Serdica J. Computing **6** (2012), 253–266

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

A NECESSARY AND SUFFICIENT CONDITION FOR THE EXISTENCE OF AN (n, r)-ARC IN PG$(2, q)$ AND ITS APPLICATIONS

Noboru Hamada, Tatsuya Maruta*, Yusuke Oya

Abstract. Let q be a prime or a prime power ≥ 3. The purpose of this paper is to give a necessary and sufficient condition for the existence of an (n, r)-arc in PG$(2, q)$ for given integers n, r and q using the geometric structure of points and lines in PG$(2, q)$ for $n > r \geq 3$. Using the geometric method and a computer, it is shown that there exists no $(34, 3)$ arc in PG$(2, 17)$, equivalently, there exists no $[34, 3, 31]_{17}$ code.

1. Introduction. We denote by $\mathbb{F}_q$ the field of q elements with $q \geq 3$. A linear code over $\mathbb{F}_q$ of length n, dimension k is a k-dimensional subspace $\mathcal{C}$ of the vector space $\mathbb{F}_q^n$ of n-tuples over $\mathbb{F}_q$. The vectors in $\mathcal{C}$ are called codewords. $\mathcal{C}$ is called an $[n, k, d]_q$ code if every non-zero codeword has at least d non-zero entries and some codeword has exactly d non-zero entries [4], [10], [11], [12].

Let A be a set of n points in PG$(2, q)$. If A satisfies the following conditions:

ACM Computing Classification System (1998): E.4.

Key words: (n, r)-arcs, projective plane, linear codes.

*This research was partially supported by Grant-in-Aid for Scientific Research of Japan Society for the Promotion of Science under Contract Number 24540138.

(a) $|A \cap L| \le r$ for every line L,

(b) $|A \cap L| = r$ for some line L,

then A is called an (n,r)-*arc* of PG$(2,q)$, where $n > r$ and $2 \le r \le q-1$. It is known [3] that if $q < n-3 \le 2q$, then there exists an $(n,3)$-arc of PG$(2,q)$ if and only if there exists an $[n,3,n-3]_q$ code.

Problem 1. *For an integer r with $2 \le r \le q-1$, find $m_r(2,q)$, the largest value of n for which an (n,r)-arc exists in PG$(2,q)$.*

It is known that $m_r(2,p) \le (r-1)p+1$ for any prime p and any integer $r \le (p+3)/2$ and $m_r(2,p) = (r-1)p+1$ for $p = 3,5,7$ and for $2 \le r \le p-1$. Problem 1 has been completely solved for $3 \le q \le 9$ [11]. For $11 \le q \le 19$, the values of $m_r(2,q)$ are known as Table 1 [2], [3], [6], [7], [8]. See [11] for $r = 2$. See also [12].

There are exactly three $(9,3)$-arcs in PG$(2,4)$ [11], two $(11,3)$-arcs and six $(16,4)$-arcs in PG$(2,5)$ [5]. Marcugini et al. classified $(m_r(2,q),3)$-arcs in PG$(2,q)$ using a computer for $q = 7,8,9,11,13$ ([13], [14], [15]).

Let A be an (n,r)-arc in PG$(2,q)$. A line L with $|A \cap L| = i$ is called an i-line. Let τ_i be the number of i-lines. The list of τ_i's is called the *spectrum* of A. An easy counting argument yields the following.

Lemma 1.1. *The spectrum of an (n,r)-arc in PG$(2,q)$ satisfies*

$$\sum_{i=0}^{r} \tau_i = q^2+q+1, \tag{1.1}$$

$$\sum_{i=1}^{r} i\tau_i = n(q+1), \tag{1.2}$$

$$\sum_{i=2}^{r} i(i-1)\tau_i = n(n-1). \tag{1.3}$$

Let $L = \{P_0, P_1, \ldots, P_q\}$ be a line. Let $L_{k,1}, L_{k,2}, \ldots, L_{k,q}$ be the q lines through P_k other than L for $0 \le k \le q$. Let $Q_{i,j}$ be the intersection point of $L_{0,i}$ and $L_{1,j}$ for $1 \le i,j \le q$. Then L and $L_{k,j}$'s are the q^2+q+1 lines and $P_0, P_1, \ldots, P_q$ and $Q_{i,j}$'s are the q^2+q+1 points of PG$(2,q)$. Let $L_{k,s(k,i,j)} = \langle P_k, Q_{i,j} \rangle$, the line through P_k and $Q_{i,j}$. Then $L_{0,s(0,i,j)}, L_{1,s(1,i,j)}, \ldots, L_{q,s(q,i,j)}$ are the lines through $Q_{i,j}$ for $1 \le i,j \le q$. Hence there is a one-to-one correspondence between $Q_{i,j} \in \mathcal{Q}_q$ and $[s(0,i,j), s(1,i,j), \ldots, s(q,i,j)] \in S_q$, where

$$\text{(1.4)} \qquad \mathcal{Q}_q = \{Q_{i,j} \mid 1 \leq i,j \leq q\},$$
$$\text{(1.5)} \qquad S_q = \{[s(0,i,j), s(1,i,j), \ldots, s(q,i,j)] \mid 1 \leq i,j \leq q\}.$$

