The complete (k, 3)-arcs of $PG(2, q), q \le 13$

K. Coolsaet, H. Sticker

Department of Applied Mathematics and Computer Science, Ghent University, Krijgslaan 281-S9, B-9000 Gent, Belgium Kris.Coolsaet@UGent.be, Heide.Sticker@UGent.be

January 18, 2013

Abstract

We have classified by computer the projectively distinct complete (k, 3)arcs in PG $(2, q), q \leq 13$. The algorithm used is an application of isomorphfree backtracking using canonical augmentation, an adaptation of our earlier algorithms for the generation of (k, 2)-arcs. We describe those parts of the algorithms which are specific to the particular problem of (k, 3)-arcs. For each of these arcs we have also determined the automorphism group. The results are summarised in tables where the arcs are listed according to size and automorphism group. For the arcs with the larger automorphism groups, explicit descriptions are given. Part of the computer results can be generalized to other values of q: we describe constructions of arcs having S_4 as a group of automorphisms, arcs containing the union of three 'half conics' and arcs constructed from parts of cubic curves.

1 Introduction

Consider the Desarguesian projective plane PG(2, K) over a field K. Let k be a positive integer. A (k, n)-arc S of PG(2, K) is defined to be a set of k points of the plane such that at least one line of the plane meets S in n points but no line meets S in more than n points. A (k, 3)-arc is called *complete* if and only if it is not contained in a (k + 1, 3)-arc. By definition, a line of PG(2, K) intersects a (k, 3)-arc in either 0, 1, 2 or 3 points, in which case it is called an *external line*, a *unisecant*, a *bisecant* or a *trisecant*, respectively. In this paper, we shall mostly work

with (k, 3)-arcs and for what follows the term "arcs" will always refer to (k, 3)-arcs. Also, we will often silently drop the requirement that at least one line must contain 3 points. In other words, we will sometimes regard a (k, 2)-arc as a special case of a (k, 3)-arc. Of course, for complete (k, 3)-arcs this is not an issue because a (k, 2)-arc can never be a complete (k, 3)-arc.

We shall be interested in the case where K is the finite field of q elements, and write PG(2,q) = PG(2,K) as customary. Let $m_3(2,q)$ denote the largest size of a (k,3)-arc of PG(2,q). Then $m_3(2,q) \leq 2q+1$ for $q \geq 4$. For further information on the geometrical properties of (k,3)-arcs we refer to [5].

The subject of (k, 3)-arcs is not only interesting in its purely geometrical setting. Arcs have applications in coding theory, where they can be interpreted as linear maximum distance separable (MDS) codes. A linear $[k, d, k - d]_q$ code C such that its dual code C^{\perp} has minimum distance equal to d is called NMDS. Every $[k, 3, k - 3]_q$ NMDS code is equivalent to a (k, 3)-arc in PG(2, q) containing at least three collinear points. A (k, 3)-arc is also the complement of a t-fold blocking set with t = q - 2.

The purpose of our research is to determine by computer all complete (k, 3)-arcs in PG(2, q) up to PGL(3, q)-equivalence. Two (k, 3)-arcs are called PGL-equivalent if there exists a collineation of PGL(3, q) mapping one arc to the other. For $q \leq 9$, the classification was already done by Marcugini et al. [6, 7]. They also found that $m_3(2, 11) = 21$ and $m_3(2, 13) = 23$ and that the smallest size of a complete arc in PG(2, 13) is 15 [8]. For q = 13 they found the spectrum: there is a complete (k, 3)-arc for each $k, 15 \leq k \leq 23$ [9]. We extend this to a full classification of all complete (k, 3)-arcs in PG(2, 11) and PG(2, 13). Our programs reproduce the results of Marcugini et al. The algorithm we use is that of [3, 4], adapted to the case of (k, 3)-arcs instead of (k, 2)-arcs. This algorithm can also be used to classify the full set of arcs, i.e., not necessarily only those that are complete, in Section 3.2 we list the results for $q \leq 13$.

One of the purposes of doing a computer classification of this type is to gain further insight into the general class of objects under investigation. In our case we hope to find patterns in the vast amount of data which may for instance allow us, or other researchers, to derive new general constructions of arcs that also work for larger fields. Our results lead to several general types of arc. These are described in Section 4.

Most well-known constructions produce arcs that have an interesting (and often large) automorphism group. For this reason we list the automorphism groups of all complete arcs (cf. Tables 1-6). We also discuss the arcs with the larger automorphism groups in more detail, in order to describe them in a more elegant way than by just listing the coordinates of their points. (See Section 5 for q = 11 and Section 6 for q = 13.)

Our programs, which were written in Java, were run on a cluster of Debian Linux systems with 56 quad core Intel Xeon X3220 2.40GHz processors. The generation of all complete arcs of PG(2, 11) up to equivalence takes approximately 6 hours of CPU time. For q = 13 it took approximately 152 days of CPU time. To store the results (in compressed form) we need about 35 MByte of disk space for q = 11 and about 14 GByte for q = 13.

2 The algorithm

For the generation of the (complete) (k, 3)-arcs up to equivalence in $PG(2, q), q \leq 13$, we used an application of isomorph-free generation using canonical augmentation, as introduced by B. McKay [10]. In [3, 4], we adapted this technique to the generation of all subsets S of the set V of points of PG(2, q) up to equivalence for the group G = PGL(3, q), that satisfy a certain property P(S), where P is a set predicate with the following characteristics:

- 1. P is group invariant: P(S) if and only if $P(S^g)$, for every $S \subseteq V$ and $g \in G$;
- 2. P is *hereditary*: if P(S) then P(S') for every subset S' of S.

More specific, in [3, 4], we considered for P(S) the predicate "S is a (k, 2)-arc of PG(2,q)". In this paper we shall instead use the predicate "S is a (k, 2)-arc or a (k, 3)-arc of PG(2,q)" for P(S). This necessitates some important changes that are explained in the following subsections.

The basic idea behind the generation algorithm is the use of a function F which singles out a special orbit in the set of all orbits of the stabilizer of the arc S on the points of S, and which is group invariant. Arcs of size k + 1 are then generated from arcs of size k by adding a single point s to an arc S but only in those cases where s belongs to the special orbit $F(S \cup \{s\})$ of the generated arc. Computations are speeded up by making careful use of some invariants. These are functions that associate a value to every point and line of the plane in such a way that two points or two lines have the same invariant value whenever they are in the same orbit of the stabilizer group of the arc.

We also make use of the improvement of the algorithm as explained in [4], where we do not always have to compute the set stabilizer $G_{S'}$ for the generated arc $S' = S \cup \{s\}$. This is possible because whenever the stabilizer G_S of S is trivial, and the points of S' satisfies certain conditions, then also $G_{S'}$ must be trivial.

2.1 Invariants

Let us now explain the invariants of the arc that were used to speed up computations.

Let S be an arc, let ℓ be a line of the plane, let p be a point of the plane. Denote the number of points of S on ℓ by $d_S(\ell)$, the number of bisecants of S through p by $b_S(p)$, the number of trisecants of S through p by $t_S(p)$. Note that $d_S(\ell)$, $b_S(p)$ and $t_S(p)$ are invariant for the group G, i.e. $d_S(p) = d_{S^g}(p^g)$, $b_S(p) = b_{S^g}(p^g)$ and $t_S(p) = t_{S^g}(p^g)$ for all $g \in G$. Hence it follows that $d_S(\ell)$, $b_S(p)$ and $t_S(p)$ are also invariant for the group G_S .

For every line ℓ of the plane we define the following *line invariant*:

$$I_S(\ell) \stackrel{\text{def}}{=} h(d_S(\ell)) + \sum_{p \in \ell \setminus S} (h_1(b_S(p)) + h_2(t_S(p))).$$

where h, h_1 and h_2 denote simple hash functions (one of them, say h, can be the identity). Again I_S satisfies $I_{S^g}(\ell^g) = I_S(\ell)$ for every $g \in G$. Note that I_S can be computed quite efficiently if we keep track during the course of the algorithms of the values of $d_S(\ell)$, $b_S(p)$ and $t_S(p)$ for all lines and points of the plane.

For every point p of the plane we define a *point invariant*:

$$I_S(p) \stackrel{\text{def}}{=} \sum_{\ell, p \in \ell} h_3(I_S(\ell)),$$

where again h_3 denotes a simple hash function. Here we also have $I_{S^g}(p^g) = I_S(p)$ for every $g \in G$. The computation of the point invariant values for all points in the arc S is not very efficient, but we do not need to compute them for every generated arc S. In contrast to the (k, 2)-arcs, where each arc point p had the same value $b_S(p)$, for (k, 3)-arcs in many cases $b_S(p)$ is itself already a sufficiently strong invariant for our purposes and $I_S(p)$ is only used when this turns out not to be the case. (In our programs we use t_S instead of b_S , but because b_S and t_S are linear dependent, this is not really significant.)

