Serdica J. Computing **7** (2013), No 1, 73–80

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

CONSTRUCTION OF OPTIMAL LINEAR CODES BY GEOMETRIC PUNCTURING*

Tatsuya Maruta

Dedicated to the memory of S.M. Dodunekov (1945–2012)

Abstract. Geometric puncturing is a method to construct new codes from a given $[n,k,d]_q$ code by deleting the coordinates corresponding to some geometric object in $\mathrm{PG}(k-1,q)$. We construct $[g_q(4,d),4,d]_q$ and $[g_q(4,d)+1,4,d]_q$ codes for some d by geometric puncturing, where $g_q(k,d) = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$. These determine the exact value of $n_q(4,d)$ for $q^3-2q^2-q+1 \le d \le q^3-2q^2-(q+1)/2$ for odd prime power $q \ge 7$; $q^3-2q^2-q+1 \le d \le q^3-2q^2-q/2$ for $q = 2^h$, $h \ge 3$ and for $2q^3-5q^2+1 \le d \le 2q^3-5q^2+3q$ for prime power $q \ge 7$, where $n_q(k,d)$ is the minimum length n for which an $[n,k,d]_q$ code exists.

1. Introduction. We denote by $\mathbb{F}_q^n$ the vector space of n-tuples over $\mathbb{F}_q$, the field of q elements. A *q-ary linear code* $\mathcal{C}$ of *length* n and *dimension* k (an $[n,k]_q$ code) is a k-dimensional subspace of $\mathbb{F}_q^n$. An $[n,k,d]_q$ code $\mathcal{C}$ is an $[n,k]_q$

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

Key words: optimal linear codes, finite fields, projective geometry.

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

code with minimum weight d. The *weight* of a vector $\boldsymbol{x} \in \mathbb{F}_q^n$, denoted by $wt(\boldsymbol{x})$, is the number of nonzero coordinate positions in $\boldsymbol{x}$. So, $d = \min\{wt(\boldsymbol{c}) > 0 \mid \boldsymbol{c} \in \mathcal{C}\}$.

A fundamental problem in coding theory is to find $n_q(k,d)$, the minimum length n for which an $[n,k,d]_q$ code exists. The exact values of $n_q(4,d)$ have been determined for all d for $q \le 5$ except the cases $(q,d) = (5,81)$, $(5,82)$, $(5,161)$, $(5,162)$. See [11] for the updated tables of $n_q(k,d)$ for some small q and k. We tackle the problem to find $n_q(4,d)$ for $q \ge 7$, see [9] for the known results on $n_q(4,d)$. The Griesmer bound (see [7]) gives a lower bound on $n_q(k,d)$:

$$n_q(k,d) \ge g_q(k,d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. An $[n,k,d]_q$ code $\mathcal{C}$ is called *Griesmer* if it attains the Griesmer bound, i.e. $n = g_q(k,d)$.

Geometric puncturing is a method to construct new codes from a given $[n,k,d]_q$ code by deleting the coordinates corresponding to some geometric object in $\mathrm{PG}(k-1,q)$, which is a generalization of the well-known idea to construct Griesmer codes from a given simplex code $S_{k,q}$ (or some copies of $S_{k,q}$) by deleting the coordinates corresponding to some subspaces of $\mathrm{PG}(k-1,q)$, see Section 2. We prove the following results by geometric puncturing.

Theorem 1.1. *There exist $[g_q(4,d)+1,4,d]_q$ codes for $d = q^3 - 2q^2 - (q+1)/2$ for odd $q \ge 7$ and for $d = q^3 - 2q^2 - q/2$ for even $q \ge 8$.*

Theorem 1.2. *There exist $[g_q(4,d),4,d]_q$ codes for $d = 2q^3 - 5q^2 + q, 2q^3 - 5q^2 + 2q$ and $2q^3 - 5q^2 + 3q$ for $q \ge 7$.*

Theorem 1.3. *There exist $[g_q(4,d)+1,4,d]_q$ codes for $d = 2q^3 - 5q^2 - (s-3)q$ for $3 \le s \le q-1$, $q \ge 7$.*

As for Theorem 1.1, we pose the following conjecture, which is known to be true for $q = 3,4,5$.

