An estimate of the number of mutually orthogonal Latin squares

Chang Yanxun
Institute of Mathematics
Hebei Normal College
Shijiazhuang 050091
P. R. China

ABSTRACT. In this article we discuss the number of pairwise orthogonal Latin squares and obtain the estimate $n_r < 8(r+1)2^{4r}$ for $r \geq 2$.

1 Introduction

A *Latin square* of side n is an $n \times n$ array based on some set X of n symbols, with the property that every row and every column contains every symbol exactly once. In other words, every row and every column is a permutation of X.

Two Latin squares A and B of the same side n are called *orthogonal* if the n^2 ordered pairs (a_{ij}, b_{ij}) formed by superimposing one square on the other are all different.

Let $A_1, A_2, \ldots, A_k$ be Latin squares of the same side n. We call $\{A_1, A_2, \ldots, A_k\}$ a set of k mutually orthogonal Latin squares if A_i is orthogonal to A_j for any $i, j = 1, 2, \ldots, k$ whenever $i \neq j$. Let $N(m)$ denote the largest number of pairwise orthogonal Latin squares of order m.

Latin squares were first defined by Euler in 1782. He discussed orthogonality and in particular he considered the problem of thirty-six military officers, and conjectured that no pair of orthogonal Latin squares of side n can exist when n is congruent 2 modulo 4. G. Tarry [14] carried out a complete census of Latin squares of side 6, and proved Euler's conjecture is correct in that case. However, the rest of Euler's conjecture is wrong; Bose, Parker and Shrikhande proved in [4] that there is a pair of orthogonal Latin squares of every side greater than 6, a short proof of which was given by Stinson [13] and Zhu [17]. It was proved by Chowla et al. [8]

JCMCC 21 (1996), pp. 217-222

with the help of the Sieve methods of Brun that $N(n) > \frac{1}{3}n^{\frac{1}{91}}$ for all sufficiently large integers. After improvement by Rogers [12] and Wang [15], a crucial break through was obtained by Wilson [16] who proved the estimate $N(n) \geq n^{\frac{1}{17}}$ for sufficiently large integers. Based on an analysis of the combinatorial trick employed by R.M. Wilson, Beth [3] obtained the estimate $N(n) \geq n^{\frac{1}{14.8}}$ for sufficiently large integers by using substantially more exact results from the theory of Sieves.

Latin squares have an important role in the construction of block designs and are one of the most essential concepts in the field of design theory. Many mathematicians have worked on them; in addition to the works already cited, see [2], [6], [7], [9], [10].

Let n_r denote the smallest number such that $N(n) \geq r$ if and only if $n \geq n_r$. Beth's asymptotic estimate $N(n) \geq n^{\frac{1}{14.8}}$ for n large provides a lower bound $n_r < r^{14.8}$ for r large. But we do not know for how large r the lower bound $n_r < r^{14.8}$ is valid. In this article we will give a lower bound of n_r for any integer $r \geq 2$.

2 Preliminaries

Let π_n denote the product of all primes $p \leq n$. We quote Lemma 8.2.5 and Theorem 8.2.4 from pages 382–388 in [11] as follows.

Lemma 2.1. *If real number $x \geq 2$, then $\sum_{p \leq x} \ln p < (2 \ln 2)x$.*

Lemma 2.2. *For any real number $x \geq 1$, there exists a prime p such that $x < p \leq 2x$.*

Corollary 2.3. *If $n \geq 2$, $\pi_n < e^{(2 \ln 2)n}$.*

Proof: It is immediate from Lemma 2.1. □

We also need the following Lemmas.

Lemma 2.4. *Suppose that $n = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$ where the p_i are distinct primes and each $a_i \geq 1$. Then*

$$N(n) \geq \min_i (p_i^{a_i} - 1).$$

Lemma 2.5. [16] *If $0 \leq u \leq g$, then for any integer m*

$$N(mg + u) \geq \min\{N(m), N(m+1), N(g) - 1, N(u)\}.$$

3 The estimate of n_r

In this section we will provide a bound on n_r. First we give the following Lemmas.

