = ±2, ±14$ and $q = 61$ with $σ = ±23, ±25$.

4 The complete arcs of size 18 with $|G_S| = 36$

Consider a finite field $K$ of order $q$ with $q = 1 \pmod{3}$. Then $K$ contains an element $ω \neq 1$ such that $ω^3 = 1$ (and hence $ω^2 + ω + 1 = 0$). For $k ∈ K$ consider the set $E(k)$ of points with the following coordinates:

$$(k, 1, 1) \quad (1, k, 1) \quad (1, 1, k) \quad (k, ω, ω^2) \quad (ω^2, k, ω) \quad (ω, ω^2, k) \quad (k, ω^2, ω) \quad (ω, k, ω^2) \quad (ω^2, ω, k)$$

(Note that $|E(k)| = 9$ if and only if $k \neq 1, ω, ω^2$.)

Every set $E(k)$ is left invariant by the group $G_{18} \simeq S_3 : 3$ of order 18 that is generated by the permutations of the coordinates together with the transformation $(x, y, z) \mapsto (x, ωy, ω^2z)$. The points of $E(k)$ lie on the cubic curve with equation $k(X^3 + Y^3 + Z^3 = (k^3 + 2)XYZ$. This cubic curve is irreducible and non-singular if and only if $k \neq 0, 1, ω, ω^2$.

Lemma 3. Let $k, l ∈ K, k, l \neq 1, ω, ω^2$. Then $E(k) \cap E(l) = \emptyset$ when $k \neq l$.

Proof. Because $G_{18}$ acts transitively on both $E(k)$ and $E(l)$ it is sufficient to prove for one point of $E(l)$ that it does not belong to $E(k)$, say the point with coordinates $(l, 1, 1)$. Now, the only point of $E(k)$ for which the $Y$-coordinate is the same as the $Z$-coordinate, is the point with coordinates $(k, 1, 1)$, which is different from $(l, 1, 1)$. □

Now let $E^*(k)$ denote the dual of $E(k)$, i.e., the sets of lines with equations $Ax + By + Cz = 0$, where $(A, B, C) ∈ E(k)$. 

6
Lemma 4. Let \( k, l \in K, k, l \neq 1, \omega, \omega^2 \).

1. If \( kl = -2 \) then every line of \( E^*(l) \) intersects \( E(k) \) in exactly one point.
2. If \( kl = 1, l + k + 1 = 0, l + \omega k + \omega^2 = 0 \) or \( l + \omega^2 k + \omega = 0 \), then every line of \( E^*(l) \) intersects \( E(k) \) in exactly two points.
3. These are the only values of \( l \) for which \( E^*(l) \) intersects \( E(k) \).

Proof. Because \( G_{18} \) acts transitively on \( E^*(l) \) we need only consider one line of \( E^*(l) \), say the line with equation \( lX + Y + Z = 0 \). The conditions for one of the nine points of \( E(k) \) to lie on this line, are as follows:

\[
\begin{align*}
lk + 2 &= 0 & l + k + 1 &= 0 & l + k + 1 &= 0 \\
lk - 1 &= 0 & l + k\omega + \omega^2 &= 0 & l + k\omega^2 + \omega &= 0 \\
lk - 1 &= 0 & l + k\omega^2 + \omega &= 0 & l + k\omega + \omega^2 &= 0
\end{align*}
\]

To prove the lemma it is sufficient to show that of these 5 conditions no two can occur at the same time. This gives us 10 cases to check. Because the transformations \( l \mapsto l\omega, k \mapsto k\omega^2 \) leave these sets of conditions invariant, we can reduce the proof to the following four cases.

- \( lk + 2 = 0 \) and \( lk - 1 = 0 \). This implies \( 3 = 0 \), contradicting \( q = 1 \mod 3 \).
- \( lk + 2 = 0 \) and \( l + k + 1 = 0 \). We find \( (k - 1)(l - 1) = kl - k - l + 1 = 0 \), contradicting \( k, l \neq 1 \).
- \( lk - 1 = 0 \) and \( l + k + 1 = 0 \). Then \( (k - \omega)(l - \omega) = kl - (k + l)\omega + \omega^2 = 1 + \omega + \omega^2 = 0 \), contradicting \( k, l \neq \omega \).
- \( l + k + 1 = 0 \) and \( l + k\omega + \omega^2 = 0 \). Then \( k(\omega - 1) + (\omega^2 - 1) = 0 \), which yields \( k = \omega^2 \), again a contradiction. \( \square \)

Lemma 5. If \( k \neq 0, 1, \omega, \omega^2, -2, -2\omega, -2\omega^2 \) then \( E(k) \) is an arc. The 36 secants of this arc are the elements of \( E^*(1/k), E^*(-k - 1), E^*(-\omega k - \omega^2) \) and \( E^*(-\omega^2 k - \omega) \).

