JOURNAL OF ALGEBRA 20, 83-89 (1972)

Room Quasigroups and Fermat Primes

R. G. STANTON AND R. C. MULLIN

University of Manitoba and University of Waterloo

Received December 25, 1970

TO PROFESSOR RICHARD BRAUER, TO COMMEMORATE HIS SEVENTIETH BIRTHDAY, FEBRUARY 10, 1971

1. INTRODUCTION

A Room Square is a square of side $v = 2n + 1$ with the properties that (1) each cell is either empty or filled by an unordered pair from $v + 1$ symbols, often denoted by $1, 2,..., v, \infty$; (2) each row and column contains every symbol exactly once, that is, there are precisely n blank cells in each row and column; (3) each of the $(v + 1) v/2$ unordered pairs of symbols occurs in exactly one cell.

The definition given in the first paragraph is purely combinatorial; however, it was first pointed out by R. H. Bruck [4] that Room Squares were intimately associated with quasigroups. One numbers the rows and columns of the square from 1 to v, and then permutes elements so that one has a normalized Room Square with the pair ∞, i, appearing in cell (i, i). Then binary operations θ and ϕ are defined on $G = \{1, 2,..., v\}$ as follows:

(1) If $x \in G$, $y \in G$, $x \neq y$, and the pair x, y, lies in cell (a, b), then $x\theta y = a$, $x\phi y = b$ (thus θ and ϕ are row and column selectors);

(2) $x\theta x = x\phi x = x$ for all $x \in G$.

Thus, (G, θ) and (G, ϕ) are commutative idempotent quasigroups (Room quasigroups) on v elements and they satisfy the following orthogonality conditions:

(1) If $p \in G$, $x \in G$, $y \in G$, $x\theta y = x\phi y = p$, then $x = y = p$;

(2) If $p \in G$, $q \in G$, $p \neq q$, then there is at most one unordered pair x, y, with $x \in G$, $y \in G$, such that $x\theta y = p$, $x\phi y = q$.

As Bruck has pointed out in Ref. [4], not only does a Room Square produce a pair of orthogonal Room quasigroups (G, θ) and (G, ϕ) as above, but the converse holds; such an orthogonal pair produces a normalized Room Square by reversing the construction. We shall find it most convenient to use the combinatorial approach, and phrase our results on Room Squares; however, it is important to note that these results, as well as all other mentioned in the references, can be interpreted as results on orthogonal pairs of commutative idempotent quasigroups.

Historically, Room Squares were first defined by E. C. Howell (see Refs. [3] and [6]) and by T. G. Room [12], and a few early results appear in Refs. [1, 2, 4, 18]. We shall have need of a number of more recent results, which we tabulate here by letter.

(a) There is a Room Square of odd side v for $7 \leqslant v \leqslant 47$ (see Ref. [15]).

(b) There is a Room Square of side v for any prime power $v = p^a$, provided that v is not equal to 3, 5, 257, 65537 (see Refs. [10] and [9]). These exceptional cases occur among the Fermat numbers $F_k = 2^{2^k} + 1$, and are the cases $F_0 = 3, F_1 = 5, F_3 = 257, F_4 = 65537$.

(c) If Room Squares of sides v_1 and v_2 exist, so does a Room Square of side $v_1 v_2$ (see Refs. [13] and [14]).

(d) If Room Squares of sides v_1 and v_2 exist, so does a Room Square of side $v_1(v_2 - 1) + 1$ (see Refs. [7] and [9]).

(e) If v is not divisible by F_0, F_1, F_3, F_4, then there is a Room Square of side $2v + 1$ (see Refs. [17] and [11, Lemma 3]).

(f) If s is an odd prime power, $s \neq F_0^a$, $s \neq F_k$ (where F_k is any Fermat prime), then there is a Room Square of side $5s$ (see Ref. [8]).

(g) It follows from (b) and (c) that, if v is not divisible by F_0, F_1, F_3, or F_4, then there exists a Room Square of side v.

A complete survey of the state of the art in Room Square theory up to early 1970 is found in Ref. [16].