Let H be a set of x elements in S_q denoted by

$$\text{(1.6)} \qquad H = \{[h_{0,w}, h_{1,w}, \ldots, h_{q,w}] \mid w = 1, 2, \ldots, x\}.$$

For $0 \leq k \leq q$ and $1 \leq u \leq q$, let

$$\text{(1.7)} \qquad m_{k,u} = |\{w \in \{1, 2, \ldots, x\} \mid h_{k,w} = u\}|.$$

Theorem 1.2. *There exists an (n,r)-arc A in $PG(2,q)$ with $\tau_0 > 0$ if and only if there exists a set H with $x = n$ satisfying the following conditions.*

(a-0) $m_{k,u} \leq r$ *for any* $0 \leq k \leq q$ *and* $1 \leq u \leq q$,

(b-0) $m_{k,u} = r$ *for some* $0 \leq k \leq q$ *and* $1 \leq u \leq q$.

Theorem 1.3. *There exists an (n,r)-arc A in $PG(2,q)$ with $\tau_1 > 0$ if and only if there exists a set H with $x = n-1$ satisfying the following conditions.*

(a-1) $m_{k,u} \leq r$ *for any* $1 \leq k \leq q$ *and* $1 \leq u \leq q$,

(b-1) $m_{0,u} \leq r - 1$ *for any* $1 \leq u \leq q$,

(c-1) *either* $m_{k,u} = r$ *for some* $1 \leq k \leq q$ *and* $1 \leq u \leq q$, *or* $m_{0,u} = r - 1$ *for some* $1 \leq u \leq q$.

Theorem 1.4. *There exists an (n,r)-arc A in $PG(2,q)$ with $\tau_2 > 0$ if and only if there exists a set H with $x = n-2$ satisfying the following conditions.*

(a-2) $m_{k,u} \leq r$ *for any* $2 \leq k \leq q$ *and* $1 \leq u \leq q$,

(b-2) $m_{k,u} \leq r - 1$ *for any* $1 \leq u \leq q$ *and* $k = 0, 1$,

(c-2) *either* $m_{k,u} = r$ *for some* $2 \leq k \leq q$ *and* $1 \leq u \leq q$, *or* $m_{k,u} = r - 1$ *for some* $1 \leq u \leq q$ *and* $k = 0, 1$.

Theorems 1.3 and 1.4 can be generalized as follows. Let A be an (n, r)-arc in $\mathrm{PG}(2, q)$ with $\tau_z > 0$ for some integer $z \geq 3$. Then there exists a line $L = \{P_0, P_1, \ldots, P_q\}$ such that $A \cap L = \{P_0, P_1, \ldots, P_{z-1}\}$. Let $U = \{1, 2, \ldots, q\}$, $T_1 = \{0, 1, \ldots, z-1\}$ and $T_2 = \{z, z+1, \ldots, q\}$.

Theorem 1.5. *There exists an (n, r)-arc A in PG$(2, q)$ with $\tau_z > 0$ for some integer $z \geq 3$ if and only if there exists a set H with $x = n - z$ satisfying the following conditions.*

(a-z) $m_{k,u} \leq r$ *for any* $k \in T_2$ *and* $u \in U$,

(b-z) $m_{k,u} \leq r - 1$ *for any* $k \in T_1$ *and* $u \in U$,

(c-z) *either* $m_{k,u} = r$ *for some* $k \in T_2$ *and* $u \in U$, *or* $m_{k,u} = r - 1$ *for some* $k \in T_1$ *and* $u \in U$.

Remark 1.6. The method using the above theorems is called *Hamada's method*. To apply the theorems, we first need to construct S_q called *Hamada's set*.

Table 1. The known values and bounds on $m_r(2, q)$ for $11 \leq q \leq 19$

r \ q	11	13	16	17	19
2	12	14	18	18	20
3	21	23	28–33	28–35	31–39
4	32	38–40	52	48–52	52–58
5	43–45	49–53	65	61–69	68–77
6	56	64–66	78–82	79–86	86–96
7	67	79	93–97	95–103	105–115
8	78	92	120	114–120	126–134
9	89–90	105	129–130	137	147–153
10	100–102	118–119	142–148	154	172
11		132–133	159–164	166–171	191
12		145–147	180–181	183–189	204–210
13			195–199	205–207	225–230
14			210–214	221–225	243–250
15			231	239–243	265–270
16				256–261	286–290
17					305–310
18					324–330

It is known from Table 1 that $28 \leq m_3(2, 17) \leq 35$. Using Hamada's method and a computer, it can be shown that the following theorem holds.

Theorem 1.7. *There exists no* $(34, 3)$*-arc in* $PG(2, 17)$*. Equivalently, there exists no* $[34, 3, 31]_{17}$ *code.*

Corollary 1.8. $28 \leq m_3(2, 17) \leq 33$.

