The Nepali Math. Sc. Report
Vol. 26, No. 1 & 2, 2006.

Fixed points in group invariant subspaces

M. KAMRUL HASAN AND PARTHA PRATIM DEY

Abstract: We investigate the subspaces of fixed elements (also known as centralizers) of G-invariant subspaces of $V = \prod_1^n F$ where G is a group of $n \times n$ permutation matrices, F is the Galois field of order p^r for some $r \geq 1$ and $\prod_1^n F$ is the usual canonical vector space of dimension n over F. We are able to characterize these subspaces when $(p, |G|) = 1$. In the case, when p divides $|G|$ all we know is where to look for these subspaces, namely inside the kernel of $\beta = \sum_{g \in G} g$.

Key words : Fixed points, group-invariant subspace, idempotent, permutation matrices.

1. Introduction:

Let F be a finite field of order p^r for some prime p and $r \geq 1$. Then $V = \prod_1^n F$ is a vector space of dimension n over F with basis canonical so that a typical vector has the shape $x = (x_1, \ldots, x_n)$, $x_i \in F$, $i = 1, \ldots, n$. A $[n,s]$ subspace S over F is a space inside V of dimension s. The dual subspace $S^{\perp}$ is the subspace orthogonal to S under the usual scalar product on V. That is $S^{\perp} = \{x \in V \mid (u, x) = \sum_{i=1}^n u_i x_i = 0 \text{ for all } u \in S\}$. Then $S^{\perp}$ is a $[n, n-s]$ subspace because $\dim S + \dim S^{\perp} = \dim V$.

Let G be a group of permutation matrices of order n. A subspace S of V is called G-invariant if $(S)g \subseteq S$.

It is easy to check that if S is G-invariant, so is $S^{\perp}$. Let $s^{\perp} \in S^{\perp}$. Then $(s^{\perp}, s^{\perp}g) = (sg^t, s^{\perp}) = (sg^{-1}, s^{\perp}) = 0$, when $s \in S$ and g^t is transpose of g. Then $s^{\perp}g \in S^{\perp}$ and $S^{\perp}$ is a G-invariant subspace.

2. Characterization of Fixed Points when $(p, |G|) = 1$

Throughout this section we will assume that $F = GF(p^r)$ and $(p, |G|)$. Set $\alpha = \frac{1}{|G|} \sum_{g \in G} g$.

Since $(p, |G|) = 1$, $\frac{1}{|G|} = |G|^{-1}$ exists in F and therefore α exists in the group-ring FG. We now show that α is an idempotent. Let $v \in V = \prod_1^n F$. Then

$$v\alpha^2 = (v\alpha)\alpha = \left(v\frac{1}{|G|}\sum_{g\in G} g\right)\left(\frac{1}{|G|}\sum_{g\in G} g\right) = v\frac{1}{|G|^2}\sum_{g\in G} g\,\Big(\sum_{g\in G} g\Big) = v\frac{1}{|G|^2}\,|G|\sum_{g\in G} g$$

$$= v\frac{1}{|G|}\sum_{g\in G} g = v\alpha \text{ and } \alpha \text{ is indeed an indempotent.}$$

Next we prove a couple of theorems.

Theorem 2.1 : *Let G be a group of* $n\times n$ *permutation matrices and* $F = GF(p^r)$ with $(p,|G|) = 1$. *If S is a G-invariant subspace of* $V = \prod_1^n F$, *then* $S\alpha = \mathrm{Fix}_S(G)$

Proof: We show that $S\alpha \subseteq \mathrm{Fix}_S(G)$. Let $x \in S\alpha$. Then $x = s\alpha$ for some $s \in S$ and

$$s\alpha = s\left(\frac{1}{|G|}\sum_{g\in G} g\right) = \frac{1}{|G|}\sum_{g\in G} sg \in S.$$ Thus $x \in S$. Moreover for any $g \in G$.

$$xg = s\alpha g = s\left(\frac{1}{|G|}\sum_{g\in G} g\right)g = s\frac{1}{|G|}\sum_{g\in G} g = s\alpha = x.$$ Hence $x = \mathrm{Fix}_S(G)$.