2. Products of F_i ($i = 0, 1, 2, 3, 4$)

We begin this section by noting that a Room Square of side $F_2 = 17$ is known to exist, by (a). Hence, we leave further discussion of this prime until Section 4. We let $R = \{F_0, F_1, F_3, F_4\}$.

Lemma 1. *Let $v = F_0^{a_0} F_1^{a_1} F_3^{a_3} F_4^{a_4}$, for nonnegative integers a_0, a_1, a_3, a_4, and denote $a_0 + a_1 + a_3 + a_4$ by $w(v)$. If $w(v) \neq 1$, then there is a Room Square of side v.*

Proof. If $w(v) = 0$, then $v = 1$, and there is trivially a Room Square.

If $w(v) = 2$, there are 10 values of v to consider. If $v = F_i^2$, for some $F_i \in R$, there is a square of side v by (b). A square of side $F_0 F_1$ exists by (a). For the remaining cases, we write $F_0 F_3 = 7(111 - 1) + 1$; $F_0 F_4 =$

$19661(11 - 1) + 1$; $F_1F_3 = 107(13 - 1) + 1$; $F_1F_4 = 27307(13 - 1) + 1$; $F_3F_4 = 21931(769 - 1) + 1$. Squares of these sides exist by (d) and (g).

If $w(v) = 3$, there are 20 possible values for v. If $v = F_i^3$ for some $F_i \in R$, there is a square of side v by (b).

There is a square of side $F_0^2F_1$ by (a). For other multiples of F_0^2, we write $F_0^2F_3 = 289(9 - 1) + 1$; $F_0^2F_4 = 4337(137 - 1) + 1$; and there are squares of these sides by (d) and (g).

We dispose of the remaining multiples of F_0 as follows. Write $F_0F_1^2 = 2(37) + 1$; $F_0F_3^2 = 2(99073) + 1$; $F_0F_4^2 = 2(6442647553) + 1$; $F_0F_1F_3 = 2(1927) + 1$; $F_0F_1F_4 = 2(491527) + 1$; $F_0F_3F_4 = 2(25264513) + 1$ Squares of these sides exist by (e).

We treat the remaining multiples of F_1^2. Since $F_1^2F_3 = 73(89 - 1) + 1$ and $F_1^2F_4 = 204803(9 - 1) + 1$, squares of these sides exist by (d) and (g).

There are squares of side $F_1F_3^2$ and $F_1F_4^2$ by (f) or by consideration of the number-theoretic identities $F_1F_3^2 = 95((25(141 - 1) + 1) - 25) + 25$ $F_1F_4^2 = 130948121(165 - 1) + 1$. Also $F_1F_3F_4 = (45083)(1869 - 1) + 1$; $1869 = 21.89$; thus squares of these sides exist by (a), (c), (d), and (g). Since $F_3^2F_4 = (8454401)(513 - 1) + 1$ and $513 = 19.3^3$, there are squares of these sides by (a), (c), (d), and (g).

To complete the case when $w(v) = 3$, we write

$$F_3F_4^2 = 89539283(12337 - 9) + 9; \quad 12337 = 169.73; \quad 73 = 9(9 - 1) + 1;$$

which shows the existence of squares of these sides by the methods of Ref. [9].

Now if $w(v) \geqslant 4$, we can write $v = v_1v_2$, where v_2 is a product of 2 (not necessarily distinct) primes of v. Therefore $w(v_1) \geqslant 2$ and $w(v_2) = 2$. The lemma follows by induction, using (c).

We now use the preceding lemma to prove:

THEOREM 1. *Let U be the set of odd positive integers for which no Room Square exists; let $R = \{F_0, F_1, F_3, F_4\}$. Then there is a function $\mu\colon U \to R$ such that for each $v \in U$*

(i) $\mu(v) \mid v, \qquad (\mu(v))^2 \nmid v;$

(ii) *no other member of R divides v.*

Proof. Let v be an odd positive integer. We extend the definition of $w(v)$ given in Lemma 1 as follows. We write $v = F_0^{a_0}F_1^{a_1}F_3^{a_3}F_4^{a_4}n = mn$, where $(F_i, n) = 1$, $i = 0, 1, 3, 4$. We define $w(v)$ as $a_0 + a_1 + a_3 + a_4$. Thus $w(v) = w(m)$, and if $w(v) \neq 1$, there is a square of side v by Lemma 1, (c), and (g). If no square of side v exists, then $w(v) = 1$. In this event, we denote the unique member of R which divides v by $\mu(v)$, and the theorem follows.

