CONSTRUCTION OF OPTIMAL LINEAR CODES
BY GEOMETRIC PUNCTURING∗

Tatsuya Maruta

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 \(PG(k - 1, q)\). 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 \(q^3 - 2q^2 - q + 1 \leq d \leq q^4 - 2q^2 - (q + 1)/2\) for odd prime power \(q \geq 7\); \(q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - q/2\) for \(q = 2^h, h \geq 3\) and for \(2q^3 - 5q^2 + 1 \leq d \leq 2q^3 - 5q^2 + 3q\) for prime power \(q \geq 7\), 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 \(C\) 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 \(C\) is an \([n, k]_q\)

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

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 $q \leq 5$ 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 $q \geq 7$, see [9] for the known results on $n_q(4, d)$. The Griesmer bound (see [7]) gives a lower bound on $n_q(k, d)$:

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

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 $\text{PG}(k - 1, q)$, 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 $\text{PG}(k - 1, q)$, 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 $q \geq 7$ and for $d = q^3 - 2q^2 - q/2$ for even $q \geq 8$.

**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 $q \geq 7$.

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

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 $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2$ for $q \geq 7$.

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 $n_q(4, d) \geq g_q(4, d) + 1$ for $q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2$ for $q \geq 3$. 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
\[ q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - (q + 1)/2 \text{ for odd } q \geq 7; \]

\[ q^3 - 2q^2 - q + 1 \leq d \leq q^3 - 2q^2 - q/2 \text{ for even } q \geq 8. \]

(2) \( n_q(4, d) = g_q(4, d) \) for \( 2q^3 - 5q^2 + 1 \leq d \leq 2q^3 - 5q^2 + 3q \) for \( q \geq 7. \)

(3) \( n_q(4, d) \leq g_q(4, d) + 1 \) for \( 2q^3 - 6q^2 + 3q + 1 \leq d \leq 2q^3 - 5q^2 \) for \( q \geq 7. \)

**Remark.** As for the part (3) of Corollary 1.4, we conjecture that

\[ n_q(4, d) = g_q(4, d) + 1 \text{ holds for } 2q^3 - 6q^2 + 3q + 1 \leq d \leq 2q^3 - 5q^2 \text{ for } q \geq 7. \]

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 \( \text{PG}(r, q) \) the projective geometry of dimension \( r \) over \( \mathbb{F}_q \). A \( j \)-dimensional projective subspace of \( \text{PG}(r, q) \) 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 \( \text{PG}(r, q) \) and by \( \theta_j \) 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 \( \Sigma = \text{PG}(k - 1, q) \) denoted by \( \overline{\Sigma} \). We see linear codes from this geometrical point of view. An \( i \)-point is a point of \( \Sigma \) which has multiplicity \( i \) in \( \overline{\Sigma} \). Denote by \( \gamma_0 \) the maximum multiplicity of a point from \( \Sigma \) in \( \overline{\Sigma} \) and let \( C_i \) be the set of \( i \)-points in \( \Sigma \), \( 0 \leq i \leq \gamma_0 \). For any subset \( S \) of \( \Sigma \) we define the multiplicity of \( S \) with respect to \( \overline{\Sigma} \), denoted by \( m(S) \) or \( m_{\overline{\Sigma}}(S) \), 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 \( \overline{\Sigma} \) forms an \( n \)-set in \( \Sigma \) and the above \( m(S) \) is equal to \( |\overline{\Sigma} \cap S| \). 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

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

Such a partition of \( \Sigma \) is called an \((n, n - d)\)-arc of \( \Sigma \). Conversely an \((n, n - d)\)-arc of \( \Sigma \) 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 \([s\theta_{k-1}, k, s[q^{k-1}]]_q \) code, which is called an \( s \)-fold simplex code over \( \mathbb{F}_q \).

