

This is a preprint of an article accepted for publication in
Discrete Applied Mathematics © 2017 (copyright owner
as specified in the journal).

On the number of transversals in a class of Latin squares

D. M. Donovan

Centre for Discrete Mathematics and Computing
University of Queensland
St. Lucia 4072
AUSTRALIA
(dmd@maths.uq.edu.au)

M. J. Grannell*

School of Mathematics and Statistics
The Open University
Walton Hall
Milton Keynes MK7 6AA
UNITED KINGDOM
(m.j.grannell@open.ac.uk)

Abstract

Denote by \mathcal{A}_p^k the Latin square of order $n = p^k$ formed by the Cayley table of the additive group $(\mathbb{Z}_p^k, +)$, where p is an odd prime and k is a positive integer. It is shown that for each p there exists $Q > 0$ such that for all sufficiently large k , the number of transversals in \mathcal{A}_p^k exceeds $(nQ)^{\frac{n}{p(p-1)}}$.

Running head: Transversals.

AMS classification: 05B15.

Keywords: Latin square; Transversal.

*Corresponding author

1 Introduction

Several recent papers have addressed the issue of bounds on the numbers of transversals in Latin squares. So, suppose that \mathcal{S} is a Latin square. Denote by $T(\mathcal{S})$ the number of transversals in \mathcal{S} , and put

$$T(n) = \max\{T(\mathcal{S}) : \mathcal{S} \text{ is a Latin square of order } n\}.$$

It was shown by McKay, McLeod and Wanless [4] that for $n \geq 5$, $15^{n/5} \leq T(n) \leq 0.6135^n n! \sqrt{n}$.

The Cayley table of any finite group forms a Latin square, and such squares are called group-based. Let \mathcal{A}_n denote the cyclic Latin square of order n , that is the square formed by the Cayley table of the cyclic group $(\mathbb{Z}_n, +)$. If n is even then $T(\mathcal{A}_n) = 0$, but for odd n it was conjectured by Vardi [6] that there exist positive constants c and d such that $c^n n! \leq T(\mathcal{A}_n) \leq d^n n!$. Subsequently Cavenagh and Wanless [1] proved that for all sufficiently large n , $T(\mathcal{A}_n) > (3.246)^n$, and this appears to remain the best lower bound for any class of group-based Latin squares obtained to date.

More recently, Taranenkov [5] proved that $T(n) \leq [(1 + o(1)) \frac{n}{e^2}]^n$, while Glebov and Luria [3] have shown that $T(n) \geq [(1 - o(1)) \frac{n}{e^2}]^n$. The latter result is based on a probabilistic argument employing random Latin squares. These more recent results lend credence to Vardi's conjecture but do not address group-based squares directly.

In the current paper we take p to be an odd prime and k to be a positive integer. Then the Cayley table of the additive group $(\mathbb{Z}_p^k, +)$ forms a Latin square of order $n = p^k$ which we denote by \mathcal{A}_p^k . We will assume that this square has its rows and columns labelled in the natural way by elements of \mathbb{Z}_p^k represented as k -vectors over \mathbb{Z}_p , and when $k = 1$ we write \mathcal{A}_p rather than \mathcal{A}_p^1 . We prove that, for all sufficiently large k , \mathcal{A}_p^k has more than $(nQ)^{\frac{n}{p(p-1)}}$ transversals, where $Q > 0$ depends only on p and is independent of k .

Note added in proof: Since drafting our current paper, our attention has been drawn to the arXiv paper [2] which claims a proof of Vardi's conjecture.

2 Results

We start with the observation that \mathcal{A}_p^k has a transversal \mathcal{T} formed from its leading diagonal. We will construct a large number of transversals by carrying out transversal trades on \mathcal{T} . These trades are based on the square \mathcal{A}_p and involve transversals within this square that do not contain the (row, column, entry) triple $(0, 0, 0)$. So let T^* denote the number of transversals of \mathcal{A}_p that do not contain this triple. By transitivity, the number of transversals in \mathcal{A}_p^k that contain the triple $(0, 0, 0)$ is $T(\mathcal{A}_p^k)/p^k$, so the number of transversals not containing this triple is $T(\mathcal{A}_p^k)(1 - \frac{1}{p^k})$. In particular, $T^* = T(\mathcal{A}_p)(1 - \frac{1}{p})$, and note rather trivially that $T(\mathcal{A}_p) \geq p$.