Note that the codes obtained from $(n, 3)$-arcs are near-MDS (NMDS) codes [9]. Since the dual codes of NMDS codes are also NMDS [9], we get the following.

Corollary 1.9. *There exists no NMDS* $[34, 31, 3]_{17}$ *code.*

In Section 2, the proofs of Theorems 1.2–1.5 are given. In Section 3, a method how to construct the set S_p is given for prime p. In Section 5, the algorithm for searching a $(34, 3)$-arc in PG$(2, 17)$ to prove Theorem 1.7 by means of Theorem 1.4 is given.

2. The proofs of Theorems 1.2–1.5.

Proof of Theorem 1.2. (1) Assume there exists an (n, r)-arc A in PG$(2, q)$ with $\tau_0 > 0$ and that $L = \{P_0, P_1, \ldots, P_q\}$ is a 0-line. Then A can be expressed as $A = \{Q_{c_w,d_w} \mid 1 \leq w \leq n\}$ using some integers c_w and d_w in $\{1, 2, \ldots, q\}$. Let $L_{k,h_{k,w}}$ be the line through the two points P_k and Q_{c_w,d_w} and let

$$H = \{[h_{0,w}, h_{1,w}, \ldots, h_{q,w}] \mid w = 1, 2, \ldots, n\}. \tag{2.1}$$

Then $L_{0,h_{0,w}}, L_{1,h_{1,w}}, \ldots, L_{q,h_{q,w}}$ are the $q+1$ lines through Q_{c_w,d_w}. Let $m_{k,u}$ be the number of integers w with $1 \leq w \leq n$ such that $h_{k,w} = u$ for $0 \leq k \leq q$ and $1 \leq u \leq q$. Then $m_{k,u}$ gives the number of points in A on the line $L_{k,u}$. Hence it follows from (a) and (b) that the conditions (a-0) and (b-0) hold.

(2) Assume there exists a set H, given by (2.1), consisting of n elements in S_q which satisfies the conditions (a-0) and (b-0). Then there exists a point, denoted by Q_{c_w,d_w}, corresponding to $[h_{0,w}, h_{1,w}, \ldots, h_{q,w}]$ in H for $1 \leq w \leq n$. Let $A = \{Q_{c_w,d_w} \mid 1 \leq w \leq n\}$. Then L is a 0-line for A. It follows from (a-0) and (b-0) that the conditions (a) and (b) hold. This implies that A is an (n, r)-arc A in PG$(2, q)$ with $\tau_0 > 0$.

Proof of Theorems 1.3–1.5. Let z be a positive integer.

(1) Assume there exists an (n, r)-arc A in PG$(2, q)$ with $\tau_z > 0$ and that $L = \{P_0, P_1, \ldots, P_q\}$ is a z-line. Without loss of generality, we may assume that $A \cap L = \{P_0, P_1, \ldots, P_{z-1}\}$ and that $A = \{P_0, P_1, \ldots, P_{z-1}\} \cup \{Q_{c_w,d_w} \mid 1 \leq w \leq n - z\}$. Let $L_{k,h_{k,w}}$ be the line through the two points P_k and Q_{c_w,d_w} and let

$$H = \{[h_{0,w}, h_{1,w}, \ldots, h_{q,w}] \mid w = 1, 2, \ldots, n - z\}. \tag{2.2}$$

Then $L_{0,h_{0,w}}, L_{1,h_{1,w}}, \ldots, L_{q,h_{q,w}}$ are the $q+1$ lines through Q_{c_w,d_w}. Let $m_{k,u}$ be the number of integers w with $1 \le w \le n-z$ such that $h_{k,w} = u$ for $0 \le k \le q$ and $1 \le u \le q$. Then $m_{k,u}$ gives the number of points in A on the line $L_{k,u}$. Hence it follows from (a) and (b) that the conditions (a-z), (b-z) and (c-z) hold.
(2) Assume there exists a set H, given by (2.2), consisting of $n-z$ elements in S_q which satisfies the conditions (a-z), (b-z) and (c-z). Then there exists a point, denoted by Q_{c_w,d_w}, corresponding to $[h_{0,w}, h_{1,w}, \ldots, h_{q,w}]$ in H for $1 \le w \le n-z$. Let $A = \{P_0, P_1, \ldots, P_{z-1}\} \cup \{Q_{c_w,d_w} \mid 1 \le w \le n-z\}$. Then L is a z-line for A. It follows from (a-z), (b-z), (c-z) that the conditions (a) and (b) hold. This implies that A is an (n,r)-arc A in $\mathrm{PG}(2,q)$ with $\tau_z > 0$.

