数理解析研究所講究録
1106 巻 1999 年 102-105

On the Extension Theorem for Linear Codes
(線形符号の延長定理について)

Tatsuya MARUTA (丸田 辰哉)

Department of Information Systems
Aichi Prefectural University
Nagakute, Aichi 480-1198, Japan
e-mail : maruta@ist.aichi-pu.ac.jp

Abstract. Hill and Lizak ([1]) proved that every $[n,k,d]_q$ code with $\gcd(d,q)=1$ and with all weights congruent to 0 or d (modulo q) can be extended to an $[n+1,k,d+1]_q$ code. We give another elementary geometrical proof of this theorem.

1. Introduction

An $[n,k,d]_q$ code $\mathcal{C}$ means a linear code of length n with dimension k whose minimum Hamming distance is d over the Galois field GF(q). The weight distribution of $\mathcal{C}$ is the list of numbers A_i which is the number of codewords of $\mathcal{C}$ with weight i. We only consider *non-degenerate* codes having no coordinate which is identically zero.

Let $\mathcal{C}$ be an $[n,k,d]_q$ code with a generator matrix G. The code obtained by deleting the same coordinate from each codeword of $\mathcal{C}$ is called a *punctured code* of $\mathcal{C}$. If there exists an $[n+1,k,d+1]_q$ code $\mathcal{C}'$ whose punctured code is $\mathcal{C}$, $\mathcal{C}$ is called *extendable* (to $\mathcal{C}'$) and $\mathcal{C}'$ is an *extension* of $\mathcal{C}$. Obviously, every $[n,1,d]_q$ code is extendable.

As for the case when $k=2$, an $[n,2,d]_q$ code $\mathcal{C}$ is equivalent to the code with a generator matrix of the form

$$\begin{bmatrix} 1\cdots 1 & 1 & \cdots & 1 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 1 & 0\cdots 0 \\ 0\cdots 0 & \alpha & \cdots & \alpha & \alpha^2 & \cdots & \alpha^2 & \cdots & \alpha^{q-1} & \cdots & \alpha^{q-1} & 1\cdots 1 \end{bmatrix},$$

where α is a primitive element of GF(q). Let t_0, t_i $(1 \le i \le q-1)$, t_q be the number of columns $[1\ \ 0]^T, [1\ \ \alpha^i]^T (1 \le i \le q-1), [0\ \ 1]^T$ respectively, so that $t_0+t_1+\ldots+t_q=n$. Setting $s=\max\{t_0,t_1,\ldots,t_q\}$, we have $0 \le t_i \le s$ and $s=n-d$. So, $\mathcal{C}$ is extendable iff there exists i $(0 \le i \le q)$ with $t_i < s$. Since $\mathcal{C}$ is an $[s(q+1),2,sq]_q$ code iff $t_0=t_1=\ldots=t_q=s$, we get

Theorem 1. An $[n,2,d]_q$ code $\mathcal{C}$ is not extendable iff $n=s(q+1)$ and $d=sq$ for some integer s.

Although it is not so easy to find if an $[n,k,d]_q$ code is extendable or not when $k \geq 3$ in general, it is well known that every $[n,k,d]_2$ code with d odd is extendable (by adding an overall parity check). The following so-called extension theorem is a generalization of this fact.

Theorem 2. (Hill & Lizak [1])
Let $\mathcal{C}$ be an $[n,k,d]_q$ code with the weight distribution $\{A_i\}$. If gcd(d,q)=1 and if $i \equiv 0$ or $d \pmod q$ for all i with $A_i > 0$, then $\mathcal{C}$ is extendable to an $[n+1,k,d+1]_q$ code $\mathcal{C}'$ with the weight distribution $\{A_i'\}$ satisfying $i \equiv 0$ or $d+1 \pmod q$ for all i with $A_i' > 0$.