We now prove the other containment i.e. $Fix_S(G) \subseteq S\alpha$. Let $s \in Fix_S(G)$. Then

$$s\alpha = s\left(\frac{1}{|G|}\sum_{g\in G} g\right) = \frac{1}{|G|}\sum_{g\in G} sg = \frac{1}{|G|}\sum_{1}^{|G|} s = \frac{1}{|G|}|G|\,s = s.$$ Hence $s = s\alpha \in S\alpha$. ■

Theorem 2.2 : *Let G be a group of* $n\times n$ *permutation matrices and* $F = GF(p^r)$ with $(p,|G|) = 1$. *If S is a G-invariant subspace of* $V = \prod_1^n F$, *then* $(S\alpha)^\perp = \mathrm{Ker}\,\alpha \oplus (S^\perp)\alpha$.

Proof : We prove that $(S\alpha)^\perp \subseteq \mathrm{Ker}\alpha + (S^\perp)\alpha$. Let $x \in (S\alpha)^\perp$. Then $x - s\alpha \in \mathrm{Ker}\,\alpha$ as $\alpha^2 = \alpha$. Let us now check if $x\alpha \in S^\perp\alpha$. Since $x \in (S\alpha)^\perp$, we have $(x, s\alpha) = 0$ for $\forall s \in S$. Then $0 = (x, s\alpha) = (x\alpha^t, s) = (x\alpha, s)$ and $x\alpha \in S^\perp$. By applying α on both sides of $x\alpha \in S^\perp$ and using the idempotence, we obtain $x\alpha \in S^\perp\alpha$. Hence $x = (x - x\alpha) + \mathrm{Ker}\,\alpha$ belongs to $\mathrm{Ker}\,\alpha + (S^\perp)\alpha$. We now want to show that $\mathrm{Ker}\,\alpha + (S^\perp)\,\alpha \subseteq (S\alpha)^\perp$. Let $x \in \mathrm{Ker}\,\alpha + (S^\perp)\alpha$. Then $x = k + s^\perp\alpha$ for some $k \in K$ and $s^\perp \in S^\perp$ and $(x, s\alpha) = (k + s^\perp\alpha,\, s\alpha) = (k\alpha^t + (s^\perp\alpha)\alpha^t, s) =$ $(k\alpha + (s^\perp\alpha)\alpha, s) = (0 + s^\perp\alpha,\, s) = 0$ as $s^\perp\alpha \in S^\perp$. Hence $x \in (S\alpha)^\perp$ and $\mathrm{Ker}\alpha + (S^\perp)\alpha \subseteq (S\alpha)^\perp$. Finally, we want to check if $\mathrm{Ker}\,\alpha \cap (S^\perp)\alpha = \{0\}$. Let $x \in \mathrm{Ker}\,\alpha \cap (S^\perp)\alpha = \{0\}$. Then $x = s^\perp\alpha$. Applying α to both sides, we obtain $x\alpha = (s^\perp)\alpha^2$. Since $x \in \mathrm{Ker}\,\alpha$ and $\alpha^2 = \alpha$, the previous equality yields $0 = s^\perp\alpha$, which in turn yields $0 = x$. Thus $\mathrm{Ker}\,\alpha \cap (S^\perp)\alpha = \{0\}$.

Theorem 2.3. *Let G be a group of* $n\times n$ *permutation matrices and* $F = GF(p^r)$ *with* $(p,|G|) = 1$. If S is a G-invariant subspace of $V = \prod_1^n F$, then $\dim\, Fix_V(G) = \dim Fix_S(G) + \dim Fix_{S^\perp}(G)$

Proof: As $S\alpha \subseteq V\alpha$, we have $\dim V\alpha = \dim S\alpha + \dim((S\alpha)^\perp \cap V\alpha)$. By Theorem (2.2.), $(S\alpha)^\perp = \mathrm{Ker}\alpha \oplus (S^\perp)\alpha$ which shows $(S\alpha)^\perp \cap V\alpha = (\mathrm{Ker}\alpha \cap V\alpha) \oplus ((S^\perp)\alpha \cap V\alpha)$.

