Discrete Applied Mathematics 158 (2010) 136–146

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

On the number of transversals in Cayley tables of cyclic groups

Nicholas J. Cavenagh [a,b], Ian M. Wanless [a,*]

[a] School of Mathematical Sciences, Monash University, Vic 3800, Australia

[b] Department of Mathematics, University of Waikato, Private Bag 3105, Hamilton, New Zealand

ARTICLE INFO

Article history:
Received 31 December 2008
Received in revised form 18 August 2009
Accepted 2 September 2009
Available online 29 September 2009

Keywords:
Latin square
Transversal
Diagonally cyclic
Complete mapping
Orthomorphism
Semi-queen
Homogeneous latin bitrade
Random MOLS
Magic juggling sequence

ABSTRACT

It is well known that if n is even, the addition table for the integers modulo n (which we denote by B_n) possesses no transversals. We show that if n is odd, then the number of transversals in B_n is at least exponential in n. Equivalently, for odd n, the number of diagonally cyclic latin squares of order n, the number of complete mappings or orthomorphisms of the cyclic group of order n, the number of magic juggling sequences of period n and the number of placements of n non-attacking semi-queens on an $n \times n$ toroidal chessboard are at least exponential in n. For all large n we show that there is a latin square of order n with at least $(3.246)^n$ transversals.

We diagnose all possible sizes for the intersection of two transversals in B_n and use this result to complete the spectrum of possible sizes of homogeneous latin bitrades.

We also briefly explore potential applications of our results in constructing random mutually orthogonal latin squares.

1. Introduction

Given an $n \times n$ array of symbols, a *transversal* of the array is a selection of n entries such that exactly one entry is chosen from each row and each column and no symbol is chosen more than once. The arrays of most interest in this paper are *latin squares*. A latin square of order n is an $n \times n$ array of symbols such that each cell contains one symbol and each symbol occurs once in each row and once in each column. In this paper, rows, columns and symbols are indexed by the set $N = \{0, 1, \ldots, n-1\}$ and all calculations of indices are performed modulo n. We often consider a latin square as a set of ordered (row, column, symbol) triples; in other words, a subset of $N \times N \times N$. A *partial latin square* is a partially filled-in $n \times n$ array of symbols such that each cell contains at *most* one symbol and each symbol occurs at most once in each row and at most once in each column. Two partial latin squares are said to be *isotopic* if one can be obtained from the other by relabelling rows, columns and/or symbols. The *transpose* of a partial latin square is obtained by interchanging rows with columns. Combinatorial properties of partial latin squares are, in general, invariant under isotopy and transpose, a fact we use in this paper.

In this work we are chiefly interested in transversals in the specific latin square B_n, which is the addition table for the integers modulo n. Such transversals are equivalent, under easy bijections, to a number of other combinatorial objects including:

- diagonally cyclic latin squares of order n. A latin square L is said to be *diagonally cyclic* if $(i, j, k) \in L \iff (i+1, j+1, k+1) \in L$.
- *complete mappings* of the cyclic group of order n.

* Corresponding author.
E-mail addresses: nicholas.cavenagh@sci.monash.edu.au (N.J. Cavenagh), ian.wanless@sci.monash.edu.au, imw@cs.anu.edu.au (I.M. Wanless).

0166-218X/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2009.09.006

- *orthomorphisms* of the cyclic group of order n.
- *magic juggling sequences* of period n, as defined in [26, p.35].
- placements of n non-attacking semi-queens on a $n \times n$ toroidal chessboard. (A semi-queen attacks any piece in its row and column, or on the same *ascending* diagonal; i.e. the diagonal which begins in the lower left and finishes in the upper right. On a toroidal chessboard these diagonals "wrap around" in the obvious fashion).

For more details on the bijections, see for example [11] or [34], and for a recent survey on transversals see [35].

Let t_n denote the number of transversals in B_n. It is well known that $t_n = 0$ when n is even (see [14] or [34] for a concise proof). For odd n, Vardi [33] posed the following conjecture:

Conjecture 1 (*Vardi*). *There exist two real constants c_1 and c_2 such that*

$$c_1^n n! \leqslant t_n \leqslant c_2^n n!$$

where $0 < c_1 < c_2 < 1$ and $n \geqslant 3$ is odd.

The upper bound of this conjecture has been verified [13,17,22]. The current best result is by McKay, et al. [22] who showed that $t_n = o(0.614^n n!)$. However, the lower bound remains an open problem. In [22], non-cyclic latin squares which contain exponentially many transversals are constructed for each n. We improve on that result in Theorem 2. Statistical estimates for the growth rate of t_n have been found by Cooper et al. [12] and Kuznetsov [18–20]. Certain congruences satisfied by t_n can be found in [32] and results on enumerating *partial* transversals of B_n are given in [31].

An exponential lower bound for t_n has been found in special cases [27], such as when n is prime but $(n-1)/2$ is not prime, or when n is divisible by a prime congruent to 1 (mod 4). However the results in this paper apply for all odd n and give stronger bounds than [27] (although in fairness to the authors of [27], they were solving a different problem that happens to imply bounds on t_n).

Our first major result is:

Theorem 1. *If n is a sufficiently large odd integer then $t_n > (3.246)^n$ and B_n has at least $(3.246)^n$ orthogonal mates.*

We do not count orthogonal mates as different if they differ only by a symbol permutation. The numbers of orthogonal mates for B_n is sequence A091261 in [29]. These numbers were computed for $n \leqslant 11$ in [21] and almost certainly grow faster than exponentially, but a lower bound does not appear to have been given before now.

The lower bound for t_n in Theorem 1 is weaker than the bound conjectured by Vardi. However, it is the first exponential lower bound for t_n that applies for general odd n. With the aid of Theorem 1 we are able to show a result that holds for even orders as well.

Theorem 2. *If n is a sufficiently large integer then there exists a latin square of order n that has at least $(3.246)^n$ transversals.*

The constructions leading to Theorem 1 have several immediate applications. In Section 4 we use them to determine all possible sizes of the intersection between two transversals in B_n. In Section 5 we will then use that result to prove the following theorem, whose meaning is explained in Section 5:

Theorem 3. *For all $k \geqslant 3$, a k-homogeneous latin bitrade of size s exists if and only if k divides s and $s \geqslant k^2$.*

We give a number of constructions in this paper but all are variants of the same basic idea. We consider blocks centered on the main diagonal of B_n. In each block we choose a transversal which uses a particular set of symbols, ensuring that we obtain a transversal of B_n from the union of the transversals of the blocks. In most cases the transversals that we use in each block can be chosen independently and this allows us to obtain exponential lower bounds on t_n.

