Atomic Latin Squares based on Cyclotomic Orthomorphisms

Ian M. Wanless*

School of Engineering and Logistics
Charles Darwin University
NT 0909 Australia
ian.wanless@cdu.edu.au

Submitted: Feb 19, 2005; Accepted: May 2, 2005; Published: May 9, 2005
Mathematics Subject Classifications: 05B15, 05C70, 11T22

Abstract

Atomic latin squares have indivisible structure which mimics that of the cyclic groups of prime order. They are related to perfect 1-factorisations of complete bipartite graphs. Only one example of an atomic latin square of a composite order (namely 27) was previously known. We show that this one example can be generated by an established method of constructing latin squares using cyclotomic orthomorphisms in finite fields. The same method is used in this paper to construct atomic latin squares of composite orders 25, 49, 121, 125, 289, 361, 625, 841, 1369, 1849, 2809, 4489, 24649 and 39601. It is also used to construct many new atomic latin squares of prime order and perfect 1-factorisations of the complete graph K_{q+1} for many prime powers q. As a result, existence of such a factorisation is shown for the first time for q in

$$\{529,2809,4489,6889,11449,11881,15625,22201,\ 24389,24649,26569,29929,32041,\\ 38809,44521,50653,51529,52441,63001,72361,76729,78125,79507,103823,\\ 148877,161051,205379,226981,300763,357911,371293,493039,571787\}.$$

We show that latin squares built by the 'orthomorphism method' have large automorphism groups and we discuss conditions under which different orthomorphisms produce isomorphic latin squares. We also introduce an invariant called the train of a latin square, which proves to be useful for distinguishing non-isomorphic examples.

*This work was undertaken at Christ Church, Oxford and at the Department of Computer Science, Australian National University.

1 Introduction

Group theorists think of the cyclic groups of prime order as their basic building blocks. Every Cayley table of a finite group is a latin square and the latin squares corresponding to cyclic groups of prime order display an atomic (in the sense of "indivisible") structure indicative of their lack of any algebraic substructure. They are the only groups whose Cayley tables form atomic latin squares (see Theorem 1). Interestingly, it has recently been discovered [11], [14], [17] that some non group-based latin squares also have atomic properties.

There is an established method, which we call the *orthomorphism method*, for constructing latin squares based on cyclotomic orthomorphisms of finite fields. We analyse some of the basic properties of latin squares built using this method and report that the method seems moderately successful in producing atomic latin squares, although as yet no pattern has emerged as to when it does. Crucially though, it provides a means for constructing atomic latin squares of composite order. The only previously known [17] example of composite order turns out to be constructible by the orthomorphism method. In addition we find 14 new composite orders for which atomic latin squares exist, including one order (625) which is a fourth power. Unfortunately, since we make crucial use of field arithmetic, the orthomorphism method cannot work for orders which are not prime powers, so the existence of atomic latin squares of these orders remains an open question.

An $n \times n$ matrix M containing symbols from a set Σ of cardinality n is a *row-latin square* if each symbol in Σ occurs exactly once in each row of M. Similarly, M is a *column-latin square* if each symbol in Σ occurs exactly once in each column of M and M is a *latin square* if it is both row-latin and column-latin. Throughout this paper we will use the symbols Σ of a latin square to index the rows and columns of that square, and Σ will always be the elements of a finite field. It is sometimes helpful to think of a latin square of order n as a set of n^2 triples of the form (row, column, symbol), where each element of a triple belongs to Σ. The latin property means that distinct triples never agree in more than one co-ordinate.

For each latin square there are six conjugate squares obtained by uniformly permuting the co-ordinates of each triple. These conjugates can be labelled by a permutation giving the new order of the co-ordinates, relative to the former order of (123). Hence, the (123)-conjugate is the square itself and the (213)-conjugate is its transpose. We say that the (123)-conjugate is the *trivial conjugate* and the other five conjugates are *non-trivial*. The (132)-conjugate is found by interchanging columns and symbols, which is another way of saying that each row, when thought of as a permutation, is replaced by its inverse. We will use L^T and L^* to denote, respectively, the (213) and (132) conjugates of a latin square L.

An *isotopism* of a latin square L is a permutation of its rows, permutation of its columns and permutation of its symbols. The resulting square is said to be *isotopic* to L and the set of all squares isotopic to L is called an *isotopy class*. In the special case when the same permutation π is applied to the rows, columns and symbols, the isotopism is an *isomorphism*. An isotopism which maps L to itself is called an *autotopism* of L and an autotopism which is an isomorphism is called an *automorphism*. In particular, by saying that a permutation π is an automorphism of L we are asserting that applying π to the rows, columns and symbols of L yields the same square back again. The *main class* of L is the set of squares which are isotopic to some conjugate of L. A latin square is said to have a *conjugate symmetry* if it is isotopic to one of its non-trivial conjugates.

A *latin subrectangle* is a rectangular submatrix R of a latin square L such that exactly the same symbols occur in each row of R. The latin subrectangle is *proper* if it has at least two rows and has (strictly) fewer columns than L. If R is a $2 \times m$ latin subrectangle and R is minimal in that it contains no $2 \times k$ latin subrectangle for $2 \leq k < m$, then we say that R is a *row cycle* of length m. Each pair of rows of L decomposes into a set of one or more row-cycles whose lengths form a partition of n, the order of L. We call this (unordered) partition the *cycle partition* corresponding to the two rows in question.

Another way to think of row cycles is in terms of the permutation which maps one row to another row. Suppose that r and s are two rows of a latin square with index set Σ. We define a permutation $\rho : \Sigma \mapsto \Sigma$ by $\rho(L_{rj}) = L_{sj}$ for each $j \in \Sigma$. Each row cycle between r and s corresponds to a cycle of the permutation ρ and vice versa. If γ is a cycle of ρ then we find the corresponding row cycle by taking all occurrences in r and s of symbols which occur in γ.

Column cycles and symbol cycles can be defined similarly to row cycles, and the operations of conjugacy interchange these objects. A column cycle is a set of entries which get mapped to a row cycle when the square is transposed. A symbol cycle is a set of entries which get mapped to a row cycle when we take the (321)-conjugate of the square. Row cycles, column cycles and symbol cycles will collectively be known as cycles.

A cycle which has length equal to the order of the square is said to be *Hamiltonian*. As an example, the (Hamiltonian) cycle between the first two rows of the latin square given in Figure 1 can be traced, in order, through the symbols $0uplsqceahjgrwtodkfvbnmxi$. We say that a latin square is *row-hamiltonian* if every row cycle is Hamiltonian. Equivalently, a latin square is row-hamiltonian if it contains no proper latin subrectangles. The basic properties of row-hamiltonian squares are studied in [17]. An infinite family of row-hamiltonian latin squares is constructed in [2]. Other infinite families can be constructed from perfect 1-factorisations of complete graphs using a well-known method studied, for example, in [3] and [19].

In this paper we are interested primarily in a stronger property related to row-hamiltonicity. We say that a latin square is *atomic* if all of its conjugates are row-hamiltonian. In other words, a square is atomic if all of its cycles are Hamiltonian. Among groups, the atomic property characterises the cyclic groups of prime order, as the next result shows.

Theorem 1 *The latin square L_G derived from the Cayley table of a group G is atomic if and only if G is a cyclic group of prime order.*

Proof: By [4, Thm 4.2.2] every conjugate of L_G is isotopic to L_G so L_G is atomic if and only if it is row-hamiltonian. Consider the row cycles of L_G between the rows corresponding to two distinct elements $g, h \in G$. It is easy to establish that each of these cycles has length equal to the order of the element hg^{-1}. Hence L_G is atomic if and only if the order of every non-identity element of G equals the order of G. The theorem follows. $\square$

We say that a latin square is *group-based* if, with appropriate borders added, it becomes the Cayley table of some group. The first detailed construction for non group-based atomic squares was an infinite family published by Owens and Preece [14]. Shortly afterwards, Wanless [17] coined the name 'atomic' and published another family. He has since discovered a parenthetical remark in a paper by Yamamoto [20] which indicates that as far back as 1961 Yamamoto had discovered the construction used in [17], although [20] contains no details.

It is known [11] that for orders up to 10 the only main classes of atomic squares are those predicted by Theorem 1, but there are exactly 7 main classes of atomic squares of order 11.

