Three Mutually Orthogonal Latin Squares

W. H. Mills

Institute for Defense Analyses, Princeton, New Jersey 08540

Communicated by Marshall Hall, Jr.

Received March 16, 1970

In a famous paper [3], Bose, Shrikhande, and Parker proved the existence of a pair of orthogonal Latin squares of order $v$ for all $v \neq 2,6$. In the present paper it is shown that there exist three mutually orthogonal Latin squares for all $v = 0,1 \pmod{4}$. This result will be needed in several future papers on the covering of pairs by quadruples.

1. Known Results

Let $N(v)$ denote the maximum number of mutually orthogonal Latin squares of order $v$. We note that any 1 by 1 matrix is a Latin square orthogonal to itself so that $N(1) = \infty$.

The following four basic lemmas are well known and proofs may be found in many places (for example [8, Ch. 7]). Lemma 4 is an immediate consequence of Lemmas 2 and 3 [7].

**Lemma 1.** If $v > 1$, then $N(v) \leq v - 1$.

**Lemma 2.** $N(vw) \geq \min\{N(v), N(w)\}$.

**Lemma 3.** If $q$ is a power of a prime and $q > 1$, then $N(q) = q - 1$.

**Lemma 4 (MacNeish).** If $v = \Pi q_i$, where the $q_i$ are powers of primes, then

$$N(v) \geq \min\{q_i - 1\}.$$

The next lemma is due to Bose, Shrikhande, and Parker (see [3, page 198] or [5, page 200]).

**Lemma 5.** If $k \leq N(m) + 1$ and $1 \leq x < m$, then

$$N(km + x) \geq \min\{N(k) - 1, N(k + 1) - 1, N(m), N(x)\}.$$
Finally, using Lemma 1, Lemma 5 can be stated in the following form:

**Lemma 6.** If \( v = km + x \), where \( 0 < x < m \) and \( N(m) \geq k - 1 \), then

\[
N(v) \geq \min\{N(k) - 1, N(k + 1) - 1, N(x)\}.
\]

### 2. Large Values of \( v \)

It is well known [4] that \( N(v) \) becomes arbitrarily large as \( v \) increases. In particular \( N(v) \geq 3 \) for all sufficiently large \( v \). We will show that \( N(v) \geq 3 \) whenever \( v \equiv 0 \) or \( 1 \) (mod 4). We begin by noting that, if \( v \not\equiv 2 \) (mod 4) and \( v \not\equiv 3, 6 \) (mod 9), then \( N(v) \geq 3 \) by Lemma 4.

**Lemma 7.** If \( v \not\equiv 2 \) (mod 4), \( 3 \mid v \), and \( v \geq 664 \), then \( N(v) \geq 3 \).

**Proof.** We write

\[
v = 8u + s,
\]

where \( u \geq 83 \) and \( 0 \leq s < 8 \). Now any five consecutive odd numbers includes at most two multiples of 3, one multiple of 5, and one multiple of 7. Hence any ten consecutive integers includes at least one not divisible by 2, 3, 5, or 7. It follows that, for some \( j \), \( 0 \leq j \leq 9 \), we must have \( u - j \geq 83 \) and \( u - j \) not divisible by 2, 3, 5, or 7. Hence \( N(u - j) \geq 10 \) by Lemma 4. We set \( k = 8, m = u - j, \) and \( x = 8j + s \). Then

\[
km + x = 8u + s = v
\]

and

\[
0 \leq x < 80 < m.
\]

If \( x = 0 \), then

\[
N(v) \geq \min\{N(k), N(m)\} = 7
\]

by Lemmas 2 and 3. On the other hand, if \( x > 0 \) we apply Lemma 6 to obtain

\[
N(v) \geq \min\{N(k) - 1, N(k + 1) - 1, N(x)\}.
\]

Now \( N(k) - 1 = 6 \) and \( N(k + 1) - 1 = 7 \) by Lemma 3. Since \( x \equiv s \equiv v \) (mod 4) we have \( x \not\equiv 2 \) (mod 4). Since \( 3 \mid v \) and \( 3 \nmid km \), we have \( 3 \nmid x \). Hence \( N(x) \geq 3 \). Therefore \( N(v) \geq 3 \) and the proof is complete.

