Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Applied Mathematics 145 (2005) 349–357
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

# Equivalence classes of matchings and lattice-square designs

William Y.-C. Chen[a], David C. Torney[b,1]

[a] *Center for Combinatorics, LPMC, Nankai University, Tianjin 300071, PR China*
[b] *Theoretical Division, T-10 Mailstop K710, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*

Received 5 July 2000; received in revised form 28 August 2003; accepted 25 February 2004

**Abstract**

We enumerate nonisomorphic lattice-square designs yielded by a conventional construction. Constructed designs are specified by words composed from finite-field elements. These words are permuted by the isomorphism group in question. The latter group contains a direct-product subgroup, acting, respectively, upon the positions and identities of the finite-field elements. We review enumeration theory for such direct-product groups. This subgroup is a direct product of a hyperoctahedral and a dihedral group, with the orbits of the hyperoctahedral group, acting on the positions of the field elements, interpretable as perfect matchings. Thus, the enumeration of dihedral equivalence classes of perfect matchings provides an upper bound on the number of nonisomorphic, constructed designs. The full isomorphism group also contains non-direct-product elements, and the isomorphism classes are enumerated using Burnside's Lemma: counting the number of orbits of a normal subgroup fixed by the quotient group. This approach is applied to constructed lattice-square designs of odd, prime-power order $\leqslant 13$.


*MSC:* 05A15; 05B30; 11T99; 20B99

*Keywords:* Collineation; Combinatorial enumeration; Design isomorphism; Dihedral group; Equivalence class; Finite field; Group action; Hyperoctahedral group; Isomorphism group; Linear algebra; Semidirect product; Spread

## 1. Introduction

From graph theory, a *perfect matching* is a partition of an even-size set into sets of size two, or pairs. Such perfect matchings are also denoted *complete matchings* or *spreads*. In the sequel, mention of matchings implies perfect matchings. Also, herein, $[j]$ denotes $\{1,2,\ldots,j\}$; $j \in \mathbb{N}$.

A lattice-square design of (odd) order $q$ is a collection of $(q+1)/2$ square matrices of order $q$. The entries of each matrix constitute a set $\Omega$, of size $q^2$. The defining characteristic of the design is that all unordered pairs of the elements of $\Omega$ occur precisely once in the individual rows and columns of its matrices [4,6].

The matrices of lattice-square designs could be used to specify the arrangement of DNA clones in square arrays [8]. Then, the rows and columns of these matrices would constitute practical "groupings" for group testing [7, Section V.6] because such groupings would be easy to implement in the laboratory using available plastic-ware.

In any case, there exists a lattice-square design of order $q$ if and only if there exists a resolvable $(q^2, q, 1)$-BIBD [15, p. 171]. In fact, a lattice-square design is equivalent to the combination of an affine plane of the same order with a matching of the set $\{1,2,\ldots,q+1\}$—whose pairs index paired parallel classes, with the latter's lines occurring on the rows and columns of a respective matrix, prefiguring the prominence of matchings herein.

Because affine planes are derivable from projective planes and because there is a well known construction for a Desarguesian plane (cf. [17, p. 81]), lattice-square designs of odd, prime-power order $q$ are constructible using linear

[1] LAUR 00-1951.

*E-mail addresses:* chen@nankai.edu.cn (W.Y.-C. Chen), dct@lanl.gov, dtorney@earthlink.net (D.C. Torney).

0166-218X/$ - see front matter 
doi:10.1016/j.dam.2004.02.013

algebra over finite fields (viz Section 3). In fact, such a construction is seen to yield many designs, but what has previously been passed over is the number of nonisomorphic designs obtained.

The detailed definition of design isomorphism is postponed to Section 3; it will be seen that all of the constructed designs would be indistinguishable from the perspective of pooling designs because they all contain the same lines. Nevertheless, the isomorphism classes are distinguishable in other applications: for instance, when the elements of $\Omega$ designate agricultural treatments and with the design matrices specifying replications, their statistical sequelae depend upon the arrangement of the lines [6, Section 12.2].

Constructed designs are parameterized by a set of words whose letters are finite-field elements—or *marks* [3]. Transformations of designs into isomorphic, constructed designs yield a corresponding permutation representation of the isomorphism group, whose orbits, on words, represent the nonisomorphic, constructed designs. We describe these particulars in full detail in Section 3. This group is sufficiently complex to discourage closed-form enumeration of its orbits. Instead, for designs of orders 3–13, the computer program GAP was used to construct the orbits [9]. Extending Pólya enumeration theory to semidirect-product groups could greatly facilitate such enumerations.

