ARCHIVUM MATHEMATICUM (BRNO)
Tomus 41 (2005), 17 – 26

EXPLORING INVARIANT LINEAR CODES THROUGH GENERATORS AND CENTRALIZERS

PARTHA PRATIM DEY

Abstract. We investigate a H-invariant linear code C over the finite field F_p where H is a group of linear transformations. We show that if H is a noncyclic abelian group and $(|H|, p) = 1$, then the code C is the sum of the centralizer codes $C_c(h)$ where h is a nonidentity element of H. Moreover if A is subgroup of H such that $A \cong Z_q \times Z_q$, $q \neq p$, then $\dim C$ is known when the dimension of $C_c(K)$ is known for each subgroup $K \neq 1$ of A. In the last few sections we restrict our scope of investigation to a special class of invariant codes, namely affine codes and their centralizers. New results concerning the dimensions of these codes and their centralizers are obtained.

1. Introduction

Given a vector space $V = V_n(F)$ of dimension $n < \infty$ over the field F, with a fixed basis specified for V, a *code* is a subset of V. A code is linear if it is a subspace of V. For F we take F_p and for basis the usual one i.e., $\{e_i \mid i = 1, \dots, n\}$ where e_i has 1 in it's i^{th} coordinate and the remaining coordinates are zero. The vectors in C are called *codewords* and a typical codeword has the following shape

$$x = (x_1, \dots, x_n), x_i \in F_p\,, \quad i = 1, \dots, n$$

See [2] and [3] for background informations on linear codes.

Definition 1.1. Let H be a group of linear transformations of a vector space V. We set

$$C_V(H) = \{v \in V \mid vh = v\}$$

for all $h \in H$. We call $C_V(H)$ the centralizer of H in V. Clearly the centralizer is a code in V.

Definition 1.2. A code C of vector space V is H-invariant if $Ch \subseteq C$ for all h in H, where H is a group of linear transformations of vector space V.

2000 *Mathematics Subject Classification*: 05E20.
Key words and phrases: invariant code, centralizer, affine plane.
Received March 30, 2003, revised January 2004.

2. Dimension of $C_V(H)$

In this section we explore the relationship between the dimensions of $C_V(H)$ and $C_C(H)$. Towards that goal, we prove the following lemma.

Lemma 2.1. *Let $V = F_p^n$ and assume C is a code of V over F_p. Let H be a group of permutation matrices of order n which leave C invariant and $(p, |V|) = 1$. Set*

$$\theta = \frac{1}{|H|} \sum_{g \in H} g \,.$$

Then (i) *θ is an idempotent,* (ii) $(C\theta)^{\perp} = \text{Ker } \theta \oplus (C^{\perp})\theta$.

Proof. (i) We compute θ^2.

$$\begin{aligned}\theta \cdot \theta &= \Big(\frac{1}{|H|} \sum_{g \in H} g\Big)\Big(\frac{1}{|H|} \sum_{g \in H} g\Big) = \frac{1}{|H|^2} |H| \sum_{g \in H} g \\ &= \frac{1}{|H|} \sum_{g \in H} g = \theta \,,\end{aligned}$$

which shows θ is an idempotent.

(ii) Let $v \in \text{Ker } \theta \cap (C^{\perp})\theta$. Then $v\theta = 0$ and $v = c^{\perp}\theta$ where $c^{\perp} \in C^{\perp}$. Because $\theta^2 = \theta$, $v = c^{\perp}\theta = c^{\perp}\theta^2 = (c^{\perp}\theta)\theta = v\theta = 0$. Thus $\text{Ker } \theta \cap (C^{\perp})\theta = \{0\}$.

Let $v \in \text{Ker } \theta \oplus (C^{\perp})\theta$. Then $v = k + (c^{\perp})\theta$ with $k \in \text{Ker } \theta$ and $c^{\perp} \in C^{\perp}$. Thus for any $c \in C$, $(c\theta, v) = (c\theta, k + (c^{\perp})\theta) = (c\theta, k) + (c\theta, (c^{\perp})\theta) = (c, k\theta^t) + (c\theta, c^{\perp}\theta)$. Since

$$\theta^t = \frac{1}{|H|} \sum_{g \in H} g^t = \frac{1}{|H|} \sum_{g \in H} g^{-1} = \frac{1}{|H|} \sum_{g \in H} g = \theta$$

and C, $C^{\perp}$ are θ-invariant, we have $(c\theta, v) = 0$ for any c, which shows $v \in (C\theta)^{\perp}$.