None of the results mentioned above has shown the existence of atomic squares of composite order. In fact the enumeration for small orders, together with Theorem 1, might lead to the suspicion that atomic squares must have prime order. That this was not the case was shown in [17] where an example of order 27 was described. Prior to the current paper that example was the only one known. In this paper we show that the orthomorphism method can be used to construct the known atomic square of order 27 and also another atomic square of the same order, but from a different main class. The method can also be used to construct atomic latin squares of the composite orders 25, 49, 121, 125, 289, 361, 625, 841, 1369, 1849, 2809, 4489, 24649 and 39601 as well as a number of non group-based examples of prime orders. Details of these constructions will be given in §6 and §8, but an explicit example is given in Figure 1. This example is noteworthy in that it is known to be the smallest atomic latin square of an order which is a non-trivial power of a prime. It is quite possibly the smallest atomic latin square of composite order, but existence for orders 15 and 21 is currently an open question.

The structure of the paper is as follows. In the next section we describe the orthomorphism method. This is an established method for building latin squares, so we briefly review the literature on the subject. In §3 we describe, without giving proofs, an important special case of our results, which corresponds to using quadratic orthomorphisms in the orthomorphism method. Then in §4 we set out the results in full generality, including proofs. We prove that each square built using the orthomorphism method has a large automorphism group. Our results also describe some circumstances under which two different applications of the orthomorphism method produce isomorphic results. In §5 we describe how the theory from the previous section can be used to run a computer search for atomic squares. In §6 we describe some atomic latin squares of composite order which were found by this search (examples of prime order are discussed in §8). In §7 we describe an invariant, called the train, which can be used for distinguishing latin squares from different main classes. Finally, in §9 we list some perfect 1-factorisations of complete graphs which we found using a variation on our search for atomic latin squares. It turns out that our method is general enough to construct a perfect 1-factorisation of K_{q+1} for every one of the sporadic values of the prime power q for which a perfect 1-factorisation has previously been published (as well as finding constructions for many new orders).

$$
\begin{array}{ccccccccccccccccccccccccc}
0 & e & x & b & f & i & g & p & j & m & k & t & c & q & l & n & r & u & s & d & v & a & w & h & o \\
u & a & i & n & v & 0 & r & l & g & x & f & o & e & c & s & m & w & p & q & k & b & h & t & j & d \\
c & t & b & s & w & x & u & m & e & a & r & l & j & o & i & q & g & v & d & h & f & n & p & k & 0 \\
l & m & 0 & c & r & n & h & q & u & s & p & j & v & w & a & f & x & k & o & b & e & d & i & t & g \\
s & x & r & u & d & h & 0 & k & t & f & i & m & o & e & j & v & l & w & c & n & g & q & a & b & p \\
a & l & h & t & m & e & x & r & d & 0 & n & p & k & f & c & s & i & g & w & q & u & v & j & o & b \\
d & j & t & o & i & m & f & 0 & c & l & x & q & w & r & v & p & n & s & a & u & k & b & h & g & e \\
f & h & p & x & t & q & w & g & v & r & l & d & a & b & o & u & 0 & c & e & j & n & k & s & m & i \\
w & u & s & f & e & b & v & a & h & q & 0 & x & i & j & m & k & t & o & n & p & d & c & g & r & l \\
e & b & n & v & j & p & d & x & l & i & q & u & f & 0 & r & t & o & h & g & c & m & w & k & s & a \\
h & w & l & k & n & v & a & s & m & d & j & 0 & g & p & e & x & c & i & b & t & r & o & q & u & f \\
j & s & w & q & g & l & t & u & o & v & c & k & b & d & p & a & e & f & x & r & 0 & i & m & n & h \\
n & g & k & 0 & p & a & i & j & x & h & b & e & l & u & q & d & m & r & v & o & w & s & c & f & t \\
i & o & g & a & k & d & e & w & n & t & h & v & p & m & u & b & j & 0 & f & x & s & l & r & c & q \\
o & c & u & e & s & j & p & t & r & b & d & w & 0 & h & n & g & k & l & i & a & q & m & f & x & v \\
x & k & m & r & l & w & c & n & q & p & u & h & s & a & 0 & o & f & b & t & e & i & g & d & v & j \\
g & q & v & j & x & k & o & b & s & e & m & n & d & l & f & i & p & t & 0 & w & h & r & u & a & c \\
m & r & o & g & u & s & k & e & i & j & v & c & n & x & t & h & a & q & l & f & p & 0 & b & d & w \\
p & f & j & d & b & g & m & i & w & n & t & s & q & v & h & c & u & a & r & 0 & o & x & l & e & k \\
r & n & c & i & 0 & o & q & v & b & w & g & a & u & t & d & l & h & e & k & s & j & f & x & p & m \\
k & v & a & w & h & c & b & d & p & o & s & f & x & i & g & r & q & n & j & m & t & e & 0 & l & u \\
q & 0 & f & h & c & t & s & o & a & k & w & g & m & n & b & j & v & d & p & l & x & u & e & i & r \\
t & d & q & l & o & u & n & h & f & c & e & i & r & k & x & w & b & j & m & g & a & p & v & 0 & s \\
v & p & d & m & q & r & l & f & 0 & u & a & b & t & g & k & e & s & x & h & i & c & j & o & w & n \\
b & i & e & p & a & f & j & c & k & g & o & r & h & s & w & 0 & d & m & u & v & l & t & n & q & x
\end{array}
$$

Figure 1: Atomic latin square of order 25

2 The orthomorphism method

A permutation θ of a field $\mathcal{F}$ is called an *orthomorphism* if the map $\phi : \mathcal{F} \mapsto \mathcal{F}$ defined by $\phi(x) = \theta(x) - x$ is also a permutation of $\mathcal{F}$. An orthomorphism θ is *canonical* if $\theta(0) = 0$.

For each $d \in \mathcal{F}$ we define the d^{th} diagonal of a latin square L to be the set of entries in cells (i, j) satisfying $j - i = d$. In particular, the 0^{th} diagonal is the main diagonal. If L is generated from its row 0 by the rule that the entry in row i on diagonal d is $i + L_{0d}$, then we say that L is *diagonally generated*. For any diagonally generated latin square the map $z \mapsto z + c$ for an arbitrary constant $c \in \mathcal{F}$ is an automorphism (see Lemma 9).

In the special case when $\mathcal{F} = \mathbb{Z}_p$ for some prime p then each of our diagonals corresponds to what is sometimes called a *broken diagonal* in the literature. A diagonally generated square in this case has the elements of $\mathbb{Z}_p$ occurring in cyclic order down each broken diagonal, and such squares have been called *diagonally cyclic*. See [18] for a survey of the many important applications of diagonally cyclic latin squares. For our purposes, the most important result in that paper is that a given permutation θ of $\mathbb{Z}_p$ can be used as row 0 of a diagonally cyclic latin square if and only if θ is an orthomorphism. More generally we have:

Lemma 1 *Let θ be a permutation of $\mathcal{F}$. There is a diagonally generated latin square L with $L_{0j} = \theta(j)$ for all $j \in \mathcal{F}$ if and only if θ is an orthomorphism of $\mathcal{F}$.*

Proof: Suppose that θ is a permutation of $\mathcal{F}$ and let M be the matrix with index set $\mathcal{F}$, which satisfies $M_{0j} = \theta(j)$ for all $j \in \mathcal{F}$ and is diagonally generated from this row. The fact that θ is a permutation and M is diagonally generated guarantees that M is row-latin. So M will be a latin square unless $M_{ij} = M_{kj}$ for some $i, j, k \in \mathcal{F}$ with $i \neq k$. But $M_{ij} = M_{kj}$ is equivalent to

$$\begin{aligned} \theta(j-i) - (j-i) = M_{0(j-i)} + i - j = M_{ij} - j = \\ M_{kj} - j = M_{0(j-k)} + k - j = \theta(j-k) - (j-k) \end{aligned}$$

which says that θ is not an orthomorphism. The result should now be clear. $\square$

Orthomorphisms are closely connected with starters; see [8] for details. The constructions that we give for perfect 1-factorisation in §9 are produced by a technique equivalent to the *quotient coset starters* as defined, for example, in [15]. Our construction for atomic latin squares is a slight generalisation of that technique in that it builds latin squares which need not be symmetric. Nevertheless, the use of orthomorphisms to build latin squares is a well established technique (see [7], [8]) for which we make no claim to originality. Also, our use of cyclotomy classes in our constructions has well established precedents in design theory, see for example [13] and [9, §4.9]. Cyclotomic orthomorphisms, and hence all of the main results of this paper, can be neatly rephrased in terms of permutation polynomials. Again, the interested reader is referred to [8] for more details.

