

Pacific Journal of Mathematics

A NOTE ON ORTHOGONAL LATIN SQUARES

K. ROGERS

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

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

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

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

- A. $N(ab) \geq \text{Min} \{N(a), N(b)\}$.
- B. $N(n) \leq n - 1$, with equality when n is a prime-power.
- C. If $k \leq 1 + N(m)$ and $1 < u < m$, then

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

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^a , is no greater than x/gn^a .

Estimate for even n . We pick k so that

$$(2) \quad \begin{cases} k \equiv -1 \pmod{2^{\lceil \log_2 n / a \rceil}}, \\ k \not\equiv 0 \text{ or } -1 \pmod{p} \text{ for } 3 \leq p \leq n^{1/\beta}, \\ k \leq n^{1/\gamma}. \end{cases}$$

Since $k = -1 + h2^{\lceil \log_2 n/\alpha \rceil}$, say, we know the number of such k is $P_\omega((1 + n^{1/\gamma})/2^{\lceil \log_2 n/\alpha \rceil}; n^{1/\beta})$. 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 :

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

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

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

$$n = n_1 + n_2k , \quad 0 < n_1 < k , \quad (n_1, k) = 1 ,$$

and

$$u = n_1 + u_1k .$$

Now choose u_1 so that :

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

By Buchstab, this is all right as long as $k \leq n^{1/\delta}$, 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

$$(4) \quad N(u) \geq k > N(k) > \frac{1}{3} n^{1/\alpha} .$$

Finally, $m = (n - u)/k$, of course ; so $m - u = \{n - (1 + k)u\}/k$, which

we want to make positive. Since $(1 + k)u \ll n^{2/\gamma+1/\delta}$, choose β so that $7 \cdot (6 - \epsilon)/\beta < 1$, or equivalently $1/\alpha < (1 - \epsilon)/7(6 - \epsilon)$. 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 $3 \leq p \leq k$. Also u is odd, by (3), and n is even; hence m is odd. Thus

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

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

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

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

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

With obvious changes in detail from the previous case, we still get $\text{Min} \{N(k), N(k + 1)\} > 1/3(n)^{1/\alpha}$, 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:

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

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

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

ROBERT OSSERMAN

Stanford University
Stanford, California

M. G. ARSOVE

University of Washington
Seattle 5, Washington

J. DUGUNDJI

University of Southern California
Los Angeles 7, California

LOWELL J. PAIGE

University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and on submission, must be accompanied by a separate author's résumé. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is \$18.00; single issues, \$5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$8.00 per volume; single issues \$2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics

Vol. 14, No. 4

August, 1964

Homer Franklin Bechtell, Jr., <i>Pseudo-Frattini subgroups</i>	1129
Thomas Kelman Boehme and Andrew Michael Bruckner, <i>Functions with convex means</i>	1137
Lutz Bungart, <i>Boundary kernel functions for domains on complex manifolds</i>	1151
L. Carlitz, <i>Rings of arithmetic functions</i>	1165
D. S. Carter, <i>Uniqueness of a class of steady plane gravity flows</i>	1173
Richard Albert Dean and Robert Harvey Oehmke, <i>Idempotent semigroups with distributive right congruence lattices</i>	1187
Lester Eli Dubins and David Amiel Freedman, <i>Measurable sets of measures</i>	1211
Robert Pertsch Gilbert, <i>On class of elliptic partial differential equations in four variables</i>	1223
Harry Gonshor, <i>On abstract affine near-rings</i>	1237
Edward Everett Grace, <i>Cut points in totally non-semi-locally-connected continua</i>	1241
Edward Everett Grace, <i>On local properties and G_δ sets</i>	1245
Keith A. Hardie, <i>A proof of the Nakaoka-Toda formula</i>	1249
Lowell A. Hinrichs, <i>Open ideals in $C(X)$</i>	1255
John Rolfe Isbell, <i>Natural sums and abelianizing</i>	1265
G. W. Kimble, <i>A characterization of extremals for general multiple integral problems</i>	1283
Nand Kishore, <i>A representation of the Bernoulli number B_n</i>	1297
Melven Robert Krom, <i>A decision procedure for a class of formulas of first order predicate calculus</i>	1305
Peter A. Lappan, <i>Identity and uniqueness theorems for automorphic functions</i>	1321
Lorraine Doris Lavalley, <i>Mosaics of metric continua and of quasi-Peano spaces</i>	1327
Mark Mahowald, <i>On the normal bundle of a manifold</i>	1335
J. D. McKnight, <i>Kleene quotient theorems</i>	1343
Charles Kimbrough Megibben, III, <i>On high subgroups</i>	1353
Philip Miles, <i>Derivations on B^* algebras</i>	1359
J. Marshall Osborn, <i>A generalization of power-associativity</i>	1367
Theodore G. Ostrom, <i>Nets with critical deficiency</i>	1381
Elvira Rapaport Strasser, <i>On the defining relations of a free product</i>	1389
K. Rogers, <i>A note on orthogonal Latin squares</i>	1395
P. P. Saworotnow, <i>On continuity of multiplication in a complemented algebra</i>	1399
Johanan Schonheim, <i>On coverings</i>	1405
Victor Lenard Shapiro, <i>Bounded generalized analytic functions on the torus</i>	1413
James D. Stafney, <i>Arens multiplication and convolution</i>	1423
Daniel Sterling, <i>Coverings of algebraic groups and Lie algebras of classical type</i>	1449
Alfred B. Willcox, <i>Šilov type C algebras over a connected locally compact abelian group. II</i>	1463
Bertram Yood, <i>Faithful $*$-representations of normed algebras. II</i>	1475
Alexander Zabrodsky, <i>Covering spaces of paracompact spaces</i>	1489