For an \( m \)-flat \( \Pi \) in \( \Sigma \) we define

\[ \gamma_j(\Pi) = \max \{m(\Delta) \mid \Delta \subset \Pi, \ \Delta \in \mathcal{F}_j \}, \quad 0 \leq j \leq m. \]
We denote simply by $\gamma_j$ instead of $\gamma_j(\Sigma)$. It holds that $\gamma_{k-2} = n - d$, $\gamma_{k-1} = n$.

When $C$ is Griesmer, the values $\gamma_j$’s are uniquely determined [10] as follows.

$$(2.1) \quad \gamma_j = \sum_{u=0}^{j} \left\lfloor \frac{d}{q^{k-1-u}} \right\rfloor \quad \text{for} \ 0 \leq j \leq k - 1.$$ 

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

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

**Proof.** Assume $\bigcup_{i \geq 1} C_i$ contains a $t$-flat $\Pi$. Let $C'_i = (C_i \setminus \Pi) \cup (C_{i+1} \cap \Pi)$ for all $i$ and let $G$ be the corresponding new multiset. Then $G$ gives an $[n' = n - \theta_t, k', d']_q$ code. For any hyperplane $\pi$ of $\Sigma$, $\pi$ meets $\Pi$ in $\theta_t-1$ or $\theta_t$ points. So, $m_G(\pi) \leq n' - d' \leq n - d - \theta_t - 1$, giving $d' \geq d - q^t$. Suppose $k' \leq k - 1$. Then, there exists a hyperplane $\pi$ of $\Sigma$ containing $\bigcup_{i \geq 1} C_i \setminus \Pi$. Since $\pi$ meets $\Pi$ in a $(t - 1)$-flat, we have $m_{\overline{G}}(\pi) = n' + \theta_{t-1} = n - q^t \leq n - d$, so $d \leq q^t$, a contradiction. Hence $k' = k$.

Assume $C$ 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 $d_i$, $0 \leq d_i \leq q - 1$, and we have $n = s\theta_{k-1} - (\sum_{i=0}^{k-2} d_i \theta_i)$. Hence $C'$ 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

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

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

For a given $[n, k, d]_q$ code $C$ and the multiset $\overline{G}$ obtained from a generator matrix $G$, we say that puncturing of $C$ 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 $d = sq^{k-1} - \sum_{i=1}^{t} u_i q^{i-1}$, where $s = \lceil d/q^{k-1} \rceil$, $k > u_1 \geq u_2 \geq \cdots \geq u_t \geq 1$, and at most $q - 1$ $u_i$’s take any given value. Let $S$ be an $s$-fold simplex code with generator matrix $G$. If there exist $t$ flats $\Pi_i \in F_{u_i-1}$ no $s + 1$ of which contain a common point, then one can construct a $[g_q(k, d), k, d]_q$ code from $S$ 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 Be
dov type was found by Belov, Logachev and Sandimirov [1] for binary codes and was

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

$$
\min \{s+1,t\} \leq sk.
$$

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 $C$ is not of Be
dov type as we see below.

**Proof of Theorem 1.2.** Let $\mathcal{H}$ be a hyperbolic quadric in $PG(3,q)$,
$q \geq 7$, 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 $P_1, \ldots, P_4$
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 $\langle \chi_1, \chi_2, \ldots \rangle$
denotes the smallest flat containing subsets $\chi_1, \chi_2, \ldots$. We set $C_0 = l_1 \cup l_2 \cup \cdots \cup l_6,$
$C_1 = (l_1, l_3) \cup (l_1, l_4) \cup (l_2, l_3) \cup (l_2, l_4) \cup (l_1, l_2) \cup \mathcal{H}) \setminus C_0$ and $C_2 = PG(3,q) \setminus (C_0 \cup C_1)$. 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 $C$. 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 $\delta_1, \ldots, \delta_{q-1}$ be the planes through $l$ other than
$\langle l, l_1 \rangle, \langle l, l_2 \rangle$. Then each $\delta_i$ meets $l_1$ and $l_2$ in the points $Q_1$ and $Q_2$, respectively,
and meets $l_3, \ldots, l_6$ in some points out of $l$. Hence, we can take a line $m_i$ in $\delta_i$
with $m_i \cap C_0 = \emptyset$ for $1 \leq i \leq q - 1$ such that $m_1 \cap l, \ldots, m_{q-1} \cap l$ are distinct
points. Applying Lemma 2.1 by deleting $t$ of the lines $m_1, \ldots, m_{q-1}$, we get a
$[n = 2q^3 - 3q^2 + 1 - t\theta_1, 4, d = 2q^3 - 5q^2 + 3q - t\theta_1]_q$ code. This code is Griesmer for $t = 1, 2$ giving Theorem 1.2 and satisfies $n = g_q(4,d) + 1$ for $3 \leq t \leq q - 1$
giving Theorem 1.3. □