Conjecture. *$n_q(4,d) = g_q(4,d)+1$ for $q^3 - 2q^2 - q + 1 \le d \le q^3 - 2q^2$ for $q \ge 7$.*

Recall that the existence of an $[n,k,d]_q$ code implies the existence of an $[n-1,k,d-1]_q$ code. The residual codes of $[g_q(4,d),4,d]_q$ codes for the values of d,q in Theorem 1.1 have parameters $[q^2-q-1,3,q^2-2q]_q$, which do not exist. Thus $n_q(4,d) \ge g_q(4,d)+1$ for $q^3-2q^2-q+1 \le d \le q^3-2q^2$ for $q \ge 3$. Hence, Theorems 1.1, 1.2 and 1.3 yield the following.

Corollary 1.4. (1) *$n_q(4,d) = g_q(4,d)+1$ for*

- $q^3 - 2q^2 - q + 1 \le d \le q^3 - 2q^2 - (q+1)/2$ *for odd* $q \ge 7$;
- $q^3 - 2q^2 - q + 1 \le d \le q^3 - 2q^2 - q/2$ *for even* $q \ge 8$.

(2) $n_q(4,d) = g_q(4,d)$ *for* $2q^3 - 5q^2 + 1 \le d \le 2q^3 - 5q^2 + 3q$ *for* $q \ge 7$.
(3) $n_q(4,d) \le g_q(4,d) + 1$ *for* $2q^3 - 6q^2 + 3q + 1 \le d \le 2q^3 - 5q^2$ *for* $q \ge 7$.

Remark. As for the part (3) of Corollary 1.4, we conjecture that $n_q(4,d) = g_q(4,d) + 1$ holds for $2q^3 - 6q^2 + 3q + 1 \le d \le 2q^3 - 5q^2$ for $q \ge 7$. Actually, this is true for $d = 2q^3 - 5q^2, 2q^3 - 5q^2 - 1, 2q^3 - 5q^2 - 2$ for $q = 8$ [8].

2. Geometric puncturing for linear codes. We denote by $\mathrm{PG}(r,q)$ the projective geometry of dimension r over $\mathbb{F}_q$. A j-dimensional projective subspace of $\mathrm{PG}(r,q)$ is called a j-flat. The 0-flats, 1-flats, 2-flats and $(r-1)$-flats are called *points, lines, planes* and *hyperplanes* respectively. We denote by $\mathcal{F}_j$ the set of j-flats of $\mathrm{PG}(r,q)$ and by θ_j the number of points in a j-flat, i.e. $\theta_j = (q^{j+1} - 1)/(q-1)$.

Let $\mathcal{C}$ be an $[n,k,d]_q$ code with generator matrix G having no coordinate which is identically zero. The columns of G can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1,q)$ denoted by $\overline{G}$. We see linear codes from this geometrical point of view. An *i-point* is a point of Σ which has multiplicity i in $\overline{G}$. Denote by γ_0 the maximum multiplicity of a point from Σ in $\overline{G}$ and let C_i be the set of i-points in Σ, $0 \le i \le \gamma_0$. For any subset S of Σ we define *the multiplicity of S with respect to $\overline{G}$*, denoted by $m(S)$ or $m_{\overline{G}}(S)$, as

$$m(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|,$$

where $|T|$ denotes the number of elements in a set T. When the code is *projective*, i.e. when $\gamma_0 = 1$, the multiset $\overline{G}$ forms an n-set in Σ and the above $m(S)$ is equal to $|\overline{G} \cap S|$. A line l with $t = m(l)$ is called a *t-line*. A *t-plane* and so on are defined similarly. Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ such that

$$n = m(\Sigma),\ n - d = \max\{m(\pi) \mid \pi \in \mathcal{F}_{k-2}\}.$$

Such a partition of Σ is called an $(n, n-d)$-*arc* of Σ. Conversely an $(n, n-d)$-arc of Σ gives an $[n,k,d]_q$ code in the natural manner. Especially when $\Sigma = C_s$ with $s \in \mathbb{N}$, $\mathcal{C}$ is an $[s\theta_{k-1}, k, sq^{k-1}]_q$ code, which is called an *s-fold simplex code over $\mathbb{F}_q$*.
For an m-flat Π in Σ we define

$$\gamma_j(\Pi) = \max\{m(\Delta) \mid \Delta \subset \Pi,\ \Delta \in \mathcal{F}_j\},\ 0 \le j \le m.$$