In almost all cases our bounds could be improved by a linear factor by "shifting" our blocks sideways. In other words, by considering blocks centered on diagonals parallel to the main diagonal and showing that different choices of diagonal give rise to disjoint sets of transversals. A more careful analysis, allowing the blocks to "slide down" the diagonals as well, might even yield a quadratic improvement. However, we have chosen not to bother about polynomial factors, since it is clear that t_n grows fast enough to make them insignificant.

2. Our first construction

We begin with a simple construction, yielding an exponential lower bound for t_n. We then examine two different ways of generalizing the basic result, in the process obtaining slightly better lower bounds for t_n. In this section n is always odd and rows, columns and symbols are each evaluated modulo n. The $j \times j$ block of B_n at the intersection of the rows and columns with indices $i, i+1, \ldots, i+j-1$, is denoted by $M_{i,j}$.

Lemma 1. *Let $n \equiv 3 \pmod 6$ and $n \geqslant 3$. Then there are at least $2^{n/3}$ transversals in B_n.*

Proof. Consider blocks of the form $M_{3i,3}$, where $0 \leqslant i < n/3$. Within each such block, we choose a transversal on symbol set $S(i) = \{6i+1, 6i+2, 6i+3\}$. Since, $\cup_i S(i) = N$, any such choice yields a transversal in B_n. Moreover, for each M_i, there are two such choices, so there are at least $2^{n/3}$ transversals in B_n. □

In practice it is easy to do much better than the previous lemma. If $n = pq$ for odd $p, q > 1$ then the latin square B_n can be partitioned into latin subsquares of order p (or, similarly, for order q). These subsquares can be used to show that $t_n \geqslant \max\big((t_p)^q t_q, (t_q)^p t_p\big)$. So if 3 divides n, we have immediately that $t_n \geqslant 3^{n/3} t_{n/3} \geqslant 3^{n/3}$, as $t_3 = 3$. We included the previous lemma to accompany the following two lemmas, which are not so easily beaten. For example, they apply for infinitely many prime orders where B_n has no non-trivial latin subsquares.

Lemma 2. *Let $n \equiv 1 \pmod 6$. Then there are at least $2^{(n-4)/3}$ transversals in B_n.*

Proof. The result is trivial for $n = 1$ so assume $n \geqslant 7$. For $0 \leqslant i \leqslant (n-13)/6$, consider transversals in blocks $M_{3i,3}$ and $M_{(n+3)/2+3i,3}$, on symbol sets $\{6i+1, 6i+2, 6i+3\}$ and $\{6i+4, 6i+5, 6i+6\}$, respectively. There are two choices for each such transversal. It remains to use symbols from the set

$$\{n-6, n-5, n-4, n-3, n-2, n-1, 0\}.$$

In block $M_{(n-7)/2,5}$ we choose one of 2 transversals on symbol set $\{n-6, n-5, n-3, n-1, 0\}$. Finally, in block $M_{n-2,2}$ we choose the transversal on symbol set $\{n-4, n-2\}$. All together, we have $2^{(n-4)/3}$ choices for transversals of the entire latin square. □

As an example of the previous lemma, the boxed entries in (1) show a transversal for $n = 13$. The 3×3 blocks ($M_{0,3}$ and $M_{(n+3)/2,3}$) are lightly shaded, while the two special blocks ($M_{(n-7)/2,5}$ and $M_{n-2,2}$) are shown with darker shading.

0	[1]	2	3	4	5	6	7	8	9	10	11	12
1	2	[3]	4	5	6	7	8	9	10	11	12	0
[2]	3	4	5	6	7	8	9	10	11	12	0	1
3	4	5	6	[7]	8	9	10	11	12	0	1	2
4	5	6	7	8	9	[10]	11	12	0	1	2	3
5	6	7	[8]	9	10	11	12	0	1	2	3	4
6	7	8	9	10	11	12	[0]	1	2	3	4	5
7	8	9	10	11	[12]	0	1	2	3	4	5	6
8	9	10	11	12	0	1	2	3	[4]	5	6	7
9	10	11	12	0	1	2	3	4	5	[6]	7	8
10	11	12	0	1	2	3	4	[5]	6	7	8	9
11	12	0	1	2	3	4	5	6	7	8	[9]	10
12	0	1	2	3	4	5	6	7	8	9	10	[11]

(1)

Lemma 3. *Let $n \equiv 5 \pmod 6$. Then there are at least $2^{(n-2)/3}$ transversals in B_n.*

Proof. The construction is very similar to Lemma 2. For $0 \leqslant i \leqslant (n-11)/6$, consider transversals in blocks $M_{3i,3}$ and $M_{(n+3)/2+3i,3}$, on symbol sets $\{6i+1, 6i+2, 6i+3\}$ and $\{6i+4, 6i+5, 6i+6\}$, respectively. There are two choices for each such transversal. It remains to use symbols from the set $\{n-4, n-3, n-2, n-1, 0\}$.

In block $M_{(n-5)/2,4}$ we choose one of 2 transversals on symbol set $\{n-4, n-3, n-1, 0\}$. Finally, in block $M_{n-1,1}$ we choose the trivial transversal which uses symbol $n-2$. In total, we have $2^{(n-2)/3}$ choices for transversals of B_n. □

Next we consider a generalisation of the above constructions. The following theorem allows the blocks of size 3 in the lemmas above to be combined into two larger blocks, in the upper left-hand and lower right-hand quadrants of B_n. We do not choose the transversals from these large blocks independently. However, it turns out there is a recursive formula for the number of such transversals.

Theorem 4. *Suppose $m \geqslant 0$. Within B_{2m+5}, let $f(m)$ be the number of ways of choosing a transversal from block $M_{0,m}$ and another transversal from $M_{m+4,m}$, while overall using each symbol from the set $\{1, 2, \ldots, 2m\}$ exactly once. Then $f(0) = 1$, $f(1) = f(2) = 0$ and for $m \geqslant 3$, $f(m)$ satisfies the recurrence relation:*

$$f(m) = f(m-1) + 4\sum_{i=0}^{m-3} f(i). \tag{2}$$

Proof. By observation, $f(0) = 1$ (the empty set is the only suitable transversal) and $f(1) = f(2) = 0$. Henceforth we assume that $m \geqslant 3$. Let T be one of the transversals enumerated by $f(m)$. Symbols 0 and $2m+1$ are excluded, so neither $(0, 0, 0) \in T$ nor $(2m+3, 2m+3, 2m+1) \in T$.

