Designs, Codes and Cryptography, 4, 123–128 (1994)

A Coding Theoretic Solution to the 36 Officer Problem

STEVEN T. DOUGHERTY
Department of Mathematics, University of Scranton, Scranton, PA 18510

Communicated by D. Jungnickel
Received May 27, 1992; Revised June 11, 1993.

Abstract. Using the tools of algebraic coding theory, we give a new proof of the nonexistence of two mutually orthogonal Latin squares of order 6.

1. Introduction

In 1782 Euler posed the following question: can 36 officers be arranged in a square of side six such that each of six ranks and each of six regiments are represented once in each row and column, [4]. Euler conjectured that there was no solution, and introduced mutually orthogonal Latin squares to decide the conjecture. G. Tarry proved him correct with an exhaustive search of all Latin squares of order 6 in 1901, [9]. Recently a more elegant proof was offered by Stinson in [8]. We present here a new proof, which will use methods which may possibly be applicable to similar problems for larger values of n. We begin with a definition.

DEFINITION. Let S be a set of cardinality n. Let A be an $n \times n$ matrix such that each row and column of A contains each element of S exactly once. Then A is a **Latin square of order** n. Let $A = (a_{ij})$ and $B = (b_{ij})$ be Latin squares of order n; if $\{(a_{ij}, b_{ij})\} = S \times S$ then A and B are said to be **orthogonal**. A set $\{A_1, A_2, \ldots, A_k\}$ with A_i orthogonal to A_j for $1 \leq i < j \leq k$ is called a set of k **Mutually Orthogonal Latin Squares.**

It is well known that k-MOLS of order n are equivalent to a $(k + 2)$-net of order n. Nets are defined as follows.

DEFINITION. A k-**net of order** n is an incidence structure consisting of n^2 points and nk lines satisfying the following four axioms:

(i) every line has n points;
(ii) parallelism is an equivalence relation on lines, where two lines are said to be parallel if they are disjoint or identical;
(iii) there are k parallel classes each consisting of n lines;
(iv) any two nonparallel lines meet exactly once.

DEFINITION. A **traversal** of a net is a set of n points having exactly one point in common with each line of the net.

The following definition of $C_p(N_k)$ is identical to the one given by Moorhouse in [6] and [7] and also identical to the definition of the code of a design given by Assmus and Key in [1]. The characteristic function of a line at a point is 1 if the point is incident with the line and 0 otherwise. We shall use l to denote both the line and its characteristic function.

DEFINITION. Let $C_p(N_k)$ be the row space over F_p generated by the characteristic functions of lines. Let $H_p(N_k)$ be the code over F_p generated by vectors of the form $l - m$ where l and m are parallel.

We take the standard definitions from algebraic coding theory. Namely, we let F be a finite field, in this setting it will always be of prime order, and then C is a linear $[n, k]$ code if C is a subspace of F^n of dimension k. Also the weight of a vector v in C, denoted by $wt(v)$, is the number of nonzero coordinates of the vector.

2. Code of Nets

We shall use $C_p(N_k)$ and $H_p(N_k)$ to give geometrical information about the nets. In order to do so we must assume that p divides n; we make that assumption for the remainder of the article. For a more complete discussion of how these codes are used see [3].

THEOREM 2.1. *If N_k has a traversal or if $k \neq rp + 1$, then dim $C_p(N_k)$ − dim $H_p(N_k) = k$.*

Proof. We know dim $C_p(N_k)$ − dim $H_p(N_k) \leq k$ since $C_p(N_k) = <m_1, \ldots, m_k, H_p(N_k)>$ where $m_i \in \mathfrak{A}_i$, and $\mathfrak{A}_i$ is the i-th parallel class. Moreoever, we may assume that $k > 1$, since dim $C_p(N_1) = n$ and dim $H_p(N_1) = n - 1$. We shall show that $\{m_1, m_2, \ldots, m_k\}$ are linearly independent over $H_p(N_k)$. First we note that since $k > 1$, no line m is in $C_p(N_k)^\perp$ since $[l, m] \neq 0$ for l and m not parallel. Hence no line m is in $H_p(N_k)$, since, clearly, $H_p(N_k) \subseteq C_p(N_k)^\perp$.

Assume $v = a_1m_1 + a_2m_2 + \cdots + a_km_k \in H_p(N_k) \subseteq C_p(N_k) \cap C_p(N_k)^\perp$. Since $v \in C_p(N_k)^\perp$, $[v, m] = 0$ for all lines m in N_k. Let $l_j \in \mathfrak{A}_j$; we have:

$$0 = [v, l_j] = [a_1m_1, l_j] + \cdots + [a_km_k, l_j] = \sum_{i \neq j} a_i.$$

Therefore $0 = (\Sigma_{i=1}^k a_i) = \cdots = (\Sigma_{i=1}^k a_i) - a_k$, and so $\Sigma_{i=1}^k a_i = a_1 = a_2 = \cdots = a_k$.

If $k \neq rp + 1$, set $a_i = a$, we have $\Sigma_{i \neq j} a_i = (k - 1)a = 0$, if $a \neq 0$ then $(k - 1) = 0$; but $k \neq rp + 1$ so $k - 1 \neq 0$, and hence $a = 0$, and in this case $\{m_1, m_2, \ldots, m_k\}$ are linearly independent.

Now let t be a transversal N_k. We know $t \in H_p(N_n)^\perp$ since $[t, m - l] = 1 - 1 = 0$ for m parallel to l. So $[v, t] = 0$, that is $[a_1m_1, t] + \cdots + [a_km_k, t] = 0$ which implies $a_1 + a_2 + \cdots + a_k = 0$, and so, again we have that $a_i = 0$ for all i, giving the result. □

LEMMA 2.1. Let n be even and set $p = 2$. Let N_k be a k-net of order n with $\mathfrak{A}_k = \{l_1^k, l_2^k, \ldots, l_n^k\}$. Assume $\Sigma\ \alpha_i^k\ l_i^k \in C_p(N_{k-1})$; where N_{k-1} is any $(k - 1)$ subnet of N_k, then we have the following relation:

$$\sum \alpha_i^k l_i^k + \sum \alpha_i^{k-1}\ l_i^{k-1} + \cdots \sum \alpha_i^1\ l_i^1 = 0.$$

Let α^j be the number of α_i^j which are 1, that is $\alpha^j = |\{\alpha_i^j \mid \alpha_i^j = 1\}|$. If α^j is odd for any j then $\dim C_p(N_k) - \dim H_p(N_k) < k$, and therefore N_k has no transversals and does not extend.

Proof. Note that $C_2(N_k) = \langle l_1^1, \ldots, l_1^k, H_2(N_k)\rangle$. For all α^j odd, take one line with nonzero coefficient out of the summation, and arrange it so that it is l_1^j. We have

$$\sum_{\alpha^j \text{ odd}} l_1^j = \sum_{i=2}^{n} \alpha_i^k l_i^k + \cdots + \sum_{i=2}^{n} \alpha^{i1} l_i^1$$

where all the weights in the summations are now even and so the right side is in $H_2(N_k)$. We now have a nontrivial linear combination of $\{l_1^1, \ldots, l_1^k\}$ in $H_2(N_k)$ and so $\dim C_2(N_k) - \dim H_2(N_k) < k$ and hence by the previous theorem N_k does not have a transversal. □

Let $n \equiv 2 \pmod 4$; then $n = 2m$ with m odd. Let N_3 be a 3-net of order n with the following parallel classes: $\mathfrak{A}_1 = \{l_1, \ldots, l_n\}$, $\mathfrak{A}_2 = \{m_1, \ldots, m_n\}$, and $\mathfrak{A}_3 = \{t_1, \ldots, t_n\}$. Set $p = 2$, for the remainder of the article.

LEMMA 2.2. If $\Sigma\ \alpha_it_i \in C_2(N_2)$, where $N_2 = \mathfrak{A}_1 \cup \mathfrak{A}_2$, then $wt(\alpha_1, \ldots, \alpha_n)$ is n, 0, or $n/2 = m$.

Proof. Let $\{q_1, \ldots, q_{n^2}\}$ be the point set of N_3 with t_i being incident with the points $q_{(i-1)n+1}$ to q_{in}. If $\Sigma\ \alpha_it_i \in C_2(N_2)$, then $\Sigma\ \alpha_it_i = \Sigma\ \beta_im_i + \Sigma\ \gamma_il_i$ for $\alpha_i, \beta_i, \gamma_i \in F_2$. If $wt(\alpha_1, \ldots, \alpha_n) = 0$, then $\Sigma\ \alpha_it_i = 0$, and $\beta_i = \gamma_i = 0$ for all i or $\beta_i = \gamma_i = 1$ for all i. If $wt(\alpha_1, \ldots, \alpha_n) = n$, then $\Sigma\ \alpha_it_i = j$, where j is the all-one vector, and $\beta_i = 1$ for all i or $\gamma_i = 1$ for all i.

Assume $wt(\alpha_1, \ldots, \alpha_n)$ is neither 0 nor n, then some $\alpha_i = 0$ and some $\alpha_j = 1$. Arrange matters so that $\alpha_1 = 1$ and $\sigma_2 = 0$; then the value of $v = \Sigma\ \alpha_it_i$ is 1 at $q_1, \ldots, q_n$ and 0 at $q_{n+1}, \ldots, q_{2n}$.

If $\gamma_i = 1$ for all i, then $\beta_i = 0$ for all i, since $v(q_1) = 1, \ldots, v(q_n) = 1$ and therefore $v = j$, and likewise if $\beta_i = 1$ for all i. Here this is not the case, since $wt(\alpha_1, \ldots, \alpha_n) \neq n$. So at least one $\gamma_i = 1$ and one $\gamma_j = 0$, and at least one $\beta_i = 1$ and one $\beta_j = 0$.

Let $\beta = wt(\beta_1, \ldots, \beta_n)$ and $\gamma = wt(\gamma_1, \ldots, \gamma_n)$. Since $v(q_i) = 1$ for $1 \leq i \leq n$, then $\beta + \gamma = n$, and since $v(q_i) = 0$ for $n + 1 \leq i \leq 2n$, then $\beta = \gamma$ since each $\beta_i m_i$ must intersect a $\gamma_i l_i$ to make it zero whenever β_i and γ_i are 1. Hence $\beta = \gamma = n/2 = m$.

We have $\Sigma\, \alpha_i t_i = \Sigma\, \beta_i m_i + \Sigma\, \gamma_i l_i$ implies $\beta = \gamma = m$, but $\Sigma\, \alpha_i t_i = \Sigma\, \beta_i m_i + \Sigma\, \gamma_i l_i$ implies $\Sigma\, \alpha_i t_i + \Sigma\, \beta_i m_i = \Sigma\, \gamma_i l_i$, so likewise $\alpha = \beta = m$. Hence $wt(\alpha_1, \ldots, \alpha_n) = 0$, n, or m. □

THEOREM 2.2. *If dim $C_2(N_3)$ − dim $C_2(N_2) < n - 1$, then N_2 does not extend to a 4-net; in fact N_3 will not have a transversal.*

Proof. We note that by Theorem 2.1, dim $C_2(N_2)$ − dim $H_2(N_2) = 2$ since $k = 2$ and $2 \not\equiv 1 \pmod 2$. Now suppose that $w = \alpha_2(t_1 + t_2) + \cdots + \alpha_n(t_1 + t_n) \in H_2(N_2) \subseteq C_2(N_2)$. Write

$$w = \left(\sum_{i=2}^{n} \alpha_i \right) t_1 + \alpha_2 t_2 + \cdots + \alpha_n t_n$$

then, when $\Sigma_{i=2}^{n}\, \alpha_i = 1$ an odd number of $\alpha_2, \ldots, \alpha_n$ are 1 and so $wt(\Sigma_{i=2}^{n}\, \alpha_i, \alpha_2, \ldots, \alpha_n)$ is even and when $\Sigma_{i=2}^{n}\, \alpha_i = 0$ an even number of $\alpha_2, \ldots, \alpha_n$ are 1 and again $wt(\Sigma_{i=2}^{n}\, \alpha_i, \alpha_2, \ldots, \alpha_n)$ is even. Thus $wt(\Sigma_{i=2}^{n}\, \alpha_i, \alpha_2, \ldots, \alpha_n)$ is even and by the previous lemma the weight is either 0 or n.

Since $t_1 + t_2, \ldots, t_1 + t_n$ generate $H_2(N_3)$ over $H_2(N_2)$, we have shown that dim $H_2(N_3)$ − dim $H_2(N_2) = n - 2$. Now, if dim $C_2(N_3)$ − dim $C_2(N_2) < n - 1$ then dim $C_2(N_3)$ − dim $H_2(N_3) \neq 3$ and hence by Theorem 2.1, does not even have a transversal and therefore does not extend. □

Therefore if dim $C_2(N_3) < 3n - 2$, the net does not complete, since dim $C_2(N_3) = n + n - 1 +$ dim $C_2(N_3)$ − dim $C_2(N_2)$. This result is shown by Moorhouse in [7] as well, but his proof relies on loops and on the work of Bruck in [2], whereas the proof above uses only elementary linear algebra. One can see that the construction of the linear combination of $n/2$ lines in the third parallel class is equivalent to the subloop condition given by Bruck in [2]. The benefit of not using loops is that loops are equivalent to 3-nets and as such cannot be used for arbitrary k-nets, whereas the methods above can be so used.

We shall now show how the methods presented here can be used to prove the nonexistence of two mutually orthogonal Latin squares of order 6. Assume that there exists a 4-net of order $n \equiv 2 \pmod 4$. Let $\mathfrak{A}_1 = \{l_i\}$, $\mathfrak{A}_2 = \{m_i\}$, $\mathfrak{A}_3 = \{t_i\}$, and $\mathfrak{A}_4 = \{s_i\}$. Assume we have the following linear combination:

$$\sum \alpha_i l_i + \sum \beta_i m_i + \sum \gamma_i t_i + \sum \delta_i s_i = 0$$

where $\alpha = wt(\alpha_i)$, $\beta = wt(\beta_i)$, $\gamma = wt(\gamma_i)$, and $\delta = wt(\delta_i)$. If any of $\alpha, \beta, \gamma, \delta$ are odd, then by Lemma 2.1 dim $C_2(N_4)$ − dim $H_2(N_4) < 4$, but this contradicts Theorem 2.1. Hence $\alpha, \beta, \gamma, \delta$ are all even.

The all one vector j is in $C_2(N_k)$, since it is the sum of any parallel class. By adding the j vector an appropriate number of times it can be arranged so that $\beta = \gamma = \delta = 2$ and α is either 4 or 2. The case $\alpha = 4$ is ruled out by a simple combinatorial argument: Simply arrange the lines from the first parallel class horizontally, with the first four being the lines with nonzero coefficients in the linear combination. On the first four lines all six of the other lines in the linear combination must intersect each line exactly once. Then the two lines from each of the second and third parallel classes must intersect the two lines in the fourth parallel class on the four points on these two lines that are not incident with any of the four lines in the first parallel class. But on each of these points there must be an even number of lines from the linear combination intersecting it, which produces a contradiction. The only case that remains is $\alpha = \beta = \gamma = \delta = 2$.

This configuration is ruled out by the following combinatorial argument which is similar to one given by Stinson in a different setting in [8].

Assume this linear combination can occur, we can write it without loss of generality as:

$$l_1 + l_2 + m_1 + m_2 + t_1 + t_2 + s_1 + s_2 = 0.$$

To see this combination, arrange the n^2 points in a square. Without loss of generality we can assume l_1 and l_2 are the first two horizontal lines and m_1 and m_2 are the first two vertical lines. The next four lines t_1, t_2, s_1, s_2 must intersect the first four lines in the 16 points where the first four lines do not intersect each other, also they must intersect each other (except for lines parallel to each other) in 4 of the 16 points not on any of $\{l_1, l_2, m_1, m_2\}$. We see that there are 8 lines involved in the linear combination and 24 points involved, where each of these 24 points has 2 lines from the linear combination incident with it, and 2 lines not in the linear combination incident with it.

Let L be the set of lines in the net and L' be the set of lines not involved in the linear combination, that is $L' = \{l_3, \ldots, l_6, m_3, \ldots, m_6, t_3, \ldots, t_6, s_3, \ldots, s_6\}$. Let P be the set of points in the net and P' be the 24 points involved in the linear combination. We shall show that the lines of L' cannot be arranged on the points of P' as is necessary in a net.

First we note that it is clear, by a simple counting argument that any line in L' is incident with 3 points in P' and 3 points in $P - P'$.

Take a line l in L', it meets three points in P', through each of these 3 points are 2 lines from the linear combination, that is 2 lines from $L - L'$, so each is incident with 2 lines in L'. Since one of these lines is l, the other is from a different parallel class. Through each of these points are 2 lines from $L - L'$, but no 2 of these 3 have the same 2 parallel classes represented with lines from L' incident with them. Thus l intersets 1 line in L' from each other parallel class at a point in P'.

Suppose that $r_1, r_2, r_3 \in L'$ form a triangle. We show that the three vertices $p_1 = r_1 \cap r_2, p_2 = r_2 \cap r_2, p_3 = r_3 \cap r_1$ cannot all belong to P'. Assume on the contrary that $p_1, p_2, p_3 \in P'$. Through p_1 are also 2 lines in $L - L'$, x and y, therefore (r_1, r_2, x, y) are concurrent. Then (w, r_2, r_3, z) are also concurrent where $w, z \in L - L'$. Note that two lines are in the same coordinate of these 4-tuples if they are parallel. Then p_3 must be incident with either z or y since r_3 meets only 2 lines from that parallel class in P' by the above explanation, which is a contradiction.

We also note that for any line in L', the points of incidence with three lines from L' that it meets in P' are distinct.

By relabeling of L' we can assume that l_i meets m_i, t_i, and s_i for $3 \leq i \leq 6$ in P'. For each $i \in \{4, 5, 6\}$, the lines m_i, s_i, t_i are not concurrent, and l_3 must meet exactly one of the three points $m_i \cap s_i$, $s_i \cap t_i$, $t_i \cap m_i$.

Suppose the lines l_3, m_4, t_4 and s_5 are concurrent, then the lines l_3, m_5, t_5, s_6 and the lines l_3, m_6, t_6, s_4 are forced to be concurrent as well. Where can the pair m_3, t_3 be? If l_4, m_3, t_3, x are concurrent then as above the lines l_4, m_3, t_3 would be concurrent, as well as the lines l_4, m_5, t_5 and the lines l_4, m_6, t_6 would be concurrent causing a pair to be repeated. The same argument shows that l_5, m_3, t_3, x and l_6, m_3, t_3, x cannot be concurrent. Therefore the pair m_3, t_3 does not occur, which is a contradiction. Hence this linear combination does not occur.

Since both combinations can be ruled out, then $\dim C_2(N_4) - \dim C_2(N_3) = n - 1 = 5$ and hence $\dim C_2(N_4) = 6 + 5 + 5 + 5 = 21$ and $\dim H_2(N_4) = 21 - 4 = 17$, which implies $\dim H_2(N_4)^{\perp} = 36 - 17 = 19$. But $C_2(N_4) \subseteq H_2(N_4)^{\perp}$, which is a contradiction, and hence there do not exist two mutually orthogonal Latin squares of order 6.

References

1. E.F. Assmus, Jr. and J.D. Key, Affine and projective planes, *Discrete Math* Vol. 83 (1990), pp. 161–187.
2. R.H. Bruck, Finite Nets I. Numerical invariants, *Can. J. Math.* 3 (1951), pp. 94–107.
3. S.T. Dougherty, Nets and their codes, Ph.D. thesis. Lehigh University (1992).
4. L. Euler, Recherches sur une nouvelle espece des quarres magiques., *Leonardi Euleri Opera Omina Ser. I*, Vol. 7, Tuebǹer, Berlin-Leipzig, (1923), pp. 291–392.
5. R.A. Fisher and F. Yates, The 6 × 6 Latin squares, *Proc. Camb. Phil. Soc.* 30 (1934), pp. 492–507.
6. G.E. Moorhouse, Bruck nets, codes, and characters of loops, *Designs, Codes and Cryptography* Vol. 1 (1991), pp. 7–29.
7. G.E. Moorhouse, On codes of Bruck nets and projective planes, *Proc. Marshall Hall Conf.* (1990).
8. D.R. Stinson, A short proof of the non-existence of a pair of orthogonal Latin squares of order six, *J. Comb. Theory* A36 (1984), pp. 373–376.
9. G. Tarry, Le probleme des 36 officers, *Compte Rendu Ass. Franc. Pour l'avacement des Sciences* Vol. 2 (1901), pp. 170–203.