On the number of transversals in a class of Latin squares

How to cite:

© 2017 Elsevier B.V.
Version: Version of Record
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.
Note

On the number of transversals in a class of Latin squares

Diane M. Donovan\textsuperscript{a}, Mike J. Grannell\textsuperscript{b,}\textsuperscript{*}

\textsuperscript{a} Centre for Discrete Mathematics and Computing, University of Queensland, St. Lucia 4072, Australia
\textsuperscript{b} School of Mathematics and Statistics, The Open University, Walton Hall, Milton Keynes MK7 6AA, United Kingdom

A R T I C L E   I N F O

Article history:
Received 27 September 2016
Accepted 17 August 2017
Available online 4 October 2017

Keywords:
Latin square
Transversal

A B S T R A C T

Denote by $A^k_p$ the Latin square of order $n = p^k$ formed by the Cayley table of the additive group $\langle \mathbb{Z}_{p^k}, + \rangle$, 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 $A^k_p$ exceeds $(nQ)^{\frac{n}{p^k-1}}$.

© 2017 Elsevier B.V. All rights reserved.

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\textsuperscript{4} that for $n \geq 5$, $15^{n/5} \leq T(n) \leq 0.6135^{n!}\sqrt{n}$. 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 $\langle \mathbb{Z}_n, + \rangle$. If $n$ is even then $T(A_n) = 0$, but for odd $n$ it was conjectured by Vardi\textsuperscript{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\textsuperscript{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\textsuperscript{5} proved that $T(n) \leq \left[\left(1 + o(1)\right)\frac{\sqrt{n}}{2}\right]^n$, while Glebov and Luria\textsuperscript{3} have shown that $T(n) \geq \left[\left(1 - o(1)\right)\frac{\sqrt{n}}{2}\right]^n$. 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 $\langle \mathbb{Z}_{p^k}, + \rangle$ forms a Latin square of order $n = p^k$ which we denote by $A^k_p$. 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 $A^1_p$. We prove that, for all sufficiently large $k$, $A^k_p$ has more than $(nQ)^{\frac{n}{p^k-1}}$ 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\textsuperscript{2} which claims a proof of Vardi’s conjecture.

* Corresponding author.

E-mail addresses: dmd@maths.uq.edu.au (D.M. Donovan), m.j.grannell@open.ac.uk (M.J. Grannell).

http://dx.doi.org/10.1016/j.dam.2017.08.021
0166-218X/© 2017 Elsevier B.V. All rights reserved.
$A^k_p =$

\[
\begin{array}{cccc}
(A^k_p, 0) & (A^k_p, 1) & \ldots & (A^k_p, p - 1) \\
(A^k_p, 1) & (A^k_p, 2) & \ldots & (A^k_p, 0) \\
\vdots & \vdots & \ddots & \vdots \\
(A^k_p, p - 1) & (A^k_p, 0) & \ldots & (A^k_p, p - 2) \\
\end{array}
\]

$A_{0,0} A_{0,1} \ldots A_{0,p-1}$

$A_{1,0} A_{1,1} \ldots A_{1,p-1}$

$\ldots$

$A_{p-1,0} A_{p-1,1} \ldots A_{p-1,p-1}$

Fig. 1. Partitioning $A^k_p$.

$\begin{array}{cccc}
(a, 0) & (b, 1) & (2b - a, 2) & \ldots & (2a - b, p - 1) \\
(2a, 0) & (a + b, 1) & (2b, 2) & \ldots & (3a - b, p - 1) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(2a - b, p - 1) & (3a - b, p - 1) & (2a, 0) & (a + b, 1) & \ldots & (4a - 2b, p - 2) \\
\end{array}$

Fig. 2. The array $A(a, b)$.

## 2. Results

We start with the observation that $A^k_p$ 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 $A^k_p$ that contain the triple $(0, 0, 0)$ is $T(A^k_p)/p^k$, so the number of transversals not containing this triple is $T(A^k_p)(1 - 1/p^k)$. In particular, $T^* = T(A_p)(1 - 1/p)$, and note rather trivially that $T(A_p) > p$.

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

Taken without the row and column labels inherited from $A^k_p$, the subarrays $A_{ij}$ and $A_{ij}^*$ are identical when $i + j = i' + j'$ in $Z_p$. 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 $A_{ij}$. 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 Fig. 2, which also shows the inherited row and column labels.

Note that the row and column labels of $A(a, b)$, inherited from $A^k_p$, 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 $A^k_p$ 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 $A^k_p$ is obtained that does not contain the triple $((a, 0), (a, 0), (2a, 0))$. Hence, for each given $a \in Z_{p}^{k-1}$, $T^*$ distinct transversals of $A^k_p$ may be obtained for each $b \in Z_{p}^{k-1}$. Furthermore, for two different values $b, b' \in Z_{p}^{k-1}$, 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 $p^k - T^*$ distinct transversals of $A^k_p$ 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 $b'$ choice is to be made. If $(a, b)$ defines one of the previous choices and $(a', b')$ is the proposed $b'$ 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 $(r b - (r - 1)a, r)$ are unequal for all $r, r' = 0, 1, \ldots, p - 1$. But these two quantities can only be equal if $r + (r - 1) a' = r + (r - 1) a$, 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 $r = 1, 2, \ldots, p - 1$. As $r$ varies from 1 to $p - 1$, $\frac{r - 1}{r}$ takes all values in $Z_p$, 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 $p^k - c - 1(p - 1)$ choices for $b'$ (rather more if there is multiple counting of excluded rows, columns and entries).

Now put $C = \left\lfloor \frac{p-1}{p-1} \right\rfloor = \frac{p^d - 1}{p-1}$ 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 $A_p^{c}$ 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

$$(T^*)(p^k - 1)(p^k - 2(p - 1)) \ldots (p^k - (c - 1)(p - 1)) = (T^*)(p - 1)^c \frac{c!}{(C - c)!}.$$ 

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 $((a_i, 0), (b_i, r - 1)a_i, r), (b_i, r - 2)a_i, r))$ 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

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

(1)

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

The final term in the summation (1) gives

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

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

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

(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

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

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 $k$,

$$T(A_p^k) > (nQ)^{\frac{n}{2p-1}},$$

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

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

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

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

since $(1 + \frac{1}{x})^{-r} \to e^{-r}$ as $r \to \infty$. Noting that $8/3e > 0.981$ and that $C = \frac{n}{6} - \frac{1}{2}$, we obtain
Corollary 2.2. For all sufficiently large $k$, $T(A_k^3) > (0.981n)^2$, where $n = 3^k$.

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

References