3. How to construct S_p for prime p. In this section, we consider the case when q is a prime p for simplicity. Let L be a line in $\mathrm{PG}(2,p)$ with $L = \{P_0, P_1, \ldots, P_p\}$. Let $L_{k,1}, L_{k,2}, \ldots, L_{k,p}$ be the p lines through P_k other than L for $0 \le k \le p$. Let $Q_{i,j} = L_{0,i} \cap L_{1,j}$ for $1 \le i,j \le p$ as in Section 1. A point P with homogeneous coordinate (a,b,c) is referred to as $P(a,b,c)$. Without loss of generality, we may assume

1. $P_0(1,0,0)$, $P_1(0,1,0)$, $Q_{1,1}(0,0,1)$ and $P_k(1,k-1,0)$ for $2 \le k \le p$,
2. $Q_{i,1}(0,1,i-1)$, $Q_{1,j}(1,0,j-1)$ for $2 \le i \le p$, $2 \le j \le p$,
3. $L_{k,u} = \langle P_k, Q_{1,u} \rangle$ for $2 \le k \le p$, $1 \le u \le p$,

where $\langle P_k, Q_{1,u} \rangle$ stands for the line through the points P_k and $Q_{1,u}$. Since $L_{0,i} = \langle P_0, Q_{i,1} \rangle$ and $L_{1,j} = \langle P_1, Q_{1,j} \rangle$ for $1 \le i,j \le p$, We get the following.

Lemma 3.1. *For $2 \le i \le p$, $2 \le j \le p$, the coordinate of the point $Q_{i,j}$ is $Q_{i,j}(1, x, (i-1)x)$ for some $x \in \mathbb{F}_p$ with $(i-1)x \equiv j-1 \mod p$.*

Recall that $L_{k,s(k,i,j)} = \langle P_k, Q_{i,j} \rangle$ for $0 \le k \le p$, $1 \le i \le p$, $1 \le j \le p$. We can construct S_p of (1.5) from the next lemma.

Lemma 3.2. *$s(k,i,j)$ is determined as follows:*

(1) $s(0,i,j) = i$ *for* $1 \le i \le p$, $1 \le j \le p$,

(2) $s(1,i,j) = j$ *for* $1 \le i \le p$, $1 \le j \le p$,

(3) $s(k,1,j) = j$ *for* $2 \le k \le p$, $1 \le j \le p$,

(4) $s(k,i,1) \equiv i + k - ik \pmod p$ *for* $k \ge 2$, $i \ge 2$,

(5) $s(k,i,j) = 1$ *for* $k \geq 2$, $i \geq 2$, $j \equiv (i-1)(k-1)+1 \pmod p$,

(6) $s(k,i,j) \equiv (i-1)(j-1)(k-1)((i-1)(k-1)-(j-1))^{-1}+1 \pmod p$ *for* $k \geq 2$, $i \geq 2$, $j \geq 2$ *with* $j \not\equiv (i-1)(k-1)+1 \pmod p$.

P r o o f. (1), (2) and (3) follow from $L_{0,i} = \langle P_0, Q_{i,1}\rangle$, $L_{1,j} = \langle P_1, Q_{1,j}\rangle$ and $L_{k,j} = \langle P_k, Q_{1,j}\rangle$ for $k \geq 2$.
(4) Assume $L_{k,u} = \langle P_k, Q_{i,1}\rangle$. Since P_k, $Q_{i,1}$ and $Q_{1,u}$ are collinear, we get

$$\begin{vmatrix} 1 & k-1 & 0 \\ 0 & 1 & i-1 \\ 1 & 0 & u-1 \end{vmatrix} = 0$$

giving $u = 1-(i-1)(k-1) \in \mathbb{F}_p$ as desired.
(5) Since $L_{k,1} = \langle P_k, Q_{1,1}\rangle = [k-1,-1,0]$, where $[a,b,c]$ stands for the line in $\mathrm{PG}(2,p)$ defined by the equation $ax+by+cz=0$ with $(a,b,c) \in \mathbb{F}_p^3 \setminus \{(0,0,0)\}$, it holds that $Q_{i,j}(1,(j-1)(i-1)^{-1},j-1) \in L_{k,1}$ if and only if $k-1-(j-1)(i-1)^{-1} = 0$, that is, $j = (i-1)(k-1)+1 \in \mathbb{F}_p$.
(6) Assume $L_{k,m} = \langle P_k, Q_{i,j}\rangle$. Since $L_{0,i} \cap L_{1,j} = Q_{i,j}(1,(j-1)(i-1)^{-1},j-1)$ and $L_{k,m} = \langle P_k, Q_{1,m}\rangle = [(k-1)(m-1),-(m-1),-(k-1)]$, we have $Q_{i,j} \in L_{k,m}$ if and only if $m = (i-1)(j-1)(k-1)((i-1)(k-1)-(j-1))^{-1}+1 \in \mathbb{F}_p$. □

In the case $i = p$, we have the following as a consequence of the above lemma.

Corollary 3.3. *The values* $s(k,p,j)$ *satisfy the following conditions:*

(1) $s(k,p,1) = k$ *for* $1 \leq k \leq p$.

(2) $s(k,p,j) = s(j,p,k)$ *for* $1 \leq k \leq p$, $1 \leq j \leq p$.

(3) $s(j,p,j) = (j+1)/2$ *for* $j = 1,3,5,\ldots,p$.

(4) $s(j,p,j) = (p+j+1)/2$ *for* $j = 2,4,6,\ldots,p-1$.

(5) *If* $k+j = p+2$ *with* $2 \leq k \leq p$, *then* $s(k,p,j) = 1$.