We denote simply by γ_j instead of $\gamma_j(\Sigma)$. It holds that $\gamma_{k-2} = n - d$, $\gamma_{k-1} = n$. When $\mathcal{C}$ is Griesmer, the values γ_j's are uniquely determined [10] as follows.

$$\gamma_j = \sum_{u=0}^{j} \left\lceil \frac{d}{q^{k-1-u}} \right\rceil \text{ for } 0 \le j \le k-1. \tag{2.1}$$

Lemma 2.1. *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with generator matrix G and let $\cup_{i=0}^{\gamma_0} C_i$ be the partition of $\Sigma = \mathrm{PG}(k-1,q)$ obtained from $\overline{G}$. Assume $d > q^t$ and that $\cup_{i\ge1} C_i$ contains a t-flat Π. Then deleting Π from $\overline{G}$ gives an $[n-\theta_t, k, d-q^t]_q$ code $\mathcal{C}'$. When $\mathcal{C}$ is Griesmer, $\mathcal{C}'$ is also Griesmer if and only if either $d \equiv 0 \pmod{q^{t+1}}$ or*

$$\frac{d}{q^{t+1}} - \left\lfloor \frac{d}{q^{t+1}} \right\rfloor > \frac{1}{q}. \tag{2.2}$$

Proof. Assume $\cup_{i\ge1} C_i$ contains a t-flat Π. Let $C_i' = (C_i \setminus \Pi) \cup (C_{i+1} \cap \Pi)$ for all i and let $\mathcal{G}$ be the corresponding new multiset. Then $\mathcal{G}$ gives an $[n' = n - \theta_t, k', d']_q$ code. For any hyperplane π of Σ, π meets Π in θ_{t-1} or θ_t points. So, $m_{\mathcal{G}}(\pi) \le n' - d' \le n - d - \theta_{t-1}$, giving $d' \ge d - q^t$. Suppose $k' \le k-1$. Then, there exists a hyperplane π of Σ containing $(\cup_{i\ge1} C_i) \setminus \Pi$. Since π meets Π in a $(t-1)$-flat, we have $m_{\overline{G}}(\pi) = n' + \theta_{t-1} = n - q^t \le n - d$, so $d \le q^t$, a contradiction. Hence $k' = k$.
Assume $\mathcal{C}$ is Griesmer and let $s = \lceil d/q^{k-1} \rceil$. Then d can be uniquely expressed as $d = sq^{k-1} - (\sum_{i=0}^{k-2} d_i q^i)$ with integers d_i, $0 \le d_i \le q-1$, and we have $n = s\theta_{k-1} - (\sum_{i=0}^{k-2} d_i \theta_i)$. Hence $\mathcal{C}'$ is Griesmer if $d \equiv 0 \pmod{q^{t+1}}$. Assume $d \not\equiv 0 \pmod{q^{t+1}}$. Note that (2.2) holds if and only if $d_t < q-1$, for

$$\frac{d}{q^{t+1}} - \left\lfloor \frac{d}{q^{t+1}} \right\rfloor = 1 - \frac{\sum_{i=0}^{t} d_i q^i}{q^{t+1}} \le 1 - \frac{d_t}{q}.$$

Since $g_q(k, d-q^t) = n - \theta_t$ if and only if $d_t < q-1$, our assertion follows. $\square$

For a given $[n,k,d]_q$ code $\mathcal{C}$ and the multiset $\overline{G}$ obtained from a generator matrix G, we say that puncturing of $\mathcal{C}$ by deleting some geometric object from $\overline{G}$ is *geometric*. The geometric puncturing from a given simplex code by deleting some flats is a well-known method to construct Griesmer codes. For given q, k and d, write $d = sq^{k-1} - \sum_{i=1}^{t} q^{u_i - 1}$, where $s = \lceil d/q^{k-1} \rceil$, $k > u_1 \ge u_2 \ge \cdots \ge u_t \ge 1$, and at most $q-1$ u_i's take any given value. Let $\mathcal{S}$ be an s-fold simplex code with generator matrix G. If there exist t flats $\Pi_i \in \mathcal{F}_{u_i-1}$ no $s+1$ of which contain a common point, then one can construct a $[g_q(k,d), k, d]_q$ code from $\mathcal{S}$ by deleting $\Pi_1, \ldots, \Pi_t$ from $\overline{G}$. Such codes are called Griesmer codes *of Belov type* [5]. The necessary and sufficient condition for the existence of Griesmer codes of Belov type was found by Belov, Logachev and Sandimilov [1] for binary codes and was generalized to q-ary linear codes by Hill [4] and Dodunekov [2] as follows.

