1973

Kronecker products and BIBDS

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Publication Details
Kronecker products and BIBDS

Abstract
Recursive constructions are given which permit, under conditions described in the paper, a \((v, b, r, k, \lambda)\)-configuration to be used to obtain a \((v', b', r', k, \lambda)\)-configuration.

Although there are many equivalent definitions we will mean by a \((v, b, r, k, \lambda)\)-configuration or BIBD that \((0, 1)\)-matrix \(A\) of size \(v \times b\) with row sum \(r\) and column sum \(k\) satisfying

\[ AA^T = (r - \lambda)I + \lambda J \]

where, as throughout the remainder of this paper, \(I\) is the identity matrix and \(J\) the matrix with every element +1 whose sizes should be determined from the context or by a subscript \((J_n\) is square of order \(n\)).

Disciplines
Physical Sciences and Mathematics

Publication Details
Note

Kronecker Products and BIBDs

JENNIFER WALLIS

Faculty of Mathematics, University of Newcastle, N.S.W., 2308, Australia

Communicated by M. Hall, Jr.

Received April 13, 1971

Recursive constructions are given which permit, under conditions described in the paper, a \((r, b, r, k, \lambda)\)-configuration to be used to obtain a \((r', b', r', k, \lambda')\)-configuration.

Although there are many equivalent definitions we will mean by a \((r, b, r, k, \lambda)\)-configuration or BIBD that \((0, 1)\)-matrix \(A\) of size \(r \times b\) with row sum \(r\) and column sum \(k\) satisfying

\[
AA^T = (r - \lambda)I + \lambda J
\]

where, as throughout the remainder of this paper, \(I\) is the identity matrix and \(J\) the matrix with every element \(\pm 1\) whose sizes should be determined from the context or by a subscript (\(J_n\) is square of order \(n\)).

In the case of block matrices, \((X)_{ij}\) and \((X_{ij})\) mean the matrix whose \((i, j)\)-th block is \(X\); for example, \((T^i)_{ij}\) is the matrix whose \((i, j)\)-th block is \(T^{i-j}\). We define the Kronecker product of two matrices \(A = (a_{ij})\) of order \(m \times n\) and \(B\) of any order as the \(m \times n\) block matrix

\[
A \times B = (a_{ij}B)_{ij}.
\]

For more details the reader is referred to Marshall Hall [1].

We will use \(T\) for the circulant matrix of order \(q\) given by

\[
T = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 \\
1 & 0 & 0 & \cdots & 0 & 0 & 1
\end{bmatrix}.
\]

For \(q\) a prime we have shown in Jennifer Wallis [3] that

\[
Q = (T^{(q-1)(i-1)})_{ij}
\]
satisfies

\[ QQ^T = qI_v \times I_v + (J_v - I_v) \times J_v, \]

\[ J \cdot Q = qJ. \]

We are concerned with the existence of a \((0, 1)\) matrix \(Q\) of size \(mv \times v^2\) which satisfies

\[ QQ^T = vI_v \times I_v + (J_v - I_v) \times J_v, \]

\[ JQ = mJ; \] \hspace{1cm} (1) \]

if such a matrix exists we will say \(P(m, v)\) holds. Thus the result cited above shows that \(P(q, q)\) holds for any prime \(q\); we also showed in [3] that \(P(q, q)\) holds for any prime power \(q\). Further, it was proved in [4] that \(P(m, v)\) holds if and only if there exists a set of \(m - 2\) mutually orthogonal Latin squares of order \(v\), and that a \((0, 1)\) matrix \(Q\) satisfying (1) must have the form

\[ Q = \begin{bmatrix} E \\ A \\ \vdots \\ A_{m-1} \end{bmatrix}, \]

where \(E\) and the \(A_i\) are of size \(v \times v^2\) and have constant row sums \(v\) and column sums 1. From the latter fact it is clear that if \(Q\) satisfies (1) then the matrix formed by deleting \(A_n\) and subsequent blocks satisfies (1) with \(m\) replaced by \(n\), so

\[ P(m, v) \Rightarrow P(n, v) \quad \text{when} \quad n < m. \]

If we are referring to \(P(m, v)\), then \(Q\), \(E\) and \(A_i\) will mean the matrices just mentioned.

**Main Theorem**

We shall exploit the following theorem, which is a generalization of Lemma 6 of [3]:

**Theorem 1.** Suppose \(B\) is a \((v, b, r, k, \lambda)\)-configuration and suppose \(R\) is a \((0, 1)\) matrix of size \(b v \times t v^2\) satisfying

\[ RR^T = a_1J_v I_v + a_2(J_v - I_v) \times J_v, \]

\[ JR = kJ, \] \hspace{1cm} (2) \]
where \( a_2 \) divides \( \lambda \). Then necessarily \( la_1 = kt \) and \( (l - 1) a_2 = (k - 1) a_1 \), and

\[
[I_t \times B \mid R, R, \ldots, R] \quad (\lambda \mid a_2 \text{ copies of } R)
\]

is an \((lv, lb + \lambda tv^2, r + \lambda av^2, k, \lambda)\)-configuration.