The functions t_S and I_S each induce a partition on S which we will denote by $t_S \setminus S$, resp. $I_S \setminus S$. Two points p, p' belong to the same part $U \in t_S \setminus S$ ($I_S \setminus S$) if and only if $t_S(p) = t_S(p')$ ($I_S(p) = I_S(p')$), and in that case we shall write $t_S(U) \stackrel{\text{def}}{=} t_S(p)$ ($I_S(U) \stackrel{\text{def}}{=} I_S(p)$). We will call elements of these partitions *t*-quasi-orbits and *I*quasi-orbits of S.

Note that $U \in t_S \setminus S$ satisfies $U^g = U$ for every $g \in G_S$ and therefore any t-quasiorbit U is a union of orbits of G_S on S. The same holds for all I-quasi-orbits. In other words, $G_S \setminus S$ is a refinement of $t_S \setminus S$ and of $I_S \setminus S$. In particular, every singleton t- or I-quasi-orbit $\{p\}$ must be a true orbit of G_S .

2.2 Canonical forms for (k,3)-arcs

While the invariants t_S and I_S play a crucial role in the canonical augmentation algorithm, there are (rare) occasions where they are not sufficient to ensure isomorphfree generation. In those cases we need to use some kind of canonical form of the generated set S. Fortunately, the data we gather to compute the invariants can also be put to good use when constructing such a canonical form. We want to construct a canonical form for S in which certain known points have minimal values for I.

It is for example very easy to see that the two points p_1 and p_2 with minimal invariants, i.e., satisfying $I(p_1) \leq I(p_2) \leq I(p)$ for all $p \in S - \{p_1, p_2\}$, can always be mapped by a projectivity to two chosen points, say the points e_1, e_2 with coordinates (1, 0, 0) and (0, 1, 0). With (k, 2)-arcs this principle can easily be extended to four points, but for (k, 3)-arcs there are some complications.

The first complication already arises for the point p_3 with third smallest invariant. We have two possibilities: if p_1, p_2, p_3 are not collinear, then p_3 can be mapped to $e_3(0, 0, 1)$, otherwise it can be mapped to $f_3(1, 1, 0)$.

We can however be sure that if the third point cannot be mapped to $e_3(1,0,0)$ then the fourth point can (otherwise there would be four points on the same line). More generally, among the five points with smallest invariants, we will always be able to find four that form a quadrangle. The fourth point of the quadrangle can then be mapped to $e_4(1,1,1)$. Whence the following definition :

Let J_S denote an invariant (in our case $J_S = I_S$ or t_S). Then a (k, 3)-arc S will be called *J*-quasi-canonical if and only if the following conditions are satisfied :

- $e_1, e_2, e_3, e_4 \in S$,
- $J_S(e_1) \le J_S(e_2) \le J_S(e_3) \le J_S(e_4)$
- There exist at most one point $p \in S \{e_1, e_2, e_3, e_4\}$ such that $J_S(p) < J_S(e_4)$.
- If such p exists, it lies on at least one of the lines $e_i e_j$, or equivalently, $\{e_1, e_2, e_3, e_4, p\}$ is not a (5, 2)-arc.
- If such p lies on exactly one line $e_i e_j$, then $J_S(p) \ge J_S(e_i), J_S(e_j)$.

Proposition 1 Let S be a (k, 3)-arc of PG(2, K) with $|S| \ge 5$. Then S^G contains at least one J-quasi-canonical element.

Proof: We can always find a set $P = \{p_1, \ldots, p_5\} \subseteq S$ of 5 points of S that satisfy the condition $J_S(p_1) \leq J_S(p_2) \leq \cdots \leq J_S(p_5)$. (Take p_1 to be one of the points of S

for which J_S is minimal, take p_2 to be one of the points of $S - \{p_1\}$ for which J_S is minimal, ...)

Now define the point p_* as follows :

- If no three points among p_1, \ldots, p_5 are collinear, then $p_* \stackrel{\text{def}}{=} p_5$.
- If P contains exactly one collinear triple, say $p_i p_j p_k$ with i < j < k, then $p_* \stackrel{\text{def}}{=} p_k$.
- If P contains two collinear triples, then p_* is the point these triples have in common.

Define $P' = P - \{p_*\}$. By the choice of p_* , P' contains no collinear triples. Write $P' = \{p_i, p_j, p_k, p_\ell\}$ with $i < j < k < \ell$. Now, there exists a (unique) projectivity g that maps p_i to e_1 , p_j to e_2 , p_k to e_3 and p_ℓ to e_4 .

We leave it to the reader to verify that S^g is J-quasi-canonical.

The proof of this proposition is constructive and can easily be extended to an algorithm which finds *all J*-quasi-canonical elements of S^G .

Now, fix an ordering on the points of the plane and extend this to a lexical ordering of subsets of points of equal size. We are finally in a position to define the *canonical* form of an arc. Let S denote a (k, 3)-arc with $k \ge 5$.

- 1. If the t-quasi-orbit partition of S contains at least one singleton, then define $\operatorname{can}(S)$ to be the smallest of all t-quasi-canonical arcs in S^G with respect to this lexical ordering.
- 2. Otherwise, define can (S) to be the smallest of all *I*-quasi-canonical arcs in S^G with respect to this lexical ordering.

Although the definition of the canonical form is rather involved, in practice it can be computed quite efficiently, especially when all relevant invariant values are known beforehand.

2.3 The function F

We can now use the invariants on the points and the canonical form to construct the function F used in the algorithm. We define F as follows:

- 1. If the *t*-quasi-orbit partition of *S* contains at least one singleton, then we define F(S) to be the singleton $\{p\}$ for which $t_S(p)$ is minimal.
- 2. Otherwise, if the *I*-quasi-orbit partition of *S* contains at least one singleton, then we define F(S) to be the singleton $\{p\}$ for which $I_S(p)$ is minimal.
- 3. Otherwise $F(S) \stackrel{\text{def}}{=} e_1^{hG_S}$ where $h \in G$ is such that $S = \operatorname{can}(S)^h$ and e_1 is as in Section 2.2. In simple terms: F selects that orbit of G_S whose representative corresponds to e_1 in the canonical form of S.

Note that we only use the point invariant $I_S(p)$ if there is no unique value among all values $t_S(p)$ for all $p \in S$. This only happens in 41% of the cases for q = 11 and in 38% of the cases for q = 13.

3 Results

3.1 Complete (k,3)-arcs of $PG(2,q), q \le 13$

As mentioned in the introduction, we have been able to compute a full classification of the projectively distinct complete (k, 3)-arcs in PG(2, q) for all $q \leq 13$. For each of these arcs we have also determined its automorphism group, i.e., the subgroup of PGL(3, q) that stabilizes the set of points of the arc. The results are summarised in Tables 1-6.

In these tables k denotes the size of the arcs in the corresponding column, and N_k the number of projectively distinct complete arcs of that size. For each k we specify a list of possible automorphism groups G_S and the corresponding number of k-arcs with an automorphism group of that type. (We use the 'Atlas'-notation for the groups [2].) The underlined cases will be discussed in later sections.

Note that the number of projectively distinct complete (k, 3)-arcs in $PG(2, q), q \leq 9$ was already found by Marcugini et al. [6, 7, 8, 9]. However for q = 8 and q = 9, they did not give the automorphism groups of the arcs. For q = 11, they only found that $m_3(2, 11) = 21$ and that only two non-equivalent (21, 3)-arcs exist. For q = 13, they found 7 non-equivalent arcs of size $m_3(2, q) = 23$ and 33 non-equivalent of size 15. They also found the spectrum for q = 13: there is a complete (k, 3)-arc for each $k, 15 \leq k \leq 23$.

k =	9	k =	10	k = 1	11	
$N_k =$	= 2	N_k =	= 2	$N_k = 2$		
G_S	#	G_S	#	G_S	#	
S_3	1	3	2	D_8	1	
D_{12}	1			5:4	1	

Table 1: Numbers of complete (k, 3)-arcs in PG(2, 5) listed according to size and automorphism group.

k =	9	k =	11	k =	12	<i>k</i> =	= 13	k = 14		k = 1	15
$N_k =$	= 1	N_k :	= 8	$N_k =$	= 69	N_k :	= 44	$N_k = 2$		$N_k =$	1
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
[216]	1	1	1	1	55	1	23	1	1	$\underline{S_4:3}$	1
		2	4	2	4	2	15	6	1		
		2^{2}	1	3	7	3	2				
		S_3	2	S_3	1	2^{2}	2				
				3^{2}	1	S_3	2				
				$3S_3$	1						

Table 2: Numbers of complete (k, 3)-arcs in PG(2, 7) listed according to size and automorphism group.

k =	11	k =	= 12	<i>k</i> =	= 13	k = 14		<i>k</i> =	= 15
N_k	= 4	N_k	= 22	$N_k = 674$		N_k	= 472	N_k =	= 43
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
2	3	1	19	1	584	1	471	1	25
2^{3}	1	3	3	2	67	2	1	2	3
				3	18			3	3
				4	1			2^{2}	6
				S_3	4			4	1
								S_3	3
								A_4	2

Table 3: Numbers of complete (k, 3)-arcs in PG(2, 8) listed according to size and automorphism group.

