Rendiconti di Matematica, Serie VII
Volume 16, Roma (1996), 537-544

A complete 24-arc in PG(2,29) with the automorphism group PSL(2,7)

J. M. CHAO – H. KANETA

Riassunto: *Si dimostra che esiste un 24-arco completo in $PG(2,29)$ che ammette $PSL(2,7)$ come gruppo di automorfismi.*

Abstract: *There exists a complete 24-arc in $PG(2,29)$ with the projective automorphim group isomorphic to $PSL(2.7)$.*

1 – Introduction

Let F_q be the finite field of q elements, and let $PG(r,q)$ be the r-dimensional projective space over F_q . An n-arc K in $PG(r,q)$ is a n-point set ($n \geq r+1$) such that any $r+1$ points of K are in general position, namely no hyperplane contains them. A $(q+1)$-point set $\{(1,t,t^2,\dots,t^r);\ t \in F_q \cup \{\infty\}\}$, where $t=\infty$ defines the point $(0,0,\dots,1)$, in $PG(r,q)$ is an arc, provided $r \leq q-2$. An arc projectively equivalent to the $(q+1)$-arc is called a normal rational curve. An arc contained in a normal rational curve is called classical, while an arc not contained in any normal rational curve is called non-classical. Let C be an $[n\,,r{+}1]$ MDS code over F_q. The automorphism group Aut(C) of C is the factor group $\{A=[\sigma]D \text{ such that } \mathrm{C}A=\mathrm{C}\}/\{aE_n;\ a\in F_q\backslash\{0\}\}$.

Key Words and Phrases: *Arcs – MDS codes*
A.M.S. Classification: 11T71 – 94B27

Here $[\sigma]$ is a permutation matrix of degree n such that $[x_1, \dots, x_n][\sigma] = [x_{\sigma(1)}, \dots, x_{\sigma(n)}]$, and D is a non- singular diagonal matrix with F_q entries. Let $G = [g_{ij}]$ be a generator matrix of C, namely $r+1$ rows of G form a basis of C. Then $K = \{P_j = (g_{1,j}, \dots, g_{r+1,j})^T;\ 1 \le j \le n\}$ is an n-arc, and Aut(C) is isomorphic to the automorphism group Aut(K) of K, the set of projectivities of $PG(r,q)$ leaving K invariant. Conversely an n-arc in $PG(r,q)$ gives rise to an $[n, r+1]$ MDS code. We refer [11] and [10] for detailed information on arcs.

Let $m(r,q)$ be the maximum size of arcs in $PG(r,q)$. Clearly $m(r,q) = r+1$ if $r > q-2$. To be specific we assume that q is odd and $q \ge 7$. As is well known, $m(2,q) = q+1$ and a $(q+1)$-arc as well as a q-arc in $PG(2,q)$ is classical. Besides there exists a non-classical arc in $PG(2,q)$. Let $m'(2,q)$ be the maximum size of non-classical arcs in $PG(2,q)$. So far $m'(2,q)$ is known up to $q \le 29$:

q	7	9	11	13	17	19	23	25	27	29
$m'(2,q)$	6	8	10	12	14	14	17	21	22	24

Furthermore non-classical $m'(2,q)$-arcs are projectively equivalent for $q = 9, 11, 13, 17, 25$ and 27. It remains open whether non-classical $m'(2,29)$-arcs in $PG(2,29)$ are unique. (For $q \le 9$ see [9]. For $q = 11$ see [13]. For $q = 13$ see [1],[8] and [14]. For $q = 17$ and 19 see [4] and [14]. For $23 \le q \le 29$ see [6]). When $3 \le r \le q-3$, there exists a non-classical arc in $PG(r,q)$ if and only if $r \le m'(2,q) - 4$. Let $m'(r,q)$ be the maximum size of non-classical arcs in $PG(r,q)$ for $3 \le r \le m'(2,q) - 4$ (note that $m'(2,q) - 4 \le q - 5$). We remark that $m'(r,q) \le q$ if and only if $m(r,q) = q+1$ and every $(q+1)$-arc in $PG(r,q)$ is classical, where $3 \le r \le m'(2,q) - 4$. The only known case where $m'(r,q) > q$ is $m'(4,9) = 10$.

