On the number of transversals in a class of Latin squares

How to cite:

© 2017 Elsevier B.V.

Version: Accepted Manuscript

Link(s) to article on publisher’s website:
http://dx.doi.org/doi:10.1016/j.dam.2017.08.021

Copyright and Moral Rights for the articles on this site are retained by the individual authors and/or other copyright owners. For more information on Open Research Online’s data policy on reuse of materials please consult the policies page.
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 $A_{p^k}^n$ 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 $A_{p^k}^n$ exceeds $(nQ)^{n^{p^k-1}}$.

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 $S$ is a Latin square. Denote by 
$T(S)$ the number of transversals in $S$, and put

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

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 $A_n$ 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 $T(A_n) = 0$, but for odd $n$ it was conjectured by Vardi [6] that there 
exist positive constants $c$ and $d$ such that $c^n n! \leq T(A_n) \leq d^n n!$. Subsequently 
Cavenagh and Wanless [1] proved that for all sufficiently large $n$, $T(A_n) > (3.246)^n$, and this appears to remain the best lower bound for any class of 
group-based Latin squares obtained to date.

More recently, Taranenko [5] proved that $T(n) \leq [(1 + o(1)) \frac{n}{p} \log p]^n$, while Glebov and Luria [3] have shown that $T(n) \geq [(1 - o(1)) \frac{n}{p} \log p]^n$. 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 $A_{p^k}$. 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 $A_p$ rather than 
$A_{p^1}$. We prove that, for all sufficiently large $k$, $A_{p^k}$ has more than $(nQ)_p^p$ 
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 $A_{p^k}$ has a transversal $T$ formed from its 
leading diagonal. We will construct a large number of transversals by carrying 
out transversal trades on $T$. These trades are based on the square $A_p$ 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 $A_p$ 
that do not contain this triple. By transitivity, the number of transversals in $A_{p^k}$ 
that contain the triple $(0, 0, 0)$ is $T(A_{p^k})/p^k$, so the number of transversals not 
containing this triple is $T(A_{p^k})(1 - \frac{1}{p^k})$. In particular, $T^* = T(A_p)(1 - \frac{1}{p})$, and 
ote rather trivially that $T(A_p) \geq p$. 

2
For $k \geq 2$, the square $A_p^k$ 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.

\[
A_p^k = \begin{pmatrix}
(A_p^{k-1}, 0) & (A_p^{k-1}, 1) & \cdots & (A_p^{k-1}, p - 1) \\
(A_p^{k-1}, 1) & (A_p^{k-1}, 2) & \cdots & (A_p^{k-1}, 0) \\
\vdots & \vdots & \ddots & \vdots \\
(A_p^{k-1}, p - 1) & (A_p^{k-1}, 0) & \cdots & (A_p^{k-1}, p - 2)
\end{pmatrix}
\]

\[
= \begin{pmatrix}
A_{0,0} & A_{0,1} & \cdots & A_{0,p-1} \\
A_{1,0} & A_{1,1} & \cdots & A_{1,p-1} \\
\vdots & \vdots & \ddots & \vdots \\
A_{p-1,0} & A_{p-1,1} & \cdots & A_{p-1,p-1}
\end{pmatrix}
\]

Figure 1: Partitioning $A_p^k$.

Taken without the row and column labels inherited from $A_p^k$, 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 $A_p$, 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 $A_p$, denoted by $A(a,b)$, as shown in Figure 2, which also shows the inherited row and column labels.

\[
\begin{array}{cccc}
(a, 0) & (a_0, 0) & (b, 1) & (2b - a, 2) \cdots (2a - b, p - 1) \\
(b, 1) & (a + b, 1) & (2b_2) & \cdots (3a - b, p - 1) \\
\vdots & \vdots & \vdots & \vdots \\
(2a - b, p - 1) & (3a - b, p - 1) & (2a_0) & (a + b, 1) \cdots (4a - 2b, p - 2)
\end{array}
\]