For $k \geq 2$, the square \mathcal{A}_p^k can be partitioned into p^2 subarrays by writing the row labels, the column labels and the entries in the form (z, i) where $z \in \mathbb{Z}_p^{k-1}$ and $i \in \mathbb{Z}_p$. This is shown schematically in Figure 1 with the row and column labels omitted.

$$\mathcal{A}_p^k = \begin{array}{|c|c|c|c|} \hline (\mathcal{A}_p^{k-1}, 0) & (\mathcal{A}_p^{k-1}, 1) & \dots & (\mathcal{A}_p^{k-1}, p-1) \\ \hline (\mathcal{A}_p^{k-1}, 1) & (\mathcal{A}_p^{k-1}, 2) & \dots & (\mathcal{A}_p^{k-1}, 0) \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline (\mathcal{A}_p^{k-1}, p-1) & (\mathcal{A}_p^{k-1}, 0) & \dots & (\mathcal{A}_p^{k-1}, p-2) \\ \hline \end{array}$$

$$= \begin{array}{|c|c|c|c|} \hline A_{0,0} & A_{0,1} & \dots & A_{0,p-1} \\ \hline A_{1,0} & A_{1,1} & \dots & A_{1,p-1} \\ \hline \vdots & \vdots & \vdots & \vdots \\ \hline A_{p-1,0} & A_{p-1,1} & \dots & A_{p-1,p-1} \\ \hline \end{array}, \text{ say.}$$

Figure 1: Partitioning \mathcal{A}_p^k .

Taken without the row and column labels inherited from \mathcal{A}_p^k , the subarrays $A_{i,j}$ and $A_{i',j'}$ are identical when $i + j = i' + j'$ in \mathbb{Z}_p . However, we will associate each of these subarrays with their original row and column labels.

Our transversal trades will be based on copies of \mathcal{A}_p , each having precisely one entry from each $A_{i,j}$. Specifically, one (row, column, entry) triple is selected from the leading diagonal of $A_{0,0}$, say $((a, 0), (a, 0), (2a, 0))$, and one triple is selected from $A_{0,1}$ having the same row entry, say $((a, 0), (b, 1), (a + b, 1))$. These two choices are sufficient to determine a copy of \mathcal{A}_p , denoted by $A(a, b)$, as shown in Figure 2, which also shows the inherited row and column labels.

$$\begin{array}{|c|c|c|c|c|} \hline & (a, 0) & (b, 1) & (2b - a, 2) & \dots & (2a - b, p - 1) \\ \hline (a, 0) & (2a, 0) & (a + b, 1) & (2b, 2) & \dots & (3a - b, p - 1) \\ \hline (b, 1) & (a + b, 1) & (2b, 2) & (3b - a, 3) & \dots & (2a, 0) \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline (2a - b, p - 1) & (3a - b, p - 1) & (2a, 0) & (a + b, 1) & \dots & (4a - 2b, p - 2) \\ \hline \end{array}$$

Figure 2: The array $A(a, b)$.

Note that the row and column labels of $A(a, b)$, inherited from \mathcal{A}_p^k , have the form $(rb - (r - 1)a, r)$ and the entries have the form $(rb - (r - 2)a, r)$, both for $r = 0, 1, \dots, p - 1$.

The leading diagonal of $A(a, b)$ lies in the leading diagonal of \mathcal{A}_p^k and therefore this diagonal of $A(a, b)$ forms a part of the transversal \mathcal{T} . There are T^* transversals in $A(a, b)$ that do not contain the triple $((a, 0), (a, 0), (2a, 0))$. If the diagonal transversal of $A(a, b)$ in \mathcal{T} is traded for any one of these T^* transversals, then a new transversal in \mathcal{A}_p^k is obtained that does not contain the triple $((a, 0), (a, 0), (2a, 0))$. Hence, for each given $a \in \mathbb{Z}_p^{k-1}$, T^* distinct transversals of \mathcal{A}_p^k may be obtained for each $b \in \mathbb{Z}_p^{k-1}$. Furthermore, for two different

values $b, b' \in \mathbb{Z}_p^{k-1}$, the arrays $A(a, b)$ and $A(a, b')$ only intersect in the cell $((a, 0), (a, 0))$, and so by varying b , a total of $p^{k-1}T^*$ distinct transversals of \mathcal{A}_p^k may be obtained that do not contain the triple $((a, 0), (a, 0), (2a, 0))$.