3 Quadratic Orthomorphisms

In this section we discuss an important special case of our results. This case corresponds to the quadratic orthomorphisms studied by Evans [7]. All results in this section will be stated without proof since they are special cases of more general results which will be proved, in full, in the next section. We introduce them here because they are simpler than the general statements and hence serve as an easily accessible introduction. The quadratic case is also worth special attention since it is particularly effective for our purposes, as we shall see in later sections.

Throughout this section $\mathcal{F}$ will be a field of finite order $q = p^r$, where p is an odd prime. All calculations will take place within $\mathcal{F}$. The set S will comprise the non-zero squares in $\mathcal{F}$ and the set $\mathcal{F}^\#$ is defined to be $\mathcal{F} \setminus \{0, 1\}$. For any $c, d \in \mathcal{F}^\#$ we define a matrix $L = \mathcal{L}[c, d]$ of order q by

$$L_{ij} = \begin{cases} i + c(j-i) & \text{if } j - i \in S, \\ i + d(j-i) & \text{if } j - i \notin S, \end{cases} \tag{1}$$

where the rows and columns of L are indexed by $\mathcal{F}$. For L to be a latin square it is necessary and sufficient that $cd \in S$ and $(1-c)(1-d) \in S$. In what follows we assume that c, d have been chosen to satisfy this condition.

Each conjugate of the square L defined by (1) is a square of the same form, but possibly with different constants c, d. The transpose L^T of L is given by $\mathcal{L}[c', d']$ where $c' = 1 - c$, $d' = 1 - d$ if $q \equiv 1 \bmod 4$ and $c' = 1 - d$, $d' = 1 - c$ if $q \equiv 3 \bmod 4$. The row-inverse L^* of L is given by $\mathcal{L}[c'', d'']$ where $c'' = 1/c$, $d'' = 1/d$ if $c \in S$ and $c'' = 1/d$, $d'' = 1/c$ if $c \notin S$.

The latin square $\mathcal{L}[c, d]$ is isomorphic to $\mathcal{L}[d, c]$ and is also isomorphic to $\mathcal{L}[c^p, d^p]$. Furthermore, for any fixed $f \in \mathcal{F}$ the map $x \mapsto x + f$ is an automorphism of L, as is the map $x \mapsto x \cdot s$ for any fixed $s \in S$. So L has an automorphism group of order which is some multiple of $\frac{1}{2}q(q-1)$. These automorphisms imply that if $q \equiv 3 \bmod 4$ then L is semi-regular, in the sense of Anderson [1]. This means that every pair of rows of L has the same cycle partition. On the other hand if $q \equiv 1 \bmod 4$ then every pair of rows has one of at most two possible cycle partitions. These restrictions give us hope of finding row-hamiltonian examples, since fewer things have to be right in order for every row-cycle to be hamiltonian. By the same token, since each conjugate of L is of the type defined by (1), it is easy to find such L that are atomic, at least when compared to other constructions which the author has tried.

4 Cyclotomic Orthomorphisms

In this section we describe a general method for constructing latin squares which in a number of instances succeeds in building atomic squares. The method is related to the cyclotomic orthomorphisms studied by Evans [7]. The quadratic case presented in the previous section is a special case of the method studied here. The claims made in the previous section will be proved in this section, since they are special cases of the theorems below.

As in the previous section, $\mathcal{F}$ will be a field of finite order $q = p^r$ where p is an odd prime and $\mathcal{F}^{\#} = \mathcal{F} \setminus \{0, 1\}$. All calculations will take place within $\mathcal{F}$ and $\mathcal{F}$ will be used to index the rows and columns of our latin squares. We will use x to denote a primitive element in $\mathcal{F}$, so that $\mathcal{F} = \{0, x, x^2, x^3, \ldots, x^{q-1}\}$.

Suppose that $q \equiv 1 \bmod t$ for some positive integer t and define $u = (q-1)/t$. For $i \in \mathbb{Z}_t$ we define

$$\mathcal{C}_i = \{x^{mt+i} : m \in \mathbb{Z}\}$$

which we call the i^{th} *cyclotomy class* (with respect to t). Each cyclotomy class contains exactly u elements of $\mathcal{F}$ and between them they partition the non-zero elements of $\mathcal{F}$. We refer to t as the *degree*. The quadratic case in the previous section corresponds to choosing the degree $t = 2$, in which case $\mathcal{C}_0 = S$, the set of non-zero squares. Hence the following definition is a generalisation of (1).

For any $c_0, c_1, \ldots, c_{t-1} \in \mathcal{F}^{\#}$ we define a matrix $L = \mathcal{L}[c_0, c_1, \ldots, c_{t-1}]$ of order q by

$$L_{ij} = \begin{cases} i & \text{if } i = j, \\ i + c_s(j-i) & \text{whenever } j - i \in \mathcal{C}_s. \end{cases} \tag{2}$$

We call the individual c_i *scaling factors* and refer to $[c_0, c_1, \ldots, c_{t-1}]$ as the *vector of scaling factors*.

Lemma 2 *The necessary and sufficient condition that* (2) *defines a row-latin square is that $a + \alpha \not\equiv b + \beta$ mod t for distinct $\alpha, \beta \in \mathbb{Z}_t$, where $a, b \in \mathbb{Z}_t$ are defined by $c_\alpha \in \mathcal{C}_a$ and $c_\beta \in \mathcal{C}_b$.*

Proof: First suppose that $a + \alpha \equiv b + \beta \bmod t$ where $c_\alpha \in \mathcal{C}_a$ and $c_\beta \in \mathcal{C}_b$ for distinct $\alpha, \beta \in \mathbb{Z}_t$. Consider an entry e in row 0 which occupies a column $j \in \mathcal{C}_\alpha$. Then $e = L_{0j} = c_\alpha j \in \mathcal{C}_a \mathcal{C}_\alpha = \mathcal{C}_{a+\alpha}$. Similarly, if $k \in \mathcal{C}_\beta$ then $L_{0k} \in \mathcal{C}_{b+\beta} = \mathcal{C}_{a+\alpha}$. But there are $2u$ elements in $\mathcal{C}_\alpha \cup \mathcal{C}_\beta$ and only u elements in $\mathcal{C}_{a+\alpha}$, from which it follows that some symbol must be repeated in row 0 and L is not row-latin. This establishes the necessity of our condition.

To prove sufficiency we assume that the condition holds and suppose that $L_{ij} = L_{ik}$ for some $i, j, k \in \mathcal{F}$ where $j \neq k$. We may assume that $j \neq i$ and $k \neq i$ since $L_{ii} = i \neq L_{il}$ for all $l \neq i$ by definition, given that $c_s \neq 0$ for all $s \in \mathbb{Z}_t$. Hence there exist $\alpha, \beta \in \mathbb{Z}_t$ such that $j - i \in \mathcal{C}_\alpha$ and $k - i \in \mathcal{C}_\beta$. Now $L_{ij} = L_{ik}$ and (2) together imply that

$$c_\alpha(j-i) = c_\beta(k-i). \tag{3}$$

Define $a, b \in \mathbb{Z}_t$ by $c_\alpha \in \mathcal{C}_a$ and $c_\beta \in \mathcal{C}_b$. Then $c_\alpha(j-i) \in \mathcal{C}_a \mathcal{C}_\alpha = \mathcal{C}_{a+\alpha}$ and $c_\beta(k-i) \in \mathcal{C}_b \mathcal{C}_\beta = \mathcal{C}_{b+\beta}$, so (3) implies that $a + \alpha \equiv b + \beta \bmod t$. By assumption this means that $\alpha = \beta$, but then (3) immediately implies that $j = k$. This contradiction proves the theorem. $\square$

In order to establish conditions under which (2) defines a latin square we next consider the transpose of the matrix defined by (2). For the following result note that $ut = q - 1$ is even so that one of u or t must be even.

Lemma 3 *The transpose L^T of the matrix L defined by* (2) *is a matrix of the same form, defined by $L^T = \mathcal{L}[c'_0, c'_1, \ldots, c'_{t-1}]$ where for each $s \in \mathbb{Z}_t$,*

$$c'_s = \begin{cases} 1 - c_s & \text{if } u \text{ is even,} \\ 1 - c_{s+t/2} & \text{if } u \text{ is odd.} \end{cases}$$

Proof: By the choice of x we know that $-1 = x^{(q-1)/2} = x^{ut/2}$. Hence, $-1 \in \mathcal{C}_h$ where $h = 0$ if u is even and $h = t/2$ if u is odd.