We now show that $(C\theta)^{\perp} \subseteq \text{Ker } \theta \oplus (C^{\perp})\theta$. Let $v \in (C\theta)^{\perp}$, which implies $(v, c\theta) = 0$ for any $c \in C$. But $0 = (v, c\theta) = (v\theta^t, c) = (v\theta, c)$ and so $v\theta \in C^{\perp}$. As θ is an idempotent, $v\theta$ also belongs to $(C^{\perp}\theta)$. Thus $v = (v - v\theta) + v\theta$, where $v - v\theta \in \text{Ker } \theta$ because $(v - v\theta)\theta = v\theta - v\theta^2 = v\theta - v\theta = 0$. We therefore conclude that $(C\theta)^{\perp} = \text{Ker } \theta \oplus (C^{\perp})\theta$. □

Next we prove the following theorem.

Theorem 2.2. *Assume C is a code of $V = F_p^n$. Let H be a group of permutation matrices which leave C invariant. If $(p, |H|) = 1$, then*
(i) $C_C(H) = C\theta$,
(ii) $\dim C_V(H) = \dim C_C(H) + \dim C_{C^{\perp}}(H)$.

Proof. (i) Let $v \in C\theta$. Then $v = c\theta$ for some $c \in C$. Let h be an arbitrary element from H. Then

$$vh = c\theta h = c\Big(\frac{1}{|H|} \sum_{g \in H} g\Big) = c\Big(\frac{1}{|H|} \sum_{g \in H} g\Big) = c\theta = v \,,$$

which shows $v \in C_C(H)$. Conversely, suppose $v \in C_C(H)$. Then $v \in C$ and $vg = v$ for an arbitrary $g \in H$. Thus

$$v\theta = v\Big(\frac{1}{|H|}\sum_{g\in H} g\Big) = \frac{1}{|H|}\sum_{g\in H} vg = \frac{1}{|H|}|H|v = v\,,$$

which shows $v \in C\theta$.

(ii) Let θ be the idempotent of the Lemma 2.1. As $(C\theta) \subset (V\theta)$, we have $\dim V\theta = \dim C\theta + \dim\big((C\theta)^\perp \cap V\theta\big)$. By the lemma above, $(C\theta)^\perp = \text{Ker}\ \theta \oplus (C^\perp\theta)$ which shows $(C\theta)^\perp \cap V\theta = (\text{Ker}\ \theta \cap V\theta) \oplus \big((C^\perp\theta) \cap V\theta\big)$. Assume $x \in V\theta \cap \text{Ker}\ \theta$. Then $x = v\theta$ for some $v \in V$. Thus $x = v\theta = v\theta^2 = (v\theta)\theta = x\theta = 0$. This shows $(C\theta)^\perp \cap V\theta = (C^\perp)\theta \cap V\theta = (C^\perp)\theta$. Thus $\dim V\theta = \dim C\theta + \dim C^\perp\theta$. Now we apply (i) to obtain $\dim C_V(H) = \dim C_C(H) + \dim C_{C^\perp}(H)$. □

3. Invariant codes and their centralizers

The aim of this section is to explore the relationship between the dimensions of the code and its centralizer codes. Towards that goal we present the following two theorems.

Theorem 3.1. *Let C be a code over F_p and let H be a group of linear transformations which leave C invariant. Suppose $(|H|, p) = 1$. Then*

$$C = C_C(H) \oplus U$$

where

$$U = \Big\{c - c\theta \mid c \in C,\ \theta = \frac{1}{H}\sum_{h\in H} h\Big\}$$

Moreover, U is an invariant subcode of C.

Proof. Since $C_C(H) \subseteq C$ and $U \subseteq C$, we have $C_C(H) + U \subseteq C$. For any $c \in C$, we may write $c = c\theta + (c - c\theta)$ where $c\theta \in C_C(H)$ as

$$c\theta h = c\Big(\frac{1}{|H|}\sum_{g\in H} g\Big)h = c\Big(\frac{1}{|H|}\sum_{g\in H} g\Big) = c\theta\,.$$

Clearly $c - c\theta \in U$ and hence $c \in C_C(H) + U$. Thus $C = C_C(H) + U$.

