A NOTE ON ORTHOGONAL LATIN SQUARES

KENNETH ROGERS

1. Introduction. The purpose of this note is to give an improved estimate for $N(n)$, the maximal number of pairwise orthogonal Latin squares, by following the method of Chowla, Erdös and Straus [2]. The difference is that we use a result of Buchstab [1] rather than that of Rademacher in the sieve argument. Our result is that if c is any number less than $1/42$, then for all large n we have $N(n) > n^c$.

In the notation of Buchstab, write $P_\omega(x; x^{1/\alpha})$ for the number of positive integers not exceeding x which do not lie in any of the progressions a_0 mod p_0, a_i mod p_i, or b_i mod p_i, where $p_0 = 2$, and p_i runs over the primes from 3 to $x^{1/\alpha}$. The subscript ω refers to the fact that P depends on the a_i, b_i. Buchstab proves that

$$P_\omega(x; x^{1/\alpha}) > \lambda(\alpha)\frac{c'x}{(\log x)^2} + 0\left(\frac{x}{(\log x)^3}\right), \tag{1}$$

where c' is a constant 0.4161 and $\lambda(5) \geqq 0.96$.

The properties of $N(n)$ used for the proof are those of [2]:

A. $N(ab) \geqq \operatorname{Min}\{N(a), N(b)\}$.

B. $N(n) \leqq n - 1$, with equality when n is a prime-power.

C. If $k \leqq 1 + N(m)$ and $1 < u < m$, then

$$N(u + km) \geqq \operatorname{Min}\{N(k), N(k+1), 1 + N(m), 1 + N(u)\} - 1.$$

We note that A and B are due to H. F. MacNeish, while C was found by Bose and Shrikhande.

2. Lower estimation of $N(n)$. We must deal separately with odd n and even n, and we use a fact proven in [1], called there "Lemma D":

D. The number of integers no greater than x, which have a prime factor in common with n and greater than n^g, is no greater than x/gn^g.

Estimate for even n. We pick k so that

$$\begin{cases} k \equiv -1 \pmod{2^{[\log_2 n/\alpha]}}, \\ k \not\equiv 0 \text{ or } -1 \pmod{p} \text{ for } 3 \leqq p \leqq n^{1/\beta}, \\ k \leqq n^{1/\gamma}. \end{cases} \tag{2}$$

Received December 11, 1963. Partially supported by NSF contract GP 1925.

Since $k = -1 + h2^{[\log_2 n/\alpha]}$, say, we know the number of such k is $P_\omega((1 + n^{1/\gamma})/2^{[\log_2 n/\alpha]}; n^{1/\beta})$. In view of Buchstab's theorem, we take $1/\gamma - 1/\alpha = 5/\beta$ and then have, for some positive constant c and all large n,

$$P_\omega > c \cdot \frac{n^{5/\beta}}{\log^2 n},$$

Our k have no prime factor below $n^{1/\beta}$, so to choose k also prime to n we must deal with the primes in n which are greater than $n^{1/\beta}$. By D, the number of integers below $n^{1/\gamma}$, which have a prime factor which exceeds $n^{1/\beta}$ and divides n, is at most $n^{1/\gamma}/(1/\beta)n^{1/\beta}$. Since we want this to be less than the number of k, we take $1/\gamma = (6-\varepsilon)/\beta$, where $0 < \varepsilon < 1$. Then, for all large n we can choose k as above so as to be prime to n. Note that we now have $1/\alpha = (1 - \varepsilon)/\beta$. Since all prime factors of k exceed $n^{1/\beta}$, and due to the restrictions on $k+1$, we deduce from A and B that:

$$N(k) > n^{1/\beta} - 1$$

$$N(k + 1) > \operatorname{Min}\left(\frac{1}{2}n^{1/\alpha}, n^{1/\beta}\right) - 1,$$

and we note that for all large n both these estimates exceed $n^{1/\alpha}/3$. Now, since we want to have $n = u + mk$, write