Assume $x \in V\alpha \cap \mathrm{Ker}\alpha$. Then $x \in V\alpha$ for some $v \in V$. Thus $x = v\alpha = v\alpha^2 = (v\alpha)\alpha = x\alpha = 0$. This shows $(S\alpha)^{\perp} \cap V\alpha = (S^{\perp})\alpha \cap V\alpha = (S^{\perp})\alpha$. Thus $\dim V\alpha = \dim S\alpha + \dim S^{\perp}\alpha$. Now we apply Theorem (2.1) to obtain $\dim \mathrm{Fix}_V(G) = \dim Fix_S(G) + \dim Fix_{S^{\perp}}(G)$. □

Notice that the theorem above may not work if $(p,|G|) \neq 1$. Consider for example $G = <12\ldots n)>$, a cyclic group of order n generated by permutation $(12\ldots n)$ acting on $V = Z_2^n$. Notice that $Fix_V(G) = \{0\ldots 0, 1\ldots 1\}$ and $S = Fix_V(G)$ is a G-invariant subspace in V. If n is odd i.e. $(p,|G|) = 1$ then $\mathrm{Fix}_{S^{\perp}}(G)$ comprises of zero element only and $\dim Fix_V(G) = \dim Fix_S(G) + \dim Fix_{S^{\perp}}(G) = 1$. But when is even i.e. $(p,|G|) = 2$, $\dim Fix_V(G) = \dim Fix_S(G) = \dim Fix_{S^{\perp}}(G) = 1$ and the equality in Theorem (2.3) fails to hold. Since $\dim Fix_V(G) = \dim Fix_S(G) + \dim Fix_{S^{\perp}}(G)$, one wonders if $Fix_V(G) = Fix_S(G) \oplus Fix_{S^{\perp}}(G)$ holds under the conditions of Theorem (2.3). But one immediately notices that $Fix_S(G) \cap Fix_{S^{\perp}}(G)$ may not always be the zero space. For example, if we let $G = <(123)>, (4)$, $V = \prod_1^n GF(4)$ and $S = <111>$, then $Fix_S(G) = Fix_{S^{\perp}}(G) = S$, and hence $Fix_S(G) \cap Fix_{S^{\perp}}(G)$ is not the zero space. This raises the question : when is then $\mathrm{Fix}_V(G) = Fix_S(G) \oplus Fix_{S^{\perp}}(G)$? The following theorem tries to answer that question.

Theorem 2.4. *Let G be a group of $n \times n$ permutation matrices and $F = GF(p^r)$ with $(p,|G|) = 1$. If S is a G-invariant subspace of $V = \prod_1^n F$, such that $Fix_S(G) \cap Fix_{S^{\perp}}(G) = \{0\}$, then $\mathrm{Fix}_V(G) = Fix_S(G) \oplus Fix_{S^{\perp}}(G)$,*

Proof: Let $x \in Fix_S(G) + Fix_{S^{\perp}}(G)$. Then $x = s + s^{\perp}$ where $s \in Fix_S(G)$ and $s^{\perp} \in Fix_{S^{\perp}}(G)$. Hence $xg = (s + s^{\perp})g = sg + s^{\perp}g = s + s^{\perp} = x$ and $x \in Fix_V(G)$, which follows $Fix_S(G) + Fix_{S^{\perp}}(G) \subseteq Fix_V(G)$. As $(p,|G|) = 1$, by Theorem (2.3), we have $\dim Fix_V(G) = \dim Fix_S(G) + \dim Fix_{S^{\perp}}(G)$.

