CODES OF NETS WITH TRANSLATIONS

G. E. Moorhouse
University of Wyoming, Laramie WY 82071

1. Introduction

A **k-net of order** n is an incidence structure consisting of a set $\mathcal{P}$ of n^2 points, together with nk distinguished subsets $\ell_{ij} \subset \mathcal{P}$ called lines $(1 \le i \le k,\ 1 \le j \le n)$, such that

$$|\ell_{ij} \cap \ell_{i'j'}| = \begin{cases} 1 & \text{if } i \ne i'; \\ 0 & \text{if } i = i',\ j \ne j'; \\ n & \text{if } i = i',\ j = j'. \end{cases}$$

Thus the lines are partitioned into k parallel classes $\{\ell_{ij} : 1 \le j \le n\}$, $1 \le i \le k$, and each line has n points. Note that an $(n+1)$-net is the same thing as an affine plane of order n. For any k-net $\mathcal{N}$ and any k'-subset of the parallel classes of $\mathcal{N}$, we obtain a **k'-subnet** $\mathcal{N}' \subseteq \mathcal{N}$ of order n, also with point set $\mathcal{P}$. The description of nets found here is more amenable to our specialized rank computations than to a broader presentation; more general information concerning nets is found in Baer (1939), Beth et al. (1985), Bruck (1951) and (1963), Jungnickel (1990), and Pickert (1975).

We denote the p-rank of a net $\mathcal{N}$ (the p-rank of its incidence matrix) by $\operatorname{rank}_p \mathcal{N}$. In Moorhouse (1990) we proposed the following conjecture, supported by numerous computational examples:

Conjecture 1. *Let $\mathcal{N}_k$ be any k-net of order n, and let $\mathcal{N}_{k-1}$ be any $(k-1)$-subnet thereof. If p is any prime such that $p^2 \nmid n$, then*

$$\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \ge n - k + 1.$$

The only interesting primes are those dividing n, since as shown in Moorhouse (1990), for $k \ge 1$ we have $\operatorname{rank}_p \mathcal{N}_k \le (n-1)k + 1$, in which equality holds if $p \nmid n$. Furthermore Conjecture 1 holds trivially for $k \le 2$, and its validity for $k = 3$ has been shown using the theory of loop characters (see Theorem 5 below).

In Sections 2 and 3 we prove Theorems 2, 3, and Corollary 4.

Theorem 2. *Conjecture 1 holds for 4-nets constructed from $3 \times p$ difference matrices over cyclic groups of prime order p, that is, for 4-nets of prime order p admitting a central translation of order p.*

Theorem 3. *Let $\mathcal{N}_k$ be a translation k-net with abelian translation group $T = G \times G$, $k \geq 2$, and let $\mathcal{N}_{k-1}$ be any $(k-1)$-subnet thereof. Let $\mathbb{F}_p$ be a field of prime order p, and let $\mathcal{A}$ be the augmentation ideal of the group algebra $\mathbb{F}_p[G]$. Then*

$$\operatorname{rank}_p \mathcal{N}_k - \operatorname{rank}_p \mathcal{N}_{k-1} \geq \dim \mathcal{A}^{k-1}.$$

Corollary 4. *Conjecture 1 holds for translation nets with abelian translation groups.*

The values $\dim \mathcal{A}^{k-1}$ are determined by Jennings (1941); see Theorem 11 below. In case $k = 3$, the lower bound of Theorem 3 holds with equality since the subgroup $G_2 = \langle [G, G], G^p \rangle$ of Theorem 11 coincides with the subloop K of Theorem 5. It is hoped that these results may generalize to other nets without the assumption of translations, after replacing group algebras by loop algebras; see Bruck (1944). We are encouraged in this direction by the fact that many of the relevant facts concerning group algebras, including parts of Theorem 11 below, would seem to extend to loop algebras.

The following five additional results are shown in Moorhouse (1990); our reference for loop theory is Bruck (1958).

Theorem 5. *Let G be a loop of order n, and let $\mathcal{N}$ be the corresponding 3-net. Let p be a prime such that $p^e \,||\, n$ (meaning that p^e is the highest power of p dividing n). Then*

$$\operatorname{rank}_p \mathcal{N} = 3n - 2 - s \geq 3n - 2 - e$$

where $p^s = [G : K]$ and K is the unique minimal normal subloop of G such that G/K is an elementary abelian p-group.