3. Squares of Side $5s$

In this section, we eliminate the Fermat prime $F_1 = 5$ from further consideration by showing that (for $s > 1$) a Room Square of side $5s$ always exists. If s is a prime power other than 3^a or a Fermat prime F_k, the result is simply (f). If $s = 3^a$, we appeal to (a) for $a = 1$ or 2, and write $5s = 15.3^{a-2}$ for $a > 2$ (then using (a), (b), and (c)). We then establish the following theorem.

Theorem 2. *Let $F_k = 2^{2^k} + 1$; then there exists a room square of side $5F_k$.*

Proof. Since $5F_0 = 15$, $5F_1 = 25$, we see that (a) permits us to assume that $k \geqslant 2$. Then $5F_k = (5.2^{2^k} + 4) + 1 = 4(5.2^{2^k-2} + 1) + 1 = 4R + 1$. For $k \geqslant 2$, we see that $2^k - 2$ is even, and hence $R \equiv 0 \pmod 3$, say $R = 3S$. Thus $5F_k = 12S + 1$.

Now $F_k = F_0F_1 \cdots F_{k-1} + 2$, and hence the relationship $5F_k = 12S + 1$ reduces to $5F_1F_2 \cdots F_{k-1} = 4S - 3$. This trinomial relationship at once shows that $(S, 3) = 1$ and $(S, F_i) = 1$ for $i > 0$; hence, we have

$$5F_k = 12S + 1 = S(13 - 1) + 1,$$

and S is relatively prime to all F_k. Then, by results (g) and (d), we see that a square of side $5F_k$ exists. Indeed, using the construction in Ref. [9], we have the following:

Corollary 1. *There exists a square of side $5F_k$ containing a subsquare of side 13 ($k \geqslant 2$).*

By virtue of Ref. [8], it is possible now to consider the general case $5s$. We do this in the following:

Theorem 3. *If $v = 5s$, where s is an odd integer > 1, then there is a Room Square of side v.*

Proof. In Ref. [8] it is shown that there is a Room Square of side $5p$ for all odd non-Fermat primes p. By Theorem 2, there is a square of side $5p$ for all Fermat primes p. Now let us assume that v is such that the theorem fails. By Theorem 1 and the above remarks, v may be written as $v = 5pr$ where r is a prime and a square of side r exists, since r is not divisible by any member of R. Thus there is a square of side $(5p)^r$ by (c), and this fact contradicts the choice of v. Thus Theorem 3 is proved.

4. Products of Fermat Numbers

We really only have to consider primes in the set of F_k's; of course, it is not known whether there are any such for $k > 4$. The following results can be obtained.

THEOREM 4. *There exists a Room Square of side $3F_k$ for all k.*

Proof. $3F_0 = 9$, $3F_1 = 15$, and we appeal to (a). The case $3F_2 = 51$ was first treated in Ref. [5]; so take $k \geqslant 3$. From the identity $3F_k = 2(3.2^{2^k-1} + 1) + 1 = 2(6.2^{2^k-2} + 1) + 1 = 2(6.4^{2^k-1} + 1) + 1 = 2R + 1$, we see that $R = 0 \pmod 5$, say $R = 5S$, and deduce that $3F_k = 10S + 1$. From $F_k = 2 + F_0F_1 \cdots F_{k-1}$, we obtain $3F_0F_2 \cdots F_{k-1} + 1 = 2S$ and deduce that $(S, F_i) = 1$ for $F_i \neq 5$.