Proof. The values of \( l \) from the conditions in the proof of Lemma 4 for the 4 secants through the point with coordinates \((k, 1, 1)\) are exactly \( l = 1/k, -k - 1, -\omega k - \omega^2 \) and \(-\omega^2 k - \omega \). Also from that proof it follows that these secants are distinct when \( l \neq 1, \omega, \omega^2 \). For \( l = 1/k \) this yields \( k \neq 1, \omega, \omega^2 \), for \( l = -k - 1 \) this yields \( k \neq -2, \omega, \omega^2 \), for \( l = -\omega k - \omega^2 \) this yields \( k \neq 1, \omega^2, -2\omega \) and for \( l = -\omega^2 k - \omega \), this yields \( k \neq 1, -2\omega^2, \omega \). \( \square \)

The projectivity \((x, y, z) \mapsto (wx, y, z)\) maps \( E(k) \) onto \( E(k\omega) \). The projectivity \( \theta \) given by

\[
\theta : (x \ y \ z) \mapsto (x \ y \ z) \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ \omega^2 & \omega & \end{pmatrix}
\]

interchanges \( E(k) \) and \( E^*(\frac{k+2}{k-1}) \). In particular, the set \( E(k) \cup E(\frac{k+2}{k-1}) \) is invariant under \( \theta \) and has the group \( G_{36} = \langle G_{18}, \theta \rangle \) as an automorphism group. This group has order 36.

The three arcs of size 18 in \( PG(2, 31) \) which have \( G_{36} \) as a group of autoorphisms, are given by the following

Theorem 6. In \( GF(31) \) the following are arcs of size 18:

\[
E(6) \cup E(14), \quad E(8) \cup E(28), \quad E(7) \cup E(19)
\]
Theorem 7. Consider a finite field \( \text{GF}(q) \) with \( q = 1 \pmod{6} \). Let \( \omega \in \text{GF}(q) \) such that \( \omega^3 = 1, \omega \neq 1 \). Let \( a \in \text{GF}(q) \) such that

\[
a \notin \{0, \pm 1, \pm \omega^2, \pm 2, \pm 2\omega, \pm 2\omega^2, \pm \sqrt{-1}, \pm \sqrt{-3}, \pm \frac{2}{3} \sqrt{-3} \}
\]

then \( W \cup S(a) \) is a 20-arc.

Proof. (Note that \( \omega - \omega^2 = \sqrt{-3} \).) By the above we know that \( S(a) \) and \( W \) are arcs. It is also easily seen that they are disjoint. We therefore only need to prove that any line connecting a point \( P \) of \( W \) and a point \( Q \) of \( S(a) \) does not intersect \( W \) or \( S(a) \) in any further points.

Because \( W \) and \( S(a) \) are orbits of \( S_4 \), we may assume without loss of generality that \( P \) is the point with coordinates \((\omega^2, \omega, 1)\). Moreover, for \( Q \) we only need to consider one point for each orbit in \( S(a) \) of the stabilizer of \( P \) in \( S_4 \). The orbits of this stabilizer on \( S(a) \) are as follows:

\[
\{(a, 1, 1), (1, a, 1), (1, 1, a)\}, \quad \{(a, -1, 1), (1, a, -1), (-1, 1, a)\}, \\
\{(a, 1, -1), (-1, a, 1), (1, -1, a)\}, \quad \{(a, -1, -1), (-1, a, -1), (-1, -1, a)\}.
\]
There are therefore four cases to consider:

<table>
<thead>
<tr>
<th></th>
<th>( f_1(X, Y, Z) )</th>
<th>( f_2(X, Y, Z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>((a, 1, 1))</td>
<td>((1 - \omega)X + (\omega^2 - a)Y + \omega(a - \omega)Z = 0)</td>
<td>(0)</td>
</tr>
<tr>
<td>((a, -1, 1))</td>
<td>((-1 - \omega)X + (\omega^2 - a)Y + \omega(a + \omega)Z = 0)</td>
<td>(-2\omega)</td>
</tr>
<tr>
<td>((a, 1, -1))</td>
<td>((-1 - \omega)X + (\omega^2 + a)Y + \omega(-a + \omega)Z = 0)</td>
<td>(2\omega(a + \omega))</td>
</tr>
<tr>
<td>((a, -1, -1))</td>
<td>((1 - \omega)X + (\omega^2 + a)Y + \omega(-a - \omega)Z = 0)</td>
<td>(2\omega(a + \omega))</td>
</tr>
</tbody>
</table>

Note that \( f_3, f_4 \) can be obtained from \( f_2, f_1 \) by substituting \(-a\) from \(a\). The table below lists all values of \( f_1(X, Y, Z) \) and \( f_2(X, Y, Z) \) for the 20 points of \( W \cup S(a) \).