In principle, we wish to carry out these trades sequentially for as many values of a as is possible. The obstacle is that having carried out a trade using $A(a, b)$, and having chosen $a' \neq a$, the choice of b' is constrained by the need to ensure that $A(a', b')$ avoids the rows, columns and entries of $A(a, b)$. So suppose that trades have already been made using $c-1$ choices of (a, b) and that a c^{th} choice is to be made. If (a, b) defines one of the previous choices and (a', b') is the proposed c^{th} choice, with $a' \neq a$, then to ensure that rows and columns do not clash it is necessary and sufficient that $(r'b' - (r-1)a', r')$ and $(rb - (r-1)a, r)$ are unequal for all $r, r' = 0, 1, \dots, p-1$. But these two quantities can only be equal if $r' = r$, and then only if $rb' - (r-1)a' = rb - (r-1)a$. Hence the rows and columns of $A(a, b)$ and $A(a', b')$ are distinct provided that $b' \neq b + \frac{r-1}{r}(a' - a)$ for $r = 1, 2, \dots, p-1$. As r varies from 1 to $p-1$, $\frac{r-1}{r}$ takes all values in \mathbb{Z}_p , apart from the value 1. Hence in selecting b' it is necessary to avoid the $p-1$ values $b + \rho(a' - a)$ for $\rho = 0, 2, 3, \dots, p-1$ for each previous choice of (a, b) . By arguing in a similar fashion regarding entries, we obtain exactly the same condition to avoid entry clashes between $A(a, b)$ and $A(a', b')$. It follows that at the c^{th} choice, there are at least $p^{k-1} - (c-1)(p-1)$ choices for b' (rather more if there is multiple counting of excluded rows, columns and entries).

Now put $C = \lfloor \frac{p^{k-1}}{p-1} \rfloor = \frac{p^{k-1}-1}{p-1}$ and let $c \leq C$ be a positive integer. Then it is possible to choose c subarrays of the form $A(a, b)$ that are pairwise disjoint as regards rows, columns and entries. Suppose that the subarrays chosen are $A(a_i, b_i)$ for $i = 1, 2, \dots, c$. Then the number of transversals in \mathcal{A}_p^k that do not contain any of the triples $((a_i, 0), (a_i, 0), (2a_i, 0))$ for $i = 1, 2, \dots, c$, and which can be constructed by trades on these arrays is at least

$$\begin{aligned} (T^*)^c (p^{k-1})(p^{k-1} - (p-1))(p^{k-1} - 2(p-1)) \dots (p^{k-1} - (c-1)(p-1)) \\ > (T^*(p-1))^c \frac{C!}{(C-c)!} \end{aligned}$$

To see that these transversals are all distinct, consider any one of them, say \mathcal{T}^* . Each a_i for $i = 1, 2, \dots, c$ can be identified from those diagonal entries of $A_{0,0}$ that do not form part of \mathcal{T}^* . Having identified an a_i , there will be a triple of \mathcal{T}^* of the form $((a_i, 0), (rb_i - (r-1)a_i, r), (rb_i - (r-2)a_i, r))$ where $r \neq 0$. From this triple, r can be identified and hence also b_i . Thus the subarrays $A(a_i, b_i)$ can be recovered from \mathcal{T}^* , and the distinctness of the transversals follows. In fact any distinct choices of up to C values for a_i will yield distinct transversals. Hence we obtain the following theorem.

Theorem 2.1 *If p is an odd prime and k is a positive integer, then the number of transversals in the Latin square \mathcal{A}_p^k , denoted by $T(\mathcal{A}_p^k)$, satisfies the inequality*

$$T(\mathcal{A}_p^k) > \sum_{c=0}^C \binom{p^{k-1}}{c} (T^*(p-1))^c \frac{C!}{(C-c)!} \quad (1)$$

where $C = \frac{p^{k-1}-1}{p-1}$ and $T^* = T(\mathcal{A}_p)(1 - \frac{1}{p})$.