There are precisely two choices for symbol 1: either $(0, 1, 1) \in T$ or $(1, 0, 1) \in T$, implying $(2, 0, 2) \in T$ or $(0, 2, 2) \in T$, respectively. Similarly, there are precisely two choices for symbol $2m$: either $(2m+2, 2m+3, 2m) \in T$ or $(2m+3, 2m+2, 2m) \in T$, implying $(2m+3, 2m+1, 2m-1) \in T$ or $(2m+1, 2m+3, 2m-1) \in T$, respectively.

Let $g(m)$ be the number of transversals T satisfying the same conditions as those counted by $f(m)$, but in addition we specify that: $(0, 1, 1), (2, 0, 2), (2m+2, 2m+3, 2m), (2m+3, 2m+1, 2m-1) \in T$. Then, by the symmetry of interchanging rows with columns, $f(m) = 4g(m)$. For the remainder of this proof T denotes one of the transversals counted by $g(m)$. Let

$$\begin{aligned} P(k) = {} & \big\{(0, 1, 1)\big\} \cup \big\{(2 + 2i, 0 + 2i, 2 + 4i) : 0 \leqslant i \leqslant \lceil k/2 \rceil - 1\big\} \\ & \cup \big\{(1 + 2i, 3 + 2i, 4 + 4i) : 0 \leqslant i \leqslant \lfloor k/2 \rfloor - 1\big\} \\ & \cup \big\{(i, i, 2i - (2m + 5)) : m + 4 \leqslant i \leqslant m + 3 + k\big\} \\ & \cup \big\{(2m + 1, 2m + 2, 2m - 2), (2m + 2, 2m + 3, 2m), (2m + 3, 2m + 1, 2m - 1)\big\}. \end{aligned}$$

For $0 \leqslant k \leqslant m-3$ we will show by induction that if $P(k) \not\subseteq T$ then there are $g(m-1)+f(m-3)+f(m-4)+\cdots+f(m-k-2)$ distinct choices for T.

Suppose $P(0) \not\subseteq T$. Then $(2m + 1, 2m + 2, 2m - 2) \notin T$ so $(m - 1, m - 1, 2m - 2) \in T$ and then the only way to include symbol $2m - 3$ is if $(2m, 2m + 2, 2m - 3) \in T$. We claim that the number of remaining choices is equal to $g(m - 1)$. To see this, observe that it remains to place symbols $3, 4, \ldots, 2m - 4$ in the blocks $M_{0,m-1}$ and $M_{m+4,m-1}$, where $(0, 1, 1), (2, 0, 2)$ and $(2m, 2m + 2, 2m - 3) \in T$, and row $2m + 2$ and column $2m + 1$ are excluded. Since $M_{m+4,m-1}$ is symmetric, we could equally assume that $(2m+2, 2m, 2m-3) \in T$ and that row $2m+1$ and column $2m+2$ are excluded. Now, block $M_{0,m-1}$ in B_{2m+5} is equal to block $M_{0,m-1}$ in B_{2m+3}. Also, block $M_{m+4,m-1}$ in B_{2m+5} is equivalent to the block $M_{m+3,m-1}$ in B_{2m+3} under the map $(i, j, k) \to (i - 1, j - 1, k)$. So, working in B_{2m+3} rather than B_{2m+5}, we have that $(2m + 1, 2m - 1, 2m - 3) \in T$ and that row $2m$ and column $2m + 1$ are excluded. The number of ways to complete T then is exactly $g(m - 1)$. This proves our claim, and thus also the base case of the induction.

To show the inductive step, we now count the choices of T for which $P(k) \subseteq T$ but $P(k + 1) \not\subseteq T$.

If k is even (respectively, odd), the only choice for symbol $2k + 2$ is cell $(k + 2, k)$ (respectively, $(k, k + 2)$). Now $(m + 4 + k, m + 4 + k, 2k + 3) \notin T$ since $P(k + 1) \not\subseteq T$, so the only choice for symbol $2k + 3$ is cell $(k + 1, k + 2)$, for k even, or $(k + 2, k + 1)$, for k odd. The remaining elements of T must come from cells

$$\{k + 3, k + 4, \ldots, m - 1\} \times \{k + 3, k + 4, \ldots, m - 1\}$$

and

$$\{m + k + 4, m + k + 5, \ldots, 2m\} \times \{m + k + 4, m + k + 5, \ldots, 2m\}.$$

Thus, by isotopism, the number of ways of choosing the remaining elements of T is $f(m - k - 3)$.

Employing induction, we see that there are $g(m - 1) + f(m - 3) + f(m - 4) + \cdots + f(1)$ distinct choices of T for which $P(m - 3) \not\subseteq T$. There is a unique choice of T for which $P(m - 3) \subseteq T$: if m is even $T = P(m - 3) \cup \{(m - 3, m - 1, 2m - 4), (m - 1, m - 2, 2m - 3)\}$, while if m is odd $T = P(m - 3) \cup \{(m - 1, m - 3, 2m - 4), (m - 2, m - 1, 2m - 3)\}$.

Since $f(0) = 1$ and $f(m) = 4g(m)$, the recurrence relation (2) follows. □

Next, we analyse the recurrence relation (2) to obtain a better lower bound for t_n.

Corollary 1. *Let* $w = (181 + 24\sqrt{78})^{1/3}$ *and* $c = 12w/(w^2 + w - 23)$. *Then*

$$f(n) = \frac{2 + o(1)}{c^2 - c + 6} c^n \approx 0.221 \times (2.31)^n. \tag{3}$$

In particular, $t_n \geqslant 2f\left(\frac{1}{2}(n - 5)\right) \geqslant \big(0.0542 + o(1)\big) \times (1.52)^n$ *for* $n \geqslant 5$.

Proof. It is a standard exercise in generating functions to solve the recurrence (2). Let $F(x) = \sum_{m \geqslant 0} f(m)x^m$. Then (2) implies that

$$F(x) - 1 = x\big(F(x) - 1\big) + \frac{4x^3 F(x)}{1 - x}$$

and hence $F(x) = (1 - x)^2/(1 - 2x + x^2 - 4x^3)$. Now c is the reciprocal of the real root of $1 - 2x + x^2 - 4x^3$. Applying standard methods (e.g. Theorem 9.2 of [25] or Theorem 4 of [5]) to $F(x)$ gives (3).

