Proc. Marshall Hall Conf., Vermont, Sept. 1990

ON CODES OF BRUCK NETS AND PROJECTIVE PLANES

G. Eric Moorhouse

Dedicated to the memory of Marshall Hall, Jr.

Abstract. We summarize some recent results concerning codes of finite nets, which are of interest in the search for non-Desarguesian planes of prime order and certain composite orders. The p-ranks of 3-nets are determined by algebraic properties of the defining loops, and p-ranks of k-nets admitting certain abelian groups of translations are bounded by algebraic properties of the groups. Here we discuss the relationship between the p-ranks of two k-nets, and the p-rank of their direct product.

1. Introduction

The application of coding theory to the study of finite projective planes, has traditionally involved (i) an attempt to determine, at least partially, the weight distribution of the code of the plane, and (ii) a consideration of possible 'shapes' of small-weight codewords in the plane. There are intelligent reasons for following this approach: for example the extended $\mathbb{F}_p$-code of a projective plane of order n, is self-dual when $p \,||\, n$, whence the MacWilliams relations impose restrictions on the weight distribution. Thus, for example, the determination of the complete binary weight enumerator of any projective plane of order 10 by the combined work of MacWilliams et al [12] and Lam et al [9], led to the eventual announcement of the non-existence of a projective plane of order 10 by Lam et al [10].

However this approach has failed to prove any general results concerning non-existence or classification of planes of suitable orders. Weight distributions are hard to determine! Consider that at the time of writing, the author is unaware that a determination has been made of weight enumerators for any planes of orders exceeding 8. We suggest therefore a different approach to studying the code of a plane, namely the consideration of the contribution of each successive parallel class of an affine plane (or, more generally, a net) to the total p-rank. Some justification for this approach is offered by the following result.

Theorem 1 ([13]). *An explicit basis for the $\mathbb{F}_p$-code of* 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 (i.e. $\frac{1}{2}p(p+1)$ lines in all).*

The fact that the p-rank of AG$(2,p)$ is $\frac{1}{2}p(p+1)$ is well-known; however the only standard proof of this fact (eg. [11]) relies on the theory of invariant factors (or elementary divisors) of matrices, a 'non-constructive' proof in that it supplies no explicit basis. The arbitrariness in the choice of lines from successive parallel classes in forming our basis, is a special feature of desarguesian nets, in which the 'layers' of the code may be viewed as MDS codes of length p, as shown in [13]; this feature has no analogue for general nets, as computational examples of the author show. However for general nets of order n with $p \,||\, n$, the author has conjectured that the contribution of the k-th parallel class to the overall p-rank, is at least $n-k+1$; we express this more precisely below as the Main Conjecture. Theorem 1 guarantees that desarguesian nets of prime order satisfy this conjectured lower bound, with equality.

Recall that a **k-net of order** n is an incidence structure consisting of n^2 points and nk distinguished subsets called lines, such that

(i) every line has exactly n points;
(ii) parallelism (the property of being either equal or disjoint) is an equivalence relation on the lines;
(iii) there are k parallel classes, each consisting of n lines, and
(iv) any two non-parallel lines meet exactly once.

(See [1], [3], [5], [8].) Thus an $(n+1)$-net of order n is the same thing as an affine plane of order n. The p-rank of a k-net $\mathcal{N}$ of order n, denoted $\operatorname{rank}_p \mathcal{N}$, is the p-rank of its point-line incidence matrix. In [13] we posed the following conjecture, substantiated by numerous computational examples:

Main Conjecture (MC). *Let $\mathcal{N}_k$ be any k-net of order n, and let $\mathcal{N}_{k-1}$ be any $(k-1)$-subnet thereof (i.e. a $(k-1)$-net of order n obtained by omitting one of the k parallel classes of $\mathcal{N}_k$). If p is any prime such that $p \,||\, n$, then*

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

Our main interest in this investigation is that the validity of MC would imply that any projective plane of order $n \equiv 2 \mod 4$, or of *squarefree* order n (i.e. n is a product of distinct primes) is in fact desarguesian of prime order; the reason for this is found in [13]. Combining results of [13] and [14], we have:

Theorem 2. *MC holds in each of the following special cases:*

(i) for $k \leq 3$;

(ii) for translation nets with abelian translation groups; and

(iii) for 4-nets of prime order p with a central translation, i.e. for 4-nets constructible from $3 \times p$ difference matrices over a group of prime order p.

In proving Theorem 2(iii) we used the uniseriality of $\mathbb{F}_p[G]$ for $|G| = p$; hence a generalization to $|G| = n$ for $p \,||\, n$ is not immediately apparent. The case of 3-nets in Theorem 2(i), follows directly from the following result shown in [13] using the theory of loop characters:

Theorem 3. *Let G be a loop of order n, and let $\mathcal{N}$ be the corresponding 3-net. Let p be a prime such that $p^e \,||\, n$ (i.e. 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.