In this note we shall show that there exists a complete 24-arc in $PG(2,29)$ with the automorphism group isomorphic to $PSL(2,7)$. This example suggests that $m'(2,q)$-arcs in $PG(2,q)$ or more generally, $m'(r,q)$ -arcs in $PG(r,q)$ are worth studying.

2 – A complete 24-arc in $PG(2,29)$

Throughout this section $\zeta = 3$ stands for the primitive element of F_{29}, $\xi = 5$ for the primitive element of F_7. A point in $PG(r,q)$ with the homogeneous coordinates $[x_0,\dots,x_r]^T$ will be denoted by $(x_0,\dots,x_r)^T$. For example $e_1 = (1,0,0)^T$, $e_2 = (0,1,0)^T$ and $e_3 = (0,0,1)^T$ are three points of $PG(2,q)$. A projectivity defined by a non-singular matrix $[a_{ij}]$ with F_q entries will be denoted by (a_{ij}).

Lemma 2.1. *Let U, V and W be projectivities of $PG(2,29)$ such that*

$$U = \begin{pmatrix} \zeta^0 & 0 & 0 \\ 0 & \zeta^4 & 0 \\ 0 & 0 & \zeta^{12} \end{pmatrix}, \quad V = \begin{pmatrix} \zeta^{19} & \zeta^0 & \zeta^{20} \\ \zeta^0 & \zeta^{20} & \zeta^{19} \\ \zeta^{20} & \zeta^{19} & \zeta^0 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Then
(1) *$U^7 = id$, $V^2 = id$ and $W^3 = id$.*
(2) *$WV = VW^2$.*
(3) *$UW = WU^2$.*
(4) *$U^{1/a}VU^aW^{\log_\xi a} = VU^{-a}V$ for $a = \xi^k \in F_7\backslash\{0\}$ with $\log_\xi a = k$.*

Proof. Multiplication of matrices yields (1) to (3). According as k ranges from 0 to 5, the equality (4) takes the form $UVU = VU^{-1}V$, $U^3VU^5W = VU^2V$, $U^2VU^4W^2 = VU^3V$, $U^{-1}VU^{-1} = VUV$, $U^4VU^2W = VU^5V$ and $U^5VU^3W^2 = VU^4V$. These equalities can be verified by matrix multiplication.

Theorem 2.2. *There exists uniquely a group homomorphism φ from $PSL(2,7)$ into $PGL(3,29)$ sending u, v and w to U, V and W respectively, where*

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad v = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad w = \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \in PSL(2,7)\,.$$

In fact φ is an isomorphism of $PSL(2,7)$ into $PGL(3,29)$.

PROOF. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2,7)$ with $det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = 1$. Since

$$g = \begin{pmatrix} 1 & a/c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & cd \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} \quad \text{if} \quad c \neq 0\,,$$

we define $\varphi(g)$ to be $U^{a/c}VU^{cd}W^{\log_\xi c}$ when $c \neq 0$. Since

$$g = \begin{pmatrix} 1 & b/d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -cd \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \text{ if } d \neq 0\,,$$

we define $\varphi(g)$ to be $U^{b/d}VU^{-cd}VW^{-\log_\xi d}$ when $d \neq 0$. In order to see that φ is well defined we shall show that $U^{a/c}VU^{cd}W^{\log_\xi c} = U^{b/d}VU^{-cd}VW^{-\log_\xi d}$ when $cd \neq 0$. This equality is equivalent to $U^{1/cd}VU^{cd}W^{\log_\xi cd} = VU^{-cd}V$, which is nothing but Lemma 2.1(4). We shall show that φ is a homomorphism. Suppose $c \neq 0$. By Lemma 2.1(3) we get $\varphi(gu) = \varphi(g)U$. By Lemma 2.1(1) we get $\varphi(gv) = \varphi(g)V$. The equality $\varphi(gw) = \varphi(g)W$ is trivial. Similarly equalities $\varphi(gu) = \varphi(g)U$, $\varphi(gv) = \varphi(g)V$ and $\varphi(gw) = \varphi(g)W$ hold even when $c = 0$ and $d \neq 0$. Since any $h \in PSL(2,7)$ is product of u, v and w, φ is a homomorphism. It remains to show that φ is injective. Assume that $\varphi(g) = id$. If $c \neq 0$, no homogeneous coordinates of $\varphi(g)e_1$ vanish, hence $\varphi(g) \neq id$, a contradiction. We may further assume that $c = 0$ and $\varphi(g) = U^{b/d}W^{-\log_\xi d}$. Applying $\varphi(g)$ to a point $(1,1,1)^T$, we see that $b = 0$ and $d = \xi^{3k}$, namely $g = id \in PSL(2,7)$.