We now prove that $C_C(H) \cap U = \{0\}$. Let $x \in C_C(H) \cap H$. Since $x \in C_C(H)$, we have

$$x\theta = x\Big(\frac{1}{|H|}\sum_{h\in H} h\Big) = \frac{1}{|H|}\sum_{h\in H} xh = \frac{1}{|H|}\sum_{1}^{|H|} x = x\,.$$

On the other hand, $x = c - c\theta$ for some $c \in C$ since $x \in U$. This implies $x\theta = c\theta - c\theta^2 = c\theta - c\theta = 0$ as $c\theta \in C_C(H)$. As $x\theta = x$, we have $x = 0$. □

Theorem 3.2. *Let C be a code over F_p and let H be a noncyclic abelian group of linear transformations which leave C invariant. Suppose $(|H|, p) = 1$, then*

$$C = \sum_{h\in H^\#} C_C(h)$$

where $H^\#$ denotes the nonidentity elements of H.

Proof. Let $h \in H^{\#}$. Then $h^m = 1$ for some m and p does not divide m. So h satisfies the equation $x^m - 1 = 0$ over F_p. Since p does not divide m, $mx^{m-1} \neq 0$, which shows that the minimal polynomial of h has distinct roots. Thus h is diagonalizable over F_p. Since H is abelian and each element of H is diagonalizable, the elements in H are simultaneously diagonalizable i.e., $C = \langle u_1 \rangle \oplus \cdots \oplus \langle u_s \rangle$ where $\{u_1, \ldots, u_s\}$ is a basis of eigenvectors for the elements of H. We now define a homomorphism ϕ from H to $\mathrm{Aut}(\langle u_i \rangle)$ by

$$\phi(h)(u_i) = u_i h\,.$$

Then $H/\operatorname{Ker}\phi$ can be imbedded in $\mathrm{Aut}(\langle u_i \rangle)$. Since $\operatorname{Ker}\phi \subseteq C_H(u_i)$ and $\langle u_i \rangle \cong Z_p$, we have $H/C_H(u_i)$ imbedded in Z_{p-1}. This shows $H/C_H(u_i)$ is cyclic and because H is not cyclic, $C_H(u_i) \neq 1$. Thus $\langle u_i \rangle \subseteq C_C(h_i)$ for some $h_i \in H$. Hence

$$C \subseteq \sum_{i=1}^{s} C_C(h_i) \subseteq C$$

and the proof is complete. □

Now we are ready to prove our main result.

Theorem 3.3. *Let C be the code over F_p and H be a group of linear transformations which leave C invariant. Suppose $H \cong Z_q \times Z_q$ for some q, $q \neq p$. Then*

$$\dim C = \sum_{i=1}^{q+1} \dim C_C(h_i) - q \dim C_C(H)$$

where $h_1, \ldots, h_{q+1}$ are generators of the $q+1$ subgroups of order q.

Proof. Since $(|H|, p) = 1$, by Theorem 3.1, $C = C_C(H) \oplus U$. We apply Theorem 3.2 to get

$$U = \sum_{i=1}^{q+1} C_U(h_i)\,,$$

where $h_1, \ldots, h_{q+1}$ generate $q+1$ distinct subgroups of H of order q. We claim that U is direct sum of the $C_U(h_i)$s. For $i \neq j$,

$$C_U(h_i) \cap C_U(h_j) \subseteq C_U(\langle h_i, h_j \rangle) = C_U(H) \subseteq U \cap C_C(H) = \{0\}\,.$$

