A Note on Power Sets of Latin Squares

József Dénes
Csaba Utca 10 v 42
Budapest 1122, Hungary

Gary L. Mullen*
Mathematics Department
Pennsylvania State University
University Park, PA 16802, U.S.A.
email: mullen@math.psu.edu

Stephan J. Suchower
Daniel H. Wagner, Associates
Station Square Two
Paoli, PA 19301, U.S.A.

Dedicated to the memory of Professor E. T. Parker who contributed so much to the theory of latin squares.

Abstract. In this note we study a group operation on the set of all row latin squares of order n and as a result, are able to provide a short disproof of the Euler conjecture for infinitely many values of n. We also discuss several related conjectures.

In [13] Norton observed that all row latin squares of size $n \times n$ form a group Q_n whose order is $(n!)^n$ and that Q_n is a direct product of n copies of S_n, the symmetric group on n symbols. A square matrix is called a row latin square if each of its rows contains each of the elements $1, \dots, n$ exactly once. Hence a row latin square R may be viewed as an n-tuple $(\alpha_1, \dots, \alpha_n)$ of permutations where the i-th row of R may be viewed as the image of $1, \dots, n$ under the permutation α_i. Thus if $S = (\beta_1, \dots, \beta_n)$ is another row latin square of order n, then the product square RS is given by $(\alpha_1\beta_1, \dots, \alpha_n\beta_n)$ where $\alpha_i\beta_i$ denotes the usual composition of the permutations α_i and β_i.

Suppose L is a latin square of order n and that the order of L in Q_n is m. If $L, L^2, \dots, L^{m-1}$ are all latin squares, then the set $\{L, L^2, \dots, L^{m-1}\}$ is called a latin power set. Our interest in looking for latin power sets is motivated by the fact that the squares $L, L^2, \dots, L^{m-1}$ are mutually orthogonal, see Norton [13, Cor. 4a]. Recall that two latin squares of order n are orthogonal if upon superposition

AMS(MOS) subject classifications (1985 revision). 05B15
*This author would like to thank the National Security Agency for partial support under grant agreement #MDA904-92-H-3044.

each of the n^2 possible ordered pairs occurs exactly once and that a set of squares is orthogonal if each pair of distinct squares is orthogonal.

With this as motivation, for $n = 10$ we conducted an extensive but not exhaustive machine search for a latin power set containing three elements. Unfortunately however, none were found. The following power set containing two mutually orthogonal latin squares of order 10 was found by machine.

$$L = \begin{array}{cccccccccc} 1 & 3 & 4 & 2 & 6 & 7 & 5 & 9 & 10 & 8 \\ 10 & 2 & 5 & 3 & 4 & 8 & 6 & 7 & 1 & 9 \\ 9 & 10 & 3 & 5 & 8 & 1 & 2 & 4 & 6 & 7 \\ 7 & 9 & 1 & 4 & 10 & 5 & 3 & 2 & 8 & 6 \\ 3 & 8 & 10 & 7 & 5 & 2 & 9 & 6 & 4 & 1 \\ 5 & 1 & 8 & 9 & 2 & 6 & 4 & 10 & 7 & 3 \\ 8 & 4 & 6 & 10 & 1 & 9 & 7 & 5 & 3 & 2 \\ 2 & 7 & 9 & 6 & 3 & 10 & 1 & 8 & 5 & 4 \\ 4 & 6 & 2 & 8 & 7 & 3 & 10 & 1 & 9 & 5 \\ 6 & 5 & 7 & 1 & 9 & 4 & 8 & 3 & 2 & 10 \end{array} \qquad L^2 = \begin{array}{cccccccccc} 1 & 4 & 2 & 3 & 7 & 5 & 6 & 10 & 8 & 9 \\ 9 & 2 & 4 & 5 & 3 & 7 & 8 & 6 & 10 & 1 \\ 6 & 7 & 3 & 8 & 4 & 9 & 10 & 5 & 1 & 2 \\ 3 & 8 & 7 & 4 & 6 & 10 & 1 & 9 & 2 & 5 \\ 10 & 6 & 1 & 9 & 5 & 8 & 4 & 2 & 7 & 3 \\ 2 & 5 & 10 & 7 & 1 & 6 & 9 & 3 & 4 & 8 \\ 5 & 10 & 9 & 2 & 8 & 3 & 7 & 1 & 6 & 4 \\ 7 & 1 & 5 & 10 & 9 & 4 & 2 & 8 & 3 & 6 \\ 8 & 3 & 6 & 1 & 10 & 2 & 5 & 4 & 9 & 7 \\ 4 & 9 & 8 & 6 & 2 & 1 & 3 & 7 & 5 & 10 \end{array}$$