<table>
<thead>
<tr>
<th>((X, Y, Z))</th>
<th>( f_1(X, Y, Z) )</th>
<th>( f_2(X, Y, Z) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\omega^2, \omega, 1))</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>((-\omega^2, \omega, 1))</td>
<td>(2 - 2\omega^2)</td>
<td>(-2\omega)</td>
</tr>
<tr>
<td>((\omega^2, -\omega, 1))</td>
<td>(2\omega(a - \omega^2))</td>
<td>(2\omega(a + \omega))</td>
</tr>
<tr>
<td>((-\omega^2, -\omega, 1))</td>
<td>(2\omega(a - \omega))</td>
<td>(2\omega(a + \omega))</td>
</tr>
<tr>
<td>((\omega, \omega^2, 1))</td>
<td>((\omega - \omega^2)(2 + a))</td>
<td>((\omega - \omega^2)a)</td>
</tr>
<tr>
<td>((-\omega, \omega^2, 1))</td>
<td>(\omega - \omega^2)a)</td>
<td>(-2 + (\omega - \omega^2)a)</td>
</tr>
<tr>
<td>((\omega, -\omega^2, 1))</td>
<td>(-a - 2\omega)</td>
<td>(-a - 2\omega)</td>
</tr>
<tr>
<td>((-\omega, -\omega^2, 1))</td>
<td>(-a - 2\omega)</td>
<td>(-a + 2\omega)</td>
</tr>
<tr>
<td>((a, 1, 1))</td>
<td>0</td>
<td>(-2(a - \omega^2))</td>
</tr>
<tr>
<td>((a, -1, 1))</td>
<td>(2(a - \omega^2))</td>
<td>0</td>
</tr>
<tr>
<td>((a, 1, -1))</td>
<td>(-2\omega(a - \omega))</td>
<td>(2\omega^2a)</td>
</tr>
<tr>
<td>((a, -1, -1))</td>
<td>(2(1 - \omega)a)</td>
<td>(-2\omega(a + \omega))</td>
</tr>
<tr>
<td>((1, a, 1))</td>
<td>((2 + a)(1 - a))</td>
<td>(2\omega^2 - a - a^2)</td>
</tr>
<tr>
<td>((-1, a, 1))</td>
<td>(2\omega - a - a^2)</td>
<td>(-a(a + 1))</td>
</tr>
<tr>
<td>((1, a, -1))</td>
<td>(-a + 2\omega a)</td>
<td>(a(\omega^2 - \omega - a))</td>
</tr>
<tr>
<td>((-1, a, -1))</td>
<td>(-2 + (\omega^2 - \omega)a - a^2)</td>
<td>(-a - 1)(\omega^2 - a)</td>
</tr>
<tr>
<td>((1, 1, a))</td>
<td>(\omega(a - 1)(a + 2))</td>
<td>(\omega(a + 1)(a + 2)</td>
</tr>
<tr>
<td>((-1, 1, a))</td>
<td>(-2 + \omega a + \omega a^2)</td>
<td>(a(\omega^2 - 1 + \omega a))</td>
</tr>
<tr>
<td>((1, -1, a))</td>
<td>(\omega(a + 1)(a + 2\omega^2))</td>
<td>(\omega(a - 1))</td>
</tr>
<tr>
<td>((-1, -1, a))</td>
<td>(\omega(a^2 + (\omega^2 - \omega)a + 2))</td>
<td>(\omega(a^2 - a - 2\omega))</td>
</tr>
</tbody>
</table>

The set \( W \cap S(a) \) will be an arc if and only if none of the expressions in the last two columns is equal to zero (except for the 4 entries that have already been noted as such), also with \(-a\) substituted for \(a\). This yields

\[
a \neq \pm 1, \pm \omega, \pm \omega^2, \pm 2, \pm 2\omega, \pm 2\omega^2, \pm \sqrt{-3}, \pm \frac{2}{3}\sqrt{-3}
\]

and

\[
a^2 \neq a - 2\omega, a^2 \neq a - 2\omega^2, a^2 \neq \sqrt{-3}a + 2 \neq 0.
\]

These last conditions can be rewritten as

\[
a \neq \frac{1}{2}(\pm 1 \pm \sqrt{\pm 4\sqrt{-3} - 3}), \frac{1}{2}(\pm \sqrt{-3} \pm \sqrt{-11}).
\]

Together with (3) these form the conditions of the theorem.

In GF(31) the conditions of this theorem translate to

\[
a \neq 0, \pm 1, \pm 5, \pm 6, \pm 2, \pm 10, \pm 12, \pm 11, \pm 3, \pm 8, \pm 9, \pm 15, \pm 4,
\]

leaving only \(a = \pm 7, \pm 13, \pm 14\) as possibilities.
Acknowledgements

We are grateful to Ghent University, the Hercules Foundation and the Flemish Government — department EWI, for providing the computational resources (Stevin Supercomputer Infrastructure) and services which were used to obtain our results.

References