This shows our claim is true for $n = 2$. Assume the claim is true for $n = k$ i.e.,

$$\sum_{i=1}^{k} C_U(h_i) = \oplus \sum_{i=1}^{k} C_U(h_i)\,.$$

Let

$$c \in \Big(\oplus \sum_{i=1}^{k} C_U h_i \Big) \cap C_U(h_{k+1})\,.$$

Then

$$c = \sum_{i=1}^{k} u_i$$

implies

$$ch_{k+1} = \sum_{i=1}^{k} u_i h_{k+1}$$

where $u_i \in C_U(h_i)$. Since $(u_i h_{k+1})h_i = (u_i h_i)h_{k+1} = u_i h_{k+1}$, we have $u_i h_{k+1} \in C_U(h_i)$. As $c = ch_{k+1}$,

$$c = \sum_{i=1}^{k} u_i h_{k+1} = \sum_{i=1}^{k} u_i \,.$$

By uniqueness of expression for c, $u_i = u_i h_{k+1}$. So $u_i \in C_U(h_i) \cap C_U(h_{k+1}) = \{0\}$, by the first part of the proof. Thus $c = 0$ and

$$U = \oplus \sum_{i=1}^{k+1} C_U(h_i)\,.$$

We now prove that $C_C(h_i) = C_C(H) \oplus C_U(h_i)$ for $i = 1, \ldots, q+1$. Clearly $C_C(H) \oplus C_U(h_i) \subseteq C_C(h_i)$. Let $c \in C_C(h_i)$. Then $c = c\theta + (c - c\theta)$. Since $h\theta = h$ for any $h \in H$, we have $c\theta \in C_C(H)$. Moreover, as H is abelian and $c \in C_C(h_i)$, we get $(c - c\theta)h_i = ch_i - c\theta h_i = ch_i - ch_i\theta = c - c\theta$ which shows $c - c\theta \in C_U(h_i)$. Thus $C_C(h_i) = C_C(H) + C_U(h_i)$. Since $C_U(h_i) \subseteq U$, the sum is direct. Thus

$$\begin{aligned}
\dim C &= \dim C_C(H) + \sum_{i=1}^{q+1} \dim C_U(h_i) \\
&= \dim C_C(H) + \sum_{i=1}^{q+1} \big(\dim C_C(h_i) - \dim C_C(H) \big) \\
&= \sum_{i=1}^{q+1} \dim C_C(h_i) - q \dim C_C(H)\,.
\end{aligned}$$

□

4. Affine code as an invariant linear code

We begin this section with a definition.

Definition 4.1. If $A = (a_{ij})$ is a $r \times r$ matrix and $B = (b_{ij})$ is a $s \times s$ matrix, then the Kronecker product $A \otimes B$ is the $rs \times rs$ matrix given by

$$A \otimes B = (a_{ij}B)_{rs \times rs}.$$

Throughout this section π will denote a plane of order n affording a $P{-}L$ transitivity G with center at C and axis L, the line at infinity. We coordinatize π by using Hall's method with entries from $G \times G$ where $G = \{g_1, \ldots, g_n\}$. Let Δ_a be the row vector which lists the finite points of $x = a$ i.e. $\Delta_a = \{(g_a, g_1), \ldots, (g_a, g_n)\}$. We index the first n^2 columns of the incidence matrix A of π by Δ_a's, $1 \le a \le n$ and the last $n+1$ columns, by the infinite points $(1), \ldots, (n+1)$. The first n^2 rows are indexed by the families $F_m, m = 1, \ldots, n$ where

$$F_m = \{l_m g_k \mid k = 1, \ldots, n\} \cup (m),\ \ m = 1, \ldots, n$$

and l_m is the line joining (g_1, g_1) and (m). That is, $l_m = \{(g_k, g_{mk}) | k = 1, \ldots, n\} \cup (m)$ and g_{mk} is some element of G. The last $(n+1)$ rows are indexed by the lines through $(n+1)$ in the following order $x = a$, $a = 1, \ldots, n$, and L, where $x = a$ is the line $l_a = \{(g_a, g_k) \mid k = 1, \ldots, n\}$ and L is the line at infinity. Then the incidence matrix of π is given by

$$A = \begin{bmatrix} M & B^t \\ B & C \end{bmatrix}$$

where M is the incidence matrix of the n^2 finite points and n^2 lines that do not contain $(n+1)$. B on the other hand is the incidence matrix of n^2 points and $(n+1)$ lines containing $(n+1)$. Thus

$$B = \begin{bmatrix} \varepsilon_1 \otimes 1_n \\ \vdots \\ \varepsilon_n \otimes 1_n \\ 0 \ldots 0 \end{bmatrix}$$