Corollary 6. *Let $\mathcal{N}$ be a 3-net of order $n \equiv 2 \mod 4$. If $\mathcal{N}$ is extendable to a 4-net, then* $\operatorname{rank}_2 \mathcal{N} = 3n - 2$.

A 3-net is **cyclic** if it is coördinatized by a cyclic group, or equivalently, if it is obtainable from a Latin square in which all rows are cyclic shifts of the first row.

Theorem 7. *Let G be a loop of order n, with corresponding 3-net $\mathcal{N}$.*

(i) Suppose that n is squarefree (that is, n is a product of distinct primes), or that G is a nilpotent group. Then $\mathcal{N}$ is cyclic if and only if $\operatorname{rank}_p \mathcal{N} = 3n - 3$ *for every prime $p \mid n$.*

(ii) Suppose that G is a nilpotent loop. Then G is generated by a single element, if and only if $\operatorname{rank}_p \mathcal{N} \geq 3n - 3$ *for every prime $p \mid n$.*

Theorem 8. *An explicit basis for the $\mathbb{F}_p$-code of* $\mathrm{AG}(2, p)$ *is obtained by choosing all p lines of some parallel class, followed by any $p-1$ lines from any other parallel class, plus any $p-2$ lines from yet another parallel class, and so on, finally taking 0 lines from the last remaining parallel class; this gives $\frac{1}{2}p(p+1)$ lines in all. In particular, Conjecture 1 holds with equality in the case of subnets of* $\mathrm{AG}(2, p)$.

Actually the final assertion of Theorem 8 is obtainable from Corollary 4 without appeal to the proof in Moorhouse (1990).

Our main interest in Conjecture 1 is due to the following:

1.9 Theorem. *Suppose that Π is a projective plane of order n, where n is squarefree or $n \equiv 2 \mod 4$. If Conjecture 1 holds for n, then n is prime and Π is Desarguesian.*

2. 4-Nets of Prime Order with Translations

A **central** (or 'strict') **translation** of a net $\mathcal{N}$ is an automorphism of $\mathcal{N}$ preserving each parallel class of $\mathcal{N}$, and fixing every line in some parallel class (called the **direction** of the translation). We show how nets with such strict translations may be constructed; see also Beth et al. (1985), Jungnickel (1990).

Suppose that G is a group of order n, and that $\sigma_3, \sigma_4, \ldots, \sigma_k : G \to G$ are bijections such that whenever $i \neq j$, the map $g \mapsto \sigma_i(g)\sigma_j(g)^{-1}$ is also a bijection $G \to G$. Then the sets

$$\ell_{1g} = \{(g, y) : y \in G\}, \quad g \in G,$$
$$\ell_{2g} = \{(x, g) : x \in G\}, \quad g \in G,$$
$$\ell_{ig} = \{(x, g\sigma_i(x)) : x \in G\}, \quad 3 \leq i \leq k, \ g \in G$$

form a k-net $\mathcal{N}$ of order n on the point set $\mathcal{P} = G \times G$. For $h \in G$ define $\tau_h : \mathcal{P} \to \mathcal{P}$ by $\tau_h(x, y) = (x, hy)$. Then τ_h maps $\ell_{1g} \mapsto \ell_{1g}$, $\ell_{ig} \mapsto \ell_{i,hg}$ for $2 \leq i \leq k$, and thus $\mathcal{N}$ admits a group of central translations whose common direction is the first parallel class $\{\ell_{1g} : g \in G\}$. Moreover every net with the latter property is constructible in this way. It is customary to specify $\mathcal{N}$ by the *difference matrix*

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \sigma_3(g_1) & \sigma_3(g_2) & \cdots & \sigma_3(g_n) \\ \sigma_4(g_1) & \sigma_4(g_2) & \cdots & \sigma_4(g_n) \\ \vdots & \vdots & & \vdots \\ \sigma_k(g_1) & \sigma_k(g_2) & \cdots & \sigma_k(g_n) \end{pmatrix}$$

where $g_1, g_2, \ldots, g_n$ are the elements of G in some order (see Beth et al. (1985), Jungnickel (1990)); however, the language of difference matrices will not be required for our presentation. We also remark that there is no loss of generality in assuming that $\sigma_3(g) = g$ for all $g \in G$, and $\sigma_i(g_1) = g_1 = 1$ for all i.