To obtain the lower bound for t_n observe that $f(m)$ is the number of transversals in B_{2m+5} within blocks $M_{0,m}, M_{m,4}, M_{m+4,m}$ and $M_{2m+4,1}$, such that $M_{m,4}$ and $M_{2m+4,1}$ contain transversals on the symbol set $\{2m+1, 2m+2, 2m+3, 2m+4, 0\}$. There is only one cell in $M_{2m+4,1}$ and two choices for the transversal in $M_{m,4}$, as in Lemma 3. This shows that B_{2m+5} has at least $2f(m)$ transversals. In other words,

$$t_n \geqslant 2f\left(\frac{1}{2}(n - 5)\right) = \frac{4 + o(1)}{c^2 - c + 6} c^{(n-5)/2} \geqslant \big(0.0542 + o(1)\big) \times (1.52)^n$$

for $n \geqslant 5$. □

Table 1
Transversals of standard blocks.

b	β_b	$(\beta_b)^{1/b}$
3	2	1.259
5	6	1.430
7	28	1.609
9	244	1.841
11	2544	2.039
13	35600	2.239
15	659632	2.443
17	15106128	2.644
19	425802176	2.845
21	14409526080	3.046
23	577386122880	3.246

3. A more general construction

In this section we give a more general construction which produces a better lower bound on t_n. The disadvantage is that we will be forced to rely on computational evidence whereas the constructions in Section 2 can be analysed entirely by hand. Nevertheless, the idea is similar.

As in previous constructions, we look for certain transversals that lie within blocks placed down the main diagonal. Most of these blocks will be of order $b \leqslant n-2$, but because we cannot rely on b dividing n, we use two blocks R and S of other sizes. We refer to the blocks other than R and S as *standard blocks*. The construction used in Lemmas 1–3 is the case $b = 3$. In (1) the standard blocks are lightly shaded while R and S are the darker shade.

Let $M_{i,j}$ be as defined in the previous section. For a standard block we have $j = b$, which we choose to be odd. In a standard block $M_{i,b}$ we use the symbols $2i + \frac{1}{2}(b-1), \ldots, 2i + \frac{3}{2}(b-1)$ in our transversal. In other words, we choose a set of consecutive symbols that is symmetric about $2i + b - 1$, the symbol in the middle cell of $M_{i,b}$. The number of ways of choosing a transversal of $M_{i,b}$ that contains the desired symbols is independent of i. We denote it by β_b. The first few values of β_b are given in Table 1, together with the first 4 digits of the decimal expansion of $(\beta_b)^{1/b}$, which will be relevant in subsequent calculations. Note that by rounding down we have given a lower bound on $(\beta_b)^{1/b}$ in each case.

A useful check of program correctness is that β_b forms sequence A002047 in Sloane's encyclopedia [29], which had previously been computed by other people for $s \leqslant 19$. In [3], A002047 is the number of $3 \times b$ zero-sum arrays, defined as follows. Let $b = 2c + 1$. A $3 \times b$ *zero-sum array* is one in which each row is a permutation of $-c, -c+1, \ldots, c-1, c$ and each column adds to zero. There is an easy bijection between such arrays and our transversals. We simply identify the array $A = [a_{ij}]$ with the transversal $\{(c + a_{1j}, c + a_{2j}, 2c - a_{3j}) : j = 1, \ldots, b\}$ of $M_{0,b}$.

Returning to our construction, we take $k = \lfloor \frac{n-b}{2b} \rfloor$, $s = \frac{1}{2}(n - b - 2bk)$ and $r = s + b$. This means that $n = 2kb + r + s$ and we can take $2k$ standard blocks, together with $R = M_{kb,r}$ and $S = M_{n-s,s}$ to make up the blocks for our transversal T. That is, T is a union of transversals of the stated blocks.

The standard blocks we use are $M_{ib,b}$ and $M_{(k+i)b+r,b}$ for $i = 0, \ldots, k-1$. Between them they will contribute the symbols $\frac{1}{2}(b-1), \frac{1}{2}(b-1)+1, \ldots, 2kb + \frac{1}{2}(b-3)$ to T. Therefore, in $R \cup S$ we need to select the symbols

$$\Omega = \left\{0, 1, \ldots, \frac{1}{2}(b-3)\right\} \cup \left\{2kb + \frac{1}{2}(b-1), \ldots, n-1\right\}.$$

Note that every symbol that occurs in S is also in Ω (in general, R does not have this property). This facilitates the following algorithm for calculating the number $\gamma_{s,b}$ of transversals of $R \cup S$ that use the symbols in Ω.

(0) Initialise $\gamma_{s,b}$ to zero.
(1) Find all transversals of S and categorising them into *types* according to which symbols they use.
(2) For each type from (1), we see how many transversals of R use the remaining symbols from Ω.
(3) Multiply the number of transversals of a given type (from (1)) by the number of ways to complete each such transversal (from (2)) and add this to $\gamma_{s,b}$.

Step (1) is independent of b, so it need only be performed once for each value of s. The number of transversals of S and the number of different types that they fall into, is given in Table 2 for $s \leqslant 18$. The last column shows the maximum number of transversals that there are in a type. The corresponding minimum is 1, since in all cases the transversal formed by the main diagonal of S is in a type on its own.

A useful check of program correctness is that the numbers in the second column of Table 2 form sequence A099152 in Sloane's encyclopedia [29], which had previously been computed by other people for $s \leqslant 13$.

Next we give, in Table 3, the values of $\gamma_{s,b}$ calculated by the above algorithm for small values of s and b. Question marks in the table denote that the value was not computed exactly. However, for all $s < b \leqslant 15$ we did at least a partial computation to locate some transversals. The lower bound on $\gamma_{s,b}$ thereby obtained was sufficient for our next calculation to be performed.

For any given n we can form transversals of B_n by taking a suitable transversal of $R \cup S$ in $\gamma_{s,b}$ ways, together with independently chosen transversals of the standard blocks, each of which has β_b options. For each s, b this gives a lower

Table 2
Transversals of S.

s	Transversals of S	Types	Largest type
1	1	1	1
2	1	1	1
3	3	2	2
4	7	4	2
5	23	9	6
6	83	22	8
7	405	59	28
8	2113	167	48
9	12657	490	244
10	82297	1486	476
11	596483	4639	2544
12	4698655	14805	5952
13	40071743	48107	35600
14	367854835	158808	94456
15	3622508685	531469	659632
16	38027715185	1799659	1984176
17	424060091065	6157068	15106128
18	5006620130753	21258104	51493696

Table 3
Values of $\gamma_{s,b}$ for some $s < b \leqslant 15$.

s	b						
	3	5	7	9	11	13	15
1	2	6	44	396	4568	73544	1493440
2	2	14	100	852	11272	193240	4228944
3		62	452	4948	71800	1357000	32368208
4		206	2452	32956	531208	10758584	270818864
5			14860	251836	4758168	108243880	2968949584
6			94028	2166924	52310968	1390993352	42462117232
7				22500132	686097704	21764575960	758409431888
8				233196484	9290502504	364185909592	?
9					132763306520	6488289379176	?
10					1922269430872	?	?