Since $Fix_S(G) \cap Fix_{S^{\perp}}(G) = \{0\}$, $\dim (Fix_S(G) + Fix_{S^{\perp}}(G)) = \dim Fix_S(G) + \dim Fix_{S^{\perp}}(G)$. Hence $\dim Fix_V(G) = \dim (Fix_S(G) + Fix_{S^{\perp}}(G)$, which yields the desired equality $Fix_V(G) = Fix_S(G) \oplus Fix_{S^{\perp}}(G)$. ■

Corollary (2.5). Lie *G* be a group of *of $n \times n$ permutation matrices and $F = GF(p^r)$ with* $(p,|G|) = 1$. If S is a *G-invariant subspace of $V = \prod_1^n F$, such that $S \cap S^{\perp} = \{0\}$, then $Fix_V(G) = Fix_S(G) \oplus Fix_{S^{\perp}}(G)$.*

Proof: Follows immediately from the theorem above. ■

Notice that condition if $(p,|G|) = 1$ in Theorem (2.4) is a sufficiency condition, not a necessary one. To see this, we consider $G = <(12)(3)(4)>$ acting on $V = Z_2^4$ and $S = \{0000, 0010\}$. One checks that in spite of $(p,|G|) = 2$, $Fix_V(G)$. is still $Fix_S(G) \oplus Fix_{S^{\perp}}(G)$.

3. Characterization of Fixed Points when $(p,|G|) \neq 1$

Finally we consider the case when p divides $|G|$. We set $\beta = \sum_{g \in G} g$ and produce the following theorem, which states that when p divides $|G|$, the fixed points reside inside Ker β.

Theorem. *Let G be a group $n \times n$ permutation matrices and $F = GF(p^r)$ with p dividing $|G|$. If S is a G- invariant subspace of $V = \prod_1^n F$, then $S\beta \subseteq Fix_s(G) \subseteq$ Ker β.*

Proof: We first show that $S\beta \subseteq Fix_S(G)$. Let $v \in S\beta$ i.e. $v = s\beta$ for some $s \in S$. Then $vg = s\beta g = s(\sum_{g \in G} g)g = s\sum_{g \in G} g = s\beta = v$. Hence $v = Fix_s(G)$. To see the other containment i.e. $Fix_S(G) \subseteq$ Ker β, we let $v \in Fix_s(G)$ and apply β on it. Then

$$v\beta = v\sum_{g \in G} g = \sum_{g \in G} vg = \sum_{1}^{|G|} v = |G|v = 0. \quad \blacksquare$$

Notice that the containment $Fix_S(G) \subseteq$ Ker β may not hold if $(p,|G|) = 1$. To see this we consider the following example

Let $G = <(123)(4)>$ and $V = Z_2^4$. Then one checks that

$$\beta = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ and for any $v = (v_1, v_2, v_3, v_4) \in V$, $v\beta = (\sum_{i=1}^3 v_i, \sum_{i=1}^3 v_i, \sum_{i=1}^3 v_i, v_4)$.

Hence $V\beta = \{0000, 0001, 1110, 1111\}$,

On the other hand, $|G| = 3$ and $3 = 1 \pmod 2$, so we have $\beta = \alpha$ and by Theorem (2.1) of the previous section, $v\beta = V\alpha = Fix_V(G)$. Thus $Fix_V(G) = \{0000, 0001, 1110, 1111\}$. But from $v\beta = (\sum_{i=1}^3 v_i, \sum_{i=1}^3 v_i, \sum_{i=1}^3 v_i, v_4)$, we learn that for a vector in V to be in Ker β, the last coordinate must be zero. So the vectors 0001, 1111 in $Fix_V(G)$ with their last coordinate 1 can't be in Ker β. This proves the fact that the containment $s\beta \subseteq Fix_S(G) \subseteq$ Ker β for an arbitrary G-invariant subspace S is specific to the case when p divides $|G|$.

REFERENCES

[1] Hoque K. A., P. P. Dey., *Invariant Linear Codes and their Dimensions*, Proc. Of the International Conference on Information Knowledge Engineering.

[2] Lander E.S., Symmetric Designs : *An Algebraic Approach*, London-New York- New Rochelle-Melbourne-Sydney : Cambridge Press, (1983).

M. KAMRUL HASAN, PARTHA PRATIM DEY
Department of Computer Science & Engineering,
North South University,
Bangladesh.
Email:ppd@northsouth.edu