We develop some notation which will be useful in handling codes of such nets. Let $\mathbb{F}_p^{\mathcal{P}}$ be the n^2-dimensional vector space over $\mathbb{F}_p$ consisting of all functions $\mathcal{P} \to \mathbb{F}_p$. To each line ℓ_{ig} of $\mathcal{N}$ there corresponds the characteristic function

$$\chi_{ig} : \mathcal{P} \to \mathbb{F}_p, \qquad \chi_{ig}(x, y) = \begin{cases} 1, & (x, y) \in \ell_{ig}, \\ 0, & (x, y) \notin \ell_{ig}. \end{cases}$$

We may define the $\mathbb{F}_p$-code of $\mathcal{N}$ as

$$\mathcal{C}_p(\mathcal{N}) = \sum_{i=1}^{k} \sum_{g \in G} \mathbb{F}_p \chi_{ig},$$

which is the subspace of $\mathbb{F}_p^{\mathcal{P}}$ spanned by the characteristic functions of the line sets. The p-rank of $\mathcal{N}$ is then

$$\operatorname{rank}_p \mathcal{N} = \dim \mathcal{C}_p(\mathcal{N}).$$

If $1 \le i_0 \le k$, then a $(k-1)$-subnet $\mathcal{N}_{k-1} \subset \mathcal{N}$ is formed by excluding the i_0-th parallel class of $\mathcal{N}$, and the $\mathbb{F}_p$-code of $\mathcal{N}_{k-1}$ is

$$\mathcal{C}_p(\mathcal{N}_{k-1}) = \sum_{\substack{1 \le i \le k \\ i \ne i_0}} \sum_{g \in G} \mathbb{F}_p \chi_{ig}.$$

Clearly we have:

Lemma 10. *With the above notation, we have* $\operatorname{rank}_p \mathcal{N} - \operatorname{rank}_p \mathcal{N}_{k-1} = n - \dim \mathcal{V}$, *where* $\mathcal{V}$ *is the vector space consisting of all sequences* $(a_g : g \in G)$, *where* $a_g \in \mathbb{F}_p$, *such that* $\sum_{g \in G} a_g \chi_{i_0 g} \in \mathcal{C}_p(\mathcal{N}_{k-1})$.

For a group G, recall that the **augmentation ideal** of the group algebra $\mathbb{F}_p[G]$ is the ideal defined by

$$\mathcal{A} = \left\{ \sum_{g \in G} a_g g \in \mathbb{F}_p[G] \ : \ \sum_{g \in G} a_g = 0 \right\}.$$

The j-th power of $\mathcal{A}$ is the ideal spanned over $\mathbb{F}_p$ by

$$\big\{ (1-x_1)(1-x_2)\dots(1-x_j) \ : \ x_1, x_2, \dots, x_j \in G \big\}.$$

In case G is cyclic of order p, it is well known that $\mathcal{A}$ is nilpotent, and that the *only* ideals of $\mathbb{F}_p[G]$ are those in the chain

$$\mathbb{F}_p[G] \supset \mathcal{A} \supset \mathcal{A}^2 \supset \dots \supset \mathcal{A}^{p-1} \supset \mathcal{A}^p = 0,$$

so A^{p-j} is the unique ideal of $\mathbb{F}_p[G]$ of dimension j. It also follows that $\operatorname{Ann} \mathcal{A}^j = \mathcal{A}^{p-j}$ where $\operatorname{Ann} \mathcal{B} = \big\{ \alpha \in \mathbb{F}_p[G] \ : \ \alpha\beta = 0 \ \text{ for all } \beta \in \mathcal{B} \big\}$ is the **annihilator** of an arbitrary ideal $\mathcal{B} \subseteq \mathbb{F}_p[G]$.