Lemma 3.1. *For any odd integer $r \geq 5$, there is an integer m prime to $(r+1)!$ satisfying $m \leq 2^r - 1$, such that $N(m) \geq r$ and $N(m+1) \geq r$.*

Proof: By Lemma 2.2, there is an odd prime p such that

$$\frac{r}{2} < p \leq r.$$

Let q be any prime divisor of $2^p - 1$ and let

$$d = \gcd(p, q-1). \tag{1}$$

Since $2^p \equiv 1 \pmod{q}$, by the definition of q, and since $2^{q-1} \equiv 1 \pmod{q}$, by Fermat's theorem, we get $2^d \equiv 1 \pmod{q}$, thus $d \neq 1$. This implies $d = p$. From (1) we get $p|(q-1)$. Since p is an odd prime, $q \geq 2p+1 > r+1$. Since $r < q-1$, each prime divisor q of 2^p-1 satisfies $N(q) > r$. By Lemma 2.4 we have $N(2^p-1) > r$ and a $N(2^p) = 2^p - 1 \geq r$. Also, 2^p-1 is prime to $(r+1)!$ because each prime divisor q is greater than $r+1$. Define $m = 2^p-1$. Then m is prime to $(r+1)!$ as well as to π_{r+1} and

$$m = 2^p - 1 \leq 2^r - 1.$$

□

Lemma 3.2. *Let m, r be defined as in Lemma 3.1. For any positive integer n, define $h = 0$ (if n is even) or any given positive integer (if n is odd). Then there are odd integers t and u such that $N(|t|)$, $N(u) \geq r+1$, $0 < u \leq 2^h m \pi_{r+1}$ and*

$$n = 2^h m t + u.$$

Proof: By Lemma 3.1, $(m, (r+1)!) = 1$. By the definition of h, for every prime $q \leq r+1$, there exists an odd integer t_q satisfying the following congruences

$$t_q \not\equiv 0, \; n - 2^h m t_q \not\equiv 0 \pmod{q}. \tag{2}$$

By the Chinese Remainder Theorem the congruences

$$t \equiv t_q \pmod{q}, \text{ for every prime } q \leq r+1,$$

have a simultaneous solution t. By (2), $(t, q) = 1$ for every prime $q \leq r+1$, which implies $N(|t|) \geq r+1$. Now put $u = n - 2^h m t$, congruences (2) imply $u \not\equiv 0 \pmod{q}$ for any prime $q \leq r+1$. It follows that $N(|u|) \geq r+1$. So

$$n = 2^h m t + u \text{ and } N(|t|), N(|u|) \geq r+1. \tag{3}$$

It is easy to show that $t \pm \pi_{r+1}$ and $u \pm 2^h m\pi_{r+1}$ satisfy (3). Hence, we may assume that $0 < u \leq 2^h m\pi_{r+1}$ with $N(u) \geq r+1$. □

Lemma 3.3. *When* $r \geq 5$, $n_r < (2^r - 1)2^{r+1}(r+1)\pi_{r+1}$.

Proof: By taking $h = \lfloor \log_2(r+1) \rfloor + 1$ (if n is odd) or 0 (if n is even) in Lemma 3.2, any $n \geq (2^r - 1)2^{r+1}(r+1)\pi_{r+1}$ can be written as

$$n = 2^h mt + u, \qquad 0 < u \leq 2^h m\pi_{r+1} \tag{4}$$

where $N(|t|)$, $N(u) \geq r+1$. So

$$2^h mt + u \geq (2^r - 1)2^{r+1}(r+1)\pi_{r+1}.$$

By Lemma 3.1, noticing that $m \leq 2^r - 1$ and $2^{h-1} \leq r+1$, we have

$$\begin{aligned} 2^h mt &\geq (2^r - 1)2^{r+1}(r+1)\pi_{r+1} - u \\ &\geq (2^r - 1)2^{r+1}(r+1)\pi_{r+1} - 2^h m\pi_{r+1} \\ &\geq (2^r - 1)2^{r+1}(r+1)\pi_{r+1} - 2(r+1)(2^r - 1)\pi_{r+1} \\ &= 2(2^r - 1)(r+1)\pi_{r+1}(2^r - 1) \end{aligned}$$