Simpler problems, subsumed by our enumerations, are treated in modest generality in Section 2. Because, for example, a subgroup of the isomorphism group comprises the actions of the dihedral group on matchings of marks, we directly enumerate the respective number of orbits of matchings, affording an upper bound on the number of nonisomorphic constructed designs. We also enumerate the orbits of matchings under cyclic groups and, also, the orbits of ordered partitions, with block size two, under the dihedral group—orbits occurring in our subsequent enumeration of nonisomorphic designs.

## 2. Enumeration of sequences under direct-product actions

Let there be given a set of letters, each representing a color. Then, colorings of combinatorial objects are specified by words composed from these letters [13,14], with the letter at each position specifying the coloring of a respective "point" of the object.

To determine the number of distinctly colored objects one must, in general, consider at least two types of group actions. First, there is the "symmetry group" $\mathscr{G}$ of the object, taken to act on the points, and hence, on the positions of the letters. Second, there is a group $\mathscr{H}$ of letter-identity permutations, specifying equivalent alphabets (or palettes). The isomorphism group is the direct product of these two groups, say, $\mathscr{G} \otimes \mathscr{H}$, acting on a Cartesian product: the set of letter positions $\times$ the set of letter identities, thus, having natural actions on words. Note that direct-product groups have been considered in the context of combinatorial enumeration [2,14]; we focus on a special case.

For the sequel, we need only address sets of words containing all arrangements of the letters of a given alphabet: $S(m)$ denotes the set of all $m$-sequences having distinct letters from $[m]$, with $m \in \mathbb{N}$. To apply the Burnside Lemma, we require $F(\gamma\eta)$: the number of elements of $S(m)$ fixed by $\gamma\eta$, with $\gamma\eta \in \mathscr{G} \otimes \mathscr{H}$. Recall that the *cycle structure* of a permutation equals $1^{k_1}2^{k_2}\cdots m^{k_m}$: indicating that there are $k_i$ cycles of length $i$ in the decomposition of this permutation into cycles.

**Theorem 1.** *If the cycle structure of $\gamma$ is not the same as $\eta$, $F(\gamma\eta)$ equals zero. Otherwise,*

$$F(\gamma\eta) = \prod_i k_i! i^{k_i}.$$

*Here, the product is over the lengths, $i$, of the cycles in, say, $\gamma$, of multiplicity $k_i$.*

**Proof.** For an $m$-sequence of distinct letters to be fixed by $\gamma\eta$, the actions of $\gamma$ and of $\eta$ must be equal and opposite. This is evidently possible only if their cycle structures are identical: i.e. for every $i$, equality holds for the $k_i$'s. If so, then, for all $i$, each of the $k_i!$ pairings of $i$-cycles, with one cycle from $\gamma$ and the other from $\eta$, specifies $\prod_i i^{k_i}$ $m$-sequences which are fixed by $\gamma\eta$—which may be seen as follows. Each cycle of the positions, $(j_1\, j_2 \cdots j_i)$, paired with a cycle of the letter identities, denoted $(\ell_{j_1}\, \ell_{j_2} \cdots \ell_{j_i})$, evidently fixes the subsequence $\ell_{j_i}\, \ell_{j_{i-1}} \ldots \ell_{j_1}$: letter $\ell_{j_i}$ occurs at position $j_1$, letter $\ell_{j_{i-1}}$ occurs at position $j_2$, and so on, and this pair of cycles also plainly fixes any cyclic permutation of this subsequence. □

### 2.1. Applications to matchings and ordered partitions

The hyperoctahedral group $\mathscr{B}_{2n}$, acting on arrangements of $[2n]$ via letters' indices, readily yields equivalence classes of $S(2n)$ corresponding to matchings. For example, $\mathscr{B}_2$ may be taken to be $\langle(1\,2)\rangle$, and, for $2 \leqslant n$, a suitable permutation representation of the hyperoctahedral group $\mathscr{B}_{2n}$ is generated by permutations $(1\,2)$, $(1\,3)(2\,4)$ and $(1\,3\cdots 2n-1)$

$(2\,4\cdots 2n)$. Thus, if an element of $S(2n)$ yields a matching via assignment of the digits at positions 1 and 2 to the first block, the digits at positions 3 and 4 to the second block, and so on, then this representation of $\mathscr{B}_{2n}$ has orbits containing all the elements of $S(2n)$ corresponding to a each matching. Therefore, the orbits of $\mathscr{B}_{2n} \otimes \mathscr{D}_{2n}$ are 1–1 with the equivalence classes of matchings under dihedral actions on the identities of the elements of the matched set.

The Burnside Lemma [12, Theorem 10.5] may be used to enumerate $D_{2n}$, the number of dihedral equivalence classes of matchings of $[2n]$; $n \in \mathbb{N}$. Here we apply Theorem 1, substituting the relevant cycle-index polynomials.