(6) *If* $k+j \neq p+2$ *with* $2 \leq k \leq p$ *and* $2 \leq j \leq p$, *then* $s(k,p,j) \equiv (jk-1)/(k+j-2) \pmod p$.

Corollary 3.4. *For* $2 \leq i \leq p-1$ *and* $1 \leq j \leq p$, $[s(1,i,j), s(2,i,j),\ldots,$ $s(p,i,j)]$ *is obtained from* $[s(1,p,j), s(2,p,j),\ldots, s(p,p,j)]$ *by the permutation on* *the entries such that* $s(k,i,j) = s(c(k,i),p,j)$ *for* $k = 1, 2, \ldots, p$, *where* $c(k,i) \equiv p + k - (k-1)i \pmod p$.

Proof. We have $s(1,i,j) = s(c(1,i),p,j) = j$ by part (2) of Lemma 3.2.

Assume $k \geq 2$, $i \geq 2$, $j \geq 2$ with $j \not\equiv (i-1)(k-1)+1 \pmod p$ so that part (6) of Lemma 3.2 holds. Then $s(k,i,j) = d \in \{1, 2, \ldots, p\}$ such that

$$((i-1)(k-1)-(j-1))(d-1) \equiv (i-1)(j-1)(k-1) \pmod p.$$

Since $(p-1)(c(k,i)-1)-(j-1) \equiv (i-1)(k-1)-(j-1)$ and $(p-1)(j-1)(c(k,i)-1) \equiv (i-1)(j-1)(k-1) \pmod p$, we get $s(k,i,j) = s(c(k,i),p,j)$.

Next, assume $k \geq 2$, $i \geq 2$ and $j = 1$ so that part (4) of Lemma 3.2 holds. Then $s(k,i,1) \equiv i+k-ik$ and $s(c(k,i),p,1) \equiv p + c(k,i) - p \cdot c(k,i) \equiv i+k-ik \pmod p$. This implies $s(k,i,1) = s(c(k,i),p,1)$.

Finally, assume $k \geq 2$, $i \geq 2$ and $j \equiv (i-1)(k-1)+1 \pmod p$ so that part (5) of Lemma 3.2 holds. Then $s(k,i,j) = s(c(k,i),p,j) = 1$ since $(p-1)(c(k,i)-1)+1 \equiv (i-1)(k-1)+1 \equiv j \pmod p$. Thus $s(k,i,j) = s(c(k,i),p,j)$. $\square$

Since there is a one-to-one correspondence between $[s(0,i,j), \ldots, s(p,i,j)] \in S_p$ and $Q_{i,j} \in \mathcal{Q}_q$, $Q_{i,j}$ is also referred to as $Q_{i,j}[s(0,i,j), \ldots, s(p,i,j)]$.

Example 3.5. For $p = 5$, we get the following by Lemmas 3.1 and 3.2:

$P_0(1,0,0)$, $P_1(0,1,0)$, $P_2(1,1,0)$, $P_3(1,2,0)$, $P_4(1,3,0)$, $P_5(1,4,0)$,

$Q_{1,1}(0,0,1) = Q_{1,1}[1,1,1,1,1,1]$, $Q_{2,1}(0,1,1) = Q_{2,1}[2,1,5,4,3,2]$,
$Q_{1,2}(1,0,1) = Q_{1,2}[1,2,2,2,2,2]$, $Q_{2,2}(1,1,1) = Q_{2,2}[2,2,1,3,5,4]$,
$Q_{1,3}(1,0,2) = Q_{1,3}[1,3,3,3,3,3]$, $Q_{2,3}(1,2,2) = Q_{2,3}[2,3,4,1,2,5]$,
$Q_{1,4}(1,0,3) = Q_{1,4}[1,4,4,4,4,4]$, $Q_{2,4}(1,3,3) = Q_{2,4}[2,4,2,5,1,3]$,
$Q_{1,5}(1,0,4) = Q_{1,5}[1,5,5,5,5,5]$, $Q_{2,5}(1,4,4) = Q_{2,5}[2,5,3,2,4,1]$,

$Q_{3,1}(0,1,2) = Q_{3,1}[3,1,4,2,5,3]$, $Q_{4,1}(0,1,3) = Q_{4,1}[4,1,3,5,2,4]$,
$Q_{3,2}(1,3,1) = Q_{3,2}[3,2,3,4,1,5]$, $Q_{4,2}(1,2,1) = Q_{4,2}[4,2,5,1,4,3]$,
$Q_{3,3}(1,1,2) = Q_{3,3}[3,3,1,5,4,2]$, $Q_{4,3}(1,4,2) = Q_{4,3}[4,3,2,4,5,1]$,
$Q_{3,4}(1,4,3) = Q_{3,4}[3,4,5,3,2,1]$, $Q_{4,4}(1,1,3) = Q_{4,4}[4,4,1,2,3,5]$,
$Q_{3,5}(1,2,4) = Q_{3,5}[3,5,2,1,3,4]$, $Q_{4,5}(1,3,4) = Q_{4,5}[4,5,4,3,1,2]$,

$Q_{5,1}(0,1,4) = Q_{5,1}[5,1,2,3,4,5]$,
$Q_{5,2}(1,4,1) = Q_{5,2}[5,2,4,5,3,1]$,
$Q_{5,3}(1,3,2) = Q_{5,3}[5,3,5,2,1,4]$,
$Q_{5,4}(1,2,3) = Q_{5,4}[5,4,3,1,5,2]$,
$Q_{5,5}(1,1,4) = Q_{5,5}[5,5,1,4,2,3]$.