Theorem 2.2 ([4]). *There exists a $[g_q(k,d),k,d]_q$ code of Belov type if and only if*

$$\sum_{i=1}^{\min\{s+1,t\}} u_i \le sk.$$

As a consequence of Theorem 2.2, it can be shown that for given k and q, there exist Griesmer $[n,k,d]_q$ codes if d is large enough, see [3], [4]. Lemma 2.1 is useful to find optimal linear codes even when $\mathcal{C}$ is not of Belov type as we see below.

Proof of Theorem 1.2. Let $\mathcal{H}$ be a hyperbolic quadric in $\mathrm{PG}(3,q)$, $q \ge 7$, and let l_1 and l_2 be two skew lines contained in $\mathcal{H}$. We further take two skew lines l_3 and l_4 contained in $\mathcal{H}$ meeting l_1 and l_2 and four points $P_1,\dots,P_4$ of $\mathcal{H}$ so that $l_1 \cap l_3 = P_1$, $l_1 \cap l_4 = P_2$, $l_2 \cap l_3 = P_3$, $l_2 \cap l_3 = P_4$. Let l_5 be the line $\langle P_1,P_4\rangle$ and let l_6 be the line $\langle P_2,P_3\rangle$, where $\langle \chi_1,\chi_2,\dots\rangle$ denotes the smallest flat containing subsets $\chi_1,\chi_2,\dots$. We set $C_0 = l_1 \cup l_2 \cup \cdots \cup l_6$, $C_1 = (\langle l_1,l_3\rangle \cup \langle l_1,l_4\rangle \cup \langle l_2,l_3\rangle \cup \langle l_2,l_4\rangle \cup \mathcal{H}) \setminus C_0$ and $C_2 = \mathrm{PG}(3,q) \setminus (C_0 \cup C_1)$. Then $\lambda_0 = 6q-2$, $\lambda_1 = 5q^2-10q+5$, $\lambda_2 = q^3-4q^2+5q-2$, where $\lambda_i = |C_i|$. Taking the points of C_i as the columns of a generator matrix i times, we get a Griesmer $[2q^3-3q^2+1,4,2q^3-5q^2+3q]_q$ code, say $\mathcal{C}$. This construction is due to [8].

Now, take a line l contained in $\mathcal{H}$ such that l is skew to l_3 and l_4. Let $l \cap l_1 = Q_1$, $l \cap l_2 = Q_2$ and let $\delta_1,\dots,\delta_{q-1}$ be the planes through l other than $\langle l,l_1\rangle$, $\langle l,l_2\rangle$. Then each δ_i meets l_1 and l_2 in the points Q_1 and Q_2, respectively, and meets $l_3,\dots,l_6$ in some points out of l. Hence, we can take a line m_i in δ_i with $m_i \cap C_0 = \emptyset$ for $1 \le i \le q-1$ such that $m_1 \cap l,\dots,m_{q-1} \cap l$ are distinct points. Applying Lemma 2.1 by deleting t of the lines $m_1,\dots,m_{q-1}$, we get a $[n = 2q^3-3q^2+1-t\theta_1,4,d = 2q^3-5q^2+3q-tq]_q$ code. This code is Griesmer for $t = 1,2$ giving Theorem 1.2 and satisfies $n = g_q(4,d)+1$ for $3 \le t \le q-1$ giving Theorem 1.3. $\square$

An f-set F in $\mathrm{PG}(k-1,q)$ is called an (f,m)-*minihyper* if

$$m = \min\{|F \cap \pi| \mid \pi \in \mathcal{F}_{k-2}\}.$$

For example, a t-flat is a (θ_t,θ_{t-1})-minihyper and a blocking b-set in some plane is a $(b,1)$-minihyper, see [6] for blocking sets in $\mathrm{PG}(2,q)$. To prove Theorem 1.1, we generalize Lemma 2.1 to the following.