In detail, consider the permutation representation of $\mathscr{D}_{2n}$ generated by $(1\,2\ldots 2n)$ and $(1)(2\,2n)(3\,2n-1)\cdots(n\,n+2)(n+1)$. The corresponding cycle-index polynomial $Z_{\mathscr{D}_{2n}}$ is well known [5,14, p. 169]:

$$Z_{\mathscr{D}_{2n}}(x_1, x_2, \ldots, x_{2n}) = \frac{1}{4n}\sum_{k|2n}\phi(k)x_k^{2n/k} + \frac{1}{4}(x_2^n + x_1^2 x_2^{n-1}), \tag{1}$$

where $\phi(k)$ denotes the Euler totient function. The construction of $\mathscr{B}_{2n}$—as the wreath product $\mathscr{S}_n[\mathscr{S}_2]$ [14, p. 178]—yields its cycle-index polynomial:

$$Z_{\mathscr{B}_{2n}}(x_1, x_2, \ldots, x_{2n}) = \sum_{(i)} \frac{(x_1^2 + x_2)^{i_1}(x_2^2 + x_4)^{i_2}\cdots(x_j^2 + x_{2j})^{i_j}}{i_1!2^{i_1}\quad i_2!4^{i_2}\quad\cdots\quad i_j!(2j)^{i_j}}.$$

Here, $(i)$ indicates that the range of summation is restricted to distinct sequences of non-negative, integral indices $i_\ell$; $1 \leqslant \ell \leqslant n$, satisfying $\sum_{\ell=1}^{n} \ell i_\ell = n$: i.e. the unordered, integer partitions of $n$. Also, for a given sequence of indices, $j$ denotes the index of the largest nonzero $i_\ell$.

Then, the Burnside Lemma yields $D_{2n}$, in terms of a sum of $F(\beta\delta)$ over $\beta\delta \in \mathscr{B}_{2n} \otimes \mathscr{D}_{2n}$:

$$D_{2n} = \frac{1}{4n}\left\{ g(2n)n! + \sum_{\ell|2n} b(\ell, 2n)d(\ell, 2n)\,(2n/\ell)!\ell^{2n/\ell} \right\} \tag{2}$$

with

$$g(2n) = \sum_{0\leqslant i,j:i+2j=n} \frac{i}{i!j!},$$

$$b(\ell, 2n) = \begin{cases} \displaystyle\sum_{0\leqslant i,j:i+2j=2n/\ell} \frac{1}{\ell^i i!(2\ell)^j\ j!}, & \ell \equiv 0 \,(\mathrm{mod}\, 2), \\ \dfrac{1}{(2\ell)^{n/\ell}\ (n/\ell)!}, & \ell \equiv 1 \,(\mathrm{mod}\, 2), \ \text{and} \end{cases}$$

$$d(\ell, 2n) = \phi(\ell) + n\delta_{\ell 2},$$

$n \in \mathbb{Z}$, where the Kronecker delta $\delta_{\ell 2}$ equals unity if $\ell = 2$ and equals zero otherwise. The function $g(2n)$ is derived from the right-hand monomial of $Z_{\mathscr{D}_{2n}}$, identifying the coefficients of the corresponding monomial in $Z_{\mathscr{B}_{2n}}$ and using Theorem 1. The function $d(\ell, 2n)$ similarly incorporates the remaining terms of $Z_{\mathscr{D}_{2n}}$, and the function $b(\ell, 2n)$ arises from the sum of the coefficients for the corresponding terms of $Z_{\mathscr{B}_{2n}}$. Numerical values of $D_{2n}$ follow:

| $2n$ | $D_{2n}$ | $C_{2n}$ |
|---|---|---|
| 2 | 1 | 1 |
| 4 | 2 | 2 |
| 6 | 5 | 5 |
| 8 | 17 | 18 |
| 10 | 79 | 105 |
| 12 | 554 | 902 |
| 14 | 5283 | 9749 |
| 16 | 65,346 | 127,072 |
| 18 | 966,156 | 1,915,951 |
| 20 | 16,411,700 | 32,743,182 |

This table also includes analogously derived values of $C_{2n}$: the number of equivalence classes of matchings of $[2n]$—with the cyclic group $\mathscr{Z}_{2n} \subset \mathscr{D}_{2n}$ permuting the letter identities.