As for the correspondence between $Q_{i,j} \in \mathcal{Q}_q$ and $[s(0,i,j), s(1,i,j), \ldots, s(q,i,j)] \in S_q$ for $q = 7, 11, 13, 16, 17, 19$, see [16].

Example 3.6. It is known that $m_3(2,5) = 11$. It follows from Lemma 1.1 that there exists a $(11,3)$-arc in PG$(2,5)$ with $\tau_2 > 0$. Let $A = \{P_0, P_1, Q_{1,1}, Q_{2,2}, Q_{2,4}, Q_{3,3}, Q_{3,5}, Q_{4,3}, Q_{4,5}, Q_{5,2}, Q_{5,4}\}$, see the previous example for the coordinates of the points in A. Then the corresponding set $H \subset S_5$ is $H = \{[1,1,1,1,1,1], [2,2,1,3,5,4], [2,4,2,5,1,3], [3,3,1,5,4,2], [3,5,2,1,3,4], [4,3,2,4,5,1], [4,5,4,3,1,2], [5,2,4,5,3,1], [5,4,3,1,5,2]\}$ and the values $m_{k,u}$ corresponding to H are given by

$$\begin{aligned}
(m_{01}, m_{02}, m_{03}, m_{04}, m_{05}) &= (1,2,2,2,2),\\
(m_{11}, m_{12}, m_{13}, m_{14}, m_{15}) &= (1,2,2,2,2),\\
(m_{21}, m_{22}, m_{23}, m_{24}, m_{25}) &= (3,3,1,2,0),\\
(m_{31}, m_{32}, m_{33}, m_{34}, m_{35}) &= (3,0,2,1,3),\\
(m_{41}, m_{42}, m_{43}, m_{44}, m_{45}) &= (3,0,2,1,3),\\
(m_{51}, m_{52}, m_{53}, m_{54}, m_{55}) &= (3,3,1,2,0).
\end{aligned}$$

Since H satisfies the conditions (a-2), (b-2), (c-2) of Theorem 1.4, it follows that A is a $(11,3)$-arc in PG$(2,5)$ with $(\tau_0, \tau_1, \tau_2, \tau_3) = (4,4,7,16)$. It is known that there are exactly two $(11,3)$-arcs in PG$(2,5)$ up to projective equivalence, see [17].

4. The basic algorithm for searching $(n,3)$-arcs. In this section, an outline of the basic algorithm used in the search is presented. The program accomplishes an exhaustive search for $(n,3)$-arcs in PG$(2,q)$ from some fixed points. It is based on a backtracking algorithm. Let K_n be a set of n points in PG$(2,q)$. The condition $|K_n \cap L| \leq 3$ for any line L in PG$(2,q)$ is called 3-ARC for K_n. The points of the plane are labeled as $R_0, R_1, \ldots, R_{q^2+q}$ (the particular order does not matter). The program retains the 3-ARC and tries to extend the starting set K_s until it reaches the length S. In doing the extension, the program exploits the information of the set T_j obtained by Hamada's method after each choice, where $T_j = \{R_i \in \mathrm{PG}(2,q) \mid K_j \cup \{R_i\}$ satisfies 3-ARC, $i > m\}$ for $m = \max\{i \mid R_i \in K_j\}$. At the choice of the jth point, the program selects a point in T_{j-1} which has a larger index than the previous choice. After each extension, it computes the set T_{j+1} for the current $(j+1,3)$-arc.

The program backtracks in three cases:

- After the choice of the Sth point;

- After the choice of the jth point $R_k \in T_{j-1}$, if $|\{R_i \mid k \le i \le q^2+q\} \cap T_{j-1}| < S-(j-1)$;
- After the extension of the jth point, if $|T_j| < S-j$ for the current T_j.

In these cases, exploiting Lemma 3.2, the program can restore the correct status after the backtracking step without previous information.