k =	12	<i>k</i> =	= 13	k = 14		<i>k</i> =	= 15	k =	16	k =	17
$N_k =$	= 4	N_k =	=453	N_k :	= 7261	$N_k =$	= 7880	$N_k =$	646	N_k :	= 6
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
2	1	1	384	1	7231	1	7523	1	613	1	4
S_3	1	2	57	2	28	2	261	2	14	2	2
[36]	1	3	7	4	2	3	73	3	11		
[54]	1	2^{2}	4			2^{2}	7	2^{2}	2		
		S_3	1			4	2	4	2		
						6	3	5	2		
						S_3	9	6	1		
						D_{10}	2	3:4	1		

Table 4: Numbers of complete (k, 3)-arcs in PG(2, 9) listed according to size and automorphism group.

k =	13	k	= 14		= 15	5		j	<i>k</i> =	= 16			k	= 17
N_k =	= 5	N_k	= 146	N_k :	= 71	584	Ν	V_k =	= 1	5744	90	N	$_{k} =$	2082781
G_S	#	G_S	#	G_S	7	#	G	r_{S}		#		G	S	#
2	1	1	138	1	70'	705		1	1	5736	77		1	2078955
6	1	2	8	2	,	794		2		6	13		2	3782
S_3	2			3		56		3		1	96		2^{2}	20
D_{10}	1			2^{2}		6	2	2^{2}			1		4	9
				4		2		6			2		5	5
				6		2	2	S_3			1		8	1
				S_3		15						$\mid L$	\mathcal{D}_8	5
				D_{10}		2						6	2_8	1
				$\underline{S_4}$		2						D	10	3
	Γ	k	- 18		k -	10		1	k _	- 20	k	·	91	
		$N_{l_{r}} =$	- 10 = 25958	5	$N_k =$	417	6	Λ	υ — Vι. =	= 15		/ — /ı. =	= 2	
	ł	Gs	#		$\frac{G_{\kappa}}{G_{\kappa}}$	#	:	G	Y C	#	-	Ga	-	-
	ł	1	$\frac{7}{25917}$	4	1	405	55		1	13	7	: 3	$\frac{n}{2}$	_
		2	23	4	2	100	76		2	2	<u>·</u>			
		3	 16	6	-3		35		_	_				
		2^2	10	1	2^2		5							
		4		4	-		1							
		5		1	S_3		3							
		S_3		$3 \ 1$	9:3		1							
		A_4		$1 \parallel $										
		S_4		$1 \parallel$										
	L	<u>-</u>						1						

Table 5: Numbers of complete (k, 3)-arcs in PG(2, 11) listed according to size and automorphism group.

k =	15	k	= 16		k = 17		k = 18		k = 19
$N_k =$	= 33	N_k :	= 95497	N_k =	= 27833779	$N_k =$	487287851	N_k =	= 644018777
G_S	#	G_S	#	G_S	#	G_S	#	G_S	#
1	13	1	95149	1	27819765	1	487274273	1	643963031
2	4	2	314	2	13907	2	10588	2	55128
3	10	3	25	3	54	3	2927	3	459
6	3	4	4	2^{2}	26	2^{2}	2	2^{2}	78
S_3	2	6	1	4	1	4	11	4	59
[36]	1	S_3	4	6	1	6	13	6	1
				S_3	23	S_3	18	S_3	14
				D_8	2	3^{2}	15	D_8	7
						$3S_3$	1		
						S_4	1		
						3^{1+2}_{+}	1		
						[36]	1		

	k = 20	k	c = 21	k	= 22	k =	23
N_k =	= 96109026	$N_k =$	= 2300204	N_k =	= 9669	N_k =	= 7
G_S	#	G_S	#	G_S	#	G_S	#
1	96105103	1	2297792	1	9618	1	5
2	3733	2	1954	2	28	2	1
3	161	3	425	3	16	4	1
2^{2}	2	2^{2}	9	4	4		
4	24	4	3	6	1		
6	3	6	8	S_3	1		
		S_3	6	7	1		
		$\underline{3^2}$	2				
		$\underline{D_{12}}$	2				
		$\underline{D_{14}}$	1				
		$3S_3$	2				

Table 6: Numbers of complete (k, 3)-arcs in PG(2, 13) listed according to size and automorphism group.

3.2 The (k,2)- and (k,3)-arcs of $PG(2,q), q \le 13$

In Table 7 we list the number of PGL-inequivalent arcs in $PG(2,q), q \leq 13$, not necessarily complete. To obtain these results we used the same algorithm of Section 2, except that we do not filter for completeness. Running times are essentially the same as for complete arcs.

	q = 5	q = 7	q = 8	q = 9	q = 11	q = 13
k = 4	2	2	2	2	2	2
k = 5	3	4	3	5	5	7
k = 6	8	17	20	31	52	88
k = 7	13	54	100	192	564	1429
k = 8	13	181	507	1343	6764	25851
k = 9	16	526	2250	8232	70555	405923
k = 10	7	907	6681	36573	574777	5175927
k = 11	2	923	12664	111833	3520995	52242283
k = 12		395	12781	209172	15291648	403124643
k = 13		65	5822	211818	44020760	2282452775
k = 14		4	871	97050	76936027	9001288813
k = 15		1	43	16386	73157838	23188169036
k = 16				734	32916332	36058738738
k = 17				6	5884405	30742092308
k = 18					333858	12779923892
k = 19					4467	2246238494
k = 20					17	140208097
k = 21					2	2507054
k = 22					0	9805
k = 23					0	7

Table 7: Numbers of PGL-inequivalent (k, 2)- or (k, 3)-arcs in PG(2, q) for $q \leq 13$

3.3 Regular (k,3)-arcs of $PG(2,q), q \le 13$

Among the complete (k, 3)-arcs of $PG(2, q), 7 \le q \le 13$ there are a few that are *regular* in the sense that every point of the arc lies on the same number of trisecants to that arc (and hence also the same number of bisecants and unisecants). We list some information on these arcs in Table 8. k denotes the size of the arcs, u, b and t denote the number of unisecants, bisecants and trisecants respectively through each point of the arc and # denotes the number of projectively distinct arcs of that size with corresponding number of unisecants, bisecants and trisecants.

	PG	(2, ')	7)		PG(2,8)					PG	(2, 9)	9)		
#	k	u	b	t	#	k	u	b	t	#	k	u	b	t
1	9	4	0	4	1	15	0	4	5	5	15	1	4	5
1	14	1	1	6						5	15	2	2	6
1	15	0	2	6						3	16	1	3	6

	PG(2, 1	1)		PG(2,13)						
#	k	u	b	t	#	k	u	b	t		
2	15	3	4	5	2	15	6	2	6		
7	15	4	2	6	4	17	4	4	6		
9	16	3	3	6	1	18	5	1	8		
21	17	2	4	6	30	18	4	3	7		
1	18	1	5	6	12	18	3	5	6		
11	18	2	3	7	2	19	2	6	6		
1	19	3	0	9	1	21	2	4	8		
2	21	1	2	9	3	21	3	2	9		

Table 8: Regular arcs in $PG(2,q), q \leq 13$

4 General constructions

4.1 Some arcs with automorphism group S_4

Among our results, there are three types of arcs that accept the symmetric group S_4 as a group of automorphisms and that can be generalized to other values of q. One has size 12, one has size 15 and one has size 18. The arc of size 12 looks very similar to the (k, 2)-arc $S^*(a) = S(2/a)$ described in [3, Proposition 3] and [4, Theorem 1]: it consists of the same set of points, but the conditions for which this set is a (k, 3)-arc are somewhat relaxed.

Theorem 1 Let $a \in GF(q)$, q odd. Let $S^*(a)$ denote the set of points of PG(2,q)with coordinates of the form $(a, \pm 1, \pm 1)$, $(\pm 1, a, \pm 1)$ or $(\pm 1, \pm 1, a)$, with independent choices of sign. Let $S^*(\infty)$ be the set of points with coordinates (1, 0, 0), (0, 1, 0) or (0, 0, 1).

The set $S^*(a) \ (= S^*(-a))$ is a (12,3)-arc of PG(2,q) if and only if

$$a \notin \{0, \pm 1, \pm \sqrt{-1}\}.$$
 (1)

The set $S^*(a) \cup S^*(\infty)$ is a (15,3)-arc if and only if a satisfies (1).

The set $S^*(a) \cup S^*(0)$ is a (18,3)-arc if and only if a satisfies (1) and

$$a \neq \pm 2, a^2 \pm a \pm 2 \neq 0. \tag{2}$$

The group S_4 acts as a group of automorphisms for each of these sets.

Proof: Note that $|S^*(a)| = 12$ if and only if $a \neq 0, \pm 1$ or ∞ and that $|S^*(0)| = 6$.

The symmetric group of order 24 acts transitively on $S^*(a)$, $S^*(0)$ and $S^*(\infty)$. Indeed, S_4 is generated by two types of transformations: the permutations of the three coordinates and the transformations changing the sign of one or more of the coordinates.

