Journal of Statistical Planning and Inference 159 (2015) 81–89

Contents lists available at ScienceDirect

Journal of Statistical Planning and Inference

journal homepage: www.elsevier.com/locate/jspi

Mutually orthogonal latin squares with large holes

Peter J. Dukes *, Christopher M. van Bommel

Mathematics and Statistics, University of Victoria, Victoria, Canada

ARTICLE INFO

Article history:
Received 17 October 2014
Accepted 19 October 2014
Available online 27 October 2014

Keywords:
Latin square
Hole
Pairwise balanced design

ABSTRACT

Two latin squares are orthogonal if, when they are superimposed, every ordered pair of symbols appears exactly once. This definition extends naturally to 'incomplete' latin squares each having a hole on the same rows, columns, and symbols. If an incomplete latin square of order n has a hole of order m, then it is an easy observation that $n \geq 2m$. More generally, if a set of t incomplete mutually orthogonal latin squares of order n have a common hole of order m, then $n \geq (t+1)m$. In this article, we prove such sets of incomplete squares exist for all $n, m \gg 0$ satisfying $n \geq 8(t+1)^2 m$.

1. Introduction

A *latin square* is an $n \times n$ array with entries from an n-element set of symbols such that every row and column is a permutation of the symbols. Often the symbols are taken to be from $[n] := \{1, \ldots, n\}$. The integer n is called the *order* of the square.

Two latin squares L and L' of order n are *orthogonal* if $\{(L_{ij}, L'_{ij}) : i, j \in [n]\} = [n]^2$; that is, two squares are orthogonal if, when superimposed, all ordered pairs of symbols are distinct. The following arrangement of playing cards illustrates a pair of orthogonal latin squares of order 4.

A♠	J♡	Q♣	K♢
J♣	A♢	K♠	Q♡
Q♢	K♣	A♡	J♠
K♡	Q♠	J♢	A♣

Euler's famous '36 officers problem' asks whether there exists a pair of orthogonal latin squares of order six. The answer in that case is negative.

A family of latin squares in which any pair are orthogonal is called a set of *mutually orthogonal latin squares*, or 'MOLS' for short. The maximum size of a set of MOLS of order n is denoted by $N(n)$. It is easy to see that $N(n) \leq n - 1$ for $n > 1$, with equality if and only if there exists a projective plane of order n. Consequently, $N(q) = q - 1$ for prime powers q. Using number sieves and some 'gluing' constructions, it has been shown in Beth, 1983 (building upon Chowla et al., 1960; Wilson, 1974a) that $N(n) \geq n^{1/14.8}$ for large n.

In this article, we are interested in an 'incomplete' variant on MOLS. First, an *incomplete latin square* of order n with a *hole* of order m is an $n \times n$ array $L = (L_{ij} : i, j \in [n])$ on n symbols (let us say $[n]$ for convenience) together with a *hole* $M \subseteq [n]$

* Corresponding author.
E-mail addresses: dukes@uvic.ca (P.J. Dukes), cvanbomm@uvic.ca (C.M. van Bommel).

http://dx.doi.org/10.1016/j.jspi.2014.10.004

such that

- L_{ij} is empty if $\{i,j\} \subseteq M$;
- L_{ij} contains exactly one symbol if $\{i,j\} \not\subseteq M$;
- every row and every column in L contain each symbol at most once; and
- symbols in M do not appear in rows or columns indexed by M.

Note that M is often taken to be an interval of consecutive rows/columns/symbols (but need not be). The definition is meant to extend to any set of symbols (and corresponding hole symbols). One feature of incomplete latin squares is that they can 'frame' latin subsquares on the hole. An example in the case $n = 5$, $m = 2$ is shown below.

		3	4	5
		4	5	3
3	4	1	2	5
4	5	2	3	1
5	3	4	1	2

Two incomplete latin squares L, L' on $[n]$ with common holes M are orthogonal if

$$\{(L_{ij}, L'_{ij}) : \{i,j\} \not\subseteq M\} = [n]^2 \setminus M^2,$$

and as before we can have sets of mutually orthogonal incomplete latin squares. A set of t such incomplete squares of order n with holes of order m is denoted by t-IMOLS$(n; m)$. Note that the case $m = 0$ or 1 reduces to ordinary MOLS. For one noteworthy example, there exist 2-IMOLS(6; 2) (see Colbourn (2006) for instance) despite the nonexistence of orthogonal latin squares of order 6 (or 2).

It is a straightforward counting argument (see Horton (1974)) that the existence of t-IMOLS$(n; m)$ requires

$$n \geq (t+1)m. \tag{1.1}$$

The special case $t = 1$ recovers the familiar condition that latin subsquares cannot exceed half the size of their embedding. On the other hand, $n \geq 2m$ is sufficient for the existence of an incomplete latin square of order n with a hole of order m. For $t = 2, 3$, the inequality (1.1) is known to be sufficient, except for small cases; see Heinrich and Zhu (1986) and Abel and Du (2003). The best presently known result for $t = 4$ is a by-product of work on 6-IMOLS$(n; m)$ in Colbourn and Zhu (1995), and so in this case $n \sim 7m$ is a barrier. This gives some evidence of the difficulty of constructing t-IMOLS$(n; m)$ near the bound for general t.

For our main result, we prove sufficiency for large n and m when (1.1) is strengthened a little.

Theorem 1.1. *There exist t-IMOLS$(n; m)$ for all sufficiently large n, m satisfying $n \geq 8(t+1)^2 m$.*

We actually obtain Theorem 1.1 as a consequence of a more general result on pairwise balanced block designs with holes. The corresponding 'inequality' we obtain in this more general case is probably far from best possible, but it reduces to a reasonable condition for our application to IMOLS. The next three sections of the article are devoted to the development and proof of our result on designs with holes. In Section 5, we conclude with a proof of Theorem 1.1 and discussion of a few related items.

2. Background on block designs

Let v be a positive integer and $K \subseteq \mathbb{Z}_{\geq 2} := \{2, 3, 4, \ldots\}$. A *pairwise balanced design* PBD(v, K) is a pair $(V, \mathcal{B})$, where

- V is a v-element set of *points*;
- $\mathcal{B} \subseteq \cup_{k \in K} \binom{V}{k}$ is a family of subsets of V, called *blocks*; and
- every two distinct points appear together in exactly one block.

In a PBD(v, K), the pairs covered by each block must partition $\binom{V}{2}$. In addition, for any point $x \in V$, the remaining $v - 1$ points must partition into 'neighborhoods' in the blocks incident with x. It is helpful to think of the resulting divisibility restrictions as, respectively, 'global' and 'local' conditions, which we state below (in reverse order).

Proposition 2.1. *The existence of a* PBD(v, K) *implies*

$$v - 1 \equiv 0 \pmod{\alpha(K)} \quad \textit{and} \tag{2.1}$$

$$v(v-1) \equiv 0 \pmod{\beta(K)}, \tag{2.2}$$

where $\alpha(K) := \gcd\{k - 1 : k \in K\}$ *and* $\beta(K) := \gcd\{k(k-1) : k \in K\}$.

The sufficiency of these conditions for $v \gg 0$ is a celebrated result due to Richard M. Wilson.