The final term in the summation (1) gives

$$\begin{aligned} T(\mathcal{A}_p^k) &> \binom{p^{k-1}}{C} (T^*(p-1))^C C! \\ &= \frac{(p^{k-1})!}{(p^{k-1}-C)!} (T^*(p-1))^C \end{aligned}$$

Applying Stirling's Theorem in the form $r! = r^{r+\frac{1}{2}} e^{-r} \sqrt{2\pi} e^{o(1)}$ (as $r \rightarrow \infty$) to this expression for large k gives

$$T(\mathcal{A}_p^k) > [p^{k-1} T^*(p-1) e^{-1}]^C \cdot \left[\left(1 - \frac{C}{p^{k-1}}\right)^{-(p^{k-1}-C+\frac{1}{2})} \right] \cdot e^{o(1)}. \quad (2)$$

For $p \geq 3$ and $k \geq 2$ we have $(1 - \frac{C}{p^{k-1}}) \leq (1 - \frac{1}{p})$ and $p^{k-1} - C + \frac{1}{2} > (p-2)C$. Hence

$$T(\mathcal{A}_p^k) > \left[p^k \left(\frac{p}{p-1}\right)^{p-4} T(\mathcal{A}_p) e^{-1} \right]^C \cdot e^{o(1)}.$$

The square \mathcal{A}_p^k has order $n = p^k$ and $C = \frac{n}{p(p-1)} - \frac{1}{p-1}$, so taking Q to be slightly less than $\left(\frac{p}{p-1}\right)^{p-4} T(\mathcal{A}_p) e^{-1}$ gives the following corollary.

Corollary 2.1 *If p is an odd prime, there exists $Q > 0$ such that for all sufficiently large k ,*

$$T(\mathcal{A}_p^k) > (nQ)^{\frac{n}{p(p-1)}},$$

where $n = p^k$.

In fact if p is also sufficiently large, then using the result of [1], we may take $Q = (3.246)^p$. However, the bound is clearly best when p is small. In the case $p = 3$, inequality (2) simplifies as follows. Firstly $T(\mathcal{A}_3) = 3$, so $T^* = 2$. Also $C = (3^{k-1} - 1)/2$ and $3^{k-1} - C + \frac{1}{2} = 3^{k-1}/2 + 1$. Hence

$$\begin{aligned} T(\mathcal{A}_3^k) &> (4 \cdot 3^{k-1} \cdot e^{-1})^C \cdot \left(\frac{1}{2} + \frac{1}{2 \cdot 3^{k-1}}\right)^{-(\frac{3^{k-1}}{2}+1)} \cdot e^{o(1)} \\ &= \left(\frac{4n}{3e}\right)^C \cdot 2^{C+\frac{3}{2}} \cdot \left(1 + \frac{1}{3^{k-1}}\right)^{-(\frac{3^{k-1}}{2}+1)} \cdot e^{o(1)} \\ &= \left(\frac{8n}{3e}\right)^C \cdot 2\sqrt{2} \cdot \frac{1}{\sqrt{e}} \cdot e^{o(1)}, \end{aligned}$$

since $(1 + \frac{1}{r})^{-r} \rightarrow e^{-1}$ as $r \rightarrow \infty$. Noting that $8/3e > 0.981$ and that $C = \frac{n}{6} - \frac{1}{2}$, we obtain

Corollary 2.2 *For all sufficiently large k , $T(\mathcal{A}_3^k) > (0.981n)^{\frac{2}{3}}$, where $n = 3^k$.*

Finally we remark that, by transitivity, the number of orthogonal mates of the Latin square \mathcal{A}_p^k is $T(\mathcal{A}_p^k)/n$ (where $n = p^k$) and so Theorem 2.1 and its corollaries also provide lower bounds for this quantity.

References

- [1] N. J. Cavenagh and I. M. Wanless. On the number of transversals in Cayley tables of cyclic groups, *Discrete Appl. Math.*, 158 (2010) 136–146.
- [2] S. Eberhard, F. Manners and R. Mrazović. Additive triples of bijections, or the toroidal semiqueens problem, *submitted* and arXiv:1510.05987v3 (2016) 22pp.
- [3] R. Glebov and Z. Luria. On the maximum number of Latin transversals, *J. Combin. Theory Ser. A*, 141 (2016) 136–146.
- [4] B. D. McKay, J. C. McLeod and I. M. Wanless. The number of transversals in a Latin square, *Des. Codes Crypt.*, 40 (2006) 269–284.
- [5] A. A. Taranenko. Multidimensional permanents and an upper bound on the number of transversals in Latin squares, *J. Combin. Des.*, 23 (2014), 305–320.
- [6] I. Vardi. *Computational recreations in mathematics*, Addison-Wesley, 1991.