Lemma 2.3. *Let $\mathcal{C}$ be an $[n,k,d]_q$ code with generator matrix G and let $\cup_{i=0}^{\gamma_0} C_i$ be the partition of $\Sigma = \mathrm{PG}(k-1,q)$ obtained from $\overline{G}$. Assume $\cup_{i>0} C_i$ contains an (f,m)-minihyper F such that $\langle \cup_{i>0} C_i \setminus F \rangle = \Sigma$. Then deleting F from $\overline{G}$ gives an $[n-f, k, d+m-f]_q$ code.*

In the proof of Theorem 1.1, we take a blocking set on some plane as F in Lemma 2.3. This shows that the object to be deleted from the multiset $\overline{G}$ to get an optimal code is not necessarily a flat in $\mathrm{PG}(k-1,q)$.

3. Proof of Theorem 1.1. We first assume that $q = p^h$, $h \in \mathbb{N}$, with an odd prime p. A *projective triangle of side* m in $\mathrm{PG}(2,q)$ is a set $\mathcal{B}$ of $3(m-1)$ points on some three non-concurrent lines l_1, l_2, l_3 such that $l_1 \cap l_2, l_2 \cap l_3, l_1 \cap l_3 \in \mathcal{B}$; $|l_i \cap \mathcal{B}| = m$ for $i = 1,2,3$ and that $Q_1 \in l_1 \cap \mathcal{B}$ and $Q_2 \in l_2 \cap \mathcal{B}$ implies $l_3 \cap \langle Q_1, Q_2 \rangle \in \mathcal{B}$. Let $\mathcal{Q}_q$ and $\mathcal{N}_q$ be the set of non-zero squares and non-squares in $\mathbb{F}_q$, respectively. Then, $|\mathcal{Q}_q| = |\mathcal{N}_q| = (q-1)/2$, and $-1 \in \mathcal{Q}_q$ if $q \equiv 1 \pmod q$ but $-1 \in \mathcal{N}_q$ if $q \equiv 3 \pmod q$. In $\mathrm{PG}(2,q)$, q odd, there exists a projective triangle of side $(q+3)/2$ which forms a minimal blocking set, see Chap. 13 of [6]. Such a $3(q+1)/2$-set can be constructed as follows.

Lemma 3.1 ([6])**.** *Let $R_0 = \mathbf{P}(1,0,0), R_1 = \mathbf{P}(0,1,0), R_2 = \mathbf{P}(0,0,1) \in \mathrm{PG}(2,q)$, and $K_0 = \{(0,1,a) \mid a \in \mathcal{Q}_q\} \subset \langle R_1, R_2 \rangle$, $K_1 = \{(1,0,b) \mid b \in \mathcal{Q}_q\} \subset \langle R_0, R_2 \rangle$, $K_2 = \{(c,1,0) \mid c = -ab^{-1},\ a,b \in \mathcal{Q}_q\} \subset \langle R_0, R_1 \rangle$. Then the $3(q+1)/2$-set $K = K_0 \cup K_1 \cup K_2 \cup \{R_0, R_1, R_2\}$ forms a projective triangle.*

Lemma 3.2. *There exists an element $\alpha \in \mathcal{N}_q$ such that $\alpha - 1 \in \mathcal{Q}_q$.*

P r o o f. Let $q = p^h$, $h \in \mathbb{N}$, p odd prime. Suppose $a - 1 \in \mathcal{N}_q$ for all $a \in \mathcal{N}_q$. Then we have $\sum_{a \in \mathcal{N}_q} a = \sum_{a \in \mathcal{N}_q} (a-1)$, giving $(q-1)/2 \equiv 0 \pmod p$, a contradiction. □

Lemma 3.3. *Let C be the conic $\{P_t = \mathbf{P}(1,u,u^2) \mid u \in \mathbb{F}_q\} \cup \{P = \mathbf{P}(0,0,1)\}$ in $PG(2,q)$, q odd. Take $\alpha \in \mathcal{N}_q$ with $\alpha - 1 \in \mathcal{Q}_q$ and let $Q_0 = \mathbf{P}(1,0,\alpha)$, $Q_1 = \mathbf{P}(1,1,\alpha)$, $l_0 = \langle P, P_0 \rangle$, $l_1 = \langle P, P_1 \rangle$, $l = \langle Q_0, Q_1 \rangle$, $Q = \mathbf{P}(0,1,0) = l \cap \ell_P$, where ℓ_P is the tangent to C at P. Then, there exists a projective triangle T contained in $l_0 \cup l_1 \cup l$ with $P_0, P_1, Q \notin T$.*