Trivially, $L_{ii} = i = L^T_{ii}$ for all $i \in \mathcal{F}$. So let i, j be distinct elements of $\mathcal{F}$ and define s by $i - j \in \mathcal{C}_s$. Then $L^T_{ij} = L_{ji} = j + c_s(i-j) = i + (1-c_s)(j-i)$. The result now follows since $j - i = (-1)(i-j) \in \mathcal{C}_{h+s}$. □

Combining the previous two lemmas immediately gives:

Lemma 4 *For* (2) *to define a latin square it is both necessary and sufficient that the following two conditions hold for all distinct $\alpha, \beta \in \mathbb{Z}_t$:*

(i) *$a + \alpha \not\equiv b + \beta \bmod t$ where $a, b \in \mathbb{Z}_t$ are defined by $c_\alpha \in \mathcal{C}_a$ and $c_\beta \in \mathcal{C}_b$.*

(ii) *$a' + \alpha \not\equiv b' + \beta \bmod t$ where $a', b' \in \mathbb{Z}_t$ are defined by $1 - c_\alpha \in \mathcal{C}_{a'}$ and $1 - c_\beta \in \mathcal{C}_{b'}$.*

The reason for choosing our coefficients c_s from $\mathcal{F}^{\#}$ rather than $\mathcal{F}$ should now be clear, since L cannot be row-latin if $c_s = 0$ and cannot be column-latin if $c_s = 1$.

For a given choice of coefficients $[c_0, c_1, \ldots, c_{t-1}]$ define $\sigma : \mathbb{Z}_t \mapsto \mathbb{Z}_t$ by $\sigma(\alpha) = a + \alpha$ where $c_\alpha \in \mathcal{C}_a$. Similarly, define $\sigma' : \mathbb{Z}_t \mapsto \mathbb{Z}_t$ by $\sigma'(\alpha) = a + \alpha$ where $1 - c_\alpha \in \mathcal{C}_a$. Then Lemma 4 can be rewritten in the following way:

Lemma 5 *For* (2) *to define a latin square it is both necessary and sufficient that σ and σ' are permutations.*

This is exactly the condition given in [7, Thm 3.7] that $[c_0, c_1, \ldots, c_{t-1}]$ yields a cyclotomic orthomorphism. We will henceforth assume that the conditions in Lemma 5 (or alternatively Lemma 4) are met, so that we do in fact have a latin square. That being the case, we can ask about its conjugates. These can be generated using Lemma 3 together with our next result.

Lemma 6 *Let L be defined by* (2)*. Then L^* is a latin square of the same form, defined by $L^* = \mathcal{L}[c''_0, c''_1, \ldots, c''_{t-1}]$ where $c''_{\sigma(s)} = c_s^{-1}$.*

Proof: Let L^* be as defined in the statement of the Lemma. We show that L^* is the (132)-conjugate of L. Trivially $L^*_{ii} = i = L_{ii}$ for all $i \in \mathcal{F}$. So suppose that i, j are distinct elements of $\mathcal{F}$ and define s by $j - i \in \mathcal{C}_s$. Then $L_{ij} = i + c_s(j-i)$ and $L^*_{i(i+c_s(j-i))} = i + c_s^{-1}(c_s(j-i)) = j$, using the fact that $c_s(j-i) \in \mathcal{C}_{\sigma(s)}$ because $j - i \in \mathcal{C}_s$. □

Next we look at two ways in which we can get isomorphic results. In doing so we will make use of the fact that all isomorphisms preserve the main diagonal of an idempotent latin square (that is, a square L for which $L_{ii} = i$ for all i). Since (2) defines an idempotent square, we may concentrate on what happens to the off-diagonal entries.

Lemma 7 *Suppose that the vector $\tilde{e} = [e_0, e_1, \ldots, e_{t-1}]$ of scaling factors is obtained by cyclically permuting the elements of $\tilde{c} = [c_0, c_1, \ldots, c_{t-1}]$. Then $L = \mathcal{L}(\tilde{c})$ is isomorphic to $E = \mathcal{L}(\tilde{e})$.*

Proof: Suppose that $c_i = e_{i+d}$ where subscripts are in $\mathbb{Z}_t$. Fix any $\lambda \in \mathcal{C}_d$ and consider the permutation τ of $\mathcal{F}$ which maps y to λy for every $y \in \mathcal{F}$. We apply τ to each component of a general off-diagonal triple (i, j, L_{ij}) of L. Define s by $j - i \in \mathcal{C}_s$. Then

$$(\tau(i), \tau(j), \tau(L_{ij})) = (\lambda i, \lambda j, \lambda(i + c_s(j - i))) = (\lambda i, \lambda j, \lambda i + c_s(\lambda j - \lambda i))$$

which is a triple in E since $\lambda j - \lambda i = \lambda(j - i) \in \mathcal{C}_d\,\mathcal{C}_s = \mathcal{C}_{d+s}$. $\square$

Lemma 8 *Suppose that the vector $\tilde{e} = [e_0, e_1, \ldots, e_{t-1}]$ of scaling factors is related to $\tilde{c} = [c_0, c_1, \ldots, c_{t-1}]$ by $e_{ip} = c_i^p$. Then $L = \mathcal{L}(\tilde{c})$ is isomorphic to $E = \mathcal{L}(\tilde{e})$.*

Proof: The Frobenius map $y \mapsto y^p$ is well known to be an isomorphism of $\mathcal{F}$. We apply this map to each component of (i, j, L_{ij}), a typical off-diagonal triple of L. Define s by $j - i \in \mathcal{C}_s$. Then by the properties of the Frobenius map we have

$$(i^p, j^p, L_{ij}^p) = (i^p, j^p, (i + c_s(j - i))^p) = (i^p, j^p, i^p + c_s^p(j^p - i^p))$$

which is a triple of E since $j^p - i^p = (j - i)^p \in \mathcal{C}_{sp}$. $\square$

One of the key reasons for the success of our construction is its large automorphism group. We have:

Lemma 9 *Let L be defined by (2). Then the permutations*

(i) *P_a defined by $P_a(z) = a + z$ for any fixed $a \in \mathcal{F}$,*

(ii) *T_a defined by $T_a(z) = az$ for any fixed $a \in \mathcal{C}_0$,*

are automorphisms of L.

Proof: To prove (i), fix $a \in \mathcal{F}$. Let (i, j, L_{ij}) be a general off-diagonal triple of L and define s by $j - i \in \mathcal{C}_s$. Then

$$(P_a(i), P_a(j), P_a(L_{ij})) = (a + i, a + j, a + i + c_s((a + j) - (a + i)))$$

which is a triple in L since $(a + j) - (a + i) = j - i \in \mathcal{C}_s$.

To prove (ii), fix $a \in \mathcal{C}_0$. Let (i, j, L_{ij}) be a general off-diagonal triple of L and define s by $j - i \in \mathcal{C}_s$. Then

$$(T_a(i), T_a(j), T_a(L_{ij})) = (ai, aj, a(i + c_s(j - i))) = (ai, aj, ai + c_s(aj - ai))$$

which is a triple in L since $aj - ai = a(j - i) \in \mathcal{C}_0\,\mathcal{C}_s = \mathcal{C}_s$. $\square$

A corollary of this last result is that $uq = |\mathcal{C}_0|\,|\mathcal{F}|$ divides $|\mathrm{aut}(L)|$, the order of the automorphism group of L. In many cases $|\mathrm{aut}(L)| = uq$, but the atomic square of order 25 given in Figure 1 is an example where the group is strictly larger, as we shall see in §6. We also note that uq is inversely proportional to the degree, which explains, at least in part, why quadratic orthomorphisms seem to be the most useful in our current quest.

Informally, one benefit of the large automorphism group is that we get quite regular cycle structure:

Lemma 10 *To establish whether L, as defined by* (2)*, is row-hamiltonian it suffices to check the cycle partition between row* 0 *and one row from each of the classes $\mathcal{C}_0$, $\mathcal{C}_1$, …, $\mathcal{C}_{t-1-h}$, where h is defined in Lemma* 3.