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

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

The leading diagonal of $A(a,b)$ lies in the leading diagonal of $A_p^k$ and therefore this diagonal of $A(a,b)$ forms a part of the transversal $T$. 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 $T$ is traded for any one of these $T^*$ transversals, then a new transversal in $A_p^k$ 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 $A_p^k$ 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 $A_p^k$ 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 $r, r' = 0, 1, \ldots, p - 1$. But these two quantities can only be equal if $r' = r$, and then only if $r'b' - (r' - 1)a' = rb - (r - 1)a$. Hence the rows and columns of $A(a, b)$ and $A(a', b')$ are distinct provided that $b' \neq b + \frac{1}{p}(a' - a)$ for $r = 1, 2, \ldots, p - 1$. As $r$ varies from 1 to $p - 1$, $\frac{1}{p}(a' - a)$ 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 $\rho = 0, 2, 3, \ldots, p - 1$ 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 $C = \left[rac{k-1}{p-1}\right] = \frac{k-1}{p-1}$ 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 $i = 1, 2, \ldots, c$. Then the number of transversals in $A_p^k$ that do not contain any of the triples $((a_i, 0), (a_i, 0), (2a_i, 0))$ for $i = 1, 2, \ldots, c$, and which can be constructed by trades on these arrays is at least

$$(T^*)^c(p^{k-1}(p^{k-1} - (p - 1))(p^{k-1} - 2(p - 1)) \ldots (p^{k-1} - (c - 1)(p - 1))$$

$$> (T^*(p - 1))^c \frac{C^c}{(C - c)!}$$

To see that these transversals are all distinct, consider any one of them, say $T^*$. Each $a_i$ for $i = 1, 2, \ldots, c$ can be identified from those diagonal entries of $A_{0,0}$ that do not form part of $T^*$. Having identified an $a_i$, there will be a triple of $T^*$ 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 $T^*$, 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 $A_p^k$, denoted by $T(A_p^k)$, satisfies the inequality

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

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

The final term in the summation (1) gives

$$T(A_p^k) > \left(\frac{p^{k-1}}{C}\right) (T^*(p - 1))^C C!$$

$$= \frac{(p^{k-1})!}{(p^{k-1} - C)!} (T^*(p - 1))^C$$

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

$$T(A_p^k) > [p^{k-1}T^*(p - 1)e^{-1}]^C \left(1 - \frac{C}{p^{k-1}}\right)^{-(p^{k-1} - C + \frac{1}{2})} \cdot e^{o(1)} \hspace{1cm} (2)$$

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

$$T(A_p^k) > \left(p^{k} \left(\frac{p}{p - 1}\right)^{p-4} T(A_p)e^{-1}\right)^C \cdot e^{o(1)}.$$

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

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

$$T(A_p^k) > (nQ)p^\frac{n}{p^k-n},$$

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 $T(A_3) = 3$, so $T^* = 2$. Also $C = (3^{k-1} - 1)/2$ and $3^{k-1} - C + \frac{1}{2} = 3^{k-1}/2 + 1$. Hence

$$T(A_3^k) > (4 \cdot 3^{k-1} \cdot e^{-1})^C \cdot \left(\frac{1}{2} + \frac{1}{3^{k-1}}\right)^{-(\frac{3^{k-1}+1}{3})} \cdot e^{o(1)}$$

$$= \left(\frac{4n}{3e}\right)^C \cdot 2^C + \frac{1}{2} \cdot \left(1 + \frac{1}{3^{k-1}}\right)^{-(\frac{3^{k-1}+1}{3})} \cdot e^{o(1)}$$

$$= \left(\frac{8n}{3e}\right)^C \cdot 2^{\sqrt{2}} \cdot \frac{1}{\sqrt{e}} \cdot e^{o(1)},$$

since $(1 + \frac{1}{r})^{-r} \to e^{-1}$ as $r \to \infty$. Noting that $8/3e > 0.981$ and that $C = \frac{n}{6} - \frac{1}{7}$, we obtain
Corollary 2.2 For all sufficiently large $k$, $T(A_{3k}^6) > (0.981n)^{\frac{4}{3}}$, where $n = 3^k$.

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

References