where ε_i is the unit vector of F_p^n whose i^{th} coordinate is one and other coordinates are zero.
The incidence matrix of the affine plane $\pi - L$ is given by the $(n^2+n) \times n^2$ matrix

$$\begin{bmatrix} M \\ B \end{bmatrix}.$$

The affine code C_A of $\pi - L$ is therefore a subspace of $V = F_p^{n^2}$ generated by the (n^2+n) nonzero row vectors of M and B over F_p. Let $\{v_{mi} \mid 1 \leq m \leq n, 1 \leq i \leq n\}$ be the row vectors of M. Then according to our construction each v_{mi} is the characteristic vector of $l_m g_i$ with it's last $n+1$ coordinates deleted. As v_{mi} is a vector with n^2 coordinates, we may position its n^2 coordinates into n blocks each containing n coordinates and corresponding to some Δ_a as described in the beginning of this section. Since $x = a$ meets $l_m g_i$ in only one point, each block of v_{mi} has 1 in exactly one of its n coordinates and the other $n-1$ coordinates are zero. Thus if e_s denotes a vector of length n whose s^{th} coordinate is 1 and other coordinates are zero, and $v_{mi} = (b_1, \ldots, b_n)$ where b_i is a vector with n coordinates, then $b_i = e_s$ for some s.

Let $v_{n+11}, \ldots, v_{n+1n}$ be the row vectors of B. Then each v_{n+1k} is the characteristic vector of $x = k$ and hence $v_{n+1k} = (0, \ldots, 1_n, \ldots, 0)$ where 1_n is in the k^{th} coordinate and is a vector of length n with all coordinates 1, and 0 is a vector of length n with all coordinates zero.

Lemma 4.2. *$I \otimes R(g)$ is the permutation matrix for $g \in G$ acting on the affine code $C_A = \langle v_{mi} \mid m = 1, \ldots, n+1; i = 1, \ldots, n \rangle$.*

Proof. Let $(l_m g_i)g = l_m g_j$. We want to show that $(v_{mi}) I \otimes R(g) = v_{mg}$. Let $v_{mi} = (b_1, \ldots, b_n)$ and $v_{mj} = (c_1, \ldots, c_n)$ where each b_i, c_i is a vector of length n with exactly one coordinate one and the other coordinates zero. Assume $b_r = e_s$ where e_s denotes a vector of length n whose s^{th} coordinate is one and other coordinates are zero. Then b_r has 1 in its s^{th} coordinate, which implies $(g_r, g_s) \in l_m g_i$. Thus $g_s = g_i g_{mr}$. On the other hand $(v_{mi})I \otimes R(g) = (b_1 R(g), \ldots, b_n R(g))$. Now $b_r R(g) = e_t$ for some t. Hence $b_r R(g) = e_s R(g) = e_t$, which shows the (s,t)-entry of $R(g)$ is 1 and $gg_s = g_t$. Because $(l_m g_i)g = g_j$, we have $gg_i = g_j$. Hence using $g_s = g_i g_{mr}$ we obtain $gg_i g_{mr} = g_t$ i.e., $g_j g_{mr} = g_t$. But $(g_r, g_j g_{mr}) \in l_m g_j$ and hence $(g_r g_t) \in l_m g_j$, which shows v_{mj} has 1 at its t^{th} coordinate in the r^{th} block i.e., $c_r = e_t = b_r R(g)$. Since r was arbitrary, $(v_{mi})I \otimes R(g) = v_{mg}$.

Finally as g fixes $x = a$, we want to show that $(v_{n+1a})I \otimes R(g) = v_{n+1a}$. Since $v_{n+1a} = (0, \ldots, 1_n, \ldots, 0)$, 1_n in the a^{th} coordinate,

$$(v_{n+1a})I \otimes R(g) = (0, \ldots, 1_n R(g), \ldots, 0) = (0, \ldots, 1_n, 0, \ldots 0) = v_{n+1a}\,.$$