Table 4
Lower bounds on t_n for different block sizes.

b	Lower bound on t_n
3	$0.398(1.259)^n$
5	$0.490(1.430)^n$
7	$0.534(1.609)^n$
9	$0.305(1.841)^n$
11	$0.257(2.039)^n$
13	$0.216(2.239)^n$
15	$0.180(2.443)^n$

bound on t_n. The bound is of the form $c(\beta_b)^{n/b}$ where $c = \gamma_{s,b}/\beta_b^{1+2s/b}$ depends only on s and b. Thus the bound grows exponentially in n, with base constant $\beta_b^{1/b}$ as given in Table 1. Taking the worst bound over the different choices of s, we get the lower bounds given in Table 4, which apply for all odd $n \neq 5$. (Our method only shows the bounds hold for odd $n \geqslant b+2$, but we can use the known values of t_n (from, e.g. [22]) to show that the bounds also hold for smaller orders, with the single exception that t_5 does not obey the bound derived from $b = 15$.)

It seems likely that choosing larger and larger block sizes will continue to improve the lower bound derived in this way, but at present we have no method to prove this.

Proof of Theorems 1 and 2. Suppose n is an odd integer. Let $b = 23$ and define k, r, s, R, S as above. Counting only transversals of B_n within R, S and the standard blocks, we find that $t_n \geqslant c(\beta_b^{1/b})^n$, where $\beta_b^{1/b} > 3.246$. We choose n sufficiently large that $c(\beta_b^{1/b})^n > n(3.246)^n$. Now in the Cayley table of any group every entry is contained in the same number of transversals, so B_n has at least $(3.246)^n$ transversals through each entry. For every transversal T that includes the entry $(0, 0, 0)$ there is a corresponding latin square

$$\{(i, j+k, k) : (i, j, i+j) \in T,\ k \in N\}$$

(with calculations modulo n) that is orthogonal to B_n. Different latin squares arise from different choices of T, but all of them have their first row in natural order. Theorem 1 follows.

To prove Theorem 2, define $P = [p_{ij}]$, a latin square indexed by $\mathbb{Z}_n \cup \{\infty\}$, by

$$p_{ij} = \begin{cases} i+j & \text{if } i,j \in \mathbb{Z}_n \text{ and } j \not\equiv i+r, \\ \infty & \text{if } i,j \in \mathbb{Z}_n \text{ and } j \equiv i+r, \\ 2i+r & \text{if } i \in \mathbb{Z}_n;\ j = \infty, \\ 2j-r & \text{if } i = \infty; j \in \mathbb{Z}_n, \\ \infty & i = j = \infty, \end{cases}$$

where r is the order of block R as defined earlier in this section. Then P is what is known as a *prolongation* of B_n, along a transversal that is disjoint from all the blocks used in bounding t_n. Hence every transversal of B_n through those blocks extends to a transversal of P by simply adjoining the entry (∞, ∞, ∞). It follows that P has at least $n(3.246)^n > (3.246)^{n+1}$ transversals, proving Theorem 2. □

4. Intersection of transversals in B_n

In this section, we examine the possible sizes of intersections of pairs of transversals in B_n. This is trivial for n even, so henceforth in this section we assume that n is odd. Rows, columns and symbols are always evaluated modulo n. Let $I(n)$ be the set of integers t for which there exist transversals T and T' in B_n such that $|T \cap T'| = t$. The main result of this section is the following.

Theorem 5. *For each odd $n \neq 5$, $I(n) = \{t : 0 \leqslant t \leqslant n-3\} \cup \{n\}$, while $I(5) = \{0, 1, 5\}$.*

It is not hard to see that it is impossible for two transversals from any $n \times n$ latin square to intersect in precisely $n-1$ or precisely $n-2$ elements. To see that $0 \in I(n)$ for $n \geqslant 3$, take any transversal $T \in B_n$, and construct a second transversal $T' = \{(r, c+1, r+c+1) : (r, c, r+c) \in T\}$, which avoids T.

The next lemma verifies that $1 \in I(n)$ for $n \geqslant 5$.

Lemma 4. *For odd $n \geqslant 5$ there exist two transversals T and T' in B_n such that $T \cap T' = \{(0, 0, 0)\}$.*

Proof. First suppose that n is not divisible by 3. Then let T be the transversal in B_n defined by $T = \{(x, -2x, -x) : 0 \leqslant x \leqslant n-1\}$ and let T' be the transpose of T. As n is not divisible by 3, the unique solution to $x \equiv -2x \bmod n$ is $x = 0$, so T and T' intersect only at $(0, 0, 0)$.

Otherwise suppose that n is divisible by 3 and $n > 3$. For each i such that $0 \leqslant i \leqslant n/3 - 2$, within B_n choose a transversal P_i using symbols $\{2+3i, 3+3i, 4+3i\}$ in the intersection of rows $\{n-5-3i, n-4-3i, n-3-3i\}$ with columns $\{6+6i, 7+6i, 8+6i\}$. There are two choices for each P_i, and at least one of these choices will avoid any cells where the row and column are equal. Thus it is possible to define transversals

$$T = \{(0, 0, 0), (n-2, 1, n-1), (n-1, 2, 1)\} \cup \bigcup_{i=0}^{n/3-2} P_i$$

and T' the transpose of T, so that $T \cap T' = \{(0, 0, 0)\}$. □

Having dealt with intersections of size 0 or 1 we now pursue a proof of Theorem 5 using the transversals identified in Section 3 in the case when $b = 7$. Consider the following four transversals of $M_{0,7}$:

$$T_1 = [3, 6, 4, 9, 8, 5, 7], \qquad T_3 = [3, 7, 6, 4, 9, 5, 8],$$
$$T_2 = [3, 6, 8, 5, 4, 9, 7], \qquad T_4 = [5, 3, 8, 6, 4, 9, 7],$$

where we have specified the transversals simply by listing the symbols to be chosen from each row in turn. Then $|T_1 \cap T_1| = 7$, $|T_1 \cap T_2| = 3$, $|T_1 \cap T_3| = 2$, $|T_2 \cap T_3| = 1$, $|T_2 \cap T_4| = 4$, and $|T_3 \cap T_4| = 0$. Hence, transversals of a standard block of order 7 have $\{0, 1, 2, 3, 4, 7\}$ as their set of possible intersection sizes. By taking T and T' to be transversals of B_n that agree in blocks R and S, it is therefore easy to arrange for $|T \cap T'|$ to take any value in $\{r+s, r+s+1, \ldots, n-3, n\}$.