Proof of Theorem 2. Let G be a cyclic group of prime order p, and let $\mathcal{N}$ be 4-net of order p with a central translation of order p. Thus we may assume that $\mathcal{N}$ is constructed as above with $k=4$, $\sigma_3 = \text{identity}$, $\sigma_4 = \sigma$, $\sigma(1) = 1$. Corresponding to the lines ℓ_{ig} defined as above, we have the characteristic functions

$$\chi_{1g}(x,y) = \delta_{x,g}, \quad \chi_{2g}(x,y) = \delta_{y,g}, \quad \chi_{3g}(x,y) = \delta_{gx,y}, \quad \chi_{4g}(x,y) = \delta_{g\sigma(x),y}$$

for $g \in G$. With Lemma 10 in mind, for given scalars $a_{ig} \in \mathbb{F}_p$ we define $\chi = \sum_{i=1}^{4} \sum_{g \in G} a_{ig}\chi_{ig} \in \mathbb{F}_p^{\mathcal{P}}$, and suppose that $\chi = 0$. Then for arbitrary $x, y \in G$ we have $0 = \chi(1,1) - \chi(x,1) - \chi(1,y) + \chi(x,y)$, or

$$0 = a_{3,1} - a_{3,x^{-1}} - a_{3,y} + a_{3,x^{-1}y} + a_{4,1} - a_{4,\sigma(x)^{-1}} - a_{4,y} + a_{4,\sigma(x)^{-1}y}\,.$$

Or writing $\alpha_i = \sum_{y \in G} a_{i,y} y \in \mathbb{F}_p[G]$ for $i = 3, 4$, we obtain

$$\begin{aligned}\alpha_3(1-x) + \alpha_4(1-\sigma(x)) &= \sum_{y \in G} \big(a_{3,y} - a_{3,x^{-1}y} + a_{4,y} - a_{4,\sigma(x)^{-1}y}\big)y \\ &= \big(a_{3,1} - a_{3,x^{-1}} + a_{4,1} - a_{4,\sigma(x)^{-1}}\big) \sum_{y \in G} y \\ &\in \mathbb{F}_p\gamma\end{aligned}$$

for all $x \in G$, where $\mathbb{F}_p\gamma = \mathcal{A}^{p-1}$ is the one-dimensional ideal of $\mathbb{F}_p$ spanned by $\gamma = \sum_{g \in G} g \in \mathbb{F}_p[G]$. Since $x \in G$ is arbitrary, we may replace x by z or by xz, where $x, z \in G$ are both arbitrary, so that

$$\begin{aligned}\big[\alpha_3(1-x) + \alpha_4(1-\sigma(x))\big]x^{-1} &\in \mathbb{F}_p\gamma, \\ \alpha_3(1-z) + \alpha_4(1-\sigma(z)) &\in \mathbb{F}_p\gamma, \\ \big[\alpha_3(1-xz) + \alpha_4(1-\sigma(xz))\big]\big(-x^{-1}\big) &\in \mathbb{F}_p\gamma.\end{aligned}$$

Adding the above relations yields

$$\alpha_4\big(1 - \sigma(x)x^{-1} - \sigma(z) + \sigma(xz)x^{-1}\big) \in \mathbb{F}_p\gamma$$

for all $x, z \in G$. This means that $\alpha_4\mathcal{B} \subseteq \mathbb{F}_p\gamma$ where $\mathcal{B} \subset \mathbb{F}_p[G]$ is the ideal generated by all expressions of the form

$$1 - \sigma(x)x^{-1} - \sigma(z) + \sigma(xz)x^{-1} = \big(1 - \sigma(x)x^{-1}\big)\big(1 - \sigma(z)\big) + \big(\sigma(xz) - \sigma(x)\sigma(z)\big)x^{-1}$$

for $x, z \in G$. We may assume that $\sigma(xz) \neq \sigma(x)\sigma(z)$ for some $x, z \in G$; otherwise $\sigma \in \operatorname{Aut} G$, in which case as will appear in Section 3, $\mathcal{N}$ is a translation 4-net of order p and hence is a 4-subnet of $\mathrm{AG}(2,p)$, and the result follows by Corollary 4 (which will be proved in Section 3), or by Theorem 8 (proved in Moorhouse (1990)).