The permutations $\alpha_1, \ldots, \alpha_{10}$ which correspond to the 10 rows $R_1, \ldots, R_{10}$ of L are given by:

$$\begin{array}{ll} \alpha_1 = (234)(567)(89A)(1) & \alpha_6 = (152)(38A)(497)(6) \\ \alpha_2 = (1A9)(354)(687)(2) & \alpha_7 = (185)(24A)(369)(7) \\ \alpha_3 = (196)(2A7)(458)(3) & \alpha_8 = (127)(395)(46A)(8) \\ \alpha_4 = (173)(298)(5A6)(4) & \alpha_9 = (148)(263)(57A)(9) \\ \alpha_5 = (13A)(286)(479)(5) & \alpha_{10} = (164)(259)(378)(A). \end{array}$$

It is easy to see from these permutations that $L^3 = I$, the identity of Q_{10}, each row of which contains $1, \ldots, 10$. Hence $L^2 = L^{-1}$ which is latin by Norton [13, Thm. 5] and moreover from [13, Cor. 4a], L and L^2 are orthogonal. A. D. Keedwell kindly pointed out to the authors that other latin squares of order 10 already in the literature also form power sets containing two elements, see for example the latin square represented by the permutations in Keedwell [10, Fig. 2].

Clearly there is no latin power set $\{L, L^2\}$ for squares of order 2 or 6 but motivated by the above examples, it is quite natural to ask whether the following holds

Conjecture. *If $n \neq 2$ or 6 then there exists a latin power set containing at least two latin squares of order n.*

The validity of our conjecture would imply a new disproof of the famous Euler conjecture concerning the nonexistence of a pair of orthogonal latin squares of order $n = 2(2k + 1)$ for $k = 0, 1, \ldots$. See [2, Ch. 11] for a history and work related to Euler's conjecture.

We first prove a few results concerning latin power sets.

Theorem 1. *If L is a Cayley table of a group G of order n with $n = p_1^{e_1} \ldots p_r^{e_r}$ where $p_1 < p_2 < \cdots < p_r$ are primes, then the set $\{L, L^2, \ldots, L^{p_1 - 1}\}$ forms a latin power set containing $p_1 - 1$ elements.*

Proof: Since all positive integers $\leq p_1 - 1$ are relatively prime to n, it is easy to see that $L, L^2, \ldots, L^{p_1-1}$ are latin squares. Moreover by Norton [13, Cor. 4a], they are mutually orthogonal.

Corollary 2. *If n is a prime there is a latin power set containing $n - 1$ elements.*

Corollary 3. *If n is odd there is a latin power set containing at least two elements.*

We remark that a special case of Theorem 1 was obtained in [12] for the case where G is the cyclic group of order n. In the cases of $n = 35, 77, 119, 143, 187$ it is worth pointing out that the above construction using power sets gives the maximal number of orthogonal squares known (4,6,6,10,10 respectively) for these values of n, see Brouwer [1, p. 167]. We also mention that if $n > 2$ is even, the paper [14] of Sinkov implies that no complete ($n - 1$ elements) latin power set exists.

In Problem 5.2 of [2, p. 488], it is asked "Is it true that there do not exist sets of $n - 1$ mutually orthogonal latin squares based on a cyclic group unless n is a prime?" Our next result gives a partial resolution to this question.

Corollary 4. *If n is not a prime then no complete latin power set containing $n - 1$ elements exists based on a group table.*

We now provide a proof of part of our conjecture.

Theorem 5. *If $n \geq 7$ and $n \equiv 0, 1 \pmod 3$ then there exists a latin power set with at least two latin squares of order n.*

Proof: A Mendelsohn triple system is a pair (M, T) where M is a set of elements and T is a collection of triples such that every ordered pair (a, b), $a \neq b$, belongs to exactly one cyclic triple of T. A Mendelsohn triple system (M, T) is of order n if the number of elements in M is n, and it is said to be resolvable if the blocks can be partitioned into n sets each containing the same number of blocks which are pairwise disjoint as sets. It is easy to see that a resolvable Mendelsohn triple system of order n can be considered as a permutation representation of a latin square of order n, see our earlier example in the case $n = 10$. Also it is clear that if L denotes a latin square which corresponds to a resolvable Mendelsohn triple system, then $L^2 = L^{-1}$ holds. Since L^{-1} must be a latin square by [13, Thm. 5], L and L^2 form a latin power set. It is known that resolvable Mendelsohn triple systems of order n exist if $n \equiv 0, 1 \pmod 3$ except for $n = 6$, see [9] or [11]. This completes the proof.

It is easy to see from Corollary 3 and Theorem 5 that our conjecture on the existence of latin power sets is true except for the case where $n = 3k + 2$ and

k is even, i.e. except when $n \equiv 2 \pmod{6}$. Also it is easily seen that we have produced an easy disproof of Euler's conjecture except for the case when $n = 3k + 2$ and k is divisible by 4, i.e. except when $n \equiv 2 \pmod{12}$. While this provides a class of counter examples to Euler's conjecture, it does not detract from Parker's achievement of providing the first disproof of the conjecture for $n = 10$, see [2, p. 397] for details.