Proof: Suppose that L has a hamiltonian row cycle between row 0 and row $\rho_i \in \mathcal{C}_i$ for each $i = 0, 1, \ldots, t-1-h$. Let r_1, r_2 be two distinct elements of $\mathcal{F}$ and define s by $r_2 - r_1 \in \mathcal{C}_s$. Referring to Lemma 3 we see that $-1 \in \mathcal{C}_h$. Hence, by interchanging the labels r_1 and r_2 if necessary, we may assume that $0 \le s \le t-1-h$. To prove the result it suffices to show that there is a hamiltonian row cycle between row r_1 and r_2.

Define $\alpha = -r_1$ and $\mu = \rho_s/(r_2 - r_1)$ and observe that $\mu \in \mathcal{C}_0$ since it is the ratio of two elements of $\mathcal{C}_s$. By Lemma 9 the cycle partition between rows r_1 and r_2 is the same as that between rows $T_\mu(P_\alpha(r_1)) = T_\mu(0) = 0$ and $T_\mu(P_\alpha(r_2)) = T_\mu(r_2 - r_1) = \rho_s$, and hence consists of a hamiltonian cycle as required. $\square$

5 The search

In this section we describe the algorithm which was used to search for atomic latin squares.

A major strength of the cyclotomic orthomorphism method is that an entire latin square can be specified by a small number of scaling factors. Hence it is feasible to use a computer to look for examples of atomic latin squares of orders which are large enough to be interesting. The characterisation in Lemma 4 is easily implemented so that we only ever choose scaling factors which will give us a latin square. Also, we can impose a lexicographic order on choices of scaling factors. Then the results of Lemma 3 and Lemma 6 can be combined to ensure that of the 6 conjugates of any latin square we only ever generate the 'least' one. Similarly, the results of Lemma 7 and Lemma 8 can be used to trim the search further, by abandoning any choice of scaling factors which is isomorphic to an earlier choice. It also makes sense to eliminate degenerate choices of scaling factors from the search. By degenerate we mean any choice which is periodic, with non-trivial period, and hence is actually an example of a lower degree orthomorphism. The extreme case is when every scaling factor is the same and the orthomorphism is linear. Linear orthomorphisms are of no interest in the current setting since they always produce group-based latin squares.

There is an important caveat to the above observations, which is this: The examples quoted over the following pages are not necessarily exactly the examples which the computer found. Sometimes we have manipulated them to make their symmetries more

	$r=2$	3	4	5	6	7	8	9	10
$t=2$	251^2	47^3	19^4	11^5	5^6	3^7	3^8	3^9	3^{10}
3	113^2	19^3	11^4	7^5	5^6				
4	47^2	13^3	7^4	5^5	3^6				
5	19^2	3^4							
6	17^2	7^3							
7	13^2								
8	11^2	3^4							
12	5^2								

Table 1: Extent of the search for atomic squares with conjugate symmetry.

transparent. This means our examples will not necessarily be lexicographically least amongst their six conjugates. For example, for a particular main class the computer may have found a representative which is equal to its (321)-conjugate, but we might choose to report the (132)-conjugate of such a square, so that it is symmetric in the usual matrix sense.

Each vector of scaling factors that passes the above tests can be fairly quickly checked to see if it produces an atomic square. Lemma 10 tells us that we need to build at most $t-h+1$ rows of a latin square and check $t-h$ row cycles. If we find any row cycle which is not Hamiltonian then clearly the square is not row-hamiltonian, but otherwise the square is. Since a square is row-hamiltonian if and only if its (132)-conjugate is row-hamiltonian [17], we can tell whether a square is atomic by confirming that its (123), (213) and (312) conjugates are row-hamiltonian.

The above approach was implemented and a number of atomic latin squares of composite order were discovered. These will be detailed in §6. It was noted that most (although not all) of the examples that the computer found had a conjugate symmetry. In particular, they were related to at least one of their non-trivial conjugates by equality, or by one of the isomorphisms shown in Lemma 7 and Lemma 8. Hence, the search was subsequently narrowed to focus on examples of this type.

The search for atomic latin squares of composite order possessing a conjugate symmetry (of the type just described) was exhaustive up to and including the order shown in Table 1. As an example, the first entry in that table shows that all quadratic orthomorphisms (hence $t=2$) were checked in all fields of order q, the square of a prime (hence $r=2$), up to and including the case $q=251^2=63001$.

A search for atomic squares of prime order will be discussed in §8.

6 Atomic squares of composite order

The computer search described in §5 uncovered 16 main classes of atomic latin squares of composite order. Those examples are summarised in Table 2 and discussed below.

Our finite fields were constructed in the computer by first finding (by trial and error)

p	r	q	$\zeta(x)$	$\tilde{c}$	Symmetry
5	2	25	x^2+x+2	$[15, 4, 22, 23, 2, 4, 1, 9, 2, 4, 1, 9]$	S^*
3	3	27	x^3+2x+1	$[20, 4]$	T
3	3	27	x^3+2x+1	$[7, 5]$	T
7	2	49	x^2+x+3	$[12, 2]$	C
11	2	121	x^2+x+7	$[94, 74, 22, 2]$	N^*
5	3	125	x^3+3x+2	$[94, 42]$	U
17	2	289	x^2+x+3	$[244, 114]$	C
19	2	361	x^2+x+2	$[163, 47]$	C
5	4	625	x^4+x^2+2x+2	$[611, 33]$	F^2
29	2	8411	x^2+x+3	$[829, 429]$	F
37	2	1369	x^2+x+5	$[182, 64]$	F
43	2	1849	x^2+x+3	$[1736, 1736, 728, 728]$	C^*
53	2	2809	x^2+x+5	$[1150, 180]$	C
67	2	4489	x^2+x+2	$[2276, 354]$	C
157	2	24649	x^2+x+6	$[2699, 2137]$	F
199	2	39601	x^2+x+6	$[21215, 9679]$	F

Table 2: Atomic latin squares of composite order.

an irreducible polynomial $\zeta(x)$ of degree r over $\mathbb{Z}_p$ with the property that, in the field of polynomials $\mathbb{Z}_p[x]$ modulo $\zeta(x)$, the polynomial x is a primitive element. This means that the non-zero elements of the field can be identified with the set $\{x, x^2, x^3, \ldots, x^{q-1}\}$ of powers of x. This allows us to adopt a shorthand which mirrors the way that polynomials were stored in the computer. Instead of writing each scaling factor as a monomial x^a we simply give the index a. For example, we use $[94, 74, 22, 2]$ as shorthand for the vector of scaling factors $[x^{94}, x^{74}, x^{22}, x^2]$.

The first three columns of Table 2 give, respectively, the values of p, r and $q = p^r$, the parameters of our field $\mathcal{F}$. Following that, we give the irreducible polynomial $\zeta(x)$ and the vector of scaling factors $\tilde{c}$.

In the final column of Table 2 we give a letter code indicating the conjugate symmetries (if any) that the atomic squares possess. The code 'T' indicates that the square equals its transpose (that is, it is symmetric in the usual sense). The code 'S' indicates that the square equals its (231) and (312) conjugates (hence it is what is called *semisymmetric*). The code 'C' indicates that the square is isomorphic to its transpose by a cyclic permutation of the scaling factors, as in Lemma 7. The code 'F' indicates that the square is isomorphic to its transpose by a cyclic permutation of the scaling factors, followed by an application of the Frobenius map, as in Lemma 8. The code 'F^2' is the same, except the Frobenius map must be applied twice. The code 'U' indicates that the square is isomorphic to its (231)-conjugate by applying the Frobenius map (and hence is also isomorphic to its (312)-conjugate). The code 'N' indicates that the square has none of the above symmetries.

It is also possible that a square might have isomorphisms additional to those predicted by Lemma 9. An asterisk is used to indicate three squares for which this occurs. The example of order 1849 is isomorphic to itself by application of the Frobenius map, then a cyclic permutation of the scaling factors. The example of order 121 has an automorphism group of size 7260, twice as large as might be expected from Lemma 9. It is not isotopic to any of its conjugates, and is currently the only known example of an atomic square of composite order with this property.