Thus $\mathcal{B} \not\subseteq \mathcal{A}^2$ and $\mathcal{B} \subseteq \mathcal{A}$, and so by the preceding remarks, we obtain $\mathcal{B} = \mathcal{A}$. Now $\alpha_4\mathcal{A} \subseteq \mathbb{F}_p\gamma$ is equivalent to $\alpha_4 \in \operatorname{Ann}\mathcal{A}^2 = \mathcal{A}^{p-2}$, so by Lemma 10,

$$\operatorname{rank}_p \mathcal{N} - \operatorname{rank}_p \mathcal{N}_3 \geq p - \dim \mathcal{A}^{p-2} = p - 2$$

where $\mathcal{N}_3$ is the 3-subnet of $\mathcal{N}$ formed by omitting the fourth parallel class. But $\operatorname{rank}_p \mathcal{N}_3 = 3p-3$ by Theorem 5, and so $\operatorname{rank}_p \mathcal{N} \geq 4p-5$. Now for *any* 3-subnet $\mathcal{N}' \subset \mathcal{N}$ we have $\operatorname{rank}_p \mathcal{N}' \leq 3p-2$ by the remarks following Conjecture 1, and so

$$\operatorname{rank}_p \mathcal{N} - \operatorname{rank}_p \mathcal{N}' \geq (4p-5) - (3p-2) = p-3$$

as required. □

3. Translation Nets

A net $\mathcal{N}$ is a **translation net** if it admits an automorphism group T (called a **translation group** of $\mathcal{N}$) which acts regularly (= sharply transitively) on the points of $\mathcal{N}$, and preserving each parallel class of $\mathcal{N}$. For a given translation net $\mathcal{N}$, the translation group T need not be abelian, or even unique. We describe how the most general translation nets with abelian translation groups are constructed, then proceed to prove Theorem 3 and Corollary 4. For more on translation nets, see Beth et al. (1985), Jungnickel (1990).

Suppose that G is a group of order n, with bijections σ_3, σ_4, ..., σ_k as in Section 2, with corresponding k-net $\mathcal{N}$ of order n defined as before. But now assume additionally that σ_3, σ_4, ..., σ_k are homomorphisms, so that $\sigma_3, \sigma_4, \ldots, \sigma_k \in \operatorname{Aut} G$. For $u, v \in G$ define $\tau_{uv} : \mathcal{P} \to \mathcal{P}$ by $\tau_{uv}(x,y) = (ux, vy)$. Then τ_{uv} maps $\ell_{1g} \mapsto \ell_{1,ug}$, $\ell_{2g} \mapsto \ell_{2,vg}$, $\ell_{ig} \mapsto \ell_{i,vg\sigma_i(u)^{-1}}$ for $3 \leq i \leq k$, so that $\mathcal{N}$ is a translation net with translation group $T = \{\tau_{uv} : u, v \in G\} \cong G \times G$. This construction does not yield the most general translation net; however every translation net with an *abelian* translation group is constructible in this way. Indeed, in proving Theorem 3 we shall assume that G is abelian, although this hypothesis is not required in the foregoing construction of $\mathcal{N}$, and so perhaps might be avoidable.

In order for Theorem 3 to be useful, for a given group algebra $\mathbb{F}_p[G]$ we shall require a knowledge of the dimensions of various powers of its augmentation ideal. Fortunately these dimensions may be derived from G by purely group-theoretic methods, as shown by Jennings (1941). Although the following result is stated in Jennings (1941) and Passman (1977) only for p-groups (when $\mathcal{A}$ is nilpotent, and coincides with the radical of $\mathbb{F}_p[G]$), nevertheless the following holds for general n, by the same proof:

Theorem 11 (Jennings, 1941)**.** *For $i \geq 1$ define $G_i = \{g \in G : g - 1 \in \mathcal{A}^i\}$. Then the following statements hold:*

(i) *$G = G_1 \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq \ldots$ is a sequence of characteristic subgroups of G, such that G_i/G_{i+1} is an elementary abelian p-group.*