To prove that $S^*(a)$ is an arc we show that no quadruple of different points of $S^*(a)$ is collinear. Because S_4 is a transitive group of automorphisms, we may chose an arbitrary element of $S^*(a)$ as the first point of each quadruple, say $P_0(a) = (1, 1, a)$.

We will also use a second type of symmetry to reduce the number of quadruples we need to consider: substituting -a for a everywhere permutes the points of $S^*(a)$ and therefore $S^*(a) = S^*(-a)$. Hence, for what follows, all conditions we derive for a must also hold for -a.

Interchanging the first two coordinates leaves $P_0(a)$ invariant and the stabilizer of $P_0(a)$ splits $S^*(a) \setminus \{P_0(a)\}$ into a singleton orbit $\{P_1(a)\}$ and 5 pairs $\{P_i(a), P'_i(a)\}$, as follows:

$P_1(a)$	=	(-1, -1, a),			
$P_2(a)$	=	(1, -1, a),	$P_2'(a)$	=	(-1, 1, a),
$P_3(a)$	=	(1, a, 1),	$P_3'(a)$	=	(a, 1, 1),
$P_4(a)$	=	(-1, a, -1),	$P_4'(a)$	=	(a, -1, -1),
$P_5(a)$	=	(a, -1, 1),	$P_5'(a)$	=	(-1, a, 1),
$P_6(a)$	=	(a, 1, -1),	$P_6'(a)$	=	(1, a, -1).

Hence, taking $P_1(a), \ldots, P_6(a)$ as representatives of these 6 orbits, it suffices to show that for each $i = 1, \ldots, 6$ the line $P_0(a)P_i(a)$ intersects $S^*(a)$ in at most three points.

In fact, it is not necessary to investigate all six of these cases. Note for instance that applying $(x, y, z) \rightarrow (y, x, -z)$ to $P_3(a)$ yields $P_5(-a)$ and applying the same transformation to $P_0(a)$ yields $P_0(-a)$. Hence $P_0(a)P_5(a)$ will intersect $S^*(a)$ in at most three points, if and only if $P_0(a)P_3(a)$ does so. The same relation exists between $P_0(a)P_6(a)$ and $P_0(a)P_4(a)$.

We may therefore restrict ourselves to the first four cases:

1. $P_0(a)P_1(a)$, with equation $f_1(x, y, z) = x - y = 0$,

- 2. $P_0(a)P_2(a)$, with equation $f_2(x, y, z) = ax z = 0$,
- 3. $P_0(a)P_3(a)$, with equation $f_3(x, y, z) = (a+1)x y z = 0$,
- 4. $P_0(a)P_4(a)$, with equation $f_4(x, y, z) = -(1 + a^2)x + (1 a)y + (1 + a)z = 0.$

In the first part of Table 9 we list the values of $f_i(r)$ for each of the 12 points r of $S^*(a)$.

For $S^*(a)$ to be a (k, 3)-arc, none of the colums for $f_1(r) \dots f_4(r)$ may contain more than 3 zeroes for rows that correspond to $S^*(a)$. From the columns for $f_1(r)$ and $f_2(r)$ we find the conditions $2 \neq 0$, $a \neq 0$, $a \neq \pm 1$ and $a^2 \neq \pm 1$. $f_3(r)$ yields the extra condition that not both $a^2 + a + 2$ and $a^2 + a - 2$ can be zero. This only happens when 4 = 0, which was already excluded bij $f_1(r)$. From $f_4(r)$, we know that at most one of $-a^3 - a + 2 = 0$, $-a^3 - a - 2 = 0$ and $a^2 + 3 = 0$ is allowed. When both $-a^3 - a + 2$ and $-a^3 - a - 2$ are zero, we again find 4 = 0. When both $-a^3 - a + 2 = 0$ and $a^2 + 3 = 0$, we find 3a - a + 2 = 0 or 2a + 2 = 0, while when both $-a^3 - a - 2 = 0$ and $a^2 + 3 = 0$, we find 3a - a - 2 = 0 or 2a - 2 = 0.

Hence, when q is odd and a satisfies (1), no four different points of $S^*(a)$ lie on the same line, and we may conclude that $S^*(a)$ is indeed a (12, 3)-arc.

Because $S^*(a)$ is a (k, 3)-arc and $S^*(\infty)$ only contains three points, a line containing four points of $S^*(a) \cup S^*(\infty)$ must contain at least one point of $S^*(a)$ and one point of $S^*(\infty)$. By symmetry, we may again choose the element $P_0(a) = (1, 1, a)$ of $S^*(a)$ as the first point of such a line. The stabilizer of $P_0(a)$ splits $S^*(\infty)$ into the singleton $\{T_1(0, 0, 1)\}$ and the pair $\{T_2(0, 1, 0), T'_2(1, 0, 0)\}$. Hence, it suffices to show that $P_0(a)T_1$ and $P_0(a)T_2$ intersect $S^*(a) \cup S^*(\infty)$ in at most three points. It is easily computed that $P_0(a)T_1 = P_0(a)P_1(a)$ and $P_0(a)T_2 = P_0(a)P_2(a)$ and hence again by inspecting the column for $f_1(r)$ and $f_2(r)$ we see that no additional conditions are needed for $S^*(a) \cup S^*(\infty)$ to be a (k, 3)-arc.

Finally, consider the set $S^*(a) \cup S^*(0)$. It is easily checked that the set $S^*(0)$ never contains more than three points on a line and when (1) is satisfied neither does $S^*(a)$. The set $S^*(0)$ has four trisecants and three bisecants. The trisecants have equations $x \pm y \pm z = 0$ with independent choices of sign, the bisecants are the lines with equations x = 0, y = 0 and z = 0.

A line containing four points of $S^*(a) \cup S^*(0)$ is one of three types. First, we have the lines that are trisecants of $S^*(a)$ and contain one point of $S^*(0)$. To avoid such lines, we must be sure that no columns of Table 9 contain more than three zeroes in rows corresponding to $S^*(a) \cup S^*(0)$. This yields the extra conditions $a \neq -2$, $a^2 \pm a + 2 \neq 0$ and $a^2 + a \pm 2 \neq 0$. Second, we have the lines that are bisecants of $S^*(a)$ and bisecants of $S^*(0)$. Such a line must be one of x = 0, y = 0 and z = 0, but none of the points $(a, \pm 1, \pm 1)$, $(\pm 1, a, \pm 1)$ or $(\pm 1, \pm 1, a)$ lies on such a line.

		$f_1(r)$	$f_2(r)$	$f_3(r)$	$f_4(r)$
					$-(1+a^2)x$
		x-y	ax-z	(a+1)x - y - z	+(1-a)y + (1+a)z
$S^*(a)$	(1, 1, a)	0	0	0	0
	(-1, -1, a)	0	-2a	-2a	2a(1+a)
	(1, -1, a)	2	0	2	2(-1+a)
	(-1, 1, a)	-2	-2a	-2(1+a)	$2(a^2+1)$
	(1, a, 1)	1-a	-1 + a	0	-2a(-1+a)
	(1, a, -1)	1-a	1+a	2	$-2(a^2+1)$
	(-1, a, -1)	-1-a	1-a	-2a	0
	(-1, a, 1)	-1-a	-1 - a	-2(1+a)	2(1+a)
	(a, 1, 1)	-1+a	$a^2 - 1$	$a^2 + a - 2$	$-a^3 - a + 2$
	(a, -1, -1)	1+a	$a^2 + 1$	$a^2 + a + 2$	$-a^3 - a - 2$
	(a, 1, -1)	-1+a	$a^2 + 1$	a(1+a)	$-a(a^2+3)$
	(a, -1, 1)	1+a	$a^2 - 1$	a(1+a)	$-a(a^2-1)$
$S^*(0)$	(1, 1, 0)	0	a	a	-a(1+a)
	(-1, 1, 0)	-2	-a	-2 - a	$a^2 - a + 2$
	(1, 0, 1)	1	-1+a	a	a(1-a)
	(-1, 0, 1)	-1	-1 - a	-2 - a	$a^2 + a + 2$
	(0, 1, 1)	-1	-1	-2	2
	(0, -1, 1)	1	-1	0	2a
$ S^*(\infty) $	(1, 0, 0)	1	a	1+a	$-a^2 - 1$
	(0, 1, 0)	-1	0	-1	1-a
	(0, 0, 1)	0	-1	-1	1+a

Table 9: Lists the values of $f_i(r)$ for each of the points in the left column (cf. proof of Theorem 1).

Last, we have the lines that are trisecants of $S^*(0)$ and contain one point of $S^*(a)$. Because $\pm 1 \pm 1 \pm a \neq 0$, this case also never occurs. Hence, when (1) and (2) are satisfied, $S^*(a) \cup S^*(0)$ is a (k, 3)-arc.

In some cases, S_4 is not the full automorphism group of $S^*(a)$. For instance, if $q \equiv 1 \pmod{3}$ and $a^3 = 1$, $a \neq 1$, then $(x, y, z) \mapsto (x, ay, a^2 z)$ extends the group of automorphisms of $S^*(a)$ to S_4 : 3.