The atomic square of order 25 in Table 2 is easily converted into the example given earlier in Figure 1. The chosen encoding is that for $i = 1, 2, \ldots, 24$ the field element x^i is written as the i^{th} letter of the alphabet and zero is written as '0'. The rows and columns are written in the order of their indices $0, a, b, c, \ldots, x$. This square is isomorphic to its transpose (and hence to all of its conjugates, since it is semisymmetric) and has an automorphism group of order 100. In addition to the 50 automorphisms predicted by Lemma 9 it has an automorphism ϕ with cycles

$$(ahmt)(bgns)(cpod)(ewqk)(flrx)(ivuj).$$

Note that f, l, r and x are the fourth roots of unity. Negation (i.e. the automorphism T_{-1} from Lemma 9) is equal to ϕ^2. While the screening described in §5 was strong enough to prevent the computer reporting multiple copies of most squares, the extra symmetries of this order 25 example resulted in the computer reporting 4 isomorphic variants of the same square. If we set

$$\begin{aligned}
\tilde{c}_1 &= [15, 4, 22, 23, 2, 4, 1, 9, 2, 4, 1, 9] \\
\tilde{c}_2 &= [13, 16, 13, 16, 14, 7, 3, 7, 2, 19, 1, 9] \\
\tilde{c}_3 &= [17, 11, 17, 11, 14, 8, 3, 8, 2, 19, 1, 9] \\
\tilde{c}_4 &= [17, 11, 13, 16, 5, 8, 10, 7, 2, 21, 1, 9]
\end{aligned}$$

then all four squares $\mathcal{L}(\tilde{c}_i)$ are semisymmetric and isomorphic to each other. In addition, both $\mathcal{L}(\tilde{c}_2)$ and $\mathcal{L}(\tilde{c}_3)$ possess a symmetry of type F and $\mathcal{L}(\tilde{c}_4)$ is, like the atomic square of order 1849, isomorphic to itself by applying the Frobenius map, then a cyclic permutation of the scaling factors. We chose to use $\mathcal{L}(\tilde{c}_1)$ because of its apparent similarity to the degree 4 example $[2, 4, 1, 9]$, especially given that $x^{15} = 1 - x^2$, $x^{22} = 1 - x$ and $x^{23} = 1 - x^9$ in the field of $\mathbb{Z}_5[x]$ modulo $x^2 + x + 2$.

The computer also reported an atomic square of order 49 with the scaling factors $[27, 22, 10, 45, 21, 9, 15, 3]$, but this turns out to be isomorphic to the one given in Table 2.

The symmetries that we have identified for our atomic squares include (but are not limited to) all the symmetries which can be demonstrated solely by means of Lemmas 3, 6, 7 and 8. Some of the squares with order exceeding 200 may possess additional symmetries which could be demonstrated by other means. However, for orders $q < 200$ nauty [12] was used to check that there are no additional symmetries (either autotopisms or conjugate symmetries) other than the ones identified above. In the process it was confirmed that the two examples of order 27 come from different main classes. These two main classes are also easily distinguished by an invariant which we introduce in the next section.

7 Trains of latin squares

There are many invariants which may be used for distinguishing latin squares from different main classes. Some of these, such as the number of transversals, can only be computed in a reasonable time for small orders. Other substructures such as latin subsquares or cycles are useless for distinguishing atomic latin squares because such squares have, by definition, no non-trivial substructures of the types mentioned.

In this section we describe a new main class invariant which is useful for distinguishing main classes of atomic latin squares. We call it the train of the latin square, in analogy to a very similar invariant which is frequently used for distinguishing non-isomorphic 1-factorisations of graphs [6], [16].

As mentioned in the introduction, we can think of a latin square L of order n with index set Σ, as a set of triples in $\Sigma^3 = \Sigma \times \Sigma \times \Sigma$. The *train* of L is a directed graph with vertex set equal to Σ^3 and each vertex has outdegree 1. The arc from a vertex $(a, b, c) \in \Sigma^3$ goes to the unique vertex $(x, y, z) \in \Sigma^3$ such that (a, b, z), (a, y, c) and (x, b, c) are triples of L.

Applying isotopisms to L simply permutes the labels within each copy of Σ in the train of L, and taking conjugates of L permutes the copies of Σ themselves. Hence we have:

Lemma 11 *If L and M are latin squares from the same main class then the trains of L and M are isomorphic (as directed graphs).*

Of course, the train of L has n^3 vertices, which makes full isomorphism testing a daunting prospect even for moderately large n. Happily, for our purposes, it turns out that atomic squares are frequently distinguishable by counting the number of *sources* (vertices of indegree zero) in their trains, and we encountered no example of a pair of atomic squares from distinct main classes which could not be distinguished by counting the vertices of indegree zero and those of indegree one. Therefore, in what follows we shall not concern ourselves with any structural information other than the indegrees of vertices in the train. For each $d \geq 0$, define s_d by saying that ns_d is the number of vertices with indegree d. Let $m = \max\{d : s_d > 0\}$. We call $[s_0, s_1, \ldots, s_m]$ the *sequence of the train*. The reason for using this sequence rather than the indegree sequence $[ns_0, ns_1, \ldots, ns_m]$ is that for all latin squares of interest in this paper (namely, the squares defined by (2) and, to a lesser extent, group tables) the s_i are necessarily integers, are considerably smaller than ns_i and can be calculated more efficiently. These assertions are based on our next two lemmas.

Lemma 12 *For any $d \geq 0$ and L defined by (2), s_d is the number of vertices $(0, b, c)$ of indegree d in the train of L, where b and c are allowed to range over the index set $\mathcal{F}$ of L.*

Proof: We associate with each vertex $(0, b, c)$ the set of n vertices

$$\{(a, b + a, c + a) : a \in \mathcal{F}\} \tag{4}$$

Lemma 9 tells us that each of the n vertices in (4) has the same indegree, and each vertex (x, y, z) of the train of L is associated with a unique $(0, b, c)$, namely $(0, y-x, z-x)$. $\square$

For an example application, consider the two atomic latin squares of order 27 defined in §6. These squares, defined by their scaling factors $[20, 4]$ and $[7, 5]$ have trains with respective sequences $[260, 261, 156, 52]$ and $[208, 313, 208]$. Hence these squares belong to two different main classes, by Lemma 11.

In the case of prime order we shall be interested in knowing that our new examples of atomic latin squares do not belong to the main class of the cyclic group. One way to be sure of this is to employ the following result.

Lemma 13 *Let L be a latin square derived from the Cayley table of a finite group G. For each $g \in G$ define $f(g)$ to be the number of solutions $x \in G$ to the equation $x^2 = g$ (in other words $f(g)$ is the number of times g occurs on the main diagonal of L). Define ϖ_i to be the number of $g \in G$ for which $f(g) = i$. Then the sequence of the train of L is* $[n\varpi_0, n\varpi_1, n\varpi_2, \ldots]$.

Proof: Let (a, b, c) be a general vertex of the train of L and let d be any solution in G to $d^2 = abc^{-1}$. The arc from vertex (x, y, z) points to (a, b, c) if and only if $xy = c$, $xb = z$ and $ay = z$. These equations are satisfied if $x = dcb^{-1}$, $y = x^{-1}c$ and $z = xb$. Moreover, this is essentially the only way they can only be satisfied. To see this, substitute $x = Xcb^{-1}$ into $ax^{-1}c = ay = z = xb$ to obtain $abc^{-1}X^{-1}c = Xc$ and hence $X^2 = abc^{-1}$. Thus the indegree of (a, b, c) is equal to $f(abc^{-1})$. For each $g \in G$ there are n^2 vertices (a, b, c) such that $abc^{-1} = g$, and these vertices together contribute n towards the $f(g)^{\text{th}}$ entry in the sequence of the train of L. $\square$

It is well known that in groups of odd order every element has a square root, so $f(g) = 1$ uniformly over $g \in G$ in that case. Hence:

Corollary 1 *If T is the train of a latin square derived from the Cayley table of a finite group G of odd order then the sequence of T is* $[0, n^2]$.

In particular this shows that the sequence of a train cannot distinguish between two non-isomorphic groups of the same odd order. However, this last result will prove very useful for establishing that a given latin square L of odd order is not based on a group. To do this it suffices to find a single source in the train of L.