(ii) *The subgroups G_i may be recursively determined by $G_1 = G$ and $G_i = \langle [G, G_{i-1}], G^p_{\lceil i/p \rceil} \rangle$ for $i \geq 2$, where $\lceil i/p \rceil$ is the least integer $\geq i/p$, and $G^p_{\lceil i/p \rceil}$ consists of all p-th powers of the elements of $G_{\lceil i/p \rceil}$.*

(iii) *$\dim\left(\mathcal{A}^j/\mathcal{A}^{j+1}\right)$ equals the coefficient of X^j in the expansion of*

$$\prod_{i=1}^{\infty} \left(1 + X^i + X^{2i} + \ldots + X^{(p-1)i}\right)^{e_i}$$

where $p^{e_i} = |G_i/G_{i+1}|$.

Observe that the above product is finite since $e_i = 0$ for i sufficiently large.

We shall also require the following, in which $\operatorname{Ann}\mathcal{B}$ is the annihilator of $\mathcal{B}$:

3.2 Lemma. *If $\mathcal{B}$ is any ideal of $\mathbb{F}_p[G]$, then $\dim \mathcal{B} + \dim \operatorname{Ann}\mathcal{B} = n$.*

Proof. $\operatorname{Ann}\mathcal{B}$ is the orthogonal complement of $\mathcal{B}$ with respect to the nondegenerate symmetric bilinear form $\left(\sum_{g\in G} a_g g\,,\, \sum_{g\in G} b_g g\right) = \sum_{g\in G} a_g b_{g^{-1}}$ defined on $\mathbb{F}_p[G]$. □

Actually, Lemma 3.2 will be required only for $\mathcal{B}$ a power of the augmentation ideal $\mathcal{A}$, in which case an explicit basis may be obtained for $\operatorname{Ann}\mathcal{B}$ if desired; see Hill (1970).

Proof of Theorem 3. The proof is trivial for $k = 2$; hence assume that $k \geq 3$. We begin with the same steps as the proof of Theorem 2 in Section 2. The characteristic functions of the line sets are

$$\chi_{1g}(x, y) = \delta_{x,g}, \quad \chi_{2g}(x, y) = \delta_{y,g}, \quad \chi_{ig}(x, y) = \delta_{g\sigma_i(x),y}$$

for $3 \leq i \leq k$; $g \in G$. We may assume that $\mathcal{N}_{k-1}$ consists of all but the k-th parallel class $\{\ell_{kg} : g \in G\}$; this is more evident from Beth et al. (1985) and Jungnickel (1990) than from the latter expressions for the χ_{ig}'s, which unfortunately make the first two parallel classes appear different by construction. For given scalars $a_{ig} \in \mathbb{F}_p$ we define $\chi = \sum_{i=1}^{k} \sum_{g\in G} a_{ig}\chi_{ig} \in \mathbb{F}_p^{\mathcal{P}}$, and suppose that $\chi = 0$. Then for arbitrary $x, y \in G$ we have

$$\begin{aligned} 0 &= \chi(1,1) - \chi(x,1) - \chi(1,y) + \chi(x,y) \\ &= \sum_{i=3}^{k} \left(a_{i,1} - a_{i,\sigma_i(x)^{-1}} - a_{i,y} + a_{i,\sigma_i(x)^{-1}y}\right). \end{aligned}$$

Letting $\alpha_i = \sum_{y\in G} a_{iy}y \in \mathbb{F}_p[G]$, we obtain

$$\sum_{i=3}^{k} \alpha_i\big(1-\sigma_i(x)\big) = \sum_{i=3}^{k}\sum_{y\in G}\big(a_{i,y}-a_{i,\sigma_i(x)^{-1}y}\big)y = \Big(\sum_{i=3}^{k}\big(a_{i,1}-a_{i,\sigma_i(x)^{-1}}\big)\Big)\sum_{y\in G} y \;\in\; \mathbb{F}_p\gamma$$

for all $x \in G$. Replacing x by x_1, x_2 or $x_1x_2 \in G$ gives

$$\begin{aligned}
\sum_{i=3}^{k} \alpha_i\big(1-\sigma_i(x_1)\big)\sigma_3(x_1)^{-1} &\in \mathbb{F}_p\gamma,\\
\sum_{i=3}^{k} \alpha_i\big(1-\sigma_i(x_2)\big) &\in \mathbb{F}_p\gamma,\\
\sum_{i=3}^{k} \alpha_i\big(1-\sigma_i(x_1x_2)\big)\big(-\sigma_3(x_1)^{-1}\big) &\in \mathbb{F}_p\gamma.
\end{aligned}$$