The application of Theorem 1 to ordered partitions of a $2n$-set into blocks of size two is simpler because the cycle-index polynomial of $\mathscr{Z}_2^n$ (which replaces $Z_{\mathscr{B}_{2n}}$) equals $((x_1^2 + x_2)/2)^n$. Applying the Burnside Lemma to $\mathscr{Z}_2^n \otimes \mathscr{D}_{2n}$ yields

"fixing monomials" of the forms $x_1^2x_2^{n-1}$, $x_2^n$ and $x_1^{2n}$. Substituting the coefficients derived from the product of cycle-index polynomials yields the number of orbits of these ordered partitions under the action of the dihedral group:

$$P_{2n} = \frac{n!}{4}\left(2+\frac{1}{n}\right) + \frac{(2n)!}{2^{n+2}n};\ n \in \mathbb{Z}. \tag{3}$$

## 3. Nonisomorphic, constructed lattice-square designs

We denote the marks of $GF(q)$ by $u_k$, $0 \leqslant k \leqslant q-1$, with $u_0$ and $u_1$ denoting the additive and multiplicative identities, respectively [3]. Furthermore, with $\zeta$ denoting a primitive root of $GF(q)$, we take $u_\ell = \zeta^{\ell-1}$; $1 \leqslant \ell \leqslant q-1$.

The entries of lattice-square-design matrices are taken to be the ordered pairs, $u_i\ u_j$, of marks; $0 \leqslant i,j < q$. Thus, our $\Omega = \{u_iu_j{:}0 \leqslant i,j < q\}$. The following inclusive definition is fundamental to our isomorphism classes of constructed designs (viz Sections 3.1 and 3.4).

**Definition 1.** Two lattice-square-design matrices are *equivalent* whenever the following construct is identical for both: a 2-set of sets, the former containing, as its elements, the set of unordered pairs of elements occurring in its rows and the set of unordered pairs occurring in its columns.

A lattice-square design may, without loss of generality, include the *trivial* matrix $\mathbf{T}_q \stackrel{\text{def}}{=} [u_i\,u_j]$; $0 \leqslant i,j < q$. For instance, $\mathbf{T}_q$ could evidently be derived from any matrix in the design by a permutation of the identities of the points of $\Omega$. Therefore, we assume that $\mathbf{T}_q$ (or an equivalent matrix) occurs in the design, anchoring our studies of isomorphism. We construct the remaining $(q-1)/2$ *nontrivial* matrices, denoted $\mathbf{M}$ (indexed 1 through $(q-1)/2$) as follows. Each of our nontrivial matrices is parameterized by four marks, say, $u_a, u_b, u_c$ and $u_d$: all unequal to $u_0$. In detail, let

$$\mathbf{M}^{(a,b;c,d)} \stackrel{\text{def}}{=} [u_au_i + u_bu_j\ u_cu_i + u_du_j]; \qquad 0 \leqslant i,j < q. \tag{4}$$

It is straightforward to establish the following result.

**Theorem 2.** *Two nontrivial matrices* $\mathbf{M}^{(a,b;c,d)}$ *and* $\mathbf{M}^{(a',b';c',d')}$ *may both occur in a lattice-square design—also containing a matrix equivalent to* $\mathbf{T}_q$*—whenever the four ratios* $u_a/u_c, u_b/u_d, u_{a'}/u_{c'}$ *and* $u_{b'}/u_{d'}$ *are distinct.*

Proof is omitted. As a consequence of Theorem 2, of the $2(q-1)$-sequences of (nonzero) marks,

$$\upsilon = u_{a_1}u_{b_1}u_{c_1}u_{d_1}u_{a_2}u_{b_2}u_{c_2}u_{d_2}\cdots u_{a_{(q-1)/2}}u_{b_{(q-1)/2}}u_{c_{(q-1)/2}}u_{d_{(q-1)/2}}, \tag{5}$$

$(q-1)^{(q-1)}(q-1)!$ specify lattice-square designs, and the set of the latter $\upsilon$'s is denoted $\Upsilon_q$. (In the sequel, we also consider the elements of $\Upsilon_q$ to be $(q-1)/2$-sequences of 4-sequence "blocks": the latter being the consecutively occurring mark parameters for the individual nontrivial matrices.)

What remains to be seen is: How many nonisomorphic designs are engendered by $\Upsilon_q$?

Note that all the designs of Theorem 2 contain the same "lines": the matrices' rows and columns, each considered as a $q$-set of the respective elements of $\Omega$. This follows from pairs of points on the lines of design matrices differing by $u_{a_\ell}\zeta^\alpha u_{c_\ell}\zeta^\alpha$ or $u_{b_\ell}\zeta^\alpha u_{d_\ell}\zeta^\alpha$; $\ell \in [(q-1)/2]$; $0 \leqslant \alpha < q-1$; thus, only the ratios $u_{a_\ell}/u_{c_\ell}$ and $u_{b_\ell}/u_{d_\ell}$ distinguish these lines. As the arrangement of these lines is plainly immaterial to the aforementioned pooling experiments, all of the designs of Theorem 2 are interchangeable for our application.

### 3.1. Constructed lattice-square design isomorphism

**Definition 2.** Two lattice-square designs are *isomorphic* whenever a permutation of the elements of $\Omