Designs, Codes and Cryptography (2020) 88:2187–2206
https://doi.org/10.1007/s10623-020-00771-6

Enumerating extensions of mutually orthogonal Latin squares

Simona Boyadzhiyska[1] · Shagnik Das[1] · Tibor Szabó[1]

Received: 8 October 2019 / Revised: 8 March 2020 / Accepted: 3 June 2020 / Published online: 30 June 2020

Abstract

Two $n \times n$ Latin squares L_1, L_2 are said to be *orthogonal* if, for every ordered pair (x, y) of symbols, there are coordinates (i, j) such that $L_1(i, j) = x$ and $L_2(i, j) = y$. A k-*MOLS* is a sequence of k pairwise-orthogonal Latin squares, and the existence and enumeration of these objects has attracted a great deal of attention. Recent work of Keevash and Luria provides, for all fixed k, log-asymptotically tight bounds on the number of k-MOLS. To study the situation when k grows with n, we bound the number of ways a k-MOLS can be extended to a $(k+1)$-MOLS. These bounds are again tight for constant k, and allow us to deduce upper bounds on the total number of k-MOLS for all k. These bounds are close to tight even for k linear in n, and readily generalise to the broader class of gerechte designs, which include Sudoku squares.

Keywords Latin squares · Orthogonal mates · Gerechte designs

Mathematics Subject Classification 05B15

Communicated by L. Teirlinck.

S. Boyadzhiyska was supported by the Deutsche Forschungsgemeinschaft (DFG) Graduiertenkolleg "Facets of Complexity" (GRK 2434). S. Das was supported in part by the Deutsche Forschungsgemeinschaft (DFG) Project 415310276. S. Das and T. Szabó were supported in part by the German-Israeli Foundation for Scientific Research and Development (GIF) Grant G-1347-304.6/2016.

✉ Shagnik Das
shagnik@mi.fu-berlin.de

Simona Boyadzhiyska
s.boyadzhiyska@fu-berlin.de

Tibor Szabó
szabo@mi.fu-berlin.de

[1] Institut für Mathematik, Freie Universität Berlin, 14195 Berlin, Germany

1 Introduction

Latin squares have a long and storied history in combinatorics, sharing connections to several other areas of mathematics and enjoying applications in statistics and experimental design. In particular, orthogonal Latin squares are equivalent to many other classical structures in design theory, and their study dates back to Euler. In this paper we shall answer questions concerning the enumeration of orthogonal Latin squares, but we first present some of the relevant background.

1.1 Background and related work

We begin by recalling the definition of a Latin square, more in an effort to present our notation than in belief that you, the reader, do not know what a Latin square is.

Definition 1 A *Latin square of order* n is an $n \times n$ matrix with entries in $[n]$ such that each $x \in [n]$ appears exactly once in every row and in every column.

It is not difficult to see that Latin squares exist for all n; indeed, a rich class of constructions are given by the Cayley tables of groups. We refer the reader to [40] for more definitions, results and proofs related to Latin squares, noting only that the number of Latin squares is log-asymptotically given by

$$L(n) = \left((1 + o(1))\frac{n}{e^2}\right)^{n^2}. \tag{1}$$

Ryser [38] showed that the lower bound follows from Van der Waerden's conjecture on permanents of matrices, which was famously later proven by Egorychev [14] and Falikman [15]. The upper bound is also closely related to permanents, as it is a consequence of Brégman's Theorem [5] (see [40, Chapter 17] for details).

In this paper, we will be concerned with orthogonal Latin squares.

Definition 2 Two Latin squares L, L' of order n are said to be *orthogonal* if, for all pairs $(x, y) \in [n]^2$, there exist unique $i, j \in [n]$ such that $L(i, j) = x$ and $L'(i, j) = y$. In this case, L' is said to be an *orthogonal mate* of L.

A k-tuple of Latin squares $(L_1, \dots, L_k)$ forms a system of k *mutually orthogonal Latin squares*, or a k*-MOLS*, if for all $1 \le i < j \le k$, the squares L_i and L_j are orthogonal.

Orthogonal Latin squares have proven interesting from both a theoretical and a practical point of view: they are related to various other classes of structures in design theory, some of which we shall encounter later, while having applications in many real-world problems. In light of these applications, the early research in this area concerned the existence of k-MOLS. In particular, there was much interest in the maximum size of a set of mutually orthogonal Latin squares; that is, the function $N(n) = \max\{k : \text{a } k\text{-MOLS of order } n \text{ exists}\}$.

It is well-known that $N(n) \le n-1$. Indeed, suppose $(L_1, \dots, L_k)$ is a k-MOLS. Observing that orthogonality is preserved under permutations of the symbols within each square, we may assume that the first row of each square is $[1, 2, \dots, n]$. Considering the entries in position $(2, 1)$, we find that all $L_i(2, 1)$ must be distinct, by orthogonality, and different from 1, since the L_i are Latin squares. Hence $k \le n - 1$.

One can further prove that one has equality if and only if a projective plane of order n exists. This shows that the precise determination of the function $N(n)$ is likely to be difficult, as the existence of projective planes for orders n that are not prime powers is a longstanding open problem. Still, several polynomial lower bounds on $N(n)$ with ever-improving exponents appear in the literature [8,37,43], with the largest one due to Lu [31], who proved $N(n) = \Omega(n^{1/14.3})$.

Given that large sets of mutually orthogonal Latin squares exist, it is natural to extend (1) and enumerate k-MOLS for $k \geq 2$. Early work in this direction was undertaken by Donovan and Grannell [10], who constructed many k-MOLS, and also sought to bound the number of orthogonal mates a Latin square can have. An important component of their argument is an upper bound on number of transversals in a Latin square, where a transversal is a selection of n cells from the square, with no two sharing the same row, column or symbol. Taranenko [39] later proved a sharp upper bound on the number of transversals in a Latin square, which, when used in Donovan and Grannell's proof, shows that a Latin square can have at most

$$\left((1+o(1))\frac{n}{e^{2+1/e}}\right)^{n^2} \tag{2}$$

orthogonal mates. Coupled with (1), this can be used to give upper bounds on the number of pairs of orthogonal Latin squares and, more generally, the number of k-MOLS (since in a k-MOLS $(L_1, \ldots, L_k)$, the Latin squares $L_2, \ldots, L_k$ must all be orthogonal mates of L_1).

More recently, tight bounds on the number of k-MOLS follow from the breakthroughs of Luria [32] and Keevash [26]. Through an elegant entropic argument, Luria gives a general upper bound on the number of perfect matchings a regular r-uniform hypergraph can have. Assuming certain pseudorandom conditions, Keevash provides a matching lower bound, coupling randomized constructions with the use of absorbers. When applied to the enumeration of k-MOLS, their theorems imply the following result, where we denote by $L^{(k)}(n)$ the number of k-MOLS of order n.

Theorem 1 [27,32] *For every fixed $k \in \mathbb{N}$, the number of k-MOLS of order n is*

$$L^{(k)}(n) = \left((1+o(1))\frac{n^k}{e^{\binom{k+2}{2}-1}}\right)^{n^2}. \tag{3}$$

1.2 Results

The one drawback of Theorem 1 is that both the lower and upper bounds in (3) require k to be fixed as n tends to infinity. In this paper we seek upper bounds that hold when k grows with n. We combine the approach of Donovan and Grannell [10] with the method of Luria [32], using entropy to bound the number of ways of extending a k-MOLS by adding an additional Latin square.

Before presenting our upper bound, let us discuss a lower bound for this number of extensions. Since every $(k+1)$-MOLS contains a k-MOLS as a prefix, Theorem 1 implies that, for fixed $k \in \mathbb{N}$, the average number of extensions of a k-MOLS to a $(k+1)$-MOLS is at least

$$\frac{L^{(k+1)}(n)}{L^{(k)}(n)} = \left((1+o(1))\frac{n}{e^{k+2}}\right)^{n^2}. \tag{4}$$

This clearly gives a lower bound for the maximum number of such extensions. In the following theorem, we provide an upper bound that is valid for all k. (Throughout this paper, all logarithms are to the base e.)

Theorem 2 *For $0 \leq k \leq n-2$, the logarithm of the number of ways to extend a k-MOLS of order n to a $(k+1)$-MOLS is at most*

$$n^2 \int_0^1 \log(1+(n-1)t^{k+2}) \mathrm{d}t.$$

We will estimate the value of this integral in Lemma 1. As a corollary, combining Theorem 2 with (4) allows us to determine the number of extensions of a k-MOLS of fixed size. In particular, setting $k=1$ bounds the number of orthogonal mates a Latin square can have, sharpening the bound in (2).

Corollary 1 *For every fixed $k \in \mathbb{N}$, the maximum number of ways to extend a k-MOLS of order n to a $(k+1)$-MOLS is*

$$\left((1+o(1))\frac{n}{e^{k+2}}\right)^{n^2}.$$

As previously stated, our primary goal is to bound the number of k-MOLS when k grows with n. We can do so by building the k-MOLS one Latin square at a time, using Theorem 2 to bound the number of choices at each step. In this way we can recover the upper bound of Theorem 1 when k is constant, but the main novelty of this paper is the following extension to larger values of k.

Corollary 2 *As $n \to \infty$,*

(i) $\log L^{(k)}(n) \leq \left(k \log n - \binom{k+2}{2} + 1 + k^2 n^{-1/(k+2)}\right) n^2$ *if $k = o(\log n)$,*

(ii) $\log L^{(k)}(n) \leq (c(\beta) + o(1))\, k n^2 \log n$ *if $k = \beta \log n$, for fixed $\beta > 0$,*

(iii) $\log L^{(k)}(n) \leq \left(\frac{1}{2} + o(1)\right) (\log k - \log\log n)\, n^2 \log^2 n$ *if $k = \omega(\log n)$,*

where in (ii) we define $c(\beta) = 1 - \beta^{-1} \int_0^\beta x(1-e^{-1/x})\mathrm{d}x \in [0,1]$.

Note that we trivially have $L^{(k)}(n) \leq L(n)^k$, which, in light of (1), gives the upper bound $\log L^{(k)}(n) \leq kn^2 \log n$. Corollary 2 provides a significant improvement over this trivial bound. Furthermore, part (i) shows that the upper bound from Theorem 1 is valid whenever $k = o\left(\frac{\log n}{\log\log n}\right)$.

It is well-known that mutually orthogonal Latin squares are equivalent to many other combinatorial structures such as transversal designs, nets and orthogonal arrays, while also being related to certain error correcting codes and affine and projective planes (see [40]), and so our results give upper bounds for the number of structures in each of these classes. In fact, we shall prove Theorem 2 for the more general class of gerechte designs (see Theorem 3), which allow us to, for instance, bound the number of sets of mutually orthogonal Sudoku squares. We discuss this particular extension further in our concluding remarks.

1.3 Organization

The remainder of this paper is organized as follows. In Sect. 2, we introduce gerechte designs and discuss an equivalent formulation that will be more convenient for our proof. We also review some basic notions about our main tool, entropy. Following that, we prove our results in Sect. 3. We then provide explicit constructions of Latin squares with many orthogonal mates in Sect. 4, and close with some further remarks and open problems in Sect. 5.

2 Designs and tools

In this section we will introduce the frameworks of gerechte designs and orthogonal arrays, in which we will prove a generalization of Theorem 2. We will also review some definitions and results regarding entropy that we shall require in our proofs.

2.1 Gerechte designs

Gerechte designs, defined below, are a special class of Latin squares introduced by Behrens in [2].

Definition 3 Let $[n]^2 = R_1 \sqcup \cdots \sqcup R_n$ be a partition of $[n]^2$ into n regions R_i such that $|R_i| = n$ for all $i \in [n]$. A *gerechte design of order n* with respect to this partition is a Latin square with the additional property that each symbol appears exactly once in each region R_i.

There are several natural examples of gerechte designs. For instance, if one takes the regions to be the n rows (or columns) of the $n \times n$ grid, a gerechte design is simply a Latin square. If $n = m^2$, and one partitions the grid into n subsquares of dimension $m \times m$, the corresponding gerechte designs are known as *Sudoku squares of order n*. Finally, given a Latin square L, define the regions $R_t = \{(i, j) : L(i, j) = t\}$ for all $t \in [n]$. A gerechte design with respect to this partition is an orthogonal mate of L.

It is natural to study orthogonality between Latin squares that are gerechte designs with respect to the same partition and, more generally, to consider systems of mutually orthogonal gerechte designs. Bailey, Cameron and Connelly [1] generalized the function $N(n)$ to the setting of gerechte designs, giving upper bounds on the size of a set of mutually orthogonal gerechte designs that are tight for some orders n.

The counting questions concerning Latin squares discussed in the introduction can also be generalized to gerechte designs, and our method will allow us to derive bounds in this broader setting. For this, note that an $n \times n$ square with entries in $[n]$ is a Latin square if and only if it is orthogonal (in the sense of Definition 2) to the square S_n, given by $S_n(i, j) = i$ for all $i, j \in [n]$, and its transpose. Similarly, it is not difficult to show that an $n \times n$ square with entries in $[n]$ is a gerechte design with respect to the regions $R_1, \ldots, R_n$ if and only if it is orthogonal to the squares S_n, S_n^T, and B, where B is given by $B(i, j) = t$ if $(i, j) \in R_t$. Note that, while the squares S_n and S_n^T are orthogonal to each other, the square B need not be orthogonal to either (that is, B need not be a Latin square).

2.2 Orthogonal arrays and nearly orthogonal arrays

When adding a square to a set of mutually orthogonal gerechte designs, we need to ensure three properties: that it is a Latin square, that it respects the regions of the design, and that it is orthogonal to the previous squares. For our proof, it will be helpful to use an equivalent but more symmetric formulation of mutually orthogonal gerechte designs, where these three properties all take the same form. We begin in the setting of mutually orthogonal Latin squares.

Definition 4 Let x, y be vectors in $[n]^{n^2}$. We say that x and y are *orthogonal* if, for all pairs $(s, t) \in [n]^2$, there exists a unique index ℓ such that $x_\ell = s$ and $y_\ell = t$. An *orthogonal array $OA(n, d)$* is an $n^2 \times d$ array A with entries in $[n]$ such that all pairs of its columns are orthogonal.

We note that in the literature orthogonal arrays are often defined more generally and Definition 4 describes what is known as an *orthogonal array with strength two and index one*. For the sake of simplicity, we omit the general definition and refer the reader to [20] for more about orthogonal arrays.

Given a k-MOLS $(L_1, \ldots, L_k)$ of order n, we can construct an orthogonal array $OA(n, k+2)$ by taking, for all $(i, j) \in [n]^2$, the vectors $[i, j, L_1(i, j), L_2(i, j), \ldots, L_k(i, j)]$ as rows of the orthogonal array (and ordering them lexicographically). Similarly, given an $n^2 \times (k + 2)$ orthogonal array A, we can construct a k-MOLS of order n by setting $L_j(A(\ell, 1), A(\ell, 2)) = A(\ell, j + 2)$ for all $1 \leq \ell \leq n^2$ and $1 \leq j \leq k$ (in fact, any two columns of the orthogonal array can be used to coordinatize the Latin squares; here we use the first two). Notice that distinct sequences of mutually orthogonal Latin squares correspond to distinct orthogonal arrays with first two columns $v_1 = [1, \ldots, 1, 2, \ldots, 2, \ldots, n, \ldots, n]^T$ and $v_2 = [1, 2, \ldots, n, 1, 2, \ldots, n, \ldots, 1, 2, \ldots, n]^T$, and hence the number of k-MOLS of order n is the same as the number of orthogonal arrays $OA(n, k + 2)$ with first columns v_1 and v_2.

We now extend these ideas to mutually orthogonal gerechte designs. Let v_3 be a vector in $[n]^{n^2}$ with each integer in $[n]$ appearing n times. Note that v_3 determines a partition of the elements of $[n^2]$ (and thus $[n]^2$, after we fix a linear ordering of this set) into n equally-sized regions. From the equivalence between mutually orthogonal Latin squares and orthogonal arrays and the discussion at the end of Sect. 2.1, we can conclude that an $OA(n, k + 2)$, whose first two columns are v_1 and v_2, and in which all other columns are also orthogonal to v_3, is equivalent to k mutually orthogonal gerechte designs with respect to the partition determined by v_3. For notational convenience, we add the column v_3 to the array and call the resulting structure an $n^2 \times (k + 3)$ *nearly orthogonal array*.

Definition 5 Given $n \in \mathbb{N}$ and $d \geq 3$, a *nearly orthogonal array* $NOA(n, d)$ is an $n^2 \times d$ array A with symbols $[n]$ such that:

(a) the first column is v_1 and the second column is v_2, as defined above,
(b) each symbol in $[n]$ appears exactly n times in the third column v_3, and
(c) for all $i \geq 4$, the ith column v_i is orthogonal to all other columns in A.

Again, it follows that the number of nearly orthogonal arrays $NOA(n, k + 3)$ is equal to the number of sets of k mutually orthogonal gerechte designs with respect to the partition defined by v_3.

2.3 Entropy

The proof of our main result is based on entropy. This method has previously given good asymptotic upper bounds for similar problems; for instance, it is used in [36] to prove Brégman's Theorem on the permanent of a matrix (which yields an asymptotically tight upper bound on the number of Latin squares), in [28] to show an upper bound on the number of Steiner triple systems, later shown to be tight in [27], and in [17] to provide a simpler proof of Taranenko's result on the maximum number of transversals in a Latin square, also shown to be tight in the same paper; see also [32] for some further applications. In this section, we review some basic facts about entropy that will be used in our proof. For more on entropy, see [9].

Let X be a discrete random variable taking values in a given finite set $\mathcal{S}$, and let $p(x) = \Pr[X = x]$ for all $x \in \mathcal{S}$. The *(base e) entropy* of X is given by

$$H(X) = -\sum_{x \in \mathcal{S}} p(x) \log p(x) = -\mathbb{E}[\log p(X)],$$

where we adopt the convention that $0 \log 0 = 0$. The entropy of X can be seen as a measure of the amount of information the random variable encodes. It is not difficult to show that

$$H(X) \leq \log |R(X)|, \tag{5}$$

where $R(X) = \{x \in \mathcal{S} : p(x) > 0\}$ is the range of the random variable, with equality if and only if X is uniformly distributed over $R(X)$.

This definition can be extended to multiple random variables in the natural way. We define the *joint entropy* of two random variables X and Y to be

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y) = -\mathbb{E}[\log p(X, Y)],$$

where $p(x, y) = \Pr[X = x, Y = y]$ denotes the joint distribution of X and Y.

The *conditional entropy* of X given Y is defined to be

$$H(X|Y) = \mathbb{E}_{y \sim Y}[H(X|Y = y)] = \sum_{y} \Pr[Y = y] H(X|Y = y).$$

Conditional entropy gives us a way to measure how much additional information we expect to learn from X once we know the value of Y. It is a simple exercise to show that the joint entropy and the conditional entropy of several random variables satisfy the following equality, known as the chain rule:

$$H(X_1, \ldots, X_n) = \sum_{i=1}^{n} H(X_i | X_1, \ldots, X_{i-1}).$$

We end this section by outlining the basic idea behind counting proofs based on entropy. Suppose we want to obtain a bound on the size of a set $\mathcal{S}$. We sample an element $X \in \mathcal{S}$ uniformly at random. By the above discussion, we have $H(X) = \log |\mathcal{S}|$, and so an upper bound on the entropy $H(X)$ yields an upper bound on $|\mathcal{S}|$. To bound $H(X)$, we break up the random variable X into simpler random variables; the chain rule then allows us to consider these new random variables one at a time.

3 Proofs of our results

We now use the material from the previous section to prove Theorem 2 and its corollaries.

3.1 Bounding the number of extensions

In the language of orthogonal arrays, Theorem 2 is a statement about the number of ways to extend an orthogonal array by one column. We will in fact prove the following more general result, bounding the number of ways to extend a nearly orthogonal array by one column. Indeed, by inserting a copy of the first column in the third column (and reordering the rows if needed), one obtains a nearly orthogonal array from an orthogonal array.

Theorem 3 *Given $n \in \mathbb{N}$ and $d \geq 3$, let A be a nearly orthogonal array $NOA(n, d)$. For each row $\ell \in [n^2]$, define*

$$r_\ell = |\{s \neq \ell : A(s, 1) = A(\ell, 1) \text{ and } A(s, 3) = A(\ell, 3)\}|, \text{ and}$$
$$c_\ell = |\{s \neq \ell : A(s, 2) = A(\ell, 2) \text{ and } A(s, 3) = A(\ell, 3)\}|.$$

Then the logarithm of the number of ways to extend A to a nearly orthogonal array with $d + 1$ columns is at most

$$\sum_{\ell=1}^{n^2} \int_0^1 \log(1 + (r_\ell + c_\ell)t^{d-1} + (n - r_\ell - c_\ell - 1)t^d)\mathrm{d}t.$$

Observe that in the gerechte design setting, for a cell $\ell \in [n]^2$, r_ℓ counts the number of other cells in the same row and region as ℓ, while c_ℓ counts the number of cells sharing the same column and region.

Before proving Theorem 3, we quickly derive Theorem 2.

Proof of Theorem 2 As previously mentioned, a Latin square is a gerechte design with respect to the partition of the cells into their rows. A k-MOLS is thus equivalent to an $NOA(n, k+3)$ with $v_3 = v_1$, and an extension to a $(k+1)$-MOLS corresponds to adding a column to obtain an $NOA(n, k+4)$.

We can thus apply Theorem 3 with $d = k + 3 \geq 3$. For our choice of v_3, we have $r_\ell = n - 1$ and $c_\ell = 0$ for all $\ell \in [n^2]$. Substituting in these values, the bound on the number of extensions is

$$\sum_{\ell=1}^{n^2} \int_0^1 \log(1 + (n - 1)t^{k+2})\mathrm{d}t = n^2 \int_0^1 \log(1 + (n - 1)t^{k+2})\mathrm{d}t,$$

as required. □

We now proceed to the proof of the general theorem.

Proof of Theorem 3 Let A be as given, and let $\mathcal{S}$ denote the set of column vectors that are valid extensions for A. Our goal is to bound $|\mathcal{S}|$. We can assume $\mathcal{S} \neq \emptyset$, otherwise we are done. Let $X \in \mathcal{S}$ be chosen uniformly at random. Then $H(X) = \log |\mathcal{S}|$, and so it suffices to bound the entropy of X. We will expose the coordinates of X one at a time, using the chain rule to express the total entropy $H(X)$ as the sum of the conditional entropies from each successive reveal.

For $\ell \in [n^2]$, we denote the ℓth coordinate of X by X_ℓ and, given a permutation π of $[n^2]$, we reveal the coordinates in the order $X_{\pi(1)}, X_{\pi(2)}, \ldots, X_{\pi(n^2)}$. The chain rule then gives

$$\begin{aligned}\log |\mathcal{S}| = H(X) &= \sum_{j=1}^{n^2} H(X_{\pi(j)} | X_{\pi(s)} : s < j)\\ &= \sum_{j=1}^{n^2} \mathbb{E}_{(x_{\pi(s)} \sim X_{\pi(s)} : s<j)} \left[H(X_{\pi(j)} | X_{\pi(s)} = x_{\pi(s)} : s < j)\right]. \qquad (6)\end{aligned}$$

Given $x \in [n]^{n^2}$, let $R_{\pi(j)}(\pi, x) = R(X_{\pi(j)} | X_{\pi(s)} = x_{\pi(s)} : s < j)$ denote the range of this conditional random variable, that is,

$$R_{\pi(j)}(\pi, x) = \left\{y \in [n] : \exists\, Y \in \mathcal{S} : Y_{\pi(j)} = y \text{ and } \forall s < j, Y_{\pi(s)} = x_{\pi(s)}\right\},$$

and let $N_{\pi(j)}(\pi, x) = \left|R_{\pi(j)}(\pi, x)\right|$ be the size of this range. Note that $R_{\pi(j)}(\pi, x)$, and hence also $N_{\pi(j)}(\pi, x)$, only depends on the first $j-1$ coordinates of x with respect to π; for $s \geq j$, the values $x_{\pi(s)}$ can be chosen arbitrarily without changing the range of the random variable.

Thus, by (5), we can bound the conditional entropy by $H(X_{\pi(j)}|X_{\pi(s)} = x_{\pi(s)} : s < j) \leq \log\left(N_{\pi(j)}(\pi, x)\right)$ for all $x \in [n]^{n^2}$. Substituting this into (6) and reordering the sum gives

$$\log |\mathcal{S}| \leq \sum_{j=1}^{n^2} \sum_{x \in [n]^{n^2}} \Pr[X = x] \log\left(N_{\pi(j)}(\pi, x)\right) = \sum_{\ell=1}^{n^2} \mathbb{E}_X\left[\log\left(N_\ell(\pi, x)\right)\right].$$

This bound holds for any permutation π, and thus it holds when we average over the choice of π. As our calculations are more convenient in the continuous setting, we sample the uniformly random permutation of $[n^2]$ by choosing a vector $\alpha = (\alpha_\ell)_{\ell=1}^{n^2}$ with $\alpha_\ell \sim U[0, 1]$ for all ℓ and defining $\pi_\alpha = \pi$ to be such that $\alpha_{\pi(1)} > \alpha_{\pi(2)} > \cdots > \alpha_{\pi(n^2)}$. We then have

$$\begin{aligned}\log |\mathcal{S}| &\leq \mathbb{E}_\alpha\left[\sum_{\ell=1}^{n^2} \mathbb{E}_X[\log(N_\ell(\pi, x))]\right] = \sum_{\ell=1}^{n^2} \mathbb{E}_X\left[\mathbb{E}_\alpha[\log(N_\ell(\pi, x))]\right] \\ &= \sum_{\ell=1}^{n^2} \mathbb{E}_X\left[\mathbb{E}_{\alpha_\ell}[\mathbb{E}_{\alpha|\alpha_\ell}[\log(N_\ell(\pi, x))]]\right] \leq \sum_{\ell=1}^{n^2} \mathbb{E}_X\left[\mathbb{E}_{\alpha_\ell}[\log(\mathbb{E}_{\alpha|\alpha_\ell}[N_\ell(\pi, x)])]\right],\end{aligned}$$

where the last inequality follows from Jensen's inequality and the concavity of $y \mapsto \log y$. It therefore suffices to show that, for all $\ell \in [n^2]$ and all $x \in \mathcal{S}$, we have

$$\mathbb{E}_{\alpha_\ell}[\log(\mathbb{E}_{\alpha|\alpha_\ell}[N_\ell(\pi, x)])] \leq \int_0^1 \log(1 + (r_\ell + c_\ell)t^{d-1} + (n - r_\ell - c_\ell - 1)t^d)\mathrm{d}t. \tag{7}$$

We first estimate the inner expectation $\mathbb{E}_{\alpha|\alpha_\ell}[N_\ell(\pi, x)] = \mathbb{E}_\alpha[N_\ell(\pi, x)|\alpha_\ell]$. By the linearity of expectation, this is equal to $\sum_{y \in [n]} \mathbb{P}\left[y \in R_\ell(\pi, x)|\alpha_\ell\right]$. Unfortunately, it is not straightforward to determine whether or not $y \in R_\ell(\pi, x)$, and so we shall instead use a simple necessary condition that we call *availability*.

Recall that for the column x to be orthogonal to the ith column of A, the pairs $(A(s, i), x_s)$ must be distinct for all $s \in [n^2]$. Therefore, if for some symbol $y \in [n]$ there is some column $i \in [d]$ and previously exposed coordinate s such that $A(s, i) = A(\ell, i)$ and $x_s = y$, we cannot also have $x_\ell = y$. In this case we declare y *unavailable*, and observe that we must have $y \notin R_\ell(\pi, x)$. Otherwise, if there is no such column i and coordinate s, we say y is *available*. We now seek to compute the probability that a symbol y is available.

Fix a symbol $y \in [n]$. If y is the true value of the entry in the ℓth coordinate of x, then y cannot possibly have been ruled out by the previously exposed entries, and is thus available with probability 1.

Now suppose $y \in [n]$ is not the true value of x_ℓ. For each $i \in [d]$, since x is orthogonal to the ith column of A, there must be a unique entry $s_i(y) \neq \ell$ such that $x_{s_i(y)} = y$ and $A(s_i(y), i) = A(\ell, i)$. In order for y to be available, ℓ must be exposed before the entries in the set $S(y) = \{s_i(y) : i \in [d]\}$.

To find the probability of y being available, then, we need to compute the size of $S(y)$. Suppose for distinct columns $1 \leq i < j \leq d$ we had $s_i(y) = s_j(y)$. It then follows that $A(s_i(y), i) = A(\ell, i)$ and $A(s_i(y), j) = A(\ell, j)$, and thus the ith and jth columns cannot be orthogonal. Since A is nearly orthogonal, the only possibilities are $i \in \{1, 2\}$ and $j = 3$

(by definition, all columns after the third column are orthogonal to all others, and the first two columns are orthogonal by construction).

Therefore $|S(y)| = d$, unless either $s_1(y) = s_3(y)$ or $s_2(y) = s_3(y)$. Note that these cannot happen simultaneously, as we have ruled out $s_1(y) = s_2(y)$, and thus in these cases we have $|S(y)| = d - 1$. There are r_ℓ choices of $s \neq \ell$ for which $A(s, 1) = A(\ell, 1)$ and $A(s, 3) = A(\ell, 3)$, and hence r_ℓ values y for which $s_1(y) = s_3(y)$. By orthogonality of x with the first column of A, these values are all distinct. Similarly, there are c_ℓ choices for y with $s_2(y) = s_3(y)$.

To summarize, there is one choice of y that is available with probability 1, there are $r_\ell + c_\ell$ choices of y that are available only if the ℓth coordinate is exposed before some fixed set of $d - 1$ other coordinates, and the remaining $n - r_\ell - c_\ell - 1$ choices of y are available only if the ℓth coordinate precedes some d other coordinates.

A coordinate s is revealed after ℓ if $\alpha_s < \alpha_\ell$, which occurs with probability α_ℓ. Moreover, these events are independent for distinct coordinates, and so the probabilities in the latter two cases are α_ℓ^{d-1} and α_ℓ^d respectively. This gives

$$\begin{aligned}\mathbb{E}_{\alpha|\alpha_\ell}[N_\ell(\pi, x)] &= \sum_{y\in[n]} \Pr[y \in R_\ell(\pi, x)] \leq \sum_{y\in[n]} \Pr[y \text{ is available}]\\ &= 1 + (r_\ell + c_\ell)\alpha_\ell^{d-1} + (n - r_\ell - c_\ell - 1)\alpha_\ell^d.\end{aligned}$$

Since α_ℓ is uniformly distributed over $[0, 1]$, substituting this into $\mathbb{E}_{\alpha_\ell}[\log(\mathbb{E}_{\alpha|\alpha_\ell}[N_\ell(\pi, x)])]$ results in (7), completing the proof. □

3.2 Estimating the integral

In order to apply Theorem 2, we need to understand the asymptotics of the bound it provides. In this next lemma, we show how to estimate the integral from the theorem.

Lemma 1 *Let $2 \leq d \leq n$ and $I_d = \int_0^1 \log(1 + (n-1)t^d)\mathrm{d}t$. Then*

$$I_d \leq \log\left(\frac{n-1}{e^d}\right) + \frac{d}{(n-1)^{1/d}} + \frac{3}{d(n-1)^{1/d}}.$$

Proof Set $t_0 = (n-1)^{-1/d}$. Note that $(n-1)t^d < 1$ if and only if $t < t_0$. We have

$$\begin{aligned}I_d &= \int_0^1 \log(1 + (n-1)t^d)\mathrm{d}t\\ &= \int_0^{t_0} \log(1 + (n-1)t^d)\mathrm{d}t + \int_{t_0}^1 \log((n-1)t^d)\mathrm{d}t + \int_{t_0}^1 \log\left(1 + \frac{1}{(n-1)t^d}\right)\mathrm{d}t.\end{aligned}$$

We estimate the three integrals in turn:

$$\int_0^{t_0} \log(1 + (n-1)t^d)\mathrm{d}t \leq \int_0^{t_0} (n-1)t^d \mathrm{d}t = \frac{n-1}{d+1}t^{d+1}\Big|_0^{t_0} = \frac{t_0}{d+1},$$

where for the inequality we use the fact that $\log(1 + x) \leq x$ for all $x > -1$, and in the final equality we use $t_0^d = (n-1)^{-1}$,

$$\begin{aligned}\int_{t_0}^{1} \log((n-1)t^d)\mathrm{d}t &= \int_{t_0}^{1} \log(n-1) + d\log t\,\mathrm{d}t \\ &= (1-t_0)\log(n-1) + d\,(t\log t - t)\Big|_{t_0}^{1} \\ &= (1-t_0)\log(n-1) + (t_0-1)d + t_0\log(n-1) \\ &= \log(n-1) + (t_0-1)d,\end{aligned}$$

where the penultimate equality again follows from $t_0^d = (n-1)^{-1}$, and

$$\int_{t_0}^{1} \log\left(1 + \frac{1}{(n-1)t^d}\right)\mathrm{d}t \le \int_{t_0}^{1} \frac{1}{(n-1)t^d}\mathrm{d}t = \frac{-1}{(n-1)(d-1)} + \frac{t_0}{d-1}.$$

Hence, we have

$$\begin{aligned}I_d &\le \frac{t_0}{d+1} + \log(n-1) + (t_0-1)d - \frac{1}{(n-1)(d-1)} + \frac{t_0}{d-1} \\ &\le \log\left(\frac{n-1}{e^d}\right) + \frac{d}{(n-1)^{1/d}} + \frac{3}{d(n-1)^{1/d}},\end{aligned}$$

where we ignore the negative term and bound $\frac{1}{d+1} + \frac{1}{d-1}$ by $\frac{3}{d}$. □

Corollary 1 now follows easily from Theorem 2 and Lemma 1.

Proof of Corollary 1 The lower bound comes from the average number of extensions of a k-MOLS, computed in (3). For the upper bound, Theorem 2 asserts that the logarithm of the number of extensions of a k-MOLS of order n is, in the notation of Lemma 1, at most $n^2 I_{k+2}$. By the lemma, this is bounded by

$$n^2\left(\log\left(\frac{n-1}{e^{k+2}}\right) + \frac{k+2}{(n-1)^{1/(k+2)}} + \frac{3}{(k+2)(n-1)^{1/(k+2)}}\right) \le n^2\left(\log\left(\frac{n-1}{e^{k+2}}\right) + \frac{k+4}{(n-1)^{1/(k+2)}}\right).$$

Since k is fixed as n tends to infinity, this is

$$n^2\left(\log\left(\frac{n-1}{e^{k+2}}\right) + o(1)\right) = n^2\log\left((1+o(1))\frac{n-1}{e^{k+2}}\right) = n^2\log\left((1+o(1))\frac{n}{e^{k+2}}\right),$$

giving the desired upper bound. □

Finally, we deduce our upper bound on the number of large sets of mutually orthogonal Latin squares.

Proof of Corollary 2 We can build a k-MOLS by starting with the empty 0-MOLS, and extending it by one Latin square at a time. Theorem 2 bounds the number of possible extensions at each step, and so, in the notation of Lemma 1, we have

$$\log L^{(k)}(n) \le n^2 \sum_{d=2}^{k+1} I_d. \tag{8}$$

We shall prove each part of the corollary by estimating this sum appropriately.

(i) By Lemma 1, we have

$$I_d \le \log(n-1) - d + \frac{d+2}{(n-1)^{1/d}}.$$

Hence, summing over d, we obtain

$$\sum_{d=2}^{k+1} I_d \le k\log(n-1) - \left(\binom{k+2}{2} - 1\right) + \binom{k+4}{2}(n-1)^{-1/(k+2)},$$

from which the bound follows. Note that when $k = o(\log n)$, the final summand is a lower order term compared to k^2, and we can be generous in our estimation.

(ii) When $k = \Omega(\log n)$, that final term above becomes significant. While the previous upper bound remains valid, we obtain a better result through more careful calculation. Rearranging the bound in Lemma 1 gives

$$\begin{aligned} I_d &\le \log(n-1) - d\left(1 - (n-1)^{-1/d}\right) + \frac{3}{d(n-1)^{1/d}} \\ &\le \log(n-1) - d\left(1 - e^{-\frac{\log(n-1)}{d}}\right) + \frac{3}{d}. \end{aligned}$$

Therefore we have

$$\sum_{d=2}^{k+1} I_d \le k\log(n-1) - \sum_{d=2}^{k+1} d\left(1 - e^{-\frac{\log(n-1)}{d}}\right) + \sum_{d=2}^{k+1}\frac{3}{d}.$$

The second sum, an error term, is at most $3\log(k+1)$. For the first sum, by making the substitution $x = \frac{d}{\log(n-1)}$, we observe that this is related to the estimation of the integral $\int x\left(1 - e^{-1/x}\right)\mathrm{d}x$ by the Riemann sum with step size $1/\log(n-1)$. More precisely, we have

$$\frac{1}{\log(n-1)}\sum_{d=2}^{k+1}\frac{d}{\log(n-1)}\left(1 - e^{-\frac{\log(n-1)}{d}}\right) = \int_{\frac{2}{\log(n-1)}}^{\frac{k+1}{\log(n-1)}} x\left(1 - e^{-1/x}\right)\mathrm{d}x + o(1).$$

Making the necessary substitutions and letting n tend to infinity gives the claimed bound.

(iii) When $k = \omega(\log n)$, the above integral has an infinite domain, but we shall show that it still converges. First, we estimate $e^{-1/x}$ to observe that

$$x\left(1 - e^{-1/x}\right) = 1 - \frac{1}{2x} + O(x^{-2}),$$

where the asymptotics are as x tends to infinity. Hence, when β tends to infinity,

$$\int_0^{\beta} x\left(1 - e^{-1/x}\right)\mathrm{d}x = \int_0^{\beta} 1 - \frac{1}{2x} + O(x^{-2})\mathrm{d}x = \beta - \tfrac{1}{2}\log(\beta) + O(1).$$

The result then follows by substituting this into the statement of part (ii) with $\beta = \frac{k}{\log n}$; since the integrand $x\left(1 - e^{-1/x}\right)$ is bounded and monotone increasing for large x, the Riemann sum remains a good approximation of the integral when $\beta \to \infty$. □

4 Explicit constructions

Corollary 1 establishes the existence of Latin squares with several orthogonal mates. Given the numerous applications of orthogonal Latin squares, however, it is of great interest to have explicit constructions of such squares. For instance, in the closely related problem of counting transversals in Latin squares, Taranenko [39] showed that a Latin square of order n can have at most $\left((1+o(1))\frac{n}{e^2}\right)^n$ transversals. Glebov and Luria [17] later proved that Taranenko's bound is tight via a probabilistic construction. Recent results of Eberhard et al. [12] and Eberhard [11] give a constructive proof of the theorem of Glebov and Luria, providing explicit examples of Latin squares attaining this bound (in a very precise sense). They show that the Cayley table of any abelian group G where $\sum\limits_{g\in G} g = 0$ has $\left(\frac{2\pi n^2}{\sqrt{e}} + o(1)\right)\left(\frac{n}{e^2}\right)^n$ transversals.

To see the relation between transversals and orthogonal mates, observe that the n translates of any transversal in a Cayley table partition the Latin square. For each such partition into transversals, we can construct $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ distinct orthogonal mates by assigning distinct symbols in $[n]$ to the n transversals. The results of Eberhard et al. thus imply that Cayley tables of abelian groups have at least $\left(\sqrt{\frac{8\pi^3 n^5}{e}} + o(1)\right)\left(\frac{n^2}{e^3}\right)^n$ orthogonal mates. This lower bound is much smaller than the upper bound we would like to match, because this simple argument only counts orthogonal mates of a very special type. Here we describe a construction of MacNeish [33] that allows us to significantly improve this bound, even if we still fall slightly short of the true maximum number of orthogonal mates given by Corollary 1.

The *Kronecker product* of two Latin squares L_1 and L_2 of order n_1 and n_2 respectively is the Latin square $L_1 \otimes L_2$ of order n_1n_2 given by $(L_1 \otimes L_2)((i_1, j_1), (i_2, j_2)) = (L_1(i_1, i_2), L_2(j_1, j_2))$. (Of course, the row and column indices and the symbols of $L_1 \otimes L_2$ can be seen as elements of $[n_1n_2]$ after fixing an arbitrary bijection from $[n_1] \times [n_2]$.) For a Latin square L, we write $L^{\otimes k}$ to denote the k-fold product $\underbrace{L \otimes \cdots \otimes L}_{k \text{ times}}$.

Proposition 1 *Let L_1 and L_2 be Latin squares of order n_1 and n_2 that have q_1 and q_2 orthogonal mates respectively. Then the number of orthogonal mates of $L_1 \otimes L_2$ is at least $q_1 q_2^{n_1^2} \frac{(n_1n_2)!}{n_1!(n_2!)^{n_1}}$.*

Proof We will show how orthogonal mates of L_1 and L_2 can be combined in several ways to produce orthogonal mates of the product $L_1 \otimes L_2$. For this, it is again useful to view an orthogonal mate as an ordered partition of $L_1 \otimes L_2$ into disjoint transversals.

Further observe that $L_1 \otimes L_2$ can be partitioned into n_1^2 blocks of the form $L_1(i_1, i_2) \otimes L_2$ for $i_1, i_2 \in [n_1]$. Each of these is isomorphic to L_2, and thus admits q_2 orthogonal mates.

There are q_1 orthogonal mates of L_1, and thus $\frac{q_1}{n_1!}$ *unordered* partitions of L_1 into disjoint transversals, say $\{T_1, \ldots, T_{n_1}\}$. In the product $L_1 \otimes L_2$, this partitions the blocks into n_1 disjoint sets.

Let T_j be one of the transversals in this decomposition of L_1. The corresponding blocks $T_j \otimes L_2 = \{L_1(i_1, i_2) \otimes L_2 : (i_1, i_2) \in T_j\}$ then have all distinct symbols from $[n_1]$ in the first coordinate, and hence cover each symbol in $[n_1] \times [n_2]$ precisely n_2 times. To get a transversal of $L_1 \otimes L_2$, we can choose a transversal in each block $L_1(i_1, i_2) \otimes L_2$ and stitch them together. Furthermore, if we partition each block into transversals, stitching them together gives a partition of $T_j \otimes L_2$ into transversals of $L_1 \otimes L_2$.

There are $q_2^{n_1}$ ways to choose orthogonal mates for each of the n_1 blocks in $T_j \otimes L_2$. Here we keep the ordering, as that tells us which transversals in different blocks should be stitched together. This gives us an ordered partition of $T_j \otimes L_2$ into n_2 transversals of $L_1 \otimes L_2$, and so there are $\frac{q_2^{n_1}}{n_2!}$ unordered partitions of this set of blocks into transversals.

Making these choices for each T_j, we obtain a total of $\frac{q_1}{n_1!}\left(\frac{q_2^{n_1}}{n_2!}\right)^{n_1}$ partitions of $L_1 \otimes L_2$ into $n_1 n_2$ disjoint transversals, each of which can easily be shown to be distinct. To obtain an orthogonal mate, we can order these transversals arbitrarily, and thus obtain $q_1 q_2^{n_1^2} \frac{(n_1 n_2)!}{n_1!(n_2!)^{n_1}}$ mates, as claimed. □

In particular, this implies that powers of a single Latin square have many orthogonal mates.

Corollary 3 *Let L be a Latin square of order m with q orthogonal mates. Then $L^{\otimes k}$ is a Latin square of order m^k with at least $q^{\frac{m^{2k}-1}{m^2-1}}$ orthogonal mates.*

Proof We proceed by induction. The statement is clearly true for $k = 1$. Suppose it holds for some $k \geq 1$. Then, by Proposition 1, with $L_1 = L^{\otimes k}$, $L_2 = L$, $n_1 = m^k$, $n_2 = m$, $q_1 = \frac{m^{2k}-1}{m^2-1}$, and $q_2 = q$, we know the number of mates of $L^{\otimes(k+1)}$ is at least

$$q^{\frac{m^{2k}-1}{m^2-1}} q^{m^{2k}} \frac{(m^{k+1})!}{(m^k)!(m!)^{m^k}} \geq q^{\frac{m^{2(k+1)}-1}{m^2-1}}.$$

□

If we take L to be the Cayley table of $\mathbb{Z}_3$, then we have $q = 6$. The k-fold Kronecker product of the Cayley table gives the Cayley table of the product group $\mathbb{Z}_3^k$, which by Corollary 3 has at least $(6^{1/8})^{3^{2k}-1}$ orthogonal mates. In the next corollary, we show that the constant in the base of the exponent can be made arbitrarily large at the cost of having a slightly less explicit construction.

Corollary 4 *For any $C > 0$, there are infinitely many orders n for which we can efficiently produce Latin squares with at least C^{n^2} orthogonal mates.*

Proof Let m be such that $\frac{m}{2e^3} > C$. By Corollary 1, provided m is sufficiently large, there is a Latin square L of order m with $\left((1+o(1))\frac{m}{e^3}\right)^{m^2} > C^{m^2}$ orthogonal mates; we can find such a square with a (finite) exhaustive search. By Corollary 3, we know that the Latin square $L^{\otimes k}$ of order $n = m^k$ has at least $C^{\frac{m^2(m^{2k}-1)}{m^2-1}} \geq C^{n^2}$ orthogonal mates. □

5 Concluding remarks and open questions

In this paper, by bounding the number of extensions of a set of mutually orthogonal Latin squares, we obtained upper bounds on the number of k-MOLS when k grows with n. The obvious question is how tight these bounds are — can we find corresponding lower bounds? The constructions of Donovan and Grannell [10], valid for infinitely many values of n when $k \leq \sqrt{n}$, give lower bounds of the form $\log L^{(k)}(n) = \Omega\left(\gamma(k,n)n^2 \log n\right)$, where $\gamma(k,n) = \max\left\{\frac{\log k}{k^2 \log n}, \frac{1}{k^4}\right\}$. This is considerably smaller than our upper bounds in Corollary 2, and it would be of great interest to narrow the gap. One might hope to extend the lower bounds of Keevash [26], which were tight for constant k, but, as he notes in his paper, it is unclear how his methods could be used when k grows.

Aside from the enumeration of k-MOLS, there are several other related open problems, and we elaborate on these possible directions of study below.

Orthogonal mates We have bounded the maximum number of orthogonal mates a Latin square can have, but it is natural to ask if it is typical for a Latin square to have any orthogonal mates at all. Computational results in this direction are given in [6,13,34]. His study of squares of small order led van Rees [41] to conjecture that, as $n \to \infty$, the proportion of Latin squares without orthogonal mates tends to one. On the other hand, having studied slightly larger orders, Wanless and Webb [42] suggested that the opposite may be true.

In (4), we saw that the results of Luria [32] and Keevash [26] imply that the average Latin square of order n has $\left((1+o(1))\frac{n}{e^3}\right)^{n^2}$ orthogonal mates. By Theorem 2, the same expression describes the maximum number of mates a square can have. Given the number of Latin squares (see (1)), it follows by double-counting orthogonal pairs that at least $\left((1+o(1))\frac{n}{e^2}\right)^{n^2}$ squares must have an orthogonal mate. Unfortunately, due to the lower order difference compared to (1) being in the base of the exponent, this falls short of resolving the question of whether or not most Latin squares have orthogonal mates.

Some evidence that this may not be straightforward to resolve is provided in [7], where Cavenagh and Wanless showed that, for almost all even n, there are at least $n^{(1-o(1))n^2}$ Latin squares of order n without a transversal, let alone an orthogonal mate. However, Ferber and Kwan [16] study the analogous question in Steiner triple systems, and show that almost all Steiner triple systems are almost resolvable. In the context of Latin squares, they suggest that their methods would show that almost all Latin squares have $(1-o(1))n$ disjoint transversals. Still, some new ideas would be needed to find the n disjoint transversals that form an orthogonal mate.

In Sect. 4 we showed, for any given $C > 0$, that we can, for infinitely many n, construct Latin squares of order n with at least C^{n^2} orthogonal mates. Given the existence of Latin squares with many more, namely $n^{(1+o(1))n^2}$, orthogonal mates, it is natural to seek better constructions.

Problem 1 Is there an explicit construction of a Latin square of order n with at least $n^{\Omega(n^2)}$ orthogonal mates?

In our product construction in Sect. 4, we only considered orthogonal mates consisting of very special kinds of transversals (those built within blocks, using transversals of the two factor squares). It is likely that these product squares have a much larger number of orthogonal mates, perhaps even close to the maximum possible.

We have also been vague with regards to what we mean by an explicit construction. As is customary in computer science, by *explicit* we mean there is an algorithm that constructs the Latin square in question in time polynomial in n. One can go further, and call a construction *strongly explicit* if each individual entry of the Latin square can be determined in polylogarithmic time. One can verify that our construction in the previous section is indeed strongly explicit. Yet one feels somewhat cheated, as in the first step of the construction we perform an exhaustive search to find an initial Latin square with many orthogonal mates (whose existence is guaranteed by random methods, see Corollary 1). It would be desirable to find constructions that are also "morally explicit" in the sense that they can be described mathematically, and in particular avoid any initial brute-force search. In this direction, it would be natural to investigate whether the Cayley tables of abelian groups G with $\sum_{g \in G} g = 0$ give examples of such Latin squares (cf. [11,12]).

Affine and projective planes As mentioned earlier, $(n-1)$-MOLS of order n correspond to affine, and hence projective, planes of order n. Our knowledge of lower bounds in this setting is even direr; it is conjectured that there are no such systems when n is not a prime power, and believed that there is a unique (up to isomorphism) projective plane when n is a prime. As a step towards proving these conjectures, one could seek to bound the number of affine/projective planes from above, a problem raised by Hedayat and Federer [19].

In our definition of $L^{(k)}(n)$, we do not account for isomorphism. Thus, given a single projective plane, we can permute the symbols within each square of the corresponding $(n-1)$-MOLS to obtain $(n!)^{n-1}$ distinct $(n-1)$-MOLS. This gives a lower bound of $L^{(n-1)}(n) \geq (n!)^{n-1} = e^{(1-o(1))n^2 \log n}$ whenever n is a prime power. We remark that, for certain prime powers n, Kantor [22] and Kantor and Williams [23] provide algebraic constructions of superpolynomially many non-isomorphic projective planes of order n, but this contributes a lower order term in the above bound.

For an upper bound, Corollary 2 yields $L^{(n-1)}(n) \leq e^{\left(\frac{1}{2}+o(1)\right)n^2 \log^3 n}$. However, since a projective plane corresponds to a maximum possible set of mutually orthogonal Latin squares, it has a very restricted structure, and we can take advantage of this to obtain a better upper bound. Given a projective plane Π_n of order n, a subset H of its lines is called a *defining set* if Π_n is the unique projective plane containing H — that is, the lines in H determine the remaining lines in Π_n. Building on the work of Kahn [21], Boros et al. [4] showed that every projective plane admits a small defining set.

Theorem 4 [4] *Every projective plane of order n (for n sufficiently large) contains a defining set of size at most* $22n \log n$.

This immediately improves our upper bound.

Corollary 5 $L^{(n-1)}(n) \leq e^{(22+o(1))n^2 \log^2 n}$.

Proof By Theorem 4, each projective plane of order n contains a set H of $22n \log n$ lines that determine the remaining ones uniquely. Each line is a subset of size $n+1$ of the n^2+n+1 points. Thus, there are $\binom{n^2+n+1}{n+1} = e^{(1+o(1))n \log n}$ possible lines and at most $(e^{(1+o(1))n \log n})^{22n \log n}$ possible sets H and hence projective planes of order n.

Each $(n-1)$-MOLS corresponds to an affine plane of order n (the n^2 cells represent the points, two parallel classes are formed by the rows and columns, and each of the $n-1$ Latin squares labels the lines of one of the remaining parallel classes), and every affine plane has a unique extension to a projective plane (for each parallel class, we extend the lines to a common new point, and add a line at infinity consisting of the new points). In the reverse direction, a projective plane corresponds to at most n^2+n+1 different affine planes, by choosing the line at infinity. Furthermore, each affine plane corresponds to at most $(n+1)!(n!)^{n+1} = e^{(1+o(1))n^2 \log n}$ distinct $(n-1)$-MOLS, since we can permute the parallel classes, and the lines within parallel classes. This contributes a lower order term, and so we can also bound $L^{(n-1)}(n) \leq e^{(22+o(1))n^2 \log^2 n}$. □

It would be of great interest to remove the extra logarithmic factor in the exponent of the upper bound, and thus reduce it log-asymptotically to the lower bound.

Conjecture 1

$$L^{(n-1)}(n) = e^{O\left(n^2 \log n\right)}.$$

As we obtain this many $(n-1)$-MOLS from a single projective plane, this would provide qualitative evidence in favor of the non-existence conjectures concerning projective planes. Note that a stronger result than Conjecture 1 (and a possible avenue of attack) would be to improve Theorem 4, which is not known to be tight. The best known lower bound for Theorem 4 is only linear in n, and, if every projective plane were to indeed contain a defining set of $O(n)$ lines, that would imply $L^{(n-1)}(n) = e^{\Theta(n^2 \log n)}$.

Sudoku squares As mentioned in Sect. 2.1, Sudoku squares are a special class of gerechte designs of order n, where $n = m^2$, with the array partitioned into $m \times m$ subsquares in the natural way. After Golomb [18] asked about the existence of a pair of orthogonal Sudoku squares of order 9 (corresponding to the popular puzzle), systems of k *mutually orthogonal Sudoku squares (k-MOSS)* have been studied by several authors. This research has primarily sought to determine the largest k for which a k-MOSS of order n can exist; we refer the reader to [1,24,25,29,30,35] for constructions and results in this direction.

One may ask the same counting questions as before for this restricted class of Latin squares, and these are relatively less well-studied. The number of Sudoku squares of order n is known to be $\left((1+o(1))\frac{n}{e^3}\right)^{n^2}$; the upper bound is shown independently by Luria [32] (using entropy) and Berend [3] (using Brégman's Theorem), while the matching lower bound is due to Keevash [26].

To enumerate k-MOSS for fixed k, we extend an idea of Keevash, defining a 4-uniform hypergraph H with vertices $V(H) = \left\{x_1, x_2, y_1, y_2, z_1^{(1)}, z_2^{(1)}, \ldots, z_1^{(k)}, z_2^{(k)}\right\}$ and edges $\{x_1, x_2, y_1, y_2\}$, $\left\{x_1, x_2, z_1^{(i)}, z_2^{(i)}\right\}$, $\left\{y_1, y_2, z_1^{(i)}, z_2^{(i)}\right\}$, $\left\{x_1, y_1, z_1^{(i)}, z_2^{(i)}\right\}$ and $\left\{z_1^{(i)}, z_2^{(i)}, z_1^{(j)}, z_2^{(j)}\right\}$ for all $1 \le i < j \le k$. Letting $H(\sqrt{n})$ be the $(2k+4)$-partite 4-uniform hypergraph obtained by blowing each vertex up into $\sqrt{n}$ new vertices, it follows that a k-MOSS is equivalent to a decomposition of $H(\sqrt{n})$ into copies of H. For fixed k, the results of Luria and Keevash show there are $\left((1+o(1))\frac{n^k}{e^{\binom{k+3}{2}-3}}\right)^{n^2}$ such decompositions.

Our results allow us to bound the number of ways of extending a k-MOSS by an additional Sudoku square. Since each cell shares its row (or column) with $\sqrt{n}-1$ other cells from the same subsquare, we have $r_\ell = c_\ell = \sqrt{n} - 1$ for each $\ell \in [n^2]$. Applying Theorem 3 shows that our upper bounds on k-MOSS coincide with our upper bounds on $(k+1)$-MOLS. In particular, the bound in (a) is once again tight, as it matches the average number of extensions of a k-MOSS.

Corollary 6 *(a) For all fixed k, the maximum number of extensions of a k-MOSS of order n to a* $(k+1)$*-MOSS is* $\left((1+o(1))\frac{n}{e^{k+3}}\right)^{n^2}$.

(b) For $k = k(n) \ge 0$*, the logarithm of the number of k-MOSS is at most*

$$\begin{array}{lll} (i) & \left((k+1)\log n - \binom{k+3}{2} + 3 + (k+1)^2 n^{-1/(k+3)} + o(1)\right) n^2 & \text{if } k = o(\log n), \\ (ii) & (c(\beta) + o(1))\, k n^2 \log n & \text{if } k = \beta \log n, \text{ for fixed } \beta > 0, \\ (iii) & \left(\frac{1}{2} + o(1)\right)(\log k - \log\log n) n^2 \log^2 n & \text{if } k = \omega(\log n), \end{array}$$

where $c(\beta)$*, as in Corollary 2, is defined to be* $1 - \beta^{-1}\int_0^\beta x(1 - e^{-1/x})\mathrm{d}x$.

Proof A k-MOSS corresponds to a $NOA(n, k+3)$ with $r_\ell = c_\ell = \sqrt{n} - 1$. Substituting these parameters into Theorem 3, the logarithm of the number of extensions of a k-MOSS is at most

$$\begin{aligned}
&n^2 \int_0^1 \log\left(1 + 2(\sqrt{n}-1)t^{k+2} + (n - 2\sqrt{n}+1)t^{k+3}\right) \mathrm{d}t \\
&= n^2 \int_0^1 \log\left(1 + (n-1)t^{k+3}\right) \mathrm{d}t + n^2 \int_0^1 \log\left(1 + \frac{2(\sqrt{n}-1)(1-t)t^{k+2}}{1+(n-1)t^{k+3}}\right) \mathrm{d}t.
\end{aligned}$$

The first integral is simply I_{k+3}, as evaluated in Lemma 1.

To bound the second integral, observe that

$$\begin{aligned}
\int_0^1 \log\left(1 + \frac{2(\sqrt{n}-1)(1-t)t^{k+2}}{1+(n-1)t^{k+3}}\right) \mathrm{d}t &\le \int_0^1 \frac{2(\sqrt{n}-1)(1-t)t^{k+2}}{1+(n-1)t^{k+3}} \mathrm{d}t \\
&\le \int_0^1 \frac{(2\sqrt{n-1})t^{k+2}}{1+(n-1)t^{k+3}} \mathrm{d}t \\
&= \frac{2}{(k+3)\sqrt{n-1}} \log\left(1+(n-1)t^{k+3}\right)\Big|_0^1 \\
&= \frac{2\log n}{(k+3)\sqrt{n-1}}.
\end{aligned}$$

Thus, even if we sum up over all $k \in [n]$, the contribution from this second integral is a lower order error term. Hence our upper bound on the logarithm of the number of extensions of a k-MOSS is $n^2(I_{k+3} + o(1))$, and therefore we obtain the same enumeration as when extending a $(k+1)$-MOLS. □

Aside from the general lower bound of Keevash [26], we are not aware of any lower bounds on the number of k-MOSS. It would therefore be interesting to find lower bounds on the number of k-MOSS when k grows with n.

Problem 2 How tight are the upper bounds in Corollary 6(b)? That is, for $k = k(n)$ that grows with n, can we show the existence of many distinct k-MOSS?

Acknowledgements Open Access funding provided by Projekt DEAL.

References

1. Bailey R.A., Cameron P.J., Connelly R.: Sudoku, gerechte designs, resolutions, affine space, spreads, reguli, and Hamming codes. Am. Math. Mon. **115**(5), 383–404 (2008).
2. Behrens W.U.: Feldversuchsanordnungen mit verbessertem Ausgleich der Bodenunterschiede. Z. Landwirtsc. Versuchs. Unters. **2**, 176–193 (1956).
3. Berend D.: On the number of Sudoku squares. Discret. Math. **341**(11), 3241–3248 (2018).
4. Boros E., Szőnyi T., Tichler K.: On defining sets for projective planes. Discret. Math. **303**(1–3), 17–31 (2005).
5. Bregman L.: Some properties of nonnegative matrices and their permanents. Sov. Math. Dokl. **14**, 945–949 (1973).
6. Bryant M., Figler J., Garcia R., Mummert C., Singh Y.: The number of mates of Latin squares of sizes 7 and 8. Congr. Numer. **217**, 53–64 (2013).

7. Cavenagh N.J., Wanless, I.M.: Latin squares with no transversals, Electron. J. Comb. **24.2** (2017), Paper 2.45.
8. Chowla S., Erdős P., Straus E.G.: On the maximal number of pairwise orthogonal Latin squares of a given order. Can. J. Math. **12**, 204–208 (1960).
9. Cover T.M., Thomas J.A.: Elements of Information Theory. Wiley, Hoboken (1991).
10. Donovan D.M., Grannell M.J.: On the number of transversal designs. J. Comb. Theory A **120**(7), 1562–1574 (2013).
11. Eberhard S.: More on additive triples of bijections, arXiv:1704.02407 (2017)
12. Eberhard S., Manners F., Mrazović R.: Additive triples of bijections, or the toroidal semiqueens problem. J. Eur. Math. Soc. **21**(2), 441–463 (2019).
13. Egan J., Wanless I.M.: Enumeration of MOLS of small order. Math. Comput. **85**(298), 799–824 (2016).
14. Egorychev G.P.: The solution of Van der Waerden's problem for permanents. Adv. Math. **42**, 299–305 (1981).
15. Falikman D.I.: A proof of van der Waerden's conjecture on the permanent of a doubly stochastic matrix (in Russian). Mat. Zamet. **29**, 931–938 (1981).
16. Ferber A, Kwan M.: Almost all Steiner triple systems are almost resolvable, arXiv:1907.06744 (2019)
17. Glebov R., Luria Z.: On the maximum number of Latin transversals. J. Comb. Theory A **141**, 136–146 (2016).
18. Golomb S.W.: Problem 11214. Am. Math. Mon. **113**(3), 268 (2006).
19. Hedayat A., Federer W.T.: On embedding and enumeration of orthogonal Latin squares. Ann. Math. Stat. **42**(2), 509–516 (1971).
20. Hedayat A.S., Sloane N.J.A., Stufken J.: Orthogonal Arrays: Theory and Applications. Springer Science & Business Media, New York (1999).
21. Kahn J.: On a problem of Erdős and Lovász: random lines in a projective plane. Combinatorica **12**(4), 417–423 (1992).
22. Kantor W.M.: Commutative semifields and symplectic spreads. J. Algebra **270**(1), 96–114 (2003).
23. Kantor W.M., Williams M.E.: Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. Trans. Am. Math. Soc. **356**(3), 895–938 (2004).
24. Keedwell A.D.: On Sudoku squares. Bull. Inst. Comb. Appl. **50**, 52–60 (2007).
25. Keedwell A.D.: Constructions of complete sets of orthogonal diagonal Sudoku squares. Aust. J. Comb. **47**, 227–238 (2010).
26. Keevash P.: Coloured and directed designs, arXiv:1807.05770 (2018).
27. Keevash P.: Counting Steiner triple systems, European Congress of Mathematics (2018), pp. 459–481.
28. Linial N., Luria Z.: An upper bound on the number of Steiner triple systems. Random Struct. Algor. **43**(4), 399–406 (2013).
29. Lorch J.: Mutually orthogonal families of linear Sudoku solutions. J. Aust. Math. Soc. **87**(3), 409–420 (2009).
30. Lorch J.: Orthogonal combings of linear Sudoku solutions. Aust. J. Comb. **47**, 247–264 (2010).
31. Lu M.G.: The maximum number of mutually orthogonal Latin squares. Kexue Tongbao (English Ed.) **30**, 154–159 (1985).
32. Luria Z.: New bounds on the number of n-queens configurations, arXiv:1705.05225 (2017)
33. MacNeish H.: Euler squares. Ann. Math. **23**, 52–60 (1922).
34. McKay B.D., Meynert A., Myrvold W.: Small Latin squares, quasigroups, and loops. J. Comb. Des. **15**(2), 98–119 (2007).
35. Pedersen R.M., Vis T.L.: Sets of mutually orthogonal Sudoku Latin squares. Coll. Math. J. **40**(3), 174–180 (2009).
36. Radhakrishnan J.: An entropy proof of Bregman's theorem. J. Comb. Theory A **77**(1), 161–164 (1997).
37. Rogers K.: A note on orthogonal Latin squares. Pac. J. Math. **14**, 1395–1397 (1964).
38. Ryser H.J.: Permanents and systems of distinct representatives, Combinatorial Mathematics and Its Applications. In: Proceeding of the Conference, University North Carolina, Chapel Hill, NC **1969**, 55–68 (1967).
39. Taranenko A.A.: Multidimensional permanents and an upper bound on the number of transversals in Latin squares. J. Comb. Des. **23**(7), 305–320 (2015).
40. Van Lint J.H.: A Course in Combinatorics. Cambridge University Press, Cambridge (2001).
41. Van Rees G.H.J.: Subsquares and transversals in Latin squares, Ars Combinatoria **29 B** (1990), 193–204, Twelfth British Combinatorial Conference (1989)

42. Wanless I.M., Webb B.S.: The existence of Latin squares without orthogonal mates. Des. Code Cryptogr. **40**(1), 131–135 (2006).
43. Wilson R.M.: Concerning the number of mutually orthogonal Latin squares. Discret. Math. **9**, 181–198 (1974).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.