Algorithm for searching $(S,3)$-arcs

INPUT: K_s: the set of s fixed points
OUTPUT: $\{K_S\}$: set of arcs

```
const      max = q(q + 1);
var        J:integer;
            T:array[1..S] of set of points;
            // T[i][j] means j-th point of i-th set;
            Tree:array[1..S] of integer;
  begin
     J:=s+1; Find_solution(T[J]);Tree[J]:= |T[J]|;
     while (J>s) do
     begin
        if (Tree[J]> 0) and ( J <max) then
        begin
              Tree[J]:=Tree[J]−1;
            J:=J+1; Find_solution(T[J]);
            if J= S then print:
                 K_s∪ T[1][Tree[1]]∪ T[2][Tree[2]] ∪···∪ T[J][Tree[J]];
             if |T[J]| < (S−J) then
                 Tree[J]:= 0
             else Tree[J]:= |T[J]|;
          end
        else
            J:=J−1;
     end;
  end.
```

5. The algorithm for searching $(2q,3)$-arcs in $\mathbf{PG(2,q)}$. The basic algorithm just presented was not capable of showing Theorem 1.7 in a reasonable time, so we considered how to fix as many points as possible in the $(n,3)$-arcs. Let L be a line in PG$(2,q)$ with $L = \{P_0, P_1, \dots, P_q\}$. Let $L_{k,1}, L_{k,2}, \dots, L_{k,q}$ be the q lines through P_k other than L for $0 \le k \le q$. Let $Q_{i,j} = L_{0,i} \cap L_{1,j}$ for $1 \le i, j \le q$ as in Section 1.

Let c_i be the number of i-lines on a fixed point. The vector (c_0, c_1, c_2, c_3) for a point in the $(n,3)$-arc A is called the point-type of A. As a shorthand, we denote by i^{c_i} the point-type.

Lemma 5.1. *The possible point-types p_i of points on a $(2q,3)$-arc in PG$(2,q)$ are*

$$p_1 = 1^1 2^1 3^{q-1}, p_2 = 2^3 3^{q-2}.$$

P r o o f. The point-type $p = (c_0, c_1, c_2, c_3)$ on a $(2q,3)$-arc satisfies $c_0 = 0$ and

$$\sum_{i=2}^{3} (i-1)c_i = 2q-1, \quad \sum_{i=1}^{3} c_i = q+1. \qquad \square$$

Given sets $S_1, \dots, S_n$, if it is possible to choose a different element from each set S_i, then the chosen elements are called distinct representative of the sets. We use Hall's following theorem to prove a lemma.

Theorem 5.2 ([1])**.** *The sets $A_1, \dots, A_n$ have a system of distinct representatives if and only if, for all $k = 1, \dots, n$, any k A_is contain at least k elements in their union.*

Lemma 5.3. *Let A be a $(2q,3)$-arc in PG$(2,q)$ with a point of type p_2. Assume $P_0, P_1, Q_{1,1} \in A$ and that P_0 is a point of type p_2. If L and $L_{0,1}$ are 2-lines, then a $(q-1)$-set $\{Q_{i,w_i} \mid 2 \le i \le q, 1 \le w_i \le q\} \subset A$ with distinct $w_2, \dots, w_q$ exists.*

P r o o f. Assume there exists a $(2q,3)$-arc A in PG$(2,q)$ with P_0 a point of A of type p_2, $P_1, Q_{1,1} \in A$ and that L and $L_{0,1}$ are 2-lines. Since there exist three 2-lines through P_0 by Lemma 5.1, without loss of generality, we may assume $L_{0,2}$ is a 2-line through P_0 other than L and $L_{0,1}$. Then, for all $3 \le i \le q$, $L_{0,i}$ is a 3-line. Let $B_i = \{j \mid L_{0,i} \cap L_{1,j} \cap A \ne \emptyset,\ 1 \le j \le q\}$. Then $|B_2| = 1$ and $|B_i| = 2$ for $3 \le i \le q$. Since $L_{1,j} \setminus \{P_1\}$ has at most two points of A for $1 \le j \le q$, for any k sets $B_{i_1}, \dots, B_{i_k} \in \{B_3, \dots, B_q\}$ and B_2, it holds that $| \cup_{l=1}^{k} B_{i_l} \cup B_2| \ge (2k+1)/2 = k + 1/2$ for any k. By Theorem 5.2, $B_2, \dots, B_q$ have a system of $q-1$ distinct representatives $w_2, \dots, w_q$ so that $1 \le w_i \le q$ for any i. $\square$

Lemma 5.4. *A* $(34,3)$*-arc in* $PG(2,17)$ *has a point of type* $p_2 = 2^3 3^{q-2}$.

Proof. Let A be a $(34,3)$-arc in $\mathrm{PG}(2,17)$. Since $n = 34$, $r = 3$ and $p = 17$, the possible spectrum of A is $(\tau_0, \tau_1, \tau_2, \tau_3) = (69+a, 51-3a, 3a, 187-a)$ for some integer a with $0 \le a \le 17$ from Lemma 1.1. By Lemma 5.1, the points of A are of type $p_1 = 1^1 2^1 3^{q-1}$ or $p_2 = 2^3 3^{q-2}$. Let x_i be the number of points of type p_i in A. Then $x_1 + x_2 = n = 34$. Since $\tau_1 = x_1$, we have $\tau_1 = 51 - 3a \le 34$. Since a is an integer, $\tau_1 = x_1 \le 33$. Hence $x_2 > 0$. □