LEMMA 2.3. *Let*

$$K_0 = \{e_1, e_2, e_3\}, \quad K_i = \{U^j V e_i;\, 0 \leq j \leq 6\} \qquad (i = 1,2,3)\,.$$

Then $K = K_0 \cup K_1 \cup K_2 \cup K_3$ *is a* $PSL(2,7)$*-invariant complete* 24*-arc in* $PG(2,29)$.

PROOF. $K_0 \cup \{Ve_i\}$ is a 4-arc. Since U fixes each e_i and $U \neq id$, U does not fix Ve_i. Thus $|K_i| = 7$, for the order of U is equal to 7. $K_i \cap K_j = \emptyset$ if $1 \leq i < j \leq 3$. Otherwise the intersection is a proper subset of K_i invariant under the cyclic group $\langle U \rangle$. Similarly $K_0 \cap K_i = \emptyset$ for $1 \leq i \leq 3$. Therefore K is a 24-point set. Put $L = \{\varphi(g)e_1;\, g \in PSL(2,7)\}$.

See the proof of Lemma 2.2 for the definition of the isomorphism φ. Clearly L contains K. We shall show that $G = \{g \in PSL(2,7); \varphi(g)e_1 = e_1\}$ consists of 7 points to the effect that $L = K$ (recall that $|PSL(2,7)| = 168$). Assume $g \in G$ takes the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc = 1$. Since $c \neq 0$ implies that none of the coordinates of $\varphi(g)e_1$ vanishes, we have $c = 0$. Now $\varphi(g) = U^{b/d}W^{-\log_\xi d}$. Hence $W^{-\log_\xi d}e_1 = e_1$, which yields d is equal to either 1 or ξ^3. Consequently $g = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. This g belongs to G. We will show that K is an arc. To this end we shall show that any three points P_1, P_2 and P_3 of K cannot be collinear. Put $\mathcal{P} = \{P_1, P_2, P_3\}$. We begin with the case $\mathcal{P} \subset K_0$. The three point cannot be collinear. W^{-1} acts as a cyclic permutation on $\{K_1, K_2, K_3\}$, for $W^{-1}U^jV = U^{2j}VW$ by Lemma 2.1 (1) and (2). Secondly we assume that $\{P_1, P_2\} \subset K_0$ with $P_3 \in K_1$. Since none of the homogeneous coordinates of P_3 vanishes, P_3 cannot lie on the line joining P_1 and P_2. Next we assume that $P_1 \in K_0$ with $\{P_2, P_3\} \subset K \backslash K_0$. In the case $\{P_2, P_3\} \subset K_i$ for some $1 \leq i \leq 3$ we may assume that $i = 1$, $P_2 = Ve_1$ and $P_3 = U^jVe_1$ in view of W and U. The line through P_2 and P_3 takes the form

$$X(\zeta^{10+12j} - \zeta^{10+4j}) - Y(\zeta^{1+12j} - \zeta^1) + Z(\zeta^{9+4j} - \zeta^9) = 0\,.$$

The line does not meet K_0, because none of the following three equations has a solution $0 < j < 7 : 12j \equiv 4j \pmod{28}$, $12j \equiv 0 \pmod{28}$ and $4j \equiv 0 \pmod{28}$. In the case $P_2 \in K_i$ and $P_3 \in K_k$ for some $1 \leq i < k \leq 3$ we may assume that $i = 1$, $k = 2$, $P_2 = U^jVe_1$ and $P_3 = Ve_2$. The line joining P_2 and P_3 takes the form

$$X(\zeta^{4j} - \zeta^{21+12j}) - Y(\zeta^{19} - \zeta^{1+12j}) + Z(\zeta^{20} - \zeta^{9+4j}) = 0\,.$$