Unfortunately for $n \equiv 2 \pmod{6}$ the situation is not so simple. However through the use of so called circular Tuscan-2 squares and related results one can construct latin power sets containing latin squares of various orders. As discussed in [6–8] an Italian square is an $n \times n$ array in which each of the symbols $1, 2, \ldots, n$ appears once in each row (this is of course just a row latin square). A Tuscan-k square is an Italian square with the further property that for any two symbols a and b and for each m from 1 to k, there is at most one row in which b is the m-th symbol to the right of a. A circular Tuscan-k array is an $n \times (n+1)$ array in which each of the $n+1$ symbols $0, 1, \ldots, n$ appears once in each row and in which the Tuscan-k property holds when the rows are taken to be circular, see [6–8] for details.

In [6, Thm. A] the authors prove that if an $n \times (n+1)$ circular Tuscan-k array exists then there exist k orthogonal $(n+1) \times (n+1)$ latin squares. If we use permutation representations of latin squares, this can be strengthened to

Theorem 6. *If an $n \times (n+1)$ circular Tuscan-k array exists then there exists a latin power set containing k latin squares of order $n+1$.*

In question Q5 of [6] it is asked whether for all even $n > 8$ do circular $n \times (n+1)$ Tuscan-2 arrays exist? While this question remains open it is conjectured in [6] that the answer is yes and a computer search described there shows that such circular $n \times (n+1)$ Tuscan-2 arrays do indeed exist for all even $8 < n \leq 50$. We also point out that circular Tuscan-k arrays are related to so-called 1-fold perfect Mendelsohn designs, see Hsu and Keedwell [9], where a number of constructions of Mendelsohn designs are given using generalized complete mappings of various groups.

We close by relating these power set ideas to two previously published conjectures of Dénes and Keedwell. Suppose L is a latin square whose i-th row is defined by α_i regarded as a permutation of its first row. In [4] Dénes and Keedwell indicate they have shown that if L is the Cayley table of a non-soluble group, then at least one square-root square $\sqrt{L} = (\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n})$ always exists. This led them to conjecture that in the case of a non-soluble group, at least one of the square-root squares is a latin square.

Another conjecture of Dénes and Keedwell is stated as follows in [5]: A necessary and sufficient condition for a latin square A to have an orthogonal mate is that either A^2 is a latin square or A can be represented as the product $A = BC$ of two not necessarily distinct latin squares B and C.

Acknowledgement

We would like to thank A. D. Keedwell for a number of helpful comments and criticisms.

References

[1] . A.E. Brouwer, *Recursive constructions of mutually orthogonal latin squares*, in J. Dénes and A.D. Keedwell, Latin Squares, Annals Discrete Math. 46, North-Holland, Amsterdam, 1991, 149–168.

[2] J. Dénes AND A.D. Keedwell, "Latin sauares and Their Applications." Academic Press, New York; Akadémiai Kiadó, Budapest; English Universities Press, London, 1974.

[3] J. Dénes and A.D. Keedwell, *Latin squares and one-factorizations of complete graphs: (II) Enumerating one-factorizations of the complete directed graph K_n^* using MacMahon's double partition idea*, Utilitas Math. 34 (1988), 73–83.

[4] J. Dénes and A.D. Keedwell, *A new-conjecture concerning admissibility of groups*, Europ. J. Comb. **10** (1989), 171–174.

[5] J. Dénes and A.D. Keedwell. *On two conjectures related to admissible group s and quasigroups*, Proc. Sec. Internat. Math. Mini Conf., Budapest, 1988, Periodica Polytechnica Transportation Engineering **19** (1991) 33–35.

[6] T. Etzion, S.W. Golomb, and H. Taylor, *Tuscan-k squares*, Advances in Appl. Math. **10** (1989), 164–174.

[7] S.W. Golomb, T. Etzion and H. Taylor, *Polygonal path constructions for Tuscan-k squares*, Ars Combinatoria **30** (1990), 97–140.

[8] S.W. Golomb and H. Taylor, *Tuscan squares: A new family of combinatorial designs*, Ars Combinatoria **20-B** (1985), 115–132.

[9] D.F. Hsu and A. D. Keedwell, *Generalized complete mappings, neofields, sequenceable groups, and block designs, II*, Pac. J. Math. **117** (1985), 291–312.

[10] A.D. Keedwell, *Circuit designs and latin squares*, Ars Combinatoria **17** (1984), 79–90.

[11] N.S. Mendelsohn, *A natural generalization of Steiner triple systems*, in "Computers in Number Theory", Academic Press, New York, 1971, pp. 323–338.

[12] G.L. Mullen AND J.-S. Shiue, *A simple construction for orthogonal latin rectangles*, J. Comb. Math. & Comb. Comp. **9** (1991), 161–166.

[13] D.A. Norton, *Groups of orthogonal row-latin squares*, Pacific J. Math. **2** (1952), 335–341.

[14] A. Sinkov, *A property of cyclic substitutions of even length*, Amer. Math. Mon. **42** (1935), 145–149.