8 Atomic squares of prime order

A computer search as described in §5 was used to find numerous new atomic latin squares of prime order. The only difference from the case of composite orders was that field arithmetic was handled with integers rather than polynomials. However, to be consistent with the other version of the program we stored all non-zero elements of the field as powers of a primitive root ω, which was found by trial and error. Again, we quote scaling factors by listing the indices only, so $[8, 6]$ is shorthand for $[\omega^8, \omega^6]$.

p	ω	$\tilde{c}$	Sym	Train
11	2	$[8,6]$	T	40
13	2	$[5,3]$	C	48
19	2	$[9,1]$	T	90
19	2	$[12,2]$	N	117
19	2	$[14,6,9,7,5,1]$	T	102
23	5	$[8,6]$	T	$176, 243$
23	5	$[18,12]$	T	154
23	5	$[14,2]$	N	$176, 221$
41	6	$[31,37,7,5]$	C	500
43	3	$[37,2,36,26,24,1]$	S	588
47	5	$[6,4]$	N	736
53	2	$[7,5]$	C	$832, 1301$
53	2	$[48,8]$	C	$832, 1353$
53	2	$[44,14]$	C	1092
59	2	$[51,35]$	T	928
67	2	$[31,13]$	T	1452
73	5	$[51,11]$	C	2088
73	5	$[35,13]$	C	2016
83	2	$[62,44]$	T	2460
97	5	$[60,26]$	C	3072
101	2	$[47,35]$	C	3200
101	2	$[91,61]$	C	3400
103	5	$[42,22]$	T	2448
103	5	$[22,6]$	N	2295
103	5	$[70,79,4]$	R	3570
107	2	$[30,14]$	N	3657
109	6	$[99,41]$	C	3996
109	6	$[107,75]$	C	3780
127	3	$[96,68]$	T	3906
127	3	$[81,69,39]$	R	5796
127	3	$[72,63,54]$	R	5544
131	2	$[81,41]$	T	5460
139	2	$[119,3]$	T	5658
139	2	$[109,85]$	T	6486
149	2	$[57,43]$	N	8658

Table 3: Atomic latin squares of prime order < 150.

p	ω	$\tilde{c}$	Sym	Train
151	6	$[94, 88, 43]$	S	7500
157	5	$[118, 72, 149, 17]$	T	8034
167	5	$[86, 14]$	T	9296
173	2	$[105, 77]$	C	8772
179	2	$[149, 129]$	T	7654
181	2	$[83, 69]$	C	6840
191	19	$[134, 34]$	T	11970
191	19	$[135, 107]$	T	13870
211	2	$[15, 11]$	T	15960
211	2	$[108, 86]$	T	17640
223	3	$[30, 20]$	T	11100
229	6	$[156, 98]$	C	19380
239	7	$[220, 68]$	T	14518
241	7	$[140, 62]$	C	13680
263	5	$[228, 70]$	T	15196
263	5	$[258, 82]$	T	15720
269	2	$[187, 187, 155, 155]$	T	21708
277	5	$[269, 141]$	C	16284
283	3	$[199, 145]$	T	16920
307	5	$[283, 191]$	T	20196
349	2	$[307, 283]$	C	40368
367	6	$[192, 34]$	T	47580
367	6	$[267, 35]$	T	50508
367	6	$[199, 107]$	T	47946
373	2	$[366, 296]$	C	54312
383	5	$[224, 12]$	N	51379
397	5	$[285, 257]$	C	34848

Table 4: Atomic latin squares of prime orders in the range [150,400].

In Table 3 and Table 4 we summarise the atomic squares of orders up to 400 found by our program. The first three columns give the order of the square, the primitive root used, and the vector $\tilde{c}$ of scaling factors. In the fourth column we again give a letter code indicating the conjugate symmetries (if any). The codes 'T', 'S' and 'C' have the same meanings as before. The code 'R' indicates that the square is isomorphic to its (231)-conjugate by a cyclic permutation of the scaling factors. The code 'N' indicates that the square has none of the above symmetries. In the final column we give enough of the sequence of the train of the square to distinguish it from all other currently known examples. In most cases this means just giving the first element s_0 of the sequence. Recall from the corollary to Lemma 13 that if $s_0 \neq 0$ then the square cannot be group-based. In particular, the examples in Table 3 and Table 4 are all from a main class distinct from that of the cyclic group of the same order.

Table 3 and Table 4 represents merely the start of the list of examples found by the computer, which would be much too lengthy to give in full. Considering only examples of degree 2 and which have a T or C type symmetry, the program found 256 main classes of atomic latin squares of prime orders below 10000, and continued to find many more beyond that point.

The computer reported two examples of order 11, namely the one given in the table and $[5, 3, 4, 9, 3, 3, 3, 6, 3, 1]$. However, these two examples belong to the same main class. Similarly, it reported $[4, 2, 4, 4, 10, 4, 4, 4, 9, 11, 3, 1]$, which is a variation of the square of order 13 given in the table. We were unable to exhaustively check for any larger order p whether other squares could be written, in a non-degenerate way, using an orthomorphism of degree $p - 1$.

The square of order 19 with scaling factors [12,2] is currently the smallest example of an atomic square which is not isotopic to any of its conjugates (no such examples were known prior to this paper).

9 Perfect 1-factorisations

A 1-*factor* (also called a perfect matching) of a graph G is set of edges of G which between them include every vertex exactly once. A 1-*factorisation* of G is a partition of the edges of G into 1-factors. A 1-factorisation is said to be *perfect* if the union of any two 1-factors in it is a Hamiltonian cycle. For background information on these concepts see Seah [15] or Wallis [16].

It is well known that a perfect 1-factorisation of the complete graph K_{n+1} can be used to write down a symmetric symbol-hamiltonian latin square of order n and vice versa. The relationship between these two combinatorial objects involves some subtleties, which are discussed fully in [19]. These subtleties all revolve around questions of isomorphism though, so they do not affect our present purpose, which is simply to establish existence for as many orders as possible.

There are two classical infinite families of perfect 1-factorisations of complete graphs. They show existence for, respectively, K_{p+1} and K_{2p} whenever p is an odd prime. Recently another infinite family was found [3], but it does not yield constructions for any new orders.

In addition to these infinite families, existence has been shown for K_{n+1} for some small values of n, all of which are either (i) less than 40 or (ii) a prime power. The complete list, taken from [15] together with [21] is

$$\{15, 27, 35, 39, 49, 125, 169, 243, 343, 729, 1331, 1369, 1849, 2197, \\ 3125, 6859, 12167, 16807, 29791\}. \tag{5}$$

Below we describe, in the same format used in the previous sections, constructions for symmetric symbol hamiltonian latin squares of order q, for every prime power q in (5) as well as for the following orders:

$$\{25^*, 81^*, 121^*, 361^*, 529, 625^*, 841^*, 2809, 3481^*, 3721^*, 4489, 6889, 10201^*, 11449, \\ 11881, 15625, 17161^*, 19321^*, 22201, 24389, 24649, 26569, 29929, 32041, 32761^*, \\ 38809, 44521, 50653, 51529, 52441, 63001, 72361, 76729, 78125, 79507, 103823, \\ 148877, 161051, 205379, 226981, 300763, 357911, 371293, 493039, 571787\}.$$

Orders with asterisks on them in this last list were already known to exist because of the K_{2p} construction (and may have other published constructions as well). All other orders represent new existence results.

For the case $r = 2$, we have the examples in Table 5.

For the case $r = 3$, both the atomic latin squares of order 27 quoted in §6 are symmetric and hence give perfect 1-factorisations of K_{28}. We also found the examples in Table 6, which include all cases where $p < 100$ and $p \not\equiv 1 \bmod 8$.

For $4 \leq r \leq 7$, the examples found by the computer are given in Table 7.

We remark that for all constructions in this section, Lemma 3 can be used to confirm that the latin squares are symmetric. Indeed, that lemma greatly speeded up the computer search since it shows that we only need consider the case when u is odd, and that in that case one half of the coefficients in $\tilde{c}$ are determined by the other half.

The two smallest prime powers q for which perfect 1-factorisations of K_{q+1} are currently unknown are now 289 and 961. To use the methods of the current paper to find these factorisations would require orthomorphisms of degrees at least 32 and 64 respectively.