Adding these relations yields

$$\sum_{i=4}^{k} \alpha_i\big(1-\sigma_3(x_1)^{-1}\sigma_i(x_1)\big)\big(1-\sigma_i(x_2)\big) \;\in\; \mathbb{F}_p\gamma$$

for all $x_1, x_2 \in G$. Again replacing x_2 by $x_2, x_3, x_2x_3 \in G$ and combining yields

$$\sum_{i=5}^{k} \alpha_i\big(1-\sigma_3(x_1)^{-1}\sigma_i(x_1)\big)\big(1-\sigma_4(x_2)^{-1}\sigma_i(x_2)\big)\big(1-\sigma_i(x_3)\big) \;\in\; \mathbb{F}_p\gamma$$

for all $x_1, x_2, x_3 \in G$. Continuing in this way, we eventually obtain

$$\begin{aligned}
\alpha_k\big(1-\sigma_3(x_1)^{-1}\sigma_k(x_1)\big)\big(1-\sigma_4(x_2)^{-1}\sigma_k(x_2)\big)\ldots&\\
\ldots\big(1-\sigma_{k-1}(x_{k-3})^{-1}\sigma_k(x_{k-3})\big)\big(1-\sigma_k(x_{k-2})\big) &\;\in\; \mathbb{F}_p\gamma
\end{aligned}$$

for all $x_1, x_2, \ldots, x_{k-2} \in G$. Since the maps $G \to G,\ x \mapsto \sigma_i(x)^{-1}\sigma_k(x)$ are bijective for $3 \le i < k$, we have $\alpha_k\mathcal{A}^{k-2} \subseteq \mathbb{F}_p\gamma$, or equivalently, $\alpha_k \in \operatorname{Ann}\mathcal{A}^{k-1}$. By Lemma 3.2 we have $\dim \operatorname{Ann}\mathcal{A}^{k-1} = n - \dim \mathcal{A}^{k-1}$, and so the result follows by Lemma 10. □

Proof of Corollary 4. By assumption, $p^2 \nmid n$. By Theorem 11, we have $\dim \mathcal{A}^{k-1} = \max\{n-k+1,\ n-p^s\}$ where $p^s = p$ if G has a normal subgroup of index p; $p^s = 1$ otherwise. The result follows from Theorem 3. □

R. Baer (1939), Nets and groups, *Trans. AMS* **46**, 110–141.

T. Beth, D. Jungnickel and H. Lenz (1985), *Design Theory*, Bibliographisches Institut, Zürich.

R. H. Bruck (1944), Some results in the theory of linear non-associative algebras, *Trans. AMS* **56**, 141–199.

R. H. Bruck (1951), Finite nets I. Numerical invariants, *Can. J. Math.* **3**, 94–107.

R. H. Bruck (1958), *A Survey of Binary Systems,* Springer-Verlag, Berlin.

R. H. Bruck (1963), Finite nets II. Uniqueness and embedding, *Pacific J. Math.* **13**, 421–457.

E. T. Hill (1970), The annihilator of radical powers in the modular group ring of a p-group, *Proc. AMS* **25**, 811–815.

S. A. Jennings (1941), The structure of the group ring of a p-group over a modular field, *Trans. AMS* **50**, 175–185.

D. Jungnickel (1990), Latin squares, their geometries and their groups. A survey, *Coding Theory and Design Theory Part II: Design Theory* (ed. D. Ray-Chaudhuri), Springer-Verlag, pp. 166–225.

G. E. Moorhouse (1990), Bruck nets, codes, and characters of loops, *Designs, Codes and Cryptography* (to appear).

D. S. Passman (1977), *The Algebraic Structure of Group Rings,* Wiley, New York.

G. Pickert (1975), *Projektive Ebenen,* 2nd edition, Springer-Verlag, Berlin.