Note that the line x = y always intersects $S^*(a) \cup S^*(0) \cup S^*(\infty)$ in four points (when $a \neq 0$), hence this set is never a (k, 3)-arc.

4.2 (k,3)-arcs from half conics

For q = 11 Table 5 lists 6 complete (k, 3)-arcs with an automorphism group of type D_{10} . In this section we shall describe how to construct these arcs and show that this construction can be generalised to other (small) fields, yielding arcs having a cyclic group $\frac{q-1}{2}$ or a dihedral group D_{q-1} as a group of automorphisms.

Let q be odd. Let $D \in GF(q) - \{0\}$. Denote by C_D the conic with equation $xz = Dy^2$. This conic belongs to the pencil of conics that are tangent to the lines x = 0 and z = 0 in the points P and Q with coordinates (1, 0, 0) and (0, 0, 1). These tangents intersect in the point R with coordinates (0, 1, 0).

Except for P and Q, all points of C_D can be given coordinates of the form $(1, t, Dt^2)$ with $t \neq 0$. We shall call t the *parameter* of the corresponding point of C_D .

Let C_D^+ denote the set of all points of C_D whose parameter is a non-zero square. Likewise, let C_D^- denote the set of all points of C_D with a parameter that is not a square. Note that $C_D = C_D^+ \cup C_D^- \cup \{P, Q\}$. The sets C_D^+ and C_D^- will be called *half conics*.

The sets C_D^+ and C_D^- are left invariant by a dihedral group of order q-1 generated by the projective transformations

$$\phi_1: (x, y, z) \mapsto (x, \alpha^2 y, \alpha^4 z)$$

and

$$\begin{cases} \phi_2 : (x, y, z) \mapsto (z, y, x) & \text{if } D \text{ is a square,} \\ \phi_3 : (x, y, z) \mapsto (z, \alpha y, \alpha^2 x) & \text{if } D \text{ is a non-square.} \end{cases}$$

with α a generator of the multiplicative group of GF(q). The sets C_D^+ and C_D^- are interchanged by ϕ_2 if D is a non-square, and by ϕ_3 if D is a square. In terms of parameters t, the group is generated by $t \mapsto \alpha^2 t \ (\phi_1)$ and $t \mapsto 1/Dt \ (\phi_2)$ or $t \mapsto \alpha/Dt \ (\phi_3)$. Note that any transformation of the form $(x, y, z) \mapsto (x, y, kz)$ with $k \in GF(q) - 0$, maps C_D^+ onto C_{kD}^+ . Also, the transformation $(x, y, z) \mapsto (x, \alpha y, \alpha^2 z)$ maps C_D^+ onto C_D^- .

As a consequence, when considering a number of half conics, without loss of generality we may take one of them to be C_1^+ .

It turns out that for smaller values of q we can construct (k, 3)-arcs by taking the union of three such half conics, yielding arcs of size $\frac{3}{2}(q-1)$. We have generated by computer all arcs of this form for $q \leq 79$. The results (up to equivalence) are listed in table 4.2 (together with their automorphism group). We conjecture that for q > 19 no arcs of this type exist.

q = 5		q = 11		q = 13	
$C_1^+ \cup C_1^- \cup C_2^+$	[120]	$C_1^+ \cup C_1^- \cup C_5^+$	D_{10}	$C_1^+ \cup C_1^- \cup C_7^+$	D_{12}
$C_1^+ \cup C_1^- \cup C_3^+$	D_4	$C_1^+ \cup C_1^- \cup C_7^+$	D_{10}	$C_1^+ \cup C_2^+ \cup C_4^+$	6
q = 7		$C_1^+ \cup C_1^- \cup C_9^+$	D_{10}	$C_1^+ \cup C_2^+ \cup C_{11}^+$	6
$C_1^+ \cup C_1^- \cup C_2^+$	D_6	$C_1^+ \cup C_2^+ \cup C_3^+$	5	$C_1^+ \cup C_4^+ \cup C_6^+$	6
$C_1^+ \cup C_1^- \cup C_4^+$	D_6	$C_1^+ \cup C_2^+ \cup C_4^+$	5	q = 19	
$C_1^+ \cup C_1^- \cup C_5^+$	D_6	$C_1^+ \cup C_2^+ \cup C_5^+$	5	$C_1^+ \cup C_7^+ \cup C_{11}^+$	[162]
$C_1^+ \cup C_1^- \cup C_6^+$	[54]	$C_1^+ \cup C_2^+ \cup C_{10}^+$	5	$C_1^+ \cup C_8^+ \cup C_{11}^+$	9
$C_1^+ \cup C_2^+ \cup C_3^+$	D_6	$C_1^+ \cup C_4^+ \cup C_5^+$	D_{10}		
$C_1^+ \cup C_2^+ \cup C_4^+$	[54]	$C_1^+ \cup C_4^+ \cup C_7^+$	5		
$C_1^+ \cup C_3^+ \cup C_2^-$	3^{2}	$C_1^+ \cup C_4^+ \cup C_9^+$	D_{10}		
q = 9		$C_1^+ \cup C_8^+ \cup C_9^+$	5		
$C_1^+ \cup C_1^- \cup C_{-\alpha}^+$	S_4	$C_1^+ \cup C_2^+ \cup C_{10}^-$	5		
$C_1^+ \cup C_1^- \cup C_{-\alpha^3}^+$	S_4	$C_1^+ \cup C_4^+ \cup C_9^-$	D_{10}		
$C_1^+ \cup C_\alpha^+ \cup C_{\alpha^2}^+$	4				
$C_1^+ \cup C_\alpha^+ \cup C_{\alpha^3}^+$	3:4				
$C_1^+ \cup C_{\alpha^2}^+ \cup C_{-\alpha}^+$	4				
with $\alpha = 1 + \sqrt{-1}$, i.e., $\alpha^2 + $	$\alpha = 1.$				

Table 10: Complete list of arcs, up to equivalence, that consist of three 'half conics' (for $q \leq 79$)

The arcs of this type can be roughly divided into three kinds:

• those that contain two half conics with the same index D, i.e., almost the full conic C_D ,

- those that use three half conics of the same sign,
- those that use half conics of two different signs, and never with the same index

The following lemma shows that those of the first and third kind will never be complete arcs

Lemma 1 Let $D, E, F \in GF(q)$, $D \neq E$. If $S = C_D^+ \cup C_E^+ \cup C_F^-$ is a (k, 3)-arc, then so is $S \cup \{P, Q\}$.

Proof: First note that no line through Q(0,0,1) can already contain 3 points of S. If that were the case, then each of these points would have the same middle coordinate (assuming coordinates are normalized to have first coordinate equal to 1). But the middle coordinates of C_D^+ and C_E^+ are squares, while those of C_F^- are not.

By symmetry, also no line through P(1, 0, 0) can already contain 3 points and finally, the line joining P and Q, i.e., the line with equation y = 0 does not intersect S.

Lemma 2 Let $q \equiv -1 \pmod{4}$ (i.e., -1 is not a square). Let $D, E, F \in GF(q)$, $D \neq E \neq F \neq D$. If $S = C_D^{\pm} \cup C_E^{\pm} \cup C_F^{\pm}$ (with independent choices of sign) is a (k,3)-arc, and $\{D, E, F\}$ contains at least one square and one non-square, then also $S \cup \{R\}$ is a (k,3)-arc.

Proof: A line through R(0, 1, 0) intersects S in points that have the same last coordinate. If -1 is not a square, then a half conic C_D^{\pm} can contain at most one point with a given last coordinate, and that last coordinate will be a square if and only if D is a square. As D, E, F are not all squares or all non-squares, the line can not contain 3 points of S.

From the proofs of these lemmas it follows that all three points P, Q, R can be added when the conditions of both lemmas are both satisfied.

The converse is not true: if neither lemma is satisfied this does not necessarily imply that an arc $S = C_D^{\pm} \cup C_E^{\pm} \cup C_F^{\pm}$ is complete. In fact we only find the following three complete arcs of size $\frac{3}{2}(q-1)$: in PG(2,11), $C_1^+ \cup C_4^+ \cup C_5^+$ and $C_1^+ \cup C_4^+ \cup C_9^+$ are complete. In PG(2,19) the set $C_1^+ \cup C_7^+ \cup C_{11}^+$ is complete.

There are two arcs of the second kind that merit special attention. For q = 7 and q = 19 the sets $C_1^+ \cup C_{\omega}^+ \cup C_{\omega^2}^+$ with $\omega^3 = 1$, $\omega \neq 1$ are (k, 3)-arcs. These arcs admit an additional symmetry $(x, y, z) \mapsto (x, y, \omega z)$ that permute the three half conics.

For q = 7, this arc is the set $C_1^+ \cup C_2^+ \cup C_4^+$. It is the set S_1 from Theorem 2 which is not complete. For q = 19, this arc is the set $C_1^+ \cup C_7^+ \cup C_{11}^+$ which is complete.