To achieve intersections smaller than $r+s$ we need to allow T and T' to differ in R and/or S, and this requires treating the possible values of s as different cases. For $s \in \{0, 1, 2\}$ we are forced to have $|T \cap T' \cap S| = s$ as there is only one choice for the transversal of S. However, $|T \cap T' \cap R|$ can achieve any value in $\{0, 1, \ldots, r-3, r\}$. When $s = 0$ this follows from the fact that R is, in effect, a standard block. For $s \in \{1, 2\}$ we now give transversals $R_{s,i}$ that between them achieve all the required intersections. Again we specify transversals by listing the symbols that are chosen, row by row.

$$R_{1,1} = [-5, -1, -4, -6, 1, -3, 2, 0],$$
$$R_{1,2} = [-6, -4, -1, 1, -5, -3, 2, 0],$$
$$R_{1,3} = [-6, -4, -1, -5, 2, 1, -3, 0],$$
$$R_{1,4} = [-6, -4, -5, 0, 2, 1, -3, -1]$$

$$R_{2,1} = [-8, -3, -1, -6, -7, -5, 0, 2, 1],$$
$$R_{2,2} = [-7, -8, -6, -1, 1, -5, 0, 2, -3],$$
$$R_{2,3} = [-8, -6, -7, -1, 1, -5, 0, 2, -3],$$
$$R_{2,4} = [-8, -6, -7, -1, 1, 0, -5, -3, 2],$$
$$R_{2,5} = [-8, -6, -7, 0, -1, 1, -5, -3, 2].$$

For $s \in \{3, 4, 5, 6\}$ we now present transversals $R_{s,i}$ of R that between them achieve intersections of all sizes in $\{0, 1, 2, \ldots, r-3, r\}$. We also give a transversal S_s of S that is disjoint from its transpose and uses the symbols in Ω that do not occur in $R_{s,i}$. This offers the possibility of choosing $|T \cap T' \cap S|$ to be either 0 or s. From the options we have presented it is now easy to construct transversals T and T' that prove Theorem 5.

$R_{3,1} = [-9, -10, -8, -2, 0, -7, -1, -6, 2, 1]$,
$R_{3,2} = [-10, -8, -9, -1, -2, -7, 1, -6, 0, 2]$,
$R_{3,3} = [-10, -7, -9, -1, -2, -8, -6, 2, 1, 0]$,
$R_{3,4} = [-10, -8, -2, -9, -7, 0, -1, -6, 2, 1]$,
$R_{3,5} = [-10, -8, -9, -2, 0, -7, -1, -6, 2, 1]$.
$S_3 = [-5, -3, -4]$

$R_{4,1} = [-12, -9, -5, -10, -11, -1, -8, 2, 0, -2, 1]$,
$R_{4,2} = [-11, -12, -10, -5, -2, -9, 1, -8, -1, 2, 0]$,
$R_{4,3} = [-12, -10, -11, -5, -2, -9, 1, -8, -1, 2, 0]$,
$R_{4,4} = [-12, -10, -11, -5, -1, -9, 0, -8, -2, 2, 1]$,
$R_{4,5} = [-12, -10, -11, -2, -5, -9, -1, -8, 2, 1, 0]$.
$S_4 = [-6, -7, -3, -4]$

$R_{5,1} = [-14, -10, -13, -9, -12, -3, -11, 0, 2, -1, 1, -2]$,
$R_{5,2} = [-14, -12, -13, -9, -3, -11, 0, -10, -2, 1, -1, 2]$,
$R_{5,3} = [-13, -9, -14, -12, -10, -3, -11, 0, 2, -2, 1, -1]$,
$R_{5,4} = [-14, -12, -13, -9, -3, -11, -2, -10, 2, -1, 1, 0]$,
$R_{5,5} = [-14, -12, -13, -9, -3, -11, -2, -10, 2, 0, -1, 1]$.
$S_5 = [-8, -6, -4, -7, -5]$

$R_{6,1} = [-16, -14, -12, -15, -13, -7, -3, 0, -11, 1, -1, -2, 2]$,
$R_{6,2} = [-16, -14, -15, -11, -7, -13, -1, -12, 0, -3, 1, -2, 2]$,
$R_{6,3} = [-16, -14, -12, -15, -13, -7, -2, 0, -11, -1, -3, 2, 1]$,
$R_{6,4} = [-16, -14, -15, -11, -7, -13, -2, -12, -1, 2, -3, 1, 0]$,
$R_{6,5} = [-16, -14, -15, -11, -7, -13, -3, -12, 0, 2, -2, 1, -1]$,
$R_{6,6} = [-15, -16, -14, -11, -7, -13, -3, -12, 0, 2, -2, 1, -1]$.
$S_6 = [-10, -6, -9, -5, -8, -4]$.

5. Homogeneous latin bitrades

The results from the previous section allow us to solve an open problem on homogeneous latin bitrades. A *latin bitrade* is a pair (Q, Q') of non-empty, disjoint partial latin squares such that Q and Q' have the same set of occupied cells, and each row (respectively column) of Q contains the same set of symbols as the corresponding row (resp. column) of Q'. We sometimes refer to Q as a *latin trade* and Q' as its *disjoint mate*. The *size* or *volume* of a latin bitrade is the number of filled-in cells in Q or Q'. Given two latin squares L and L' of the same order, it is not hard to show that $(L \setminus L', L' \setminus L)$ is a latin bitrade. A recent survey on latin bitrades may be found in [6].

A latin bitrade is said to be k-homogeneous if each row and each column contains 0 or k symbols and each symbol appears either 0 or k times. A number of papers [2,4,7,8] have explored the spectrum of possible sizes for k-homogeneous latin bitrades. Trivially, 2-homogeneous latin bitrades have volume divisible by 4 and are precisely the unions of disjoint 2×2 latin subsquares. For $k \geqslant 3$, the following is conjectured in [4]:

Conjecture 2. *For all $k \geqslant 3$, a k-homogeneous latin bitrade of size s exists if and only if k divides s and $s \geqslant k^2$.*

The "only if" part of the above conjecture is clear.

Lemma 5 ([2,4,7,8]). *Conjecture 2 is true in each of the following cases:*

- *all odd k,*
- *$s \geqslant k(k+u)$, where k is even but not a power of 2 and u is the smallest proper odd divisor of k,*
- *$s \geqslant 3k^2/2$ in the case when k is a power of 2*
- *all k such that $3 \leqslant k \leqslant 37$.*

A nice spinoff from the previous section is that we can verify Conjecture 2 for the unsolved cases. We make use of the following lemma, which exploits the equivalence of transversals in B_n and diagonally cyclic latin squares.