Thus $I \otimes R(g)$ fixes each v_{n+1a}. □

For $g_1, g_2 \in G$, $\big(I \otimes R(g_1)\big)\big(I \otimes R(g_2)\big) = \big(I \otimes R(g_1)R(g_2)\big) = \big(I \otimes R(g_1 g_2)\big)$. So the correspondence $g \to I \otimes R(g)$ is an isomorphism between G and $\{I \otimes R(g) \mid g \in G\}$. Hence from now on we will identify $\{I \otimes R(g) \mid g \in G\}$ with G. Because, by Lemma 4.2, $(v_{mi})g = v_{mj}$, it follows that both $C_A = \langle v_{mi} \mid 1 \le m \le n+1,\ 1 \le i \le n\rangle$ and $C_0 = \langle v_{mi} - v_{mj} \mid 1 \le m \le n+1,\ 1 \le i,\ j \le n\rangle$ are G-invariant subspaces of $F_p^{n^2}$.

5. Dimension of the affine code

Throughout this section we will assume π to be a plane of order n such that p divides n exactly to the first power. Let A be the incidence matrix of such a plane and let $w_1, \ldots, w_v$, where $v = n^2 + n + 1$, be the rows of A. Then C, the code of π is a subspace of $V = F_p^{n^2+n+1}$ spanned by $\{w_1, \ldots, w_v\}$ over F_p. Moreover, $\dim C = \frac{v+1}{2}$ by a theorem of Hall [2]. Fix a line L of π. We consider C_0 to be the subspace of C spanned by $w_i - w_j$ where w_i and w_j contain the same point of L. For any integer r, we let 1_r denote the vector of F_p^r each of whose r coordinates is 1.

Lemma 5.1. *Let C_0 be the code described above. Then*

$$\dim C_0 = \frac{n(n-1)}{2}\,.$$

Proof. We may arrange the points of π so that the last $(n+1)$ coordinates of the row vectors of A correspond to a line L, called the line at infinity. The first $n^2+n = n(n+1)$ rows of A may be partitioned into $(n+1)$ families $\{F_m \mid m = 1, \ldots, n+1\}$. Each F_m is the set of n lines of $\pi - L$ which contain the m^{th} point of L. The last row of A is the characteristic vector of L. We denote the vectors of F_m by $w_{m1}, \ldots, w_{mn}$ so that by definition $C_0 = \langle w_{mi} - w_{mj} \mid 1 \le i,\ j \le n,\ m = 1, \ldots, n+1\rangle$. The vectors which span C_0 have the last $n+1$ coordinates zero. Hence C_0 is a subspace of C consisting of vectors with the last $n+1$ coordinates zero. Now consider $U = \langle w_{11}, \ldots, w_{n+11}\rangle$ where $w_{m1} \in F_m$ is a row of A containing the m^{th} infinite point and no other infinite point. Clearly $\dim U = n+1$, as the vectors which span U are independent in the last $n+1$ coordinates.

Now $C_0 + U = C_0 \oplus U$, as the only vector of U with the last $n+1$ coordinates zero is 0. Clearly $C_0 \oplus U \subseteq C$. Now $w_{mi} = w_{m1} - (w_{m1} - w_{mi}) \in U \oplus C_0$. Also,

$$(1_{n^2}, 0) = (1, \dots, 1, 0, \dots, 0) = \sum_{k=1}^{n} w_{mk}$$

is an element of $U \oplus C_0$.

Without loss of generality, we may assume that each of $\{w_{m1} \mid 1 \le m \le n+1\}$ contains the same point, say P and therefore has the first coordinate equal to one. Hence $w_{11} + w_{21} + \cdots + w_{n+11} = (n+1, 1, \dots, 1) = 1_v \in U \oplus C_0$. Thus $1_v - (1_{n^2}, 0) = w_v \in U \oplus C_0$ where w_v is the row of A corresponding to L. This proves that $U \oplus C_0$ contains all the generators of C. Thus $U \oplus C_0 = C$ and hence $\dim C_0 = \dim C - \dim U = \frac{v+1}{2} - (n+1) = \frac{n^2+n+1+1}{2} - (n+1) = \frac{n^2-n}{2}$. □

We now consider u_{mi} to be the vector obtained from w_{mi} by deleting the last $n+1$ coordinates. Then clearly $\{u_{mi} \mid i = 1, \dots, n; m = 1, \dots, n+1\}$ is the set of $n^2 + n$ rows of an incidence matrix of the affine plane, obtained from π by deleting L and its $n+1$ points. The affine code C_A is clearly the linear subspace of $F_p^{n^2}$ spanned by the $\{u_{mi} \mid i = 1, \dots, n; m = 1, \dots, n+1\}$. We shall now find the dimension of of the affine code C_A over F_p and we will show that C_A is in fact $C_0^{\perp}$ in $F_p^{n^2}$. Here we must bear in mind that the last $n+1$ coordinates of C_0 are zero, so we can identify u_{mi} with w_{mi} and think of C_0 as a subcode of $F_p^{n^2}$.