Note that the two arcs for q = 9 with S_4 as automorphism group are arcs of the type as described in Section 4.1 with $a = \alpha^3$ for $C_1^+ \cup C_1^- \cup C_{-\alpha}^+$ and $a = \alpha$ for $C_1^+ \cup C_1^- \cup C_{-\alpha}^+$.

For completeness we would like to point out that the complete (13, 3)-arc with group D_{10} for q = 11, can be constructed by combining *two* half conics $(C_1^+ \text{ and } C_3^+)$ and the three points P, Q and R.

4.3 (k,3)-arcs from cubic curves

4.3.1 The Hessian configuration

Let $q \equiv 1 \pmod{3}$. Then the field GF(q) contains an element $\omega \neq 1$ such that $\omega^3 = 1$ (and hence $\omega^2 + \omega + 1 = 0$).

Consider the set \mathcal{H} of the nine points with the following coordinates :

The set \mathcal{H} is called the *Hessian configuration* and has many interesting properties [1, 5]. It is a (9,3)-arc such that every point lies on exactly 4 trisecants and no bisecants. There are 12 trisecants in all. The configuration of points and trisecants represents an affine plane AG(2, 3) embedded in PG(2, q). (Note that for q = 7 this arc is complete and regular.)

 \mathcal{H} is the set of intersection points of the *Hesse pencil* of cubic curves generated by xyz = 0 and $x^3 + y^3 + z^3 = 0$. In fact, \mathcal{H} is the set of nine inflection points for each of the irreducible cubics in this pencil.

Every cubic curve in the Hesse pencil is left invariant by the group G_{18} (of order 18) that is generated by the permutations of the coordinates together with the transformation $\sigma_{\omega} : (x, y, z) \mapsto (x, \omega y, \omega^2 z)$. For specific curves in the pencil the automorphism group can be larger. The group of projective transformations that leaves \mathcal{H} itself invariant has order 216.

Let C_c denote the cubic of the Hessian pencil with equation $x^3 + y^3 + z^3 + cxyz$, with $c \in GF(q)$. C_c is irreducible (and non-singular) if and only if $c \neq -3, -3\omega, -3\omega^2$. In that case, the Abelian group associated with C_c (with one of its inflection points

chosen as neutral element) has \mathcal{H} as a subgroup. It follows that $|C_c|$ must be divisible by $|\mathcal{H}| = 9$. The following table lists the largest possible value of $|C_c|$ for finite fields not larger than 256.

q	$\max_c C_c $	q	$\max_c C_c $	q	$\max_c C_c $
4	9	64	81	157	180
7	9	67	81	163	189
13	18	73	90	169	189
16	18	79	90	181	207
19	27	97	117	193	216
25	36	103	117	199	225
31	36	109	126	211	234
37	45	121	144	223	252
43	54	127	144	229	252
49	63	139	162	241	270
61	72	151	171	256	288

For many fields these cubic curves C_c provide (k, 3)-arcs of a reasonably large size. All listed sizes lie in the interval $[q + \sqrt{q} - 1, q + 2\sqrt{q} + 1]$ and in some cases (q = 4, 25, 64, 121, 256) the upper bound (the Hasse bound) is even reached.

We shall be interested in the cubic curve C_1 , i.e., the curve with equation $x^3 + y^3 + z^3 + xyz = 0$. Consider the set \mathcal{H}_1 of the nine points with the following coordinates :

$$\begin{array}{rrrrr} (1,1,-1) & (1,-1,1) & (1,-1,-1) \\ (1,\omega,-\omega^2) & (1,-\omega,\omega^2) & (1,-\omega,-\omega^2) \\ (1,\omega^2,-\omega) & (1,-\omega^2,\omega) & (1,-\omega^2,-\omega) \end{array}$$

It is easily seen that each of these points belongs to the curve C_1 .

Both \mathcal{H} and \mathcal{H}_1 are orbits of G_{18} . The set $\hat{\mathcal{H}} \stackrel{\text{def}}{=} \mathcal{H} \cup \mathcal{H}_1$ is an (18,3)-arc. The tangent to the curve C_1 in a point of \mathcal{H}_1 intersects a point of \mathcal{H} . (For example, the line x + y + 2z = 0 is a tangent at (1, 1, -1) and intersects \mathcal{H} in (1, -1, 0).) Apart from these 9 tangents (which are bisecants to the arc) all other lines connecting two points of \mathcal{H}_1 are trisecants.

As a consequence $\hat{\mathcal{H}}$ is a subgroup of the Abelian group of the curve C_1 , and hence $|C_1|$ is a multiple of 18. Note that \mathcal{H} is a subgroup of index 2 of $\hat{\mathcal{H}}$, and hence the corresponding coset \mathcal{H}_1 is necessarily a (9,2)-arc (which does not lie on a conic).

The (9, 2)-arc \mathcal{H}_1 can be extended to a (k, 3)-arc in other ways. Consider for example the set S_{ω} :

$$\begin{array}{cccc} (1,0,0) & (0,1,0) & (0,0,1) \\ (\omega^2,1,1) & (1,\omega^2,1) & (1,1,\omega^2) \end{array}$$

which consists of two orbits of G_{18} , each of size 3. It is easily seen that this set is a

(6,2)-arc, and that the 15 bisecants have the following equations :

$$\begin{array}{ll} x=0, & y=0, & z=0, \\ x=y, & y=z, & z=x, \\ x=\omega y, & y=\omega z, & z=\omega x, \\ x=\omega^2 y, & y=\omega^2 z, & z=\omega^2 x, \end{array}$$

$$\omega x+y+z=0, \quad x+\omega y+z=0, \quad x+y+\omega z=0 \end{array}$$

forming three orbits of G_{18} (of sizes 3, 9, 3). By considering one line in each orbit, it is easily seen that no bisecant of S_{ω} intersects \mathcal{H}_1 in more than one point. As both S_{ω} and \mathcal{H}_1 are (k,2)-arcs, this proves that $\mathcal{H}_1 \cup S_{\omega}$ is a (15,3)-arc.

There is another way to extend \mathcal{H}_1 to an arc with interesting properties. Consider the set \mathcal{H}'_1 obtained by extending \mathcal{H}_1 with the following orbit of G_{18} :

 $(1, 1, 1), (1, \omega, \omega^2), (1, \omega^2, \omega)$

In other words, \mathcal{H}'_1 contains the 12 points with coordinates that are of the form $(\pm 1, \pm 1, \pm 1)$, $(\pm 1, \pm \omega, \pm \omega^2)$ or $(\pm 1, \pm \omega^2, \pm \omega)$. The symmetric group S_4 acts on \mathcal{H}'_1 by permuting the coordinates and allowing independent sign changes of the coordinates. Together with σ_{ω} this group extends to a group G_{72} of automorphisms of type $S_4 : 3$, of size 72.

In fact, applying the transformation $z \mapsto \omega z$ shows that \mathcal{H}'_1 is equivalent to $S^*(\omega)$ of Theorem 1 and therefore a (12, 3)-arc (and even a (12, 2)-arc provided the characteristic of the field is not 7).

By the same theorem it can be extended to a (15,3)-arc by adding the points (1,0,0), (0,1,0) and (0,0,1), still with G_{72} as a group of automorphisms, and to an (18,3)-arc provided the characteristic of the field is not 5 or 7. The latter arc no longer has σ_{ω} as an automorphism.

4.3.2 A (18,3)-arc with $G_S \approx 3^{1+2}_+$

Theorem 2 Let $q \equiv 1 \pmod{3}$. Let $\omega \in GF(q)$, $\omega \neq 1$ such that $\omega^3 = 1$. Let $c \in GF(q)$.

Consider the sets S_1 and $S_2(c)$ of points with the following coordinates :

$$S_{1} \qquad S_{2}(c)$$

$$(1,1,1) \quad (1,1,\omega) \quad (1,1,\omega^{2}) \qquad (1,0,c) \quad (\omega,0,c) \quad (\omega^{2},0,c) \qquad (3)$$

$$(1,\omega,1) \quad (1,\omega,\omega) \quad (1,\omega,\omega^{2}) \qquad (0,c,1) \quad (0,c,\omega) \quad (0,c,\omega^{2}) \qquad (1,\omega^{2},\omega) \quad (1,\omega^{2},\omega^{2}) \qquad (c,1,0) \quad (c,\omega,0) \quad (c,\omega^{2},0)$$

Then $S_1 \cup S_2(c)$ is an (18,3)-arc if and only if $c \neq 0$ and $c^3 \neq \pm 1$. The group $G_{27} \approx 3^{1+2}_+$ of size 27, generated by the elements

$$(x, y, z) \mapsto (x, \omega y, z), \quad (x, y, z) \mapsto (x, y, \omega z), \quad (x, y, z) \mapsto (y, z, x),$$

is a group of automorphisms of $S_1 \cup S_2(c)$.

Proof: Note that $|S_1| = |S_2(c)| = 9$, as $c \neq 0$.