Lemma 6. *Let T_1 and T_2 be two transversals in B_n such that $|T_1 \cap T_2| = n - k$. Then there exists a k-homogeneous latin bitrade of size nk.*

Proof. It is routine to check that

$$Q = \{(i, c+i, r+c+i) : 0 \leqslant i \leqslant n-1, (r, c, r+c) \in T_1 \setminus T_2\},$$
$$Q' = \{(i, c+i, r+c+i) : 0 \leqslant i \leqslant n-1, (r, c, r+c) \in T_2 \setminus T_1\}$$

defines a k-homogeneous latin bitrade (Q, Q') of size nk. □

From Theorem 5, and the fact that a 3-homogeneous latin bitrade of size 15 exists [7], we have the following corollary:

Corollary 2. *Let $n \geqslant k \geqslant 3$ and n odd. Then there exists a k-homogeneous latin trade of size nk.*

We make use of the following theorem from [4]:

Theorem 6 ([4]). *Let $m \geqslant k$ and $m' \geqslant k'$. If there exists a k-homogeneous latin bitrade of size km and a k'-homogeneous bitrade of size $k'm'$, then there exists a kk'-homogeneous latin bitrade of size $kk'mm'$.*

We are now ready to prove Conjecture 2.

Proof of Theorem 3. From Lemma 5 and Corollary 2, we may assume that k and $n = s/k$ are both even. Let $k = 2^a b$ and $n = 2^c d$, where $a, c, b, d \geqslant 1$ and b and d are odd. By repeated applications of Theorem 6 with $k' = m' = 2$ we can build a 2^w-homogeneous latin bitrade of size 4^w for any integer $w \geqslant 1$. Using Theorem 6 again to combine this bitrade with appropriate base cases, we will prove the required result.

Suppose first that $a \leqslant c+2$ and $b = 1$. From Lemma 5, there exists a 4-homogeneous latin bitrade of size $2^{c-a+4}d$, which we use as our base, choosing $w = a-2$. Note that $a \geqslant 2$ since $k \geqslant 3$ (if $a = 2$, the base case proves the result without need to apply Theorem 6).

Secondly, suppose that $a \leqslant c$ and $b > 1$. Since b is odd, Lemma 5 shows the existence of a b-homogeneous latin bitrade of size $2^{c-a}bd$. We use this as our base, with $w = a$.

Finally, suppose we are not in one of the above cases. Thus $a > c$ and $2^{a-c}b \geqslant 3$ so by Corollary 2 there exists a $2^{a-c}b$-homogeneous bitrade of size $2^{a-c}bd$ which we use as our base with $w = c$. □

We note that most of the homogeneous latin trades from our constructions are neither primary nor minimal. A latin bitrade (Q, Q') is said to be *primary* if there is no latin bitrade (R, R') such that $R \subsetneq Q$ and $R' \subsetneq Q'$. A latin trade Q is said to be *minimal* if there is no latin trade $R \subsetneq Q$. A latin bitrade (Q, Q') is primary if Q is minimal but the converse is not necessarily true.

We conjecture the following:

Conjecture 3. *For all $k \geqslant 3$, a* primary *k-homogeneous latin bitrade of size s exists if and only if k divides s and $s \geqslant k^2$.*

This conjecture has been verified for odd k in [4]. The analogous conjecture for minimal latin bitrades is certainly not true; minimality is, in general, a much more restrictive condition. For $k \geqslant 3$, minimal k-homogeneous latin trades of size k^2 do not exist as these are necessarily latin squares of order k, which for $k \geqslant 3$ always strictly contain a latin trade on any pair of rows. In [7], it is shown that minimal 3-homogeneous latin bitrades of size km exist for each $m \geqslant 4$. We have shown by computer search that the smallest minimal 4-homogeneous latin trade has size 24; a bitrade formed from two such trades is shown below. This answers Open Problem 4 from [36].

1	2	3	4	·	·
5	6	1	·	2	·
6	1	2	·	·	3
2	·	·	5	3	4
·	3	·	6	4	5
·	·	4	1	5	6

2	3	4	1	·	·
6	1	2	·	5	·
1	2	3	·	·	6
5	·	·	4	2	3
·	6	·	5	3	4
·	·	1	6	4	5

For bounds on the size of the smallest minimal k-homogeneous latin trade for $k \geqslant 5$, refer to Table 1 in [10].

6. Random MOLS

In this final section we briefly discuss the significance of our results to the problem of constructing random MOLS (mutually orthogonal latin squares). First we explain what we mean by random MOLS and mention some contexts in which they may be useful.

In order to select "random MOLS" ideally we would like an efficient algorithm which, given integers n and k, returns a set of k MOLS of order n chosen uniformly at random from all such sets. This seems a very difficult problem given that even the degenerate case $k = 1$ has been only partially solved. Jacobson and Matthews [16] designed a Markov chain whose stationary distribution is uniform over Latin squares of order n. However, they were not able to say how quickly their chain converges to its stationary distribution. We are unaware of any prior work applying to the case $k \geqslant 2$. We give a result below which, for $k = 2$ and odd n, allows for the easy selection of a random pair of MOLS of order n. They are not chosen from

the whole space, but rather from a restricted set. Nevertheless that set is exponentially large in n, and the distribution is uniform. We view this as a modest first step on an interesting but difficult problem.

Probably the oldest application of MOLS is to the design of statistical experiments. See [1,28] for discussion of the randomisation that is desirable in this application.

A new technique has recently been proposed for wireless communication, and which should be readily applicable to audio and video watermarking. This technique, OFDMA, uses orthogonal tones to carry high capacity digital data. In order to spread the signal spectrum, a channel is hopped through a pattern of available tones in a prescribed manner, called a hopping pattern. All tones may be occupied during a hopping period, making this a very efficient means of data transfer. Hopping patterns are also used to defeat hackers and overcome interference. Stamatiou and Proakis [30] suggest the use of Latin squares as suitable patterns for controlling the hopping to ensure that adjacent cellular systems have at most one coincidence of tones, which is achieved by using Latin squares that are mutually orthogonal. The security of this application is enhanced by choosing the MOLS in as random a way as possible.

The constructions given in this paper allow an approach when we are considering just a pair of mutually orthogonal latin squares. Here we fix a latin square, and choose a mutually orthogonal mate uniformly at random from a subset of all possible orthogonal mates.