and

$$2^h mt \leq 2(r+1)(2^r - 1)t.$$

Thus

$$t \geq \pi_{r+1}(2^r - 1) > 0. \tag{5}$$

By (4) and (5), we have

$$0 < u \leq 2^h m\pi_{r+1} \leq 2^h(2^r - 1)\pi_{r+1} \leq 2^h t.$$

Applying Lemma 2.5 with $g = 2^h t$, noticing that $N(g) = N(t) \geq r+1$ (if n is even) and $N(g) \geq \min\{N(2^h), N(t)\} \geq r+1$ (if n is odd), we obtain

$$N(n) = N(mg + u) \geq \min\{N(m), N(m+1), N(g) - 1, N(u)\} \geq r.$$

Therefore, we get

$$n_r < (2^r - 1)2^{r+1}(r+1)\pi_{r+1}.$$

□

Lemma 3.4. [1, 5] $n_2 \leq 7$, $n_3 \leq 11$, $n_4 \leq 43$, $n_5 \leq 63$, $n_6 \leq 77$.

Theorem. *If* $r \geq 2$, *then* $n_r < 8(r+1)2^{4r}$.

Proof: When $r \geq 5$, the conclusion follows by Corollary 2.3 and Lemma 3.3. When $2 \leq r < 5$, by Lemma 3.4 it is easy to directly check that $n_r < 8(r+1)2^{4r}$. □

References

[1] J. Abel, X. Zhang and H. Zhang, Three mutually orthogonal idempotent Latin squares of orders 22 and 26, preprint.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986.

[3] T. Beth, Eine Bemerkung zur Abschätzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren, *Abh. Math. Sem. Univ. Hamburg* **53** (1983), 184–188.

[4] R.C. Bose, S.S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* **12** (1960), 189–203.

[5] A.E. Brouwer, *The number of mutually orthogonal Latin squares — a table up to order 10000*, Research Report ZW 123/79, Math. Centrum, Amsterdam, 1979.

[6] A.E. Brouwer, A series of separable designs with application to pairwise orthogonal Latin squares, *Europ. J. Combinatorics* **1** (1980), 39–41.

[7] A.E. Brouwer and G.H.J. van Rees, More mutually orthogonal Latin squares, *Discrete Math.* **39** (1982), 263–281.

[8] S. Chowla, P. Erdos and E.G. Straus, On the maximal number of pairwise orthogonal Latin squares of a given order, *Canad. J. Math.* **12** (1960), 204–228.

[9] J. Dénes and A.D. Keedwell, *Latin Squares and their Applications*, Akademai Kiudo, Budapest 1974.

[10] R.C. Mullin, P.J. Schellenburg, D.R. Stinson and S.A. Vanstone, Some results on the existence of squares, *Ann. Discrete Math.* **6** (1980), 257–274.

[11] Pan Chengdong et al, *Elementary Number Theory*, Peking University Press, 1992.

[12] K. Rogers, A note on orthogonal Latin squares, *Pacific J. Math.* **14** (1964), 1395–1397.

[13] D.R. Stinson, A short proof of non-existence of a pair orthogonal Latin squares of order 6, *J. Combinatorial Theory (A)* **36** (1984), 373–376.

[14] G. Tarry, Le probleme de 36 officiers, *Compters Rendus de L'Association Francaise Pour L'Avancement de Science* **1;2** (1900;1901), 122–123; 170–203.

[15] Wang Yuan, On the maximal number of pairwise orthogonal Latin squares, *Acta Math.* **16** (1966), 400–410.

[16] R.M. Wilson, Concerning the number of mutually orthogonal Latin squares, *Discrete Math.* **7** (1974), 181–198.

[17] L. Zhu, A short disproof of Euler's conjecture concerning orthogonal Latin squares (with editorial comment by A. D. Keedwell), *Ars Combinatoria* **14** (1982), 47–55.