Exploiting these lemmas, we introduce the improved program doing an exhaustive search for $(34,3)$-arcs in $\mathrm{PG}(2,17)$ to show Theorem 1.7 in reasonable time. Let A be a $(34,3)$-arc in $\mathrm{PG}(2,17)$. Without loss of generality, we may assume that $P_0, P_1, Q_{1,1}, Q_{2,2} \in A$ and that L and $L_{0,1}$ are 2-lines. By Lemma 5.3, A has $q-1$ points $Q_{2,w_2}, \dots, Q_{q,w_q}$ with distinct $w_2, \dots, w_q \in \{1, \dots, q\}$ such that $w_2 = 2$. First, the program sets $K_4 = \{P_0, P_1, Q_{1,1}, Q_{2,2}\}$ as the starting set and extend it to K_{19} containing the $q-1$ points using the algorithm in Section 4. Next, the program regards K_{19} as the starting set and tries to extend it to K_{34}. Thus we divide the search into two stages. When the program finished searching $(34,3)$-arcs which contains K_{19}, it backtracks from K_{19} to find a new K_{19}. Repeating this procedure, the program tries to extend every K_{19} which has 4 points $P_0, P_1, Q_{1,1}, Q_{2,2}$ to K_{34}.

Our program verified that $(34,3)$-arcs in $\mathrm{PG}(2,17)$ do not exist. Hence $m_3(2,17) \le 33$. At the end of the exhaustive search the program found 2372866546 cases for K_{19}. And the execution of the program took about 3 days.

Acknowledgement. The authors would like to thank the anonymous referees for their helpful suggestions.

REFERENCES

[1] Anderson I. A first course in Combinatorial Mathematics. Oxford University Press, 2nd ed., Oxford, 1989.

[2] Ball S. Table of bounds on three dimensional linear codes or (n,r)-arcs in $\mathrm{PG}(2,q)$. `http://www-ma4.upc.es/~simeon/codebounds.html`, January 2012

[3] Ball S., J. W. P. Hirschfeld. Bounds on (n, r) arcs and their applications to linear codes. *Finite Fields Appl.*, **3** (2005), 326–336.

[4] Bierbrauer J. Introduction to Coding Theory. Chapman & Hall/CRC, 2005.

[5] Boukliev I., S. Kapralov, T. Maruta, M. Fukui. Optimal linear codes of dimension 4 over F_5. *IEEE Trans. Inform. Theory*, **43** (1997), 308–313.

[6] Cook G. R. Arcs in a finite projective plane. PhD Thesis, University of Sussex, 2011. `http://sro.sussex.ac.uk/`

[7] Daskalov R. N. On the maximum size of some (k, r)-arcs in $\mathrm{PG}(2, q)$. *Discrete Math.*, **308** (2008), 565–570.

[8] Daskalov R. N., E. Metodieva. New arcs in $\mathrm{PG}(2, 17)$ and $\mathrm{PG}(2, 19)$. In: Proc. of the 12th Intern. Workshop ACCT, Novosibirsk, Russia, 2010, 93–97.

[9] Dodunekov S., I. Landjev. On near-MDS codes. *J. Geometry*, **54** (1995), 30–43.

[10] Hill R. Optimal linear codes. In: Cryptography and Coding II (Ed. C. Mitchell), Oxford Univ. Press, Oxford, 1992, 75–104.

[11] Hirschfeld J. W. P. Projective Geometries over Finite Fields. Clarendon Press,2nd ed., Oxford, 1998.

[12] Hirschfeld J. W. P., L. Storme. The packing problem in statistics, coding theory and finite projective spaces: update 2001. In: Finite Geometries (Eds A. Blokhuis et al.), *Developments in Mathematics*, **3** (2001), Kluwer, 201–246.

[13] Marcugini S., A. Milani, F. Pambianco. Maximal $(n, 3)$-arcs in $\mathrm{PG}(2, 11)$. *Discrete Math.*, **208/209** (1999), 421–426.

[14] Marcugini S., A. Milani, F. Pambianco. Classification of the $[n, 3, n-3]_q$ NMDS codes over $GF(7)$, $GF(8)$ and $GF(9)$. *Ars Combinatoria*, **61** (2001), 263–269.

[15] Marcugini S., A. Milani, F. Pambianco. Maximal $(n, 3)$-arcs in $\mathrm{PG}(2, 13)$. *Discrete Math.*, **294** (2005), 139–145.

[16] Maruta T. Correspondence between $Q_{i,j}$ in PG$(2,q)$ and $[s(0,i,j),\ldots,s(q,i,j)]$ in S_q.
http://www.mi.s.osakafu-u.ac.jp/~maruta/hamada-set.html

[17] Yazdi M. O. The classification of $(k;3)$-arcs over the Galois field of order five. PhD Thesis, University of Sussex, 1983.

Noboru Hamada
Osaka Women's University
Osaka 599-8531, Japan
e-mail: n-hamada@koala.odn.ne.jp

Tatsuya Maruta and Yusuke Oya
Department of Mathematics and Information Sciences
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
e-mail: maruta@mi.s.osakafu-u.ac.jp
e-mail: yuu.vim-0319@hotmail.co.jp

Received March 19, 2012
Final Accepted April 26, 2012