First consider the case $c^3 = -1$, i.e., c = -1, $-\omega$ or $-\omega^2$. In that case $S_2(c)$ is precisely the Hesse configuration \mathcal{H} . Then the trisecant of \mathcal{H} with equation x + y + z = 0 intersects S_1 in the additional points $(1, \omega, \omega^2)$ and $(1, \omega^2, \omega)$ and therefore $S_1 \cup S_2(c)$ is not an (18,3)-arc. Henceforth we shall assume that $c^3 \neq -1$.

It is easily verified that G_{27} leaves both S_1 and $S_2(c)$ invariant. If we extend G_{27} to G_{54} by the map which interchanges two coordinates, then G_{54} still leaves S_1 invariant, but not $S_2(c)$ (unless c = 1, ω or ω^2 , i.e., $c^3 = 1$).

The stabilizer of (1, 1, 1) in G_{54} consists of the 6 coordinate permutations and has three orbits on S_1 . It is therefore easily seen that the lines connecting (1, 1, 1) with any other point of S_1 have equations

$$x = y, \quad x + \omega y + \omega^2 z = 0$$

or an equation obtained from these by permuting x, y, z.

It follows that S_1 is a (9,3)-arc in which every point lies on three trisecants (the orbit of G_{54} of the first equation above) and two bisecants (the orbit of the second equation). It also follows that if $c^3 \neq 1$ then no point of $S_2(c)$ lies on a trisecant of S_1 . Likewise, if $c^3 \neq -1$, then no point of $S_2(c)$ lies on a bisecant of S_1 .

As a consequence, any line which intersects $S_1 \cup S_2(c)$ in more than three points, must intersect $S_2(c)$ in more than two points. To determine these lines, consider the stabilizer of (1, 0, c) in G_{27} . It consists of the 3 transformations that multiply the *y*-coordinate by either 1, ω or ω^2 and has 5 orbits on $S_2(c)$. The lines connecting (1, 0, c) with any other point of $S_2(c)$ have equations

$$y = 0$$
, $cx + \frac{1}{c}y - z = 0$, $cx - c^2y - z = 0$,

or equations derived from these by multiplying the coefficient of y by ω or ω^2 .

If $c^3 = -1, -\omega$ or $-\omega^2$, i.e., if $c^9 = -1$, then some of these lines will coincide and each point will then lie on 4 trisecants of $S_2(c)$. The case $c^3 = -1$ was already excluded. If $c^3 = -\omega$ or $-\omega^2$, then it is easily verified that all 18 points of $S_1 \cup S_2(c)$ lie on the (irreducible) cubic with equation $x^3 - c^3y^3 + c^6z^6$, making it an (18,3)-arc. If $c^9 \neq -1$, then the only line through (1, 0, c) which intersects $S_2(c)$ in more than two points is the line with equation y = 0. Clearly this line does not contain a point of S_1 , hence again $S_1 \cup S_2(c)$ is an (18,3)-arc.

The set S_1 consists precisely of the nine intersection points of the pencil of cubics generated by $x^3 = y^3$ and $y^3 = z^3$. In this pencil, consider the three cubics C, C', C''with equations

$$C: c^{3}(x^{3} - y^{3}) = z^{3} - y^{3}, \ C': c^{3}(z^{3} - x^{3}) = y^{3} - x^{3}, \ C'': c^{3}(y^{3} - z^{3}) = x^{3} - z^{3}.$$

Note these cubics coincide if and only if $c^6 - c^3 + 1 = 0$ and then all points of $S_1 \cup S_2(c)$ belong to that cubic. Otherwise, each of the cubics C, C', C'' intersects $S_2(c)$ in precisely three points, corresponding to the three rows in (3).

5 Special (k,3)-arcs for q = 11

5.1 The unique complete arc of size 19 with $G_S \approx 19:3$

This arc can be constructed as an orbit of the 7th power of a Singer cycle. If we take this 7th power to be

$$\phi_1: (x_0 \ x_1 \ x_2) \mapsto (x_0 \ x_1 \ x_2) \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 6 & 9 & 5 \end{pmatrix},$$

then the arc is the orbit of the point with coordinates (1, 0, 0) under the action of ϕ_1 . The automorphism group of the arc has order 57 and is generated by ϕ_1 of order 19 and

$$\phi_2 : (x_0 \ x_1 \ x_2) \quad \mapsto \quad (x_0 \ x_1 \ x_2) \left(\begin{array}{ccc} 1 & 0 & 0 \\ 5 & 8 & 6 \\ 9 & 8 & 2 \end{array} \right)$$

of order 3. We have $\phi_1 \phi_2 = \phi_2 \phi_1^{11}$.

Note that this arc is regular: through each point there are 0 bisecants, and hence 9 trisecants and 3 unisecants.

5.2 The 2 complete arcs of size 21 with $G_S \approx 7:3$

These two arcs each consists of the union of three orbits of size 7 of the 19th power of a Singer cycle. Consider the following 19th power of a Singer cycle:

$$\phi_1: (x_0 \ x_1 \ x_2) \quad \mapsto \quad (x_0 \ x_1 \ x_2) \left(\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 5 & 1 & 1 \end{array} \right).$$

The first arc then consists of the three orbits of (5, -4, 1), (-5, -5, 1) and (-2, -3, 1)under the action of ϕ_1 , while the second arc consists of the three orbits of (4, 4, 1), (-1, 2, 1) and (5, -2, 1).

The automorphism group of both arcs is generated by ϕ_1 and the following linear transformation

$$\phi_2: (x_0 \ x_1 \ x_2) \quad \mapsto \quad (x_0 \ x_1 \ x_2) \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 4 \\ 3 & 8 & 10 \end{array} \right).$$

We have $\phi_1^7 = \phi_2^3 = 1$ and $\phi_1 \phi_2 = \phi_2 \phi_1^2$.

Note that again the arcs are regular: in both cases each point of the arc lies on 9 trisecants, and hence 2 bisecants and 1 unisecant.

5.3 The complete arcs with $G_S \approx S_4$

When applying Theorem 1 to q = 11, we find that $S^*(a) \cup S^*(\infty)$ is an arc for all values of a, except for the values 0 and ± 1 (as -1 is non-square in GF(11)). This arc is only complete for 4 of these values, i.e. when $a = \pm 4$ or $a = \pm 5$. (Note that $S^*(a) = S^*(-a)$.) This results in two inequivalent complete arcs of size 15 both having S_4 as automorphism group. These arcs are regular: each point lies on 6 trisecants, 2 bisecants and 4 unisecants.

Also according to Theorem 1, the values $a = \pm 3$ are the only ones for which $S^*(a) \cup S^*(0)$ is an arc in PG(2, 11). This arc is complete and has again S_4 as automorphism group. In this case, the set $S^*(a)$ is a complete (k, 2)-arc. The twelve points of $S^*(a)$ each lie on 5 trisecants, 7 bisecants and 0 unisecants. The six points of $S^*(0)$ each lie on 7 trisecants, 3 bisecants and 2 unisecants.

5.4 The complete arcs with $G_S \approx D_{10}$

As mentioned in Section 4.2, PG(2, 11) contains six complete arcs up to isomorphism that have the dihedral group of order 10 as group of automorphisms.

When using the same notations as in Section 4.2, we find the following complete (k, 3)-arcs up to isomorphism:

$$S_{13} = C_1^+ \cup C_3^+ \cup \{P, Q, R\}$$

$$S_{15} = C_1^+ \cup C_4^+ \cup C_9^+$$

$$S_{15}' = C_1^+ \cup C_4^+ \cup C_5^+$$

$$S_{17} = C_1^+ \cup C_1^- \cup C_9^+ \cup \{P, Q\}$$

$$S_{17}' = C_1^+ \cup C_1^- \cup C_5^+ \cup \{P, Q\}$$

$$S_{17}'' = C_1^+ \cup C_4^+ \cup C_9^- \cup \{P, Q\}$$

Because all indices that appear are squares in GF(11), the group D_{12} is generated by the transformations ϕ_1 and ϕ_2 as defined in Section 4.2.

6 Special (k,3)-arcs for q = 13

6.1 The unique complete arc of size 18 with $G_S \approx S_4$

When applying Theorem 1 to q = 13 we find 6 values of a for which $S^*(a) \cup S^*(0)$ is an arc. Only for $a = \pm 6$ this arc turns out to be complete and has S_4 as automorphism group.

This arc is regular: each point lies on 7 trisecants, 3 bisecants and 4 unisecants.

6.2 The complete arcs of size 21 with $G_S \approx D_{12}$

PG(2, 13) contains two complete arcs having the dihedral group of order 12 as group of automorphisms. Both arcs consist of the same three 'half' conics as defined in Section 4.2, together with three points. Using the same notations we find

$$\begin{array}{rcl} S & = & C_1^+ \cup C_1^- \cup C_7^+ \cup \{P,Q,R\} \\ S' & = & C_1^+ \cup C_1^- \cup C_7^+ \cup \{(1,0,7),(1,0,8),(1,0,9)\} \end{array}$$

Because 7 is a non-square in GF(13), the group D_{12} is generated by ϕ_1 and ϕ_3 as defined in Section 4.2.