Any diagonally cyclic latin square is orthogonal to the *forward circulant* latin square L_n, with symbol $i - j \pmod n$ in each cell $(i, j) \in N \times N$. The constructions given in this paper allow us to choose diagonally cyclic latin squares, uniformly at random, from a set of size exponential in n. This follows from the bijection between diagonally cyclic latin squares and transversals of B_n. In order to select a transversal at random from B_n we can use standard blocks of order, say, three and select transversals within these blocks randomly and independently. Doing so allows selection of a random transversal from an exponentially large, uniform probability space.

Having chosen a random pair of MOLS, it is possible to randomise further by applying a random permutation to the rows of both squares, a second random permutation to the columns of both squares, and then to randomly permute the symbols within each square. It is also possible to interchange the two squares with probability, say, $\frac{1}{2}$. Whether these further steps are useful will depend on the application.

For some applications our random pairs of MOLS will be too highly structured and it would be very interesting to see an analogous result to the generation method known for random latin squares [16]. Also worthy of further research is the question of what properties random MOLS might be expected to have. Even random latin squares are not well understood, although a few properties are known (see e.g. [9,15,23,24]).

Acknowledgements

The author's research were supported by ARC grants DP0662946 and DP0770857, and by the VPAC and Monash Sun Grid computing facilities.

References

[1] R.A. Bailey, Strata for randomized experiments, J. Roy. Statist. Soc. Ser. B 53 (1991) 27–78.
[2] R. Bean, H. Bidkhori, M. Khosravi, E.S. Mahmoodian, k-homogeneous latin trades, Bayreuth. Math. Schr. 74 (2005) 7–18.
[3] C. Bebeacua, T. Mansour, A. Postnikov, S. Severini, On the X-rays of permutations, Electron. Notes Discrete Math. 20 (2005) 193–203.
[4] Bagheri Gh Behrooz, E.S. Mahmoodian, On the existence of k-homogeneous latin bitrades, Util. Math. (in press).
[5] E.A. Bender, Asymptotic methods in enumeration, SIAM Rev. 16 (1974) 485–515.
[6] N.J. Cavenagh, The theory and application of latin bitrades: A survey, Math. Slovac. 58 (2008) 1–28.
[7] N.J. Cavenagh, D. Donovan, A. Drápal, 3-homogeneous latin trades, Discrete Math. 300 (2005) 57–70.
[8] N.J. Cavenagh, D. Donovan, A. Drápal, 4-homogeneous latin trades, Australas. J. Combin. 32 (2005) 285–303.
[9] N.J. Cavenagh, C. Greenhill, I.M. Wanless, The cycle structure of two rows in a random latin square, Random Structures Algorithms 33 (2008) 286–309.
[10] N. Cavenagh, C. Hämäläinen, A. Drápal, Latin trades derived from groups, Discrete Math. 308 (2008) 6189–6202.
[11] N. Cavenagh, C. Hämäläinen, A. Nelson, On completing three cyclically generated transversals to a latin square, Finite Fields Appl. 15 (2009) 294–303.
[12] C. Cooper, R. Gilchrist, I. Kovalenko, D. Novakovic, Estimation of the number of good permutations, with applications to cryptography, Cybernet. Systems Anal. 35 (1999) 688–693.
[13] C. Cooper, I. Kovalenko, The upper bound for the number of complete mappings, Theory Probab. Math. Statist. 53 (1996) 77–83.
[14] M. Grüttmüller, Completing partial latin squares with two cyclically generated prescribed diagonals, J. Combin. Theory Ser. A 103 (2003) 349–362.
[15] R. Häggkvist, J.C.M. Janssen, All-even latin squares, Discrete Math. 157 (1996) 199–206.
[16] M.T. Jacobson, P. Matthews, Generating uniformly distributed random latin squares, J. Combin. Des. 4 (1996) 405–437.
[17] I.N. Kovalenko, Upper bound on the number of complete maps, Cybernet. Systems Anal. 32 (1996) 65–68.
[18] N. Yu, Kuznetsov, Applying fast simulation to find the number of good permutations, Cybernet. Systems Anal. 43 (2007) 830–837.
[19] N.Yu. Kuznetsov, Estimating the number of good permutations by a modified fast simulation method, Cybernet. Systems Anal. 44 (2008) 547–554.
[20] N.Yu. Kuznetsov, Estimating the number of latin rectangles by the fast simulation method, Cybernet. Systems Anal. 45 (2009) 69–75.
[21] B.M. Maenhaut, I.M. Wanless, Atomic latin squares of order eleven, J. Combin. Des. 12 (2004) 12–34.
[22] B.D. McKay, J.C. McLeod, I.M. Wanless, The number of transversals in a latin square, Des. Codes. Cryptogr. 40 (2006) 269–284.
[23] B.D. McKay, I.M. Wanless, Most latin squares have many subsquares, J. Combin. Theory. Ser. A 86 (1999) 323–347.
[24] B.D. McKay, I.M. Wanless, On the number of latin squares, Ann. Comb. 9 (2005) 335–344.
[25] A.M. Odlyzko, Asymptotic enumeration methods, in: Handbook of Combinatorics, Elsevier, Amsterdam, 1995, pp. 1063–1229.
[26] B. Polster, The mathematics of Juggling, Springer-Verlag, New York, 2003.
[27] I. Rivin, I. Vardi, P. Zimmerman, The n-queens problem, Amer. Math. Monthly 101 (1994) 629–639.
[28] B.H. Singer, S. Pincus, Irregular arrays and randomization, Proc. Natl. Acad. Sci. USA 95 (1998) 1363–1368.
[29] N.J.A. Sloane, The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.

[30] K. Stamatiou, J.G. Proakis, A performance analysis of coded frequency-hopped OFDMA, in: IEEE Wireless Communications and Networking Conference, WCNC, v2, (2005) pp. 1132–1137.
[31] D.S. Stones, I.M. Wanless, A congruence connecting latin rectangles and partial orthomorphisms (submitted for publication).
[32] D.S. Stones, I.M. Wanless, Compound orthomorphisms of the cyclic group (submitted for publication).
[33] I. Vardi, Computational recreations in mathematics, Addison-Wesley, Redwood City, CA.
[34] I.M. Wanless, Diagonally cyclic Latin squares, European J. Combin. 25 (2004) 393–413.
[35] I.M. Wanless, Transversals in latin squares, Quasigroups Related Systems 15 (2007) 169–190.
[36] Open problems from Workshop on latin trades Prague, 6–10 Feb 2006. http://www.karlin.mff.cuni.cz/~rozendo/op.html.