For an $[n,k,d]_q$ code $\mathcal{C}$ with a generator matrix G, the *residual code* of $\mathcal{C}$ with respect to a codeword c, denoted by Res$(\mathcal{C},c)$, is the code generated by the restriction of G to the columns where c has a zero entry. The following lemma is well known for residual codes.

Lemma 3. Take $c \in \mathcal{C}$ with weight d. Then Res$(\mathcal{C},c)$ is an $[n-d,k-1,d_0]_q$ code with $d_0 \geq \lceil d/q \rceil$, where $\lceil x \rceil$ is the smallest integer $\geq x$.

When q divides d, we can prove the following.

Theorem 4. An $[n,k,d]_q$ code $\mathcal{C}$ is not extendable if q divides d and if Res$(\mathcal{C},c)$ is an $[n-d,k-1,d_0]_q$ code with $d_0 = d/q$ for some $c \in \mathcal{C}$.

Example. Every $[q^2,4,q^2-q-1]_q$ code $\mathcal{C}_1$ is extendable by Theorem 2 (see [1]). But the extension of $\mathcal{C}_1$ is not extendable by Lemma 3 and Theorem 4.

We give the proof of Theorems 2 and 4 in Section 3. A geometrical point of view (given in Section 2), which is a generalization of the above observation for the case when $k=2$, is sometimes valid for linear codes (cf. [4],[5]). Although the original proof of Theorem 2 is elementary, we give another elementary geometrical proof to make clear the extendability of linear codes in the different way.

2. A geometric method

We denote by PG(r,q) the projective geometry of dimension r over GF(q). Assume $r \geq 2$. A j*-flat* is a projective subspace of dimension j in PG(r,q). 0-flats, 1-flats, 2-flats, $(r-2)$-flats and $(r-1)$-flats are called *points, lines, planes, secundums* and *hyperplanes* respectively. We denote by $\mathcal{F}_j$ the set of j-flats of PG(r,q). The following lemma is a characterization of hyperplanes.

Lemma 5. Let F be a proper subset of $\Sigma =$ PG(r,q). Then F is a hyperplane of Σ iff every line in Σ meets F in one point or in $q+1$ points.

Proof. Assume that every line in $\Sigma = \mathrm{PG}(r, q)$ meets a proper subset F of Σ in one point or in $q+1$ points. Let l_0 be a line in Σ. Then we can find a point $Q_0 \in F$ on l_0. Let δ_{j-1} be a $(j-1)$-flat included in F, $1 \le j \le r-1$. Taking a line l_j which is skew to δ_{j-1}, we can get a point $Q_j \in F$ (on l_j) not on δ_{j-1}. Since every line through Q_j and a point of δ_{j-1} meets F in $q+1$ points, we get $\delta_j = \langle Q_j, \delta_{j-1} \rangle \in \mathcal{F}_j$ included in F. Inductively, we get a hyperplane δ_{r-1} included in F. If a point $Q \in F$ not in δ_{r-1} exists, then we have $F = \langle Q, \delta_{r-1} \rangle = \Sigma$, a contradiction. Hence we obtain $F = \delta_{r-1}$. The converse is trivial. □

Let $\mathcal{C}$ be a (non-degenerate) $[n, k, d]_q$ code. The columns of a generator matrix of $\mathcal{C}$ can be considered as a multiset of n points in $\Sigma = \mathrm{PG}(k-1, q)$ denoted also by $\mathcal{C}$. We see linear codes from this geometrical point of view. An *i-point* is a point of Σ which has multiplicity i in $\mathcal{C}$. Let C_i be the set of i-points in Σ. For any subset S of Σ we define

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

where γ_0 is the maximum of the multiplicities of points in Σ.