6.3 Arcs related to the Hessian configuration

Because $13 \equiv 1 \pmod{3}$, the arcs defined in Section 4.3.1 exist in PG(2, 13). The set $\hat{\mathcal{H}} = \mathcal{H} \cup \mathcal{H}_1$ is a complete (18, 3)-arc for q = 13. Its group of automorphisms has size 36: it can be obtained by extending G_{18} with the following generator, of order 4 :

$$(x \ y \ z) \mapsto (x \ y \ z) \begin{pmatrix} 1 & 1 & 9 \\ 9 & 1 & 1 \\ 9 & 3 & 9 \end{pmatrix}$$

The (15,3)-arc $\mathcal{H}_1 \cup S_{\omega}$ also is complete for q = 13 and has the same group of automorphisms of size 36 as $\hat{\mathcal{H}}$.

6.4 The unique complete arc of size 18 with $G_S \approx 3^{1+2}_+$

For q = 13 and c = -2, the (18,3)-arc $S_1 \cup S_2(-2)$ as defined in Section 4.3.2 is complete with 3^{1+2}_+ as group of automorphisms.

6.5 Cubic curves of size 21

The largest size of a cubic curve in PG(2, 13) turns out to be 21, with two examples up to isomorphism.

The first example corresponds to the following equation

$$xy(x+y) = -6z^3$$

This is an irreducible cubic curve with three inflection points (coordinates: (1,0,0), (0,1,0), (1,-1,0)) and three inflectional tangents that are concurrent (x = 0, y = 0 and x + y = 0, intersecting in (0,0,1).)

The automorphism group G of this curve has size 18, is of type $3S_3$ and is generated by the permutations of x, y and -x-y and the cyclic element $z \mapsto 3z$ (with $3^3 = 1$).

Apart from the three inflection points, the curve has 18 additional points, which form an orbit of G. The points are those whose coordinates (x, y, z) satisfy $\{x, y, -x-y\} = \{1, 2, -3\}$ and $z^3 = 1$. The points P_0, \ldots, P_{20} of this curve can be numbered in a way that reflects the Abelian group of the curve (which is cyclic of order 21) :

 P_i, P_j, P_k are collinear if and only if $i + j + k \equiv 0 \pmod{21}$.

The automorphism group G can also be easily expressed in terms of this point numbering: the circular permutation $(x, y, z) \mapsto (y, -x - y, z)$ is equivalent to $P_i \mapsto P_{i+7}$, $P_i \mapsto P_{-i}$ interchanges x and -x - y, and $P_i \mapsto p_{4i}$ corresponds to $z \mapsto 3z$ (each time with index aritmetic modulo 21).

The automorphism group has two orbits of size 3 in the plane. A first orbit consists of the inflection points P_0 , P_7 and P_{14} , the second orbit corresponds to the points with coordinates (1, 1, 0), (-2, 1, 0) and (1, -2, 0). Both orbits lie on the line with equation z = 0.

These six points have an important property: every line through these points, except the line z = 0, intersects the orbit of 18 non-inflection points in at most two points.

For the first orbit this is an immediate consequence of the fact that all 21 points lie on an irreducible cubic curve. For the second orbit, consider the representative point (1, 1, 0). From (4) we compute the values of (y - x)/z for each point P_i that is not an inflection point.

The number of times a specific value k occurs in this table, is equal to the number of intersection points with the line x - y + kz = 0 through (1, 1, 0). For $k = \pm 2, \pm 5, \pm 6$ there is one intersection point, for $k = \pm 1, \pm 3, \pm 4$ there are two, but never three. This proves our claim.

From this we conclude that adding any three of these six points to the 18 non-inflection points of the cubic yields a (21,3)-arc, giving a total of 6 non-equivalent

(21,3)-arcs for q = 13. These arcs turn out to be complete. Only two of them have G as group of automorphisms. (The others have a cyclic automorphism group of order 3 or 6.)

The second example of a cubic curve of size 21 corresponds to the curve C_{21} with equation

$$x^2y + y^2z + 4z^2x = 0.$$

This cubic has no inflection points. Its automorphism group is the group 3^2 of size 9 and is generated by the transformations

$$(x, y, z) \mapsto (x, 3y, 9z), \quad (x, y, z) \mapsto (y, 4z, x).$$

The group has one orbit of size 3, with points (1,0,0), (0,1,0) and (0,0,1), and 20 orbits of size 9 (on the points of PG(2,13)). The cubic C_{21} consists of the orbit of size 3 and two orbits of size 9, with representatives (1,-1,-2) and (1,-1,5). It is a complete (21,3)-arc.

Finally, it turns out that the same group leaves invariant a different (21,3)-arc which does not lie on a cubic. It consists of the orbit of size 3 together with the two orbits of size 9 with representatives (1, 1, 2) and (1, 1, 6).

6.6 Regular arcs for q = 13

From Section 3.3 we know that PG(2, 13) contains several (k, 3)-arcs that are regular. We shall only discuss those of size 21.

The first (21,3)-arc of this type has automorphism group of type S_3 . Each point lies on 8 trisecants (and 4 bisecants and 2 unisecants). The points of this arc can be given by the following coordinates

The group S_3 acts by permuting the coordinates. The first three rows of (5) form a (12,2)-arc consisting of all points of the conic $2(x^2 + y^2 + z^2) = (x + y + z)^2$ except those on the line x + y + z = 0, i.e., (1,3,9) and (1,9,3).

The second (21,3)-arc of this type has a cyclic automorphism group of size 3. Each point lies on 9 trisecants, 2 bisecants and 3 unisecants. The points of this arcs can

be given by the following coordinates.

The automorphism group is generated by the transformation $(x, y, z) \mapsto (y, 4z, x)$ which we encountered before, and cyclically permutes the rows of (6).

The third and fourth (21,3)-arc of this type are the two arcs discussed in the last part of Section 6.5.

6.7 The unique complete arc of size 21 with $G_S \approx D_{14}$

For q = 13, there is one complete arc having the dihedral group of order 14 as automorphism group. Let C_1 be the conic with equation $x_0^2 + x_2^2 + 6x_0x_1 + 6x_1x_2 + 11x_0x_2 = 0$ and C_2 the conic with equation $x_0x_2 = x_1^2$. Then the arc consists of all points of C_1 together with the points of C_2 with coordinates $(1, t, t^2)$ with t one of the elements in the following list:

$$5, 2, 3, 1, 9, 7, 8 \tag{7}$$

The points of C_1 have the following coordinates:

$$(1,5,2), (1,1,5), (1,2,0), (0,1,0), (0,1,7), (1,8,8), (1,9,7)$$
 (8)

$$(1, 5, 9), (1, 8, 11), (1, 1, 4), (1, 0, 1), (1, 10, 10), (1, 9, 6), (1, 2, 3)$$
 (9)

The automorphism group can be generated by

$$\psi_1: (x, y, z) \mapsto (z, 12y + 10z, x + 6y + 9z)$$

of order 7 and

$$\psi_2: (x, y, z) \mapsto (z, y, x)$$

of order 2. For the arc points on $C_2 \ \psi_1$ corresponds to $t \mapsto 12/t + 10$ and ψ_2 to $t \mapsto 1/t$. The order of the points listed in (7), (8) and (9) corresponds to consecutive applications of ψ_1 . This order is reversed by ψ_2 . We have $\psi_1\psi_2 = \psi_2\psi_1^{-1}$.

References

[1] ARTEBANI M. and DOLGACHEV I., The Hesse pencil of plane cubic curves, L'Enseign. Math., 55 (2009), 235–273.

- [2] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A. and WILSON, R. A., Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
- [3] COOLSAET K. and STICKER H., A full classification of the complete k-arcs in PG(2,23) and PG(2,25), Journal of Combinatorial Designs, 17(6) (2009), 459–477.
- [4] COOLSAET K. and STICKER H., The complete k-arcs of PG(2,27) and PG(2,29), Journal of Combinatorial Designs, **19(2)** (2011), 111–130.
- [5] HIRSCHFELD J. W. P., Projective Geometries over Finite Fields (second edition), Clarendon Press, Oxford, 1998.
- [6] MARCUGINI S., MILANI A. and PAMBIANCO F., Classification of the (n, 3)arcs in PG(2, 7), Journal of Geometry, **80** (2004), 179–184.
- [7] MARCUGINI S., MILANI A. and PAMBIANCO F., Classification of the $[n, 3, n-3]_q$ codes over GF(7) GF(8) and GF(9), Ars Combinatorica, **61** (2001), 263–269.
- [8] MARCUGINI S., MILANI A. and PAMBIANCO F., Maximal (n,3)-arcs in PG(2,11), Discrete Mathematics, **208/209** (1999), 421–426
- [9] MARCUGINI S., MILANI A. and PAMBIANCO F., Maximal (n,3)-arcs in PG(2,13), Discrete Mathematics, **294** (2005), 139–145.
- [10] MCKAY B. D., Isomorph-Free exhaustive Generation, J. Algorithms, 26 (1998), 306–324.