Again the line does not meet K_0, because none of the following three equations has a solution $0 \leq j < 7 : -8j \equiv 21 \pmod{28}$, $12j \equiv 8 \pmod{28}$ and $4j \equiv 1 \pmod{28}$. Finally assume that $\mathcal{P} \subset K \backslash K_0$. In view of U we may assume that $P_1 = Ve_i$ for some i. Then $V\mathcal{P}$ contains $e_i \in K_0$. Since $V\mathcal{P}$ cannot be collinear, $\mathcal{P}$ neither. To complete the proof we shall show that K is complete. Suppose $K \cup \{P\}$ is a 25-arc. Then $K_4 = \{U^jP; 0 \leq j < 7\}$ is a 7-point set (recall that the order of U is equal to 7). We recall a theorem due to T. Szonyi and J.A. Thas [16]; if

q is odd and $n > (2q+3)/3$, then an n-arc in $PG(2,q)$ is contained in a unique complete arc. This theorem asserts that $K \cup K_4$ is a 31-arc in $PG(2,29)$. This contradicts the fact that $m(2,q) = q+1$ for $q \geq 3$.

LEMMA 2.4. *Consider a subset* $L = \{\zeta^{4j};\ 0 \leq j < 7\}$ *of* $PG(1,29)$. *The automorphism group* $\mathrm{Aut}(L)$, *namely the set of fractional linear transformations of* $F_{29} \cup \{\infty\}$ *leaving* L *invariant, contains exactly* 14 *elements;* $\zeta^{4j}t$ *and* ζ^{4j}/t.

PROOF. By the aid of a computer we verify that among $7 \cdot 6 \cdot 5$ fractional linear transformations mapping $(1, \zeta^4, \zeta^8)$ to $(\zeta^{4i}, \zeta^{4j}, \zeta^{4k})$ only 14 transformations leave L invariant.

REMARK 2.5. Let ρ be a primitive element of F_{25} such that $\rho^2 = 3\rho+2$ (see Table A of [12]). The the subset $\{\rho^{4j};\ 0 \leq j < 6\}$ of $PG(1,25)$ turns out to be equivalent to $F_5 \cup \{\infty\}$. Hence the automorphism group of the subset consists of $6 \cdot 5 \cdot 4$ elements.

THEOREM 2.6. *The automorphism group* $\mathrm{Aut}(K)$ *of the arc* K *in* Lemma 2.3 *is isomorphic to* $PSL(2,7)$.

PROOF. A line ℓ satisfying $\ell \cap K = \{e_3\}$ takes the form $X\zeta^{4j} + Y = 0$ $(0 \leq j < 7)$. Let $\mathcal{L}$ be the set of these seven lines, and let $G = \{A \in \mathrm{Aut}(K);\ Ae_3 = e_3\}$. Clearly G fixes $\mathcal{L}$. Since $\mathrm{Aut}(K)$ acts transitively on the arc K, it suffices to show that the stabilizer G consists of seven elements. Note that G contains the cyclic group $\langle U \rangle$. We shall show that $G = \langle U \rangle$. Let $A = (a_{ij})$ $(1 \leq i,j \leq 3)$ is an element of G. Recall that A maps a line $X\alpha + Y\beta + Z\gamma = 0$ to $X\alpha' + Y\beta' + Z\gamma' = 0$, where $(\alpha', \beta', \gamma') = (\alpha, \beta, \gamma)A$. Since $Ae_3 = e_3$, we have $a_{13} = a_{23} = 0$. Hence A maps a line $Xt + Y = 0$ to a line $Xt' + Y = 0$ with $t' = f(t) = (a_{11}t + a_{21})/(a_{12}t + a_{22})$. In particular $\langle U \rangle$ acts transitively on $\mathcal{L}$. Multiplying some $B \in \langle U \rangle$ to A , we may assume that $f(1) = 1$. In addition the fractional linear transformation $f(t)$ is equal to either $\zeta^{4j}t$ or ζ^{4j}/t by Lemma 2.4. Since $f(1) = 1$, $j = 0$. In the first case we get $a_{12} = a_{21} = 0$ and $a_{11} = a_{22}$. The condition $AK = K$ now implies that $A = id$. The second case cannot happen. Assume the contrary. Then $a_{11} = a_{22} = 0$ and $a_{12} = a_{21}$. Now Ae_1 and Ae_2 must be equal to e_2 and e_1 respectively. Thus $a_{31} = a_{32} = 0$. Consequently A must fix $(1, 1, \zeta^{15})^T \in K_2$. Hence $a_{12} = a_{33}$, and A is now completely determined. However we can easily see that $AK \neq K$.