P r o o f. Take non-zero elements $s, t \in \mathbb{F}_q$ so that $s \in \mathcal{Q}_q$, $t \in \mathcal{N}_q$ for $q \equiv 1 \pmod q$ and that $s \in \mathcal{N}_q$, $t \in \mathcal{Q}_q$ for $q \equiv 3 \pmod q$, and let σ be the projectivity of $\mathrm{PG}(2,q)$ given by

$$\sigma(\mathbf{P}(x,y,z)) = \mathbf{P}(sx+ty, ty, \alpha sx + \alpha ty + z)$$

for $X = \mathbf{P}(x,y,z) \in \mathrm{PG}(2,q)$. Then the three points R_0, R_1, R_2 in Lemma 3.1 are transformed by σ to Q_0, Q_1, P, respectively. For $a \in \mathcal{Q}_q$, $\sigma(\mathbf{P}(0,1,a)) =$

$\mathbf{P}(1,1,\alpha + at^{-1}) \neq P_1$ since $\alpha - 1 \in \mathcal{Q}_q$ and $-at^{-1} \in \mathcal{N}_q$. For $b \in \mathcal{Q}_q$, $\sigma(\mathbf{P}(1,0,b)) = \mathbf{P}(1,0,\alpha + bs^{-1}) \neq P_0$, for $-bs^{-1} \in \mathcal{Q}_q$. For $c = -ab^{-1}$ with $a, b \in \mathcal{Q}_q$, $\sigma(\mathbf{P}(c,1,0)) = \mathbf{P}(cs + t, t, (cs + t)\alpha) \neq Q$ since $ab^{-1} \in \mathcal{Q}_q$ and $ts^{-1} \in \mathcal{N}_q$. Hence, for the projective triangle K in Lemma 3.1, we have $\sigma(K) = T$ as desired. $\square$

A *projective triad of side* m in $\mathrm{PG}(2,q)$ is a set $\mathcal{B}$ of $3m - 2$ points on some three concurrent lines l_1, l_2, l_3 through a given point P such that $P \in \mathcal{B}$; $|l_i \cap \mathcal{B}| = m$ for $i = 1, 2, 3$ and that $Q_1 \in l_1 \cap \mathcal{B}$ and $Q_2 \in l_2 \cap \mathcal{B}$ implies $l_3 \cap \langle Q_1, Q_2 \rangle \in \mathcal{B}$.

For $q = 2^h$ with $h \geq 3$, let $tr(x) = x + x^2 + \cdots + x^{2^{h-1}}$ be the trace function over $\mathbb{F}_2$. Let $\mathcal{T}_i = \{a \in \mathbb{F}_q, tr(a) = i\}$ for $i = 0, 1$. In $\mathrm{PG}(2,q)$, q even, there exists a projective triad of side $(q + 2)/2$ which forms a minimal blocking set [6]. Such a $(3q + 2)/2$-set can be constructed as follows.

Lemma 3.4 ([6]). *For $q = 2^h$, $h \geq 3$, let $P_0 = \mathbf{P}(0,0,1), P_1 = \mathbf{P}(0,1,0), P_2 = \mathbf{P}(1,0,0), P_3 = \mathbf{P}(1,1,0) \in \mathrm{PG}(2,q)$, and $K_1 = \{(0,1,a) \mid a \in \mathcal{T}_0\} \subset \langle P_0, P_1 \rangle$, $K_2 = \{(1,0,a) \mid a \in \mathcal{T}_0\} \subset \langle P_0, P_2 \rangle$, $K_3 = \{(1,1,a) \mid a \in \mathcal{T}_0\} \subset \langle P_0, P_3 \rangle$. Then the $(3q + 2)/2$-set $K = K_1 \cup K_2 \cup K_3 \cup \{P_0\}$ forms a projective triad.*