**Proof.** By summing the entries of \( R \) in two ways we obtain \( la_1 = kt \).

It is easy to check that the matrix exhibited is the required configuration; one of the standard necessary conditions for a \((v, b, r, k, \lambda)\)-configuration is \( \lambda(v - 1) = r(k - 1) \); substituting in the parameters of the configuration we constructed we have

\[
(l - 1) a_2 = (k - 1) a_1.
\]

In the particular case where \( t = a_1 = a_2 = 1 \) and \( k = l \), the existence of a suitable \( R \) satisfying (2) is simply \( P(k, v) \).

**Corollary 2.** If there exist a \((v, b, r, k, \lambda)\)-configuration and a set of \( k - 2 \) mutually orthogonal Latin squares of order \( v \), then there is a \((kv, kb + \lambda v^2, r + \lambda v, k, \lambda)\)-configuration.

**Example.** Suppose \( v = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \) is a decomposition of \( v \) into powers of distinct primes, and suppose

\[
k \leq \min_i (p_i^{a_i}) + 1.
\]

Then there is a set of \( k - 2 \) mutually orthogonal Latin squares of order \( v \) [1, p. 192], so the existence of a \((v, b, r, k, \lambda)\)-configuration for this \( k \) and \( v \) implies the existence of a \((kv, bk + \lambda v^2, r + \lambda v, k, \lambda)\)-configuration.

**Example.** Hanani [2] has shown (in terms of Latin squares) that \( P(5, v) \) always holds when \( v \geq 52 \) and \( P(7, v) \) always holds when \( v \geq 63 \), so Corollary 2 can be applied in the corresponding cases.

**First Application**

Suppose \( q \) is a prime and \( \omega \) is a primitive \( q \)-th root of unity. \( T \) is of order \( q \). Define a \( q \times q \) matrix \( P \) by

\[
P = (p_{ij}), \quad p_{ij} = \omega^{(i-1)(j-1)}.
\]

Now define square matrices \( S_{ij}, \ i = 1, 2, \ldots, q^a \) and \( j = 1, 2, \ldots, q^a \) where
s is any positive integer, as follows: if the \((i, j)\) element of the Kronecker product of \(s\) copies of \(P\) is \(\omega^a\), then \(s_{ij} = T^a\).

Assume that \(P(k, v)\) holds for some \(k \leq q^s\). Write

\[
R = \begin{bmatrix}
S_{11} \times E & S_{12} \times E & \cdots & S_{1q^s} \times E \\
S_{21} \times A_1 & S_{22} \times A_1 & \cdots & S_{2q^s} \times A_1 \\
\vdots & \vdots & \ddots & \vdots \\
S_{k1} \times A_{k-1} & S_{k2} \times A_{k-1} & \cdots & S_{kq^s} \times A_{k-1}
\end{bmatrix}.
\]

\(R\) is a \((0, 1)\) matrix of size \(keq \times v^2q^{s+1}\), and it is readily shown that

\[RR^T = q^v I_k \times I_{q^s} + q^{s-1}(J_k - I_k) \times J_{q^s},\]

so \(R\) satisfies \((2)\) with \(v\) replaced by \(vq\), \(l = k\) and \(t = a_1 = a_2 = q^{s-1}\).

So we have proved the following:

**Theorem 3.** Suppose there exists a \((qv, b, r, k, \lambda)\)-configuration, where \(q\) is a prime, and suppose \(P(k, v)\) holds. If \(s\) is a positive integer such that \(q^{s-1}\) divides \(\lambda\) and \(k \leq q^s\), then there exists a \((keq, kb + \lambda q^2v, r + \lambdaqv, k, \lambda)\)-configuration.

Corollaries can easily be constructed using the examples in the preceding section.

**Second Application**

Suppose \(q\) is a prime and suppose \(P(k, v)\) holds where \(k \leq q + 1\). The matrices \(I\) and \(T\) will be of order \(q\).

We consider the \((0, 1)\) block matrix \(P\),

\[
P = \begin{bmatrix}
I \times A_1 & I \times A_2 & I \times A_3 & \cdots & I \times A_{k-1} \\
I \times A_1 & T \times A_2 & T^2 \times A_3 & \cdots & T^{v-1} \times A_{k-1} \\
I \times A_1 & T^2 \times A_2 & T^4 \times A_3 & \cdots & T^{2(v-1)} \times A_{k-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
I \times A_1 & T^{k-2} \times A_{k-1} & T^{2(k-2)} \times A_{k-2} & \cdots & T^{(k-2)(v-1)} \times A_{k-1}
\end{bmatrix},
\]

which is a \((k - 1) \times q\) array of \(qv \times qv^2\) blocks. Write \(E'\) for \([I \times E, I \times E, \ldots, I \times E]\), there being \(q\) copies of \(I \times E\), and denote by \(T^i \cdot P\) the result of multiplying the first of the two components of every block entry of \(P\) by \(T^i\). Then

\[
R = \begin{bmatrix}
E' & E' & E' & \cdots & E' \\
P & T \cdot P & T^2 \cdot P & \cdots & T^{v-1} \cdot P
\end{bmatrix}.
\]
is a $(0, 1)$ matrix of suitable size which satisfies (2) with $l = k$, $v$ replaced by $qv$ and $a_1 = a_2 = t = q$. Hence we have

**Theorem 4.** If $P(k, v)$ holds and there is a $(qv, b, r, k, \lambda)$-configuration, where $q$ is a prime not less than $k - 1$ and $q$ divides $\lambda$, then there exists a $(kqv, kb + \lambda q + r, r + \lambda q v, k, \lambda)$-configuration.

Again corollaries can be formed at will.

**References**