A line l with $t = c(l)$ is called a *t-line.* A *t-plane*, *t-secundum* and a *t-hyperplane* are defined similarly. Then we obtain the partition $\Sigma = C_0 \cup C_1 \cup \cdots \cup C_{\gamma_0}$ such that

$$c(\Sigma) = n, \tag{2.1}$$

$$n - d = \max\{c(\pi) | \pi \in \mathcal{F}_{k-2}\}. \tag{2.2}$$

Conversely such a partition of Σ as above gives an $[n, k, d]_q$ code in the natural manner if there exists no hyperplane including the complement of C_0 in Σ. Since an $[n+1, k, d+1]_q$ code also satisfies (2.2) we get the following.

Lemma 6. An $[n, k, d]_q$ code $\mathcal{C}$ is extendable iff there exists a point $P \in \Sigma$ such that $c(\pi) < n - d$ for all hyperplanes π through P.

We give an elementary proof of Theorem 2 using Lemma 6.

3. Proof of Theorem 2 and Theorem 4

Note that the number of i-hyperplanes is $A_{n-i}/(q-1)$ $(0 \le i \le n-d)$. So, the condition '$i \equiv 0$ or $d \pmod q$ for all i with $A_i > 0$' in Theorem 2 implies that $c(\pi) \equiv n$ or $n - d \pmod q$ for all $\pi \in \mathcal{F}_{k-2}$.

Proof of Theorem 2. Put $F = \{\pi \in \mathcal{F}_{k-2} | c(\pi) \equiv n (\bmod\ q)\}$. For any t-secundum δ of $\Sigma = \mathrm{PG}(k-1, q)$, denote by a_δ (resp. b_δ) the number of hyperplanes π through δ with $c(\pi) \equiv n (\bmod\ q)$ (resp. $c(\pi) \equiv n - d (\bmod\ q)$). Then we have $a_\delta + b_\delta = q + 1 \equiv 1$ and $(n-t)a_\delta + (n-d-t)b_\delta + t \equiv n$, so that $d(a_\delta - 1) \equiv 0 \ (\bmod\ q)$. Since $\gcd(d, q)$=1, we get $a_\delta \equiv 1 \ (\bmod\ q)$, whence $a_\delta = 1$ or $q+1$. This implies that every line in a dual space Σ^* meets F in one point or $q+1$ points. By Lemma 5, F is a hyperplane of Σ^*, whence there exists a point $P \in \Sigma$ such that the set of all hyperplanes through P is equal to F. Since $c(\pi) \equiv n (\bmod\ q)$ implies $c(\pi) < n - d$, $\mathcal{C}$ is extendable by Lemma 6. By adding P to the multiset $\mathcal{C}$, we get an extension of $\mathcal{C}$ which satisfies $c(\pi) \equiv n+1$ or $n-d \ (\bmod\ q)$ for all $\pi \in \mathcal{F}_{k-2}$. □

It follows from the above proof that the point to be added to the multiset $\mathcal{C}$ to get an extension of $\mathcal{C}$ is uniquely determined under the condition of Theorem 2.

Proof of Theorem 4. Since $\mathrm{Res}(\mathcal{C}, c)$ is an $[n-d, k-1, d/q]_q$ code for some $c \in \mathcal{C}$, there exists a t-secundum δ with $t = n - d - d/q$ in $\Sigma = \mathrm{PG}(k-1, q)$. Considering the hyperplanes through δ, we have

$$n \le (n-d-t)(q+1) + t = n,$$

whence every hyperplane through δ is a $(n-d)$-hyperplane. Hence every point in Σ is on a $(n-d)$-hyperplane, and $\mathcal{C}$ is not extendable by Lemma 6. □

References

[1] R. Hill and P. Lizak, Extensions of linear codes, Proc. IEEE Int. Syposium on Inform. Theory (Whistler, Canada, 1995) 345.

[2] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields,* Clarendon Press, Oxford, 1979.

[3] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions,* Clarendon Press, Oxford, 1985.

[4] I.N. Landjev and T. Maruta, On the minimum length of quaternary linear codes of dimension five, *Discrete Math.* (to appear).

[5] T. Maruta, On the achievement of the Griesmer bound, *Designs, Codes and Cryptography* **12** (1997), 83–87.