$$n = n_1 + n_2 k, \qquad 0 < n_1 < k, \qquad (n_1, k) = 1,$$

and

$$u = n_1 + u_1 k.$$

Now choose u_1 so that:

$$\text{(3)} \qquad \begin{cases} u_1 \not\equiv n_1 \pmod 2, \\ \left.\begin{array}{l} u_1 \not\equiv -n_1/k \pmod p, \ p \nmid k \\ u_1 \not\equiv n_2 \pmod p \end{array}\right\} 3 \leqq p \leqq k, \\ u_1 < n^{1/\delta}. \end{cases}$$

By Buchstab, this is all right as long as $k \leqq n^{1/5\delta}$, so we choose $1/\delta = 5/\gamma = 5(6-\varepsilon)/\beta$. No prime less than or equal to k can divide u: for u is prime to k, and those primes below k which don't divide k do not divide u, by (3). Hence

$$\text{(4)} \qquad N(u) \geqq k > N(k) > \frac{1}{3} n^{1/\alpha}.$$

Finally, $m = (n - u)/k$, of course; so $m - u = \{n - (1 + k)u\}/k$, which we want to make positive. Since $(1+k)u << n^{2/\gamma+1/\delta}$, choose β so that $7\cdot(6-\varepsilon)/\beta < 1$, or equivalently $1/\alpha < (1-\varepsilon)/7(6-\varepsilon)$. Thus we can achieve the conditions so far expressed for all large n, as long as α is any chosen number exceeding 42. As to $N(m)$, note that $m = n_2 - u_1 \not\equiv 0 \pmod p$ for $3 \leqq p \leqq k$. Also u is odd, by (3), and n is even; hence m is odd. Thus

$$N(m) \geqq k > N(k) > \frac{1}{3} n^{1/\alpha} . \tag{5}$$

The conditions of C apply now, and the above estimates and C imply that for any constant c less than 1/42 we have:

$$N(n) > n^c\,, \quad \textit{for all large even } n.$$

Estimate for odd n. This time k is chosen even, the conditions being:

$$\begin{aligned} &k+1 \equiv 1 \pmod{2^{[\log_2 n/\alpha]}}\,, \\ &k+1 \not\equiv 0 \text{ or } 1 \pmod p \text{ for } 3 \leqq p \leqq n^{1/\beta}\,, \\ &k+1 \leqq n^{1/\gamma}\,. \end{aligned}$$

With obvious changes in detail from the previous case, we still get $\operatorname{Min}\{N(k), N(k+1)\} > 1/3(n)^{1/\alpha}$, and $(n,k) = 1$. This time, the relation $n - u = (n_2 - u_1)k$ ensures that u is odd, but we must adjust the parity condition on u_1 to ensure that m is odd:

$$\begin{aligned} &u_1 \not\equiv n_2 \pmod 2 \\ &\left.\begin{aligned} &u_1 \not\equiv -n_1/k \pmod p, \text{ for } p \nmid k, \\ &u_1 \not\equiv n_2 \pmod p \end{aligned}\right\} 3 \leqq p \leqq k\,, \\ &u_1 < n^{1/\delta}\,. \end{aligned}$$

Thus $m = n_2 - u_1$ is odd, and now the details are as before, giving finally the following result.

THEOREM. *To each number c which is less than* 1/42, *there corresponds an integer* $n_0 = n_0(c)$, *such that for all* $n > n_0$ *we have*

$$N(n) > n^c\,.$$

REFERENCES

1. A. A. Buchstab, *Sur la decomposition des nombres paires. . . .* , Comptes Rendus (Doklady) de l'Academie des Sciences de l'URSS 1940. Volume XXIX, No. 8-9, pp. 544-548.

2. S. Chowla, P. Erdös, and E. G. Straus, *On the maximal number of pairwise orthogonal latin squares of a given order*, Can. J. Math., **12**, pp. 204-208.