Theorem 5.2. *$C_0^{\perp}$ is the affine code associated with $\pi - L$. Moreover, $\dim C_0^{\perp} = \frac{n^2+n}{2}$ if p divides n exactly to the first power.*

Proof. Let $W = \langle u_{11}, \dots, u_{n+11} \rangle$. Since $(u_{mi}, u_{ki} - u_{kj}) = 0 \pmod p$, we have $C_0 \subseteq C_0^{\perp}$ and $W \subseteq C_0^{\perp}$. Now let $x \in W \cap C_0$ so that $x = a_1 u_{11} + \cdots + a_{n+1} u_{n+11}, a_i \in F_p$. Because $W \subseteq C_0^{\perp}$, $(x, u_{mi}) = 0$ for each m. On the other hand,

$$(x, u_{mi}) = \sum_{i=1}^{n+1} a_i (u_{i1}, u_{m1}) = \sum_{i \ne m} a_i = 0\,.$$

Thus

$$a_1 = \dots a_{n+1} = \sum_{i=1}^{n+1} a_i\,.$$

Let $a_i = \lambda$. Then $x = \lambda u_{11} + \cdots + \lambda u_{n+11} = \lambda 1_{n^2}$ and $\dim (W \cap C_0) = 1$. Thus $\dim (C_0 + W) = \dim C_0 + \dim W - \dim (C_0 \cap W) = \frac{n^2-n}{2} + n + 1 - 1 = \frac{n^2+n}{2}$. On the other hand both C_0 and W are subcodes of $C_0^{\perp}$ and $\dim C_0^{\perp} = n^2 - \dim C_0 = n^2 - \frac{n^2-n}{2} = \frac{n^2+n}{2}$. Hence $C_0^{\perp} = C_0 + W$. Since $C_0 + W = \langle u_{mi} \mid m = 1, \dots, n+1; i = 1, \dots, n \rangle, C_0^{\perp}$ is the affine code of $\pi - L$. □

Corollary 5.3. *C_0 is a subcode of the affine code $C_A = C_0^{\perp}$ of codimension n.*

6. Dimension of $C_{C_A}(H)$

This final section begins with a lemma.

Lemma 6.1. *G fixes each element of C_A/C_0.*

Proof. C_0 is a subcode of C_A by Corollary . Hence C_A/C_0 is well defined. Let $g \in G$. For a generator v_{mi} of C_A, $(v_{mi} + C_0)g = (v_{mi})g + C_0 = v_{mj} + C_0$, as g is an elation and C_0 is G-invariant. But $v_{mi} - v_{mj} \in C_0$, hence $v_{mi} + C_0 = v_{mj} + C_0$. Thus $(v_{mi} + C_0)g = v_{mi} + C_0$. □

Next we quote a theorem which will be used later to prove an upcoming lemma.

Theorem 6.2. *Let G be a group of automorphisms of an abelian p-group V and assume p does not divide $|G|$. Suppose V_1 is a G-invariant direct factor of V. Then $V = V_1 \times V_2$ where V_2 is also G-invariant.*

Lemma 6.3. *Let H be a subgroup of G and $(|H|, p) = 1$. Then*

$$C_A = C_0 + M$$

where both C_0 and M are H-invariant and $\dim M = n$. Moreover

$$C_{C_A}(H) = C_{C_0}(H) \oplus C_M(H) = C_{C_0}(H) \oplus M\,.$$

Proof. Note that $C_A = C_0 \oplus M$, is a direct consequence of Corollary 6 and Theorem 6.2. We prove the next equality of the lemma.