If $(S, 5) = 1$, then $3F_k = S(11 - 1) + 1$, and (d) produces a Room Square; if $(S, 5) = 5$, write $S = 5^aT$, where $(T, 5) = 1$; then $3F_k = 5^aT(11 - 1) + 1$. For $a > 1$, a square of side 5^aT exists by (b) and (c); for $a = 1$, by (f). Hence we obtain the theorem, as well as

COROLLARY 2. *There exists a Room Square of side $3F_k$ with a subsquare of side 11 ($k \geqslant 3$).*

For completeness, we mention the trivial result:

THEOREM 5. *There exists a Room Square of side $17F_k$ for all k.*

Proof. This follows from (c), since a Room Square of side 17 exists, and (b); except for $k = 0, 1, 3, 4$. The first two cases are treated in Theorems 3 and 4; the last two follow from $17F_3 = 91(49 - 1) + 1$, $17F_4 = 2579(433 - 1) + 1$.

THEOREM 6. *There exists a Room Square of side $257F_k$ for all k.*

Proof. From the preceding results, take $k \geqslant 4$. Then $257F_k = 256(1 + 257.2^{2^k-8}) + 1 = 256R + 1$. Since $k > 3$, $R \equiv 0 \pmod 3$, say $R = 3S$; thus $257F_k = 768S + 1$. Replace F_k by $2 + F_0F_1 \cdots F_{k-1}$, and simplify to $257F_1F_2 \cdots F_{k-1} + 3^2.19 = 256S$; this shows that $(S, F_i) = 1$ for all Fermat numbers F_i. Thus, we have $257F_k = (769 - 1)S + 1$, and (g) thus gives the result.

COROLLARY 3. *There exists a Room Square of side $257F_k$ with a subsquare of side 769($k \geqslant 4$).*

Finally, we establish the following:

THEOREM 7. *There exists a Room Square of side $65537F_k$ for all k.*

Proof. In light of the previous results, we may take $k \geqslant 5$. Then $65537F_k = 65536(3R) + 1$. Also $65537F_1F_2 \cdots F_{k-1} + 43691 = 65536R$, and thus $(R, F_i) = 1$ for $i > 0$.

If $R = 3^bS$, $b \neq 1$, then a square of side R exists, and the theorem follows from the relationship $65537F_k = R(196609 - 1) + 1$, since a square of side $196609 = 1 + 3.2^{16} = 4 + 3F_0F_1F_2F_3$ does exist. If $b = 1$, we write

$65537F_k = (65536)9S + 1$, where S is prime to all F_i. Then $9.2^{16} = 589825 - 1 = 5^2(23593) - 1$, and we know that a square of side 589825 exists. This completes the theorem.
We record an obvious extension in the following theorem:

THEOREM 8. *If k and m are greater than 4, then a Room Square of side F_kF_m exists.*

Proof. Squares of sides F_k and F_m exist by (b). Hence we need merely employ (c).

COROLLARY 4. *If v is a product of n (not necessarily distinct) Fermat primes ($n > 1$), then a Room Square of side v exists.*

Proof. We write $v = P_1P_2$, where P_1 involves primes F_0, F_1, F_3, F_4; P_2 involves all other Fermat primes. Let there be r_1 primes in P_1, r_2 in P_2. If $r_1 > 1$, then a square of side P_1 exists (Lemma 1); hence a square of side P_1P_2 exists by (b) and (c). If $r_1 = 1$, $r_2 \geq 1$, we may write $P_1P_2 = (F_iF_j)\,P_3$, where i is 0, 1, 3, or 4; $j > 4$; $F_jP_3 = P_2$. Then Theorems 3, 4, 6, and 7, with (b) and (c), give the result. Finally, if $r_1 = 0$, we use Theorem 8.