Note. After writing this paper the author learnt of a preprint by Dinitz and Dukes [5] and of separate unpublished work by Volker Leck, announced in [10]. In both cases, quotient coset starters were used to construct perfect 1-factorisations for a number of the orders which are claimed as new in the present paper. As mentioned in §2, quotient coset starters are essentially the same method as used here, so it seems to be a case of an idea whose time was due.

p	q	$\zeta(x)$	$\tilde{c}$
5	25	x^2+x+2	$[7, 21, 19, 15, 8, 19, 21, 2]$
7	49	x^2+x+3	$[18, 37, 9, 25, 20, 18, 29, 29,$
			$17, 20, 43, 31, 37, 17, 1, 1]$
11	121	x^2+x+7	$[93, 115, 15, 28, 90, 78, 44, 1]$
13	169	x^2+x+1	$[124, 117, 69, 110, 103, 24, 20, 1]$
19	361	x^2+x+2	$[330, 213, 321, 218, 219, 295, 27, 1]$
23	529	x^2+x+7	$[476, 231, 167, 155, 115, 317, 256, 136,$
			$37, 188, 410, 351, 143, 6, 3, 1]$
29	841	x^2+x+3	$[218, 517, 293, 234, 432, 574, 35, 1]$
37	1369	x^2+x+5	$[585, 393, 330, 424, 361, 185, 17, 1]$
43	1849	x^2+x+3	$[1089, 1612, 241, 1663, 1544, 1706, 16, 1]$
53	2809	x^2+x+5	$[406, 1619, 2456, 1370, 173, 2426, 5, 1]$
59	3481	x^2+x+2	$[305, 1602, 141, 1858, 1650, 2613, 14, 1]$
61	3721	x^2+x+2	$[1197, 2851, 2537, 1982, 822, 338, 8, 1]$
67	4489	x^2+x+12	$[3673, 4108, 1340, 4260, 1680, 2374, 20, 1]$
83	6889	x^2+x+2	$[1655, 6480, 332, 3610, 1431, 3807, 4, 1]$
101	10201	x^2+x+3	$[2265, 3884, 3949, 5896, 3880, 757, 16, 1]$
107	11449	x^2+x+5	$[5160, 5673, 3883, 2900, 2696, 190, 32, 2]$
109	11881	x^2+x+6	$[4115, 5889, 171, 171, 6581, 3551, 1, 1]$
131	17161	x^2+x+14	$[8301, 1958, 13482, 1552, 8005, 12289, 76, 1]$
139	19321	x^2+x+1	$[1513, 16898, 11245, 9938, 12878, 489, 30, 1]$
149	22201	x^2+x+3	$[5433, 7676, 8164, 21616, 2928, 19682, 12, 1]$
157	24649	x^2+x+6	$[21516, 19316, 14337, 8123, 22533, 11362, 10, 3]$
163	26569	x^2+x+11	$[24870, 206, 2657, 1983, 14809, 14911, 19, 1]$
173	29929	x^2+x+5	$[1311, 15757, 3955, 5877, 14781, 16079, 13, 3]$
179	32041	x^2+x+7	$[10770, 18434, 30738, 28500, 27573, 30728, 8, 1]$
181	32761	x^2+x+18	$[9019, 9115, 16855, 31186, 31163, 18349, 8, 1]$
197	38809	x^2+x+3	$[5856, 23436, 38224, 35243, 27776, 17394, 19, 4]$
211	44521	x^2+x+3	$[7849, 22609, 410, 42594, 28439, 5690, 24, 1]$
227	51529	x^2+x+5	$[47860, 41567, 33795, 33795, 39131, 14692, 12, 12]$
229	52441	x^2+x+6	$[154, 23003, 40875, 40875, 15645, 37966, 1, 1]$
251	63001	x^2+x+19	$[48436, 51053, 2013, 17928, 19601, 10940, 4, 1]$
269	72361	x^2+x+2	$[70029, 48715, 60292, 60292, 25134, 56126, 18, 18]$
277	76729	x^2+x+11	$[50710, 46554, 3880, 62852, 37552, 47940, 26, 22]$

Table 5: The case $r = 2$.

p	q	$\zeta(x)$	$\tilde{c}$
5	125	x^3+3x+2	$[82, 84, 58, 4]$
7	343	x^3+3x+2	$[321, 1]$
11	1331	x^3+x+4	$[890, 36]$
13	2197	x^3+x+6	$[1687, 301, 410, 2]$
19	6859	x^3+x+4	$[336, 2]$
23	12167	x^3+x+3	$[4852, 66]$
29	24389	x^3+x+11	$[1726, 3768, 7130, 4]$
31	29791	x^3+x+14	$[20861, 125]$
37	50653	x^3+x+13	$[7825, 38009, 28181, 1]$
43	79507	x^3+x+14	$[43865, 291]$
47	103823	x^3+x+4	$[67515, 45]$
53	148877	x^3+x+5	$[84913, 85054, 9840, 17]$
59	205379	x^3+x+3	$[121588, 352]$
61	226981	x^3+x+17	$[222881, 104322, 130160, 5]$
67	300763	x^3+x+6	$[131844, 102]$
71	357911	x^3+x+8	$[284564, 508]$
79	493039	x^3+x+9	$[133959, 297]$
83	571787	x^3+x+7	$[527591, 287]$

Table 6: The case $r = 3$.

p	q	$\zeta(x)$	$\tilde{c}$
3	81	x^4+x+2	$[73, 32, 12, 16, 19, 16, 4, 4, 16, 51, 3, 73, 54, 73, 1, 1]$
5	625	x^4+x^2+2x+2	$[328, 308, 282, 227, 544, 244, 244, 244,$ $553, 190, 376, 178, 455, 1, 1, 1]$
3	243	x^5+2x+1	$[95, 11]$
5	3125	x^5+4x+2	$[404, 1685, 2583, 8]$
7	16807	x^5+x+4	$[14715, 59]$
11	161051	x^5+x^2+x+4	$[94526, 86]$
13	371293	x^5+4x+2	$[233293, 189881, 264357, 1]$
3	729	x^6+x+2	$[367, 145, 210, 6, 711, 113, 111, 1]$
5	15625	x^6+x+2	$[9591, 9728, 12498, 11874, 8690, 14037, 5, 1]$
5	78125	x^7+3x+2	$[36939, 7047, 12756, 6]$

Table 7: The cases $r = 4, 5, 6$ and 7.

References

[1] B. A. Anderson, Some perfect 1-factorizations, *Cong. Numer.* **17** (1976), 79–91.

[2] D. Bryant, B. M. Maenhaut and I. M. Wanless, A family of perfect factorisations of complete bipartite graphs, *J. Combin. Theory Ser. A* **98** (2002), 328–342.

[3] D. Bryant, B. M. Maenhaut and I. M. Wanless, New families of atomic Latin squares and perfect one-factorisations, *J. Combin. Theory Ser. A*, to appear.

[4] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[5] J. H. Dinitz and P. Dukes, Some new perfect one-factorizations of the complete graph, University of Vermont Mathematics Research Report No. 2004-01.

[6] J. H. Dinitz and W. D. Wallis, Trains: an invariant for one-factorizations, *Ars Combin.* **32** (1991), 161–180.

[7] A. B. Evans, *Orthomorphism graphs of groups*, Lect. Notes in Math. **1535**, Springer, 1992.

[8] A. B. Evans, Cyclotomy and orthomorphisms: a survey, *Util. Math.* **101** (1994), 97–107.

[9] A. V. Geramita, J. Seberry, Orthogonal designs: Quadratic forms and Hadamard matrices, Lecture Notes in Pure and Applied Mathematics **45**, Marcel Dekker, New York, 1979.

[10] V. Leck, quoted in "New results in combinatorial designs", http://www.emba.uvm.edu/∼dinitz/newresults.html

[11] B. M. Maenhaut and I. M. Wanless, Atomic latin squares of order eleven, *J. Combin. Des.* **12** (2004), 12–34.

[12] B. D. McKay, *nauty* User's Guide (Version 1.5), Australian National University, Computer Science Technical Report TR-CS-90-02.

[13] E. J. Morgan, A. P. Street and J. S. Wallis, Designs from cyclotomy, *Lect. Notes in Math.* **560** (1975), 158–176.

[14] P. J. Owens and D. A. Preece, Some new non-cyclic latin squares that have cyclic and Youden properties, *Ars Combin.* **44** (1996), 137–148.

[15] E. Seah, Perfect one-factorizations of the complete graph—a survey. *Bull. Inst. Combin. Appl.* **1** (1991), 59–70.

[16] W. D. Wallis, *One-factorizations*, Math. Appl. 390, Kluwer, Dordrecht, 1997.

[17] I. M. Wanless, Perfect factorisations of bipartite graphs and latin squares without proper subrectangles, *Electron. J. Combin.* **6** (1999), R9, 16 pp.

[18] I. M. Wanless, Diagonally cyclic latin squares, *European J. Combin.*, **25** (2004), 393–413.

[19] I. M. Wanless and E. C. Ihrig, Symmetries that latin squares inherit from 1-factorizations, *J. Combin. Des.* **13** (2005), 157–172.

[20] K. Yamamoto, Generation principles of latin squares, *Bull. Inst. Internat. Statist.* **38** (1961), 73–76.

[21] J. Z. Zhang, Some results on perfect 1-factorizations of K_{2n}, *Dianzi Keji Daxue Xuebao* **21** (1992), 434–436.