An $f$-set $F$ in $PG(k - 1, q)$ is called an $(f,m)$-mini hyper if

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

For example, a $t$-flat is a $(\theta_t, \theta_{t-1})$-mini hyper and a blocking $b$-set in some plane
is a $(b,1)$-mini hyper, see [6] for blocking sets in $PG(2,q)$. To prove Theorem 1.1,
we generalize Lemma 2.1 to the following.
Lemma 2.3. Let \( C \) be an \([n,k,d]_q\) code with generator matrix \( G \) and let 
\[ \bigcup_{i=0}^n C_i \]
be the partition of \( \Sigma = \text{PG}(k-1,q) \) obtained from \( \overline{G} \). Assume \( \bigcup_{i>0} C_i \)
contains an \((f,m)\)-minihyper \( F \) such that \( \langle \bigcup_{i>0} C_i \setminus F \rangle = \Sigma \). 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 \( \text{PG}(k-1,q) \).

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 \( \text{PG}(2,q) \) is a set \( \mathcal{B} \) of \(3(m-1)\)
points on some three non-concurrent lines \( l_1,l_2,l_3 \) such that \( l_i \cap \mathcal{B} = m \) 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 \( l_3 \cap \langle Q_1,Q_2 \rangle \subseteq \mathcal{B} \). Let \( \mathcal{Q}_q \) and \( \mathcal{N}_q \) be the set of non-zero squares and non-squares
\( \mathbb{F}_q, \) respectively. Then, \( |\mathcal{Q}_q| = |\mathcal{N}_q| = (q-1)/2 \), and \( -1 \in \mathcal{Q}_q \) if \( q \equiv 1 \) (mod \( q \))
but \( -1 \in \mathcal{N}_q \) if \( q \equiv 3 \) (mod \( q \)). In \( \text{PG}(2,q) \), \( q \) 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 \( R_0 = P(0,0,0), R_1 = P(0,1,0), R_2 = P(0,0,1) \in \text{PG}(2,q), \) and \( K_0 = \{ (0,1,a) \mid a \in \mathbb{Q}_q \} \subset \langle R_1,R_2 \rangle, K_1 = \{ (1,0,b) \mid b \in \mathbb{Q}_q \} \subset \langle R_0,R_2 \rangle, \) \( K_2 = \{ (c,1,0) \mid c = -ab^{-1}, a,b \in \mathbb{Q}_q \} \subset \langle R_0,R_1 \rangle. \) 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 \( \alpha - 1 \in \mathcal{Q}_q \).

Proof. 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 \((q - 1)/2 \equiv 0 \) (mod \( p \)),
a contradiction. \( \square \)

Lemma 3.3. Let \( C \) be the conic \( \{ P_i = P(1,u,u^2) \mid u \in \mathbb{F}_q \} \cup \{ P = P(0,0,1) \} \) in \( \text{PG}(2,q), q \) odd. Take \( \alpha \in \mathcal{N}_q \) with \( \alpha - 1 \in \mathcal{Q}_q \) and let \( Q_0 = P(1,0,\alpha), Q_1 = P(1,1,\alpha), l_0 = \langle P,P_0 \rangle, l_1 = \langle P,P_1 \rangle, l = \langle Q_0,Q_1 \rangle, Q = P(0,1,0) = l \cap l_p, \) 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 \( P_0,P_1,Q \notin T \).