5. ROOM SQUARES OF SIDE $3s$

In this section we prove the following:

THEOREM 9. *There is a Room Square of side $3s$ for all $s > 1$ except possibly when s is a prime congruent to 3 modulo 4.*

Proof. It is shown in Ref. [11] that there is a Room Square of side v for all $v > 3$ such that $v \equiv 3 \pmod{12}$. Thus, there is a square of side $3s$ for all $s > 1$ such that $s \equiv 1 \pmod 4$. Let us assume that there is no square of side $v = 3s$ for some composite $s \equiv 3 \pmod 4$. Since s is composite, it contains an odd number of prime factors (considering multiplicities). Thus either s has a prime factor $t \equiv 1 \pmod 4$ or at least 3 prime factors p, q, r, congruent to 3 mod 4. In the latter case, take $t = pq$. Then $v = 3tn$, where n is not divisible by F_1, F_3, or F_4, by Theorem 2. Thus, there is a square of side n, and a square of side $3t$, since $t \equiv 1 \pmod 4$ and $t > 1$. Therefore, there is a square of side v by (c). This contradiction establishes the result.

6. CONCLUSION

In our initial work Ref. [16] on the Room problem, we indicated the problems which would need to be investigated in order to prove a general existence theorem for Room Squares. Such a general theorem is now nearly complete in that Room Squares have been obtained for all possible sides v except for (i) $v = 3p$, p a prime, $p \equiv 3 \pmod 4$; (ii) $v = 257n$; (ii) $v = 65537n$.

With the results of the present paper and those cited in it, we can improve the list given in Ref. [16] of those orders $v < 1000$ for which the existence problem is still unsolved; 42 values of v were listed in Ref. [16], but this list has now shrunk to 13. These values are as follows:

69, 93, 129, 213, 237, 257, 321, 453, 597, 669, 717, 789, 933.

References

1. J. W. Archbold, A combinatorial problem of T. G. Room, *Mathematika* **7** (1960), 50–55.
2. J. W. Archbold and N. L. Johnson, A construction for Room's squares and an application in experimental design, *Ann. Math. Statist.* **29** (1958), 219–225.
3. George Beynon, "Bridge Director's Manual for Duplicate Games", George Coffin, Waltham, Mass., 1943.
4. R. H. Bruck, What is a Loop?, *in* "Studies in Modern Algebra" (A. A. Albert, Ed.), Prentice-Hall, Englewood Cliffs, N. J., 1963.
5. R. J. Collens and R. C. Mullin, "Some Properties of Room Squares—A Computer Search", Proceedings Louisiana Conference on Combinatorics, Graph Theory, and Computing, 87–111, Baton Rouge, 1970.
6. A. M. Gruenther, "Duplicate Bridge Complete", Bridge World Inc., New York, 1933.
7. J. D. Horton, "Variations on a Theme by Moore", 146–166, Proceedings Louisiana Conference on Combinatorics, Graph Theory, and Computing, Baton Rouge, 1970.
8. J. D. Horton, "Quintuplication of Room Squares", to appear.
9. J. D. Horton, R. C. Mullin, and R. G. Stanton, A recursive construction for Room Designs, *Aeq Math.*, to appear.
10. R. C. Mullin and E .Nemeth, An existence theorem for Room Squares, *Canad. Math. Bull.* **12** (1969), 493–497.
11. R. C. Mullin and W. D. Wallis, On the Existence of Room Squares of Order $4n$, to appear.
12. T. G. Room, A new type of magic square, *Math. Gazette* **39** (1955), 307.
13. R. G. Stanton and J. D. Horton, "Composition of Room Squares", Proceedings Coll. Comb. Math., Bolyai Janos Math. Soc., Budapest, 1969.
14. R. G. Stanton and J. D. Horton, A multiplication theorem for Room Squares, *J. Comb. Theory*, to appear.
15. R. G. Stanton and R. C. Mullin, Construction of Room Squares, *Ann. Math. Statist.* **39** (1968), 1540–1548.
16. R. G. Stanton and R. C. Mullin, "Techniques for Room Squares", 445–464, Proceedings Louisiana Conference on Combinatorics, Graph Theory, and Computing, Baton Rouge, 1970.
17. W. D. Wallis, Duplication of Room Squares, *J. Austral. Math. Soc.*, to appear.
18. L. Weisner, A Room Design of order 10, *Canad. Math. Bull.* **7** (1964), 377–378.