Using Theorem 3, in [13] we are able to characterize certain 3-nets, in particular those of squarefree order, by their p-ranks. Also Theorem 2(ii) follows from the following bound proven in [14], which in particular applies to subnets of translation planes:

Theorem 4. *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 $\mathcal{A}$ be the augmentation ideal of the group algebra $\mathbb{F}_p[G]$. Then*

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

The latter dimensions $\dim \mathcal{A}^{k-1}$ may be determined directly from the structure of G, as in [6].

In Section 2 we prove the following, which supplies some additional support for MC:

Theorem 5. *A minimal counterexample to MC is not a direct product of k-nets of smaller orders. That is, if $\mathcal{N}_k$ and $\mathcal{N}'_k$ are k-nets of orders n and n' resp. such that $p \,||\, n$ and $p \nmid n'$, and if MC holds for $\mathcal{N}_k$, then MC holds also for any direct product $\mathcal{N}_k \times \mathcal{N}'_k$ (a k-net of order nn', where $p \,||\, nn'$).*

Our proof of Theorem 5 uses only linear algebra, unlike the previous results which use loop characters and group algebras. At this stage we are not sure whether an all-out assault on MC should employ ordinary linear algebra, or deeper properties of loops and quasigroups. But there is some hope that a generalization of Theorem 3 may be possible for k-nets with $k \geq 3$: such nets correspond to suitably 'joined' quasigroups with left identity, and for such structures there is available a theory of ordinary characters [7], and a homomorphism theory (see [4]).

2. Direct Products of Nets

Given two k-nets, $\mathcal{N}_k$ of order n and $\mathcal{N}'_k$ of order n', we proceed to describe how a k-net of order nn' may be constructed, called a **direct product** of $\mathcal{N}_k$ and $\mathcal{N}'_k$; see [3] for details. Let the point sets of $\mathcal{N}_k$, $\mathcal{N}'_k$ be denoted by $\mathcal{P}$, $\mathcal{P}'$ respectively, and the parallel classes of lines by $\{\ell_{ir} : 1 \leq r \leq n\}$, $\{\ell'_{is} : 1 \leq s \leq n'\}$, $1 \leq i \leq k$, resp. Then $\{\ell_{ir} \times \ell_{is} : 1 \leq r \leq n,\ 1 \leq s \leq n'\}$, for $1 \leq i \leq k$, are the parallel classes of lines of a k-net of order nn' with point set $\mathcal{P} \times \mathcal{P}'$. We denote this net by $\mathcal{N}_k \times \mathcal{N}'_k$, although it depends in general not simply on $\mathcal{N}_k$ and $\mathcal{N}'_k$, but also on the ordering of parallel classes within $\mathcal{N}_k$ and within $\mathcal{N}'_k$.

With the above notation, and with no assumption on what power of p divides n or n', we have the following:

Lemma 6. $$nn' - \operatorname{rank}_p\left(\mathcal{N}_k \times \mathcal{N}'_k\right) + \operatorname{rank}_p\left(\mathcal{N}_{k-1} \times \mathcal{N}'_{k-1}\right) \leq \Big(n - \operatorname{rank}_p \mathcal{N}_k + \operatorname{rank}_p \mathcal{N}_{k-1}\Big)\Big(n' - \operatorname{rank}_p \mathcal{N}'_k + \operatorname{rank}_p \mathcal{N}'_{k-1}\Big).$$

We offer some remarks before proving Lemma 6. Firstly, if $p \nmid n'$ then $n' - \operatorname{rank}_p \mathcal{N}'_k + \operatorname{rank}_p \mathcal{N}'_{k-1} = 1$ by [13,Prop.2.1], and so it is clear that Theorem 5 follows from Lemma 6. Secondly, as evidence of the 'tightness' of the inequality in Lemma 6, we point out that

equality holds in certain cases, for example when $p \nmid nn'$ (again by [13,Prop.2.1]), or when $k \leq 3$. To verify equality when $k = 3$, if $\mathcal{N}_3$ and $\mathcal{N}_3'$ are coördinatized by loops G and G' respectively, then observe that $\mathcal{N}_3 \times \mathcal{N}_3'$ is coördinatized by $G \times G'$, and apply Theorem 3.