Proof. Take non-zero elements \( s,t \in \mathbb{F}_q \) so that \( s \in \mathcal{Q}_q, t \in \mathcal{N}_q \) and \( q \equiv 1 \) (mod \( q \))
and that \( s \in \mathcal{N}_q, t \in \mathcal{Q}_q \) for \( q \equiv 3 \) (mod \( q \)), and let \( \sigma \) be the projectivity
of \( \text{PG}(2,q) \) given by
\[ \sigma(P(x,y,z)) = P(sx + ty, ty, a sx + at y + z) \]
for \( X = P(x,y,z) \in \text{PG}(2,q) \). Then the three points \( R_0,R_1,R_2 \) in Lemma 3.1
are transformed by \( \sigma \) to \( Q_0,Q_1,P \), respectively. For \( a \in \mathcal{Q}_q, \sigma(P(0,1,a)) = \]
\[ \mathbf{P}(1,1,\alpha + at^{-1}) \neq P_1 \] since \( \alpha - 1 \in \mathbb{Q}_q \) and \(-at^{-1} \in \mathcal{N}_q\). For \( b \in \mathbb{Q}_q \), \( \sigma(\mathbf{P}(1,0,b)) = \mathbf{P}(1,0,\alpha + bs^{-1}) \neq P_0 \), for \(-bs^{-1} \in \mathcal{N}_q\). For \( c = -ab^{-1} \) with \( a,b \in \mathbb{Q}_q \), \( \sigma(\mathbf{P}(c,1,0)) = \mathbf{P}(cs + t,t,(cs + t)\alpha) \neq Q \) since \( ab^{-1} \in \mathbb{Q}_q \) 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 \( \text{PG}(2,q) \) 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 \( P \in \mathcal{B} \); \( \mathcal{B} \cap l_i = m \) 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 \( q_3 \cap \langle Q_1,Q_2 \rangle \in \mathcal{B} \).

For \( q = 2^h \) with \( h \geq 3 \), let \( \text{tr}(x) = x + x^2 + \cdots + x^{2^h-1} \) be the trace function over \( \mathbb{F}_2 \). Let \( T_i = \{ a \in \mathbb{F}_q, \text{tr}(a) = i \} \) for \( i = 0,1 \). In \( \text{PG}(2,q) \), \( q \) 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 \( P_0 = \mathbf{P}(0,0,1), P_1 = \mathbf{P}(0,1,0), P_2 = \mathbf{P}(1,0,0), P_3 = \mathbf{P}(1,1,0) \in \text{PG}(2,q) \), and \( K_1 = \{ (0,1,a) \mid a \in T_0 \} \subset \langle P_0, P_1 \rangle, K_2 = \{ (1,0,a) \mid a \in T_0 \} \subset \langle P_0, P_2 \rangle, K_3 = \{ (1,1,a) \mid a \in T_0 \} \subset \langle P_0, P_3 \rangle \). 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 \( \text{PG}(2,q) \) 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 \( s,t,u \in T_1 \). Then \( P_0, R_1, R_2, R_3 \) form a \((4,2)\)-arc, for \( s+t \in T_0 \) for \( s,t \in T_1 \). Take a projectivity \( \sigma \) so that \( \sigma(R_0) = Q \) 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 \( \mathcal{H} = \mathbf{V}(x_0 x_1 + x_2 x_3) \) be a hyperbolic quadric in \( \Sigma = \text{PG}(3,q) \). 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 \( C \). 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 \( \delta \) 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


Department of Mathematics
and Information Sciences
Osaka Prefecture University
Sakai, Osaka 599-8531, Japan

Received February 15, 2013
Final Accepted April 29, 2013