Let $v \in C_{C_0}(H) \cap C_M(H)$. Then $v \in C_0 \cap M = \{0\}$, hence $v = 0$. Thus $C_{C_0}(H) + C_M(H) = C_{C_0}(H) \oplus C_M(H)$. We now show that $C_{C_0}(H) \oplus C_M(H) = C_{C_A}(H)$. Let $y \in C_{C_0}(H)$ and $z \in C_M(H)$. Then $y + z \in C_0 + M = C_A$ and $(y+z)h = yh+zh = y+z$ for any h in H, which shows $C_{C_0}(H) \oplus C_M(H) \subseteq C_{C_A}(H)$. Conversely assume $v \in C_{C_A}(H)$. Then $v \in C_A = C_0 + M$, which shows $v = y + z$ for some y and z where $y \in C_0$ and $z \in M$. Since $v \in C_{C_0}(H), vh = v$ for any $h \in H$. Thus $(y + z)h = y + z$ implies $yh + zh = y + z$. Since $yh, y \in C_0$ and $zh, z \in M, C_0 \cap M = \{0\}$ implies $yh = h$ and $zh = z$. Thus $y \in C_{C_0}(H)$ and $z \in C_M(H)$, which shows $C_{C_A}(H) \subseteq C_{C_0}(H) + C_M(H)$.

Next we prove that $C_M(H) = M$. Let $h \in H$. By Lemma 6.1, h fixes each element of C_A/C_0. Thus $(m + C_0)h = m + C_0$ for any $m \in M$. Hence $mh + C_0 = m + C_0$ and $mh - m \in C_0$. On the other hand, M is h-invariant. So $mh - m \in M$. Because $M \cap C_0 = \{0\}$, we get $mh = m$ which implies $M = C_M(H)$. □

Combining Lemmas 6.1 and 6.3, we now obtain the following theorem which gives the relationship between $\dim C_{C_0}(H)$ and $\dim C_{C_A}(H)$.

Theorem 6.4. *Let π be a plane of order n such that*

(i) *p divides n exactly to the first power,and*

(ii) *the plane affords a $P - L$ transitivity G.*

Let C_A denote the affine code for $\pi - L$ over Z_p. If H is a subgroup for G such that $(|H|, p) = 1$, then

$$\dim C_{C_A}(H) = \dim C_{C_0}(H) + n\,.$$

Next we prove a theorem which states the relationship of the dimensions of $C_V(H)$ and $C_{C_A}(H)$, where $V = F_p^{n^2}$.

Theorem 6.5. *Let π and H satisfy the hypotheses of Theorem 6.4. Then*

$$\dim C_V(H) = 2\dim C_{C_A}(H) - n = 2\dim C_{C_0}(H) + n\,.$$

Proof. By Theorem 2.2, we have $\dim C_V(H) = \dim C_{C_0}(H) + \dim C_{C_0}^{\perp}(H)$. Theorem 6.4 implies $\dim C_{C_0}^{\perp}(H) = \dim C_{C_0}(H) + n$. Combining these equalities we obtain 6.5. □

Corollary 6.6. *If π and H are as in Theorem 6.4 or Theorem 6.5, then $\dim C_{C_A}(H) = \frac{n}{2}(1 + \frac{n}{|H|})$, where C_A is the affine code of π.*

Proof. Since $C_V(H)$ is spanned by the orbits of H on the n^2 affine points of the plane π and G acts semiregularly on those affine points, we have $\frac{n^2}{|H|}$ point orbits. Thus $\dim C_V(H) = \frac{n^2}{|H|}$. On the other hand, Theorem 6.5 implies $\dim C_V(H) = 2\dim C_{C_A}(H) - n$, which shows $\dim C_{C_A}(H) = \frac{n}{2} + \frac{n^2}{2|H|} = \frac{n}{2}(1 + \frac{n}{|H|})$. □

References

[1] Hall, M., *Combinatorial Theory*, New York-Chichester-Brisbane-Toronto- Singapore: Interscience (1986).

[2] Hughes, D. R. and Piper, F. C., *Projective Planes*, Berlin-Heidelberg- New York: Springer Verlag (1973).

Department of Computer Science and Engineering
North South University, Dhaka, Bangladesh
E-mail: ppd@northsouth.edu