We next establish notation for the codes of the relevant nets, and proceed to prove Lemma 6. Let $\mathbb{F}_p^{\mathcal{P}}$ denote the set of all functions $\mathcal{P} \to \mathbb{F}_p$, considered as an n^2-dimensional vector space over $\mathbb{F}_p$. Let $\chi_{ir} \in \mathbb{F}_p^{\mathcal{P}}$ be the characteristic function of ℓ_{ir}, i.e.

$$\chi_{ir}(P) = \begin{cases} 1, & P \in \ell_{ir}; \\ 0, & P \in \mathcal{P},\ P \notin \ell_{ir}. \end{cases}$$

For $1 \leq i \leq k$, let X_i be the n-dimensional subspace of $\mathbb{F}_p^{\mathcal{P}}$ spanned by the characteristic functions from the i-th parallel class of $\mathcal{N}_k$, i.e.

$$X_i = \mathbb{F}_p\chi_{i1} \oplus \mathbb{F}_p\chi_{i2} \oplus \ldots \oplus \mathbb{F}_p\chi_{in}.$$

Then the $\mathbb{F}_p$-code of $\mathcal{N}_k$ is

$$\mathcal{C}_p(\mathcal{N}_k) = \sum_{i=1}^{k} \sum_{r=1}^{n} \mathbb{F}_p\chi_{ir} = \sum_{i=1}^{k} X_i.$$

We may suppose that $\mathcal{N}_{k-1}$ includes just the *first* $k-1$ parallel classes of $\mathcal{N}_k$, so that $\mathcal{C}_p(\mathcal{N}_{k-1}) = \sum_{i=1}^{k} X_i$. In obvious similar notation for the second k-net, we have

$$\mathcal{C}_p(\mathcal{N}_k') = \sum_{i=1}^{k} \sum_{s=1}^{n'} \mathbb{F}_p\chi_{is}' = \sum_{i=1}^{k} X_i'.$$

The natural identification of $\mathbb{F}_p^{\mathcal{P}\times\mathcal{P}'}$ with $\mathbb{F}_p^{\mathcal{P}} \otimes \mathbb{F}_p^{\mathcal{P}'}$ gives

$$\mathcal{C}_p(\mathcal{N}_k \times \mathcal{N}_k') = \sum_{i=1}^{k} X_i \otimes X_i'.$$

By [2] we have

$$\begin{aligned} \left[\Big(\sum_{i=1}^{k-1} X_i\Big) \cap X_k\right] \otimes \left[\Big(\sum_{j=1}^{k-1} X_j'\Big) \cap X_k'\right] &= \left[\Big(\sum_{i=1}^{k-1} X_i\Big) \otimes \Big(\sum_{j=1}^{k-1} X_j'\Big)\right] \cap \left[X_k \otimes X_k'\right] \\ &\supseteq \Big(\sum_{i=1}^{k-1} X_i \otimes X_i'\Big) \cap \Big(X_k \otimes X_k'\Big). \end{aligned} \tag{1}$$

The dimension of the latter subspace is

$$\begin{aligned} &\dim\Big(\sum_{i=1}^{k-1} X_i \otimes X_i'\Big) + \dim\Big(X_k \otimes X_k'\Big) - \dim\Big(\sum_{i=1}^{k} X_i \otimes X_i'\Big) \\ &\qquad = \operatorname{rank}_p\big(\mathcal{N}_{k-1} \times \mathcal{N}_{k-1}'\big) + nn' - \operatorname{rank}_p\big(\mathcal{N}_k \times \mathcal{N}_k'\big). \end{aligned}$$

Similar expressions for the dimension on the left side of (1) yield the desired result. □

REFERENCES

[1] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, Zürich, 1985.

[2] N. Bourbaki, *Elements of Mathematics. Algebra I, Chapters 1-3*, Springer-Verlag, 1989, p. 306.

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

[4] ————————, *A Survey of Binary Systems*, Springer-Verlag, Berlin, 1958.

[5] ————————, "Finite nets II. Uniqueness and embedding", *Pacific J. Math.* **13** (1963), 421–457.

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

[7] K. W. Johnson and J. D. H. Smith, "Characters of finite quasigroups. I", *Europ. J. Comb.* **5** (1984) no. 1, 43–50.

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

[9] C. W. H. Lam, L. Thiel and S. Swiercz, "The nonexistence of code words of weight 16 in a projective plane of order 10", *J. Comb. Theory Ser. A* **42** (1986), 207–214.

[10] ————————, "The non-existence of finite projective planes of order 10", *Canad. J. Math* **41** (1989), 1117–1123.

[11] E. S. Lander, *Symmetric Designs: an Algebraic Approach*, Lond. Math. Soc. Lecture Notes #74, Cambridge Univ. Press, 1983.

[12] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson, "On the existence of a projective plane of order 10", *J. Comb. Theory Ser. A* **14** (1973), 66–78.

[13] G. E. Moorhouse, "Bruck nets, codes, and characters of loops", *Designs, Codes and Cryptography* **1** (1991), 7–29.

[14] ————————, "Codes of nets with translations", in *Advances in Finite Geometries and Designs*, Proc. Isle of Thorns Conf. 1990 (ed. J. W. P. Hirschfeld et al), Oxford Univ. Press, 1991, pp. 327–336.