Lemma 3.5. *Let $\{Q, Q_1, Q_2, Q_3\}$ be a $(4,2)$-arc in $PG(2,q)$ and let $l_i = \langle Q, Q_i \rangle$, $i = 1, 2, 3$. Then, there exists a projective triad T on $l_1 \cup l_2 \cup l_3$ with $Q_1, Q_2, Q_3 \notin T$.*

Proof. Let P_0, P_1, P_2, P_3, K be as in Lemma 3.4 and take three points $R_1 = \mathbf{P}(0,1,s)$, $R_2 = \mathbf{P}(1,0,t)$, $R_3 = \mathbf{P}(1,1,u)$ with $s, t, u \in \mathcal{T}_1$. Then P_0, R_1, R_2, R_3 form a $(4,2)$-arc, for $s + t \in \mathcal{T}_0$ for $s, t \in \mathcal{T}_1$. Take a projectivity σ so that $\sigma(P_0) = Q$ and $\sigma(\{R_1, R_2, R_3\}) = \{Q_1, Q_2, Q_3\}$. Then, $\sigma(K) = T$ is a projective triad on $l_1 \cup l_2 \cup l_3$ with $Q_1, Q_2, Q_3 \notin T$. $\square$

Let $\mathcal{H} = \mathbf{V}(x_0x_1 + x_2x_3)$ be a hyperbolic quadric in $\Sigma = \mathrm{PG}(3,q)$. Take $P(0,0,1,0) \in \mathcal{H}$ and $\pi = \mathbf{V}(x_3)$ (tangent plane at P). Putting $C_0 = (\mathcal{H} \cup \pi) \setminus \{P\}$ and $C_1 = \Sigma \setminus C_0$, we get a Griesmer $[q^3 - q^2 + 1, 4, q^3 - 2q^2 + q]_q$ code, say $\mathcal{C}$. Note that K contains no line, for $\gamma_1 = q$ by (2.1). Instead, we take a blocking set $\mathcal{B}$ in the plane $\delta = \mathbf{V}(x_0 + x_1)$ through P as $\mathcal{F}$ in Lemma 2.3 so that $\mathcal{B}$ is a projective triangle of side $(q + 3)/2$ for odd q and that $\mathcal{B}$ is a projective triad of side $(q + 2)/2$ for even q. Since $\delta \cap C_0$ consists of a conic, say $\mathcal{O}$, and the tangent $\ell = \delta \cap \pi$ of $\mathcal{O}$ at P, we need to take $\mathcal{B}$ in δ so that $\mathcal{B} \cap (\mathcal{O} \cup \ell) = \emptyset$, which is possible from Lemmas 3.3 and 3.5. Applying Lemma 2.3, one get the desired codes with length $g_q(4,d) + 1$. This completes the proof of Theorem 1.1. $\square$

REFERENCES

[1] Belov B. I., V. N. Logachev, V. P. Sandimirov. Construction of a class of linear binary codes achieving the Varshamov-Griesmer bound. *Problems of Info. Transmission*, **10** (1974), No 3, 211–217.

[2] Dodunekov S. M. Optimal linear codes. Doctor of Mathematical Sciences Dissertation, Institute of Mathematics, Sofia, 1985.

[3] Hamada N., T. Maruta. An improvement to the achievement of the Griesmer bound. *Serdica J. Computing,* **4** (2010), 301–320.

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

[5] Hill R., E. Kolev. A survey of recent results on optimal linear codes. In: Combinatorial Designs and their Applications (Eds F. C. Holroyd et al.), Chapman & Hall/CRC, *Res. Notes Math.*, **403** (1999), 127–152.

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

[7] Huffman W. C., V. Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge, 2003.

[8] Kanazawa R., T. Maruta. On optimal linear codes over $\mathbb{F}_8$. *Electronic J. Combin*, **18** (2011), #P34.

[9] Maruta T. On the minimum length of q-ary linear codes of dimension four. *Discrete Math.,* **208/209** (1999), 427–435.

[10] Maruta T. On the nonexistence of q-ary linear codes of dimension five. *Des. Codes Cryptogr.,* **22** (2001), 165–177.

[11] Maruta T. Griesmer bound for linear codes over finite fields. `http://www.geocities.jp/mars39geo/griesmer.htm`.

Department of Mathematics
and Information Sciences
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan
e-mail: `maruta@mi.s.osakafu-u.ac.jp`

Received February 15, 2013
Final Accepted April 29, 2013