REMARK 2.7. The 24-arc K in $PG(2,29)$ lies on the sextic curve $X^5Y + Y^5Z + Z^5X + \zeta^{24}X^2Y^2Z^2 = 0$.

REFERENCES

[1] A.H. ALI: *Classification of arcs in the plane of order 13*, Ph.D. thesis, University of Sussex, 1993.

[2] A.H. ALI – J.W.P. HIRSCHFELD – H. KANETA: *The automorphism group of a complete* $(q-1)$*-arc in* $PG(2,q)$, J. Combin. Des., **2** (1994), 131-145.

[3] A.H.ALI – J.W.P. HIRSCHFELD – H. KANETA: *On the size of arcs in projective spaces*, IEEE, Information Theory, **41** (1995), 1649-1656.

[4] J M. CHAO – H. KANETA: *Classical arcs in* $PG(r,q)$ *for* $11 \leq q \leq 19$, to appear in the Proceedings of Combinatrics '94, Roma & Montesilvano (PE).

[5] J M. CHAO – H. KANETA: *Cyclic groups of order* $q \pm 1$ *and arcs in* $PG(2,q)$, submitted.

[6] J.M. CHAO – H. KANETA: *Classical arcs in* $PG(r,q)$ *for* $23 \leq q \leq 29$, in preparation.

[7] J.C. FISHER – J.W.P. HIRSCHFELD – J. A. THAS: *Complete arcs in planes of square order*, Ann. Discrete Math., **30** (1986), 243–250.

[8] D.G. GORDON: *Orbits of arcs in projective spaces, Finite Geometry and Combinatrics London*, Math. Soc. Lecture Notes **191**, Cambridge University Press, Cambridge 1993, 161-171.

[9] J.W.P. HIRSCHFELD: *Projective Geometries over Finite Fields*, Oxford University, Oxford 1979.

[10] J.W.P. HIRSCHFELD – L. STROME: *The packing problem in statistics, coding theory and finite projective spaces*, to appear in J. Stat. Plann. Inferences

[11] J.W.P. HIRSCHFELD – J. A. THAS: *General Galois Geometries*, Oxford University Press, Oxford 1991.

[12] R. LIDLE – H. NIEDERREITER: *Finite Fields, Encyclopedia of*, Math. and its Applications, Vol.**20**, Cambridge University Press, 1984.

[13] A.R. SADEH: *The classification of k-arcs and cubic surfaces with twenty-seven lines*, Ph.D. thesis, University of Sussex, 1984.

[14] M. SCIPIONI: *Sugli archi completi nei piani desarguesiani*, Tesi di laurea, University of Rome "La Sapienza", 1990.

[15] B. SEGRE: *Le geometrie di Galois*, Ann. Mat. Pura Appl., **48** (1959), 1-97.

[16] T. Szonyi: *Complete arcs in Galois planes*, Seminario di Geometrie Combinatorie diretto da G. Tallini, n. 94, University of Rome "La Sapienza", 1989.

Lavoro pervenuto alla redazione il 9 novembre 1995
ed accettato per la pubblicazione il 3 giugno 1996.
Bozze licenziate il 2 settembre 1996

Indirizzo degli Autori:

J.M. Chao – H. Kaneta – Department of Mathematics – Faculty of Science – Okayama University – Okayama 700, Japan