**Lemma 8.** \( N(v) \geq 3 \) if \( v \not\equiv 2 \) (mod 4), \( 3 \mid v \), and \( 8m < v < 9m \) where \( m \) is one of the 24 numbers

\[
8, 11, 13, 16, 17, 19, 23, 25, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59, 61, 64, 67, 71, 73, 79.
\]
(These numbers are the prime powers, except for powers of 3, from 8 to 79.)

Proof. We set

\[ v = 8m + x. \]

Then \( 0 < x < m \) and \( x \equiv v \equiv 2 \pmod{4} \). Since \( 3 \mid v \) and \( 3 \nmid m \) we have \( 3 \nmid x \). Hence \( N(x) \geq 3 \) by Lemma 4. Moreover \( N(m) = m - 1 \geq 7 \) by Lemma 3. Thus we may apply Lemma 6 with \( k = 8 \) to conclude

\[ N(v) \geq \min\{N(8) - 1, N(9) - 1, N(x)\} \geq 3, \]

and the proof is complete.

Lemmas 7 and 8 give us \( N(v) \geq 3 \) whenever \( v \equiv 2 \pmod{4} \) and \( 3 \mid v \) except for \( v \) in the following seven intervals:

- \( 0 < v < 64, 72 < v < 88, 99 < v < 104, 117 < v < 128, \)
- \( 171 < v < 184, 225 < v < 232, 288 < v < 296. \)

Now suppose \( v \equiv 0 \) or \( 1 \pmod{4} \). We already know that \( N(v) \geq 3 \) except when \( v \equiv 3 \) or \( 6 \pmod{9} \) and \( v \) is in one of the seven intervals listed above. There are eleven values of \( v \) in these seven intervals such that \( v \equiv 0 \) or \( 1 \pmod{4} \) and \( v \equiv 3 \) or \( 6 \pmod{9} \). These are

\[ v = 12, 21, 24, 33, 48, 57, 60, 84, 120, 177, 228. \]

For the six largest of these values we use Lemma 6 with \( k = 7 \) and the \( m \) and \( x \) given in the following table:

<table>
<thead>
<tr>
<th>( v )</th>
<th>( k )</th>
<th>( m )</th>
<th>( x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>57</td>
<td>7</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>60</td>
<td>7</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>84</td>
<td>7</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>120</td>
<td>7</td>
<td>17</td>
<td>1</td>
</tr>
<tr>
<td>177</td>
<td>7</td>
<td>23</td>
<td>16</td>
</tr>
<tr>
<td>228</td>
<td>7</td>
<td>31</td>
<td>11</td>
</tr>
</tbody>
</table>

It is readily seen that in each of these cases we have

\[ v = km + x, 0 < x < m, N(m) = m - 1 > k - 1, \]

and \( N(x) \geq 3 \).

Hence Lemma 6 gives us

\[ N(v) \geq \min\{N(7) - 1, N(8) - 1, N(x)\} \geq 3. \]

(For \( v = 57, 60, 84, 120 \) see [2] and [3].)
We have shown that \( N(v) \geq 3 \) whenever \( v \equiv 0 \) or \( 1 \) (mod 4) with the possible exceptions of \( v = 12, 21, 24, 33, 48 \).

3. The Main Result

Johnson, Dulmage, and Mendelsohn [6] have shown that \( N(12) \geq 5 \). Bose and Shrikhande [2] have shown that \( N(21) \geq 4 \) and \( N(24) \geq 3 \). Bose, Shrikhande, and Parker [3] have shown that \( N(33) \geq 3 \). Finally using Lemma 2 we obtain

\[ N(48) \geq \min\{N(12), N(4)\} = 3. \]

Combining these five special results with the results of the previous section we obtain our main result:

**Theorem.** If \( v \equiv 0 \) or \( 1 \) (mod 4), then there exist at least three mutually orthogonal Latin squares of order \( v \).

**References**