JOURNAL OF COMBINATORIAL THEORY, Series A 36, 373–376 (1984)

Note

A Short Proof of the Nonexistence of a Pair of Orthogonal Latin Squares of Order Six

D. R. STINSON

Department of Computer Science,
University of Manitoba, Winnipeg, Manitoba, Canada

Communicated by the Managing Editors

Received June 3, 1982

A pair of orthogonal Latin squares of order six do not exist.

A *Latin square* of order s is an s by s array L of the symbols $\{1, 2, \ldots, s\}$, such that each symbol occurs once in each row and column of L. Two Latin squares L and M of order s are *orthogonal* if their superposition yields all s^2 possible ordered pairs (i,j), $1 \leqslant i, j \leqslant s$.

It was conjectured by Euler, and proved by Tarry [4] that there do not exist a pair of orthogonal Latin squares of order six (see also [2, 3]). These nonexistence proofs are long and require the consideration of many cases. We give a short, self-contained noncomputer proof which requires a minimum of casework.

We describe our proof in terms of transversal designs: a TD(4, 6) is a triple $(X, \mathscr{G}, \mathscr{A})$, where X is a set of size 24, $\mathscr{G}$ is a partition of X into four subsets (*groups*) of X of size six, and $\mathscr{A}$ is a set of 36 subsets (*blocks*) of X, each of size four, such that any group meets any block in a point, and any two points from different groups occur in a block. It is well known that a TD(4, 6) is equivalent to a pair of orthogonal Latin squares of order six.

Let $(X, \mathscr{G}, \mathscr{A})$ be a TD(4, 6). Then $P = (X, \mathscr{G} \cup \mathscr{A})$ is a PBD (pairwise balanced design) with 24 points and 40 blocks (36 of size four and four of size six). Let the points be named x_i $(1 \leqslant i \leqslant 24)$, and label the blocks B_j $(1 \leqslant j \leqslant 40)$, where B_1, B_2, B_3, and B_4 are the blocks of size six.

The incidence matrix of P is the $0-1$ matrix $M = (m_{ij})$ defined by

$$\begin{aligned} m_{ij} &= 1 \quad \text{if} \quad x_i \in B_j, \quad 1 \leqslant i \leqslant 24, 1 \leqslant j \leqslant 40, \\ &= 0 \quad \text{if} \quad x_i \notin B_j, \quad 1 \leqslant i \leqslant 24, 1 \leqslant j \leqslant 40. \end{aligned}$$

0097-3165/84 $3.00

The ith row of M is denoted by r_i. If we consider each r_i to be a vector in $(GF(2))^{40}$, then the r_i's span a subspace C which we call the *code* of P.

LEMMA 1 [1, Lemma 4.1]. $\dim C \leqslant 20$.

Proof. For $u, v \in (GF(2))^{40}$, let (u, v) denote the usual inner product (mod 2) and let $C^{\perp} = \{u : (u, r_i) = 0,\ 1 \leqslant i \leqslant 24)\}$. Then $(r_i, r_j) = 1$ for any i, j; so $(r_i, r_j + r_k) = 0$ for any i, j, k. It follows that $C \cap C^{\perp}$ is of codimension one in C. Hence $\dim C^{\perp} \geqslant \dim C - 1$. But $\dim C + \dim C^{\perp} = 40$, so $\dim C \leqslant 20$. ∎

Since M has 24 rows and $\dim C \leqslant 20$, there must be dependencies of the rows of M. A linear dependence can be written $\sum_{i \in I} r_i = 0$ for some $I \subseteq \{1,..., 24\}$. In terms of the design P, we have a subset $Y = \{x_i : i \in I\} \subseteq X$ such that $|B_j \cap Y|$ is even, $1 \leqslant j \leqslant 40$.

Clearly $B_1 \cup B_2$, $B_1 \cup B_3$, and $B_1 \cup B_4$ yield dependence relations. But $\dim C \leqslant 20$, so there must be one further dependence relation not generated by the above. We shall establish that there is no such dependence relation. This contradiction proves the nonexistence of a TD(4, 6).

The above may also be phrased in a coding context. The columns of M span a subspace (code) D in $(GF(2))^{24}$. A dependence relation of the rows of M corresponds to a nonzero codeword in $D^{\perp}$, the code dual to D. Lemma 1 is equivalent to $\dim D^{\perp} \geqslant 4$.

We will use the combinatorial terminology. If $Y = \{x_i : i \in I\}$ corresponds to a dependence relation we will call $\{Y, \{Y \cap B_i : 1 \leqslant i \leqslant 40\}\}$ an *even sub*-PBD. We say that Y is an *even subset* of X. Suppose an even sub-PBD has m points and b_i blocks of size i ($i = 0, 2, 4, 6$). Then simple counting yields

$$b_0 + b_2 + b_4 + b_6 = 40$$
$$2b_2 + 4b_4 + 6b_6 = 7m$$
$$b_2 + 6b_4 + 15b_6 = m(m-1)/2.$$

Then $b_4 + 3b_6 = m(m-8)/8$, which implies $m \equiv 0 \bmod 4$ and $m \geqslant 8$. Also, we may assume $m \leqslant 12$, complementing if necessary, since Y is an even subset if and only if $X \backslash Y$ is an even subset. Thus we have

LEMMA 2. *If a* TD(4,6) *exists, then it contains an even sub*-PBD *having eight or twelve points, which is not the union of two groups of the TD.*

First, we consider the case $m = 8$. We find that $b_0 = 12$, $b_2 = 28$, $b_4 = b_6 = 0$. Thus we have an "oval-like" sub-PBD: a set Y of eight points, no three collinear. Let Q be the PBD formed from P by deleting the points in Y. Then Q has 16 points, 16 blocks of size four, and 24 blocks of size two.

Let $Y = \{a, b, c, d, e, f, g, h\}$ and suppose $X \backslash Y = \{1, 2,..., 16\}$. We may

suppose that the groups of $\mathscr{G}$ are $\{1, 2, 3, 4, a, b\}$, $\{5, 6, 7, 8, c, d\}$, $\{9, 10, 11, 12, e, f\}$, and $\{13, 14, 15, 16, g, h\}$.

Now define a graph G, with vertex set $X \backslash Y$, whose edges are the 24 blocks of size two in the PBD Q.

LEMMA 3. (1) *G is triangle-free*;

(2) *G is three-regular, and any point of G is joined to precisely one point from each of the three groups of G not containing that point.*

Proof. To see that G is three-regular, choose any point i, $1 \leqslant i \leqslant 16$. If i occurs in x blocks of size two and y blocks of size four in Q, then $x + y = 7$ and $x + 3y = 15$, so $x = 3$ (and $y = 4$). The three blocks of size two must (in P) contain all six points of Y which are not in the same group as x. Thus statement (2) follows.

To prove (1), suppose that 1 5 9 is a triangle in G. In the PBD P we have a block 1 5 e g, say, and a block 1 9 c h (without loss of generality). Then the block containing 5 and 9 must be 5 9 a g or 5 9 a h, but in either case a pair is repeated. This contradiction proves that G is triangle-free. ∎

We now attempt to construct the PBD P. Let us first suppose that there is some point i ($1 \leqslant i \leqslant 16$) such that the three neighbours of i in G occur in a block of P. We can suppose that $i = 1$ has neighbours 5, 9, and 13 in G, and 2 5 9 13 is a block of P. Now, without loss of generality, we have blocks 1 6 10 14, 1 7 11 15, and 1 8 12 16; 2 5 9 13, 2 6 11 16, and 2 7 12 14; and six blocks, each of which contains one point from $\{3, 4\}$ and one from $\{5, 9, 13\}$. Thus the neighbours of 2 in G are 8, 10, and 15. The three pairs 8 10, 8 15, and 10 15 must occur in three blocks which contain 3 x or 4 y ($x, y \in \{5, 9, 13\}$). This causes a pair to be repeated (one of 3 8, 3 10, 3 15, 4 8, 4 10, or 4 15). This is a contradiction.

Thus we may assume the following property holds: (A) For any point i ($1 \leqslant i \leqslant 16$) the three pairs formed by the three neighbours of i in G occur in different blocks of P.

Now let us suppose (without loss of generality) that, in G, 1 is adjacent to 5, 9, and 13; 2 is adjacent to 6, 10, and 14; 3 is adjacent to 7, 11, and 15; and 4 is adjacent to 8, 12, and 16. By property (A), the point 1 must occur with exactly one pair from each of the three triangles 6 10 14, 7 11 15, and 8 12 16. Suppose 1 6 10 15 is a block; then 1 7 11 16 and 1 8 12 14 are forced to be blocks. The three pairs 6 10, 7 11, and 8 12 are all from the same two groups. But, then, where can the pair 5 9 occur? If 2 5 9 x is a block, then, as above, the three triples 2 5 9, 2 7 11, and 2 8 12 would occur in blocks, causing a pair to be repeated. The same argument shows that 3 5 9 x and 4 5 9 x cannot be blocks. Thus the pair 5 9 does not occur. This contradiction proves

LEMMA 4. *No* TD(4, 6) *contains an even subset with eight points* (i.e., $D^{\perp}$ *has no codewords of weight eight.*)

We must now consider the possibility $m = 12$. There are several ways the twelve points can be distributed among the four groups:

(i) 6, 6, 0, 0;
(ii) 6, 4, 2, 0;
(iii) 6, 2, 2, 2;
(iv) 4, 4, 4, 0;
(v) 4, 4, 2, 2.

Case (i) is the situation of an even subset formed by two groups; we have already noted the existence of these even subsets. For cases (ii)–(v) we use the fact that the sum of two even subsets (mod 2) is again an even subset. (This corresponds to taking the sum of two codewords in $D^{\perp}$.) In each case, add the given even subset to the even subset formed by the first two groups. In each case, an even subset of size eight or size four is produced. But we have already eliminated these cases.

Thus we have

LEMMA 5. *No* TD(4, 6) *contains an even subset of size twelve, which is not the union of two groups of the* TD.

Summarizing, we have our main theorem.

THEOREM. *There do not exist a pair of orthogonal Latin squares of side six.*

Proof. Lemmata 2–5. ∎

REFERENCES

1. W. G. BRIDGES, M. HALL, JR., AND J. L. HAYDEN, Codes and designs, *J. Combin. Theory A* **31** (1981), 155–174.
2. J. I. HALL, A. J. E. M. JANSEN, A. W. J. KOLEN, AND J. H. VAN LINT, Equidistant codes with distance 12, *Discrete Math.* **17** (1977), 71–83.
3. D. MCCARTHY, Transversals in Latin squares of order 6 and (7, 1)-designs, *Ars Combin.* **1** (1976), 261–265.
4. G. TARRY, Le problème des 36 officiers, *C. R. Assoc. Fr. Av. Sci.* **1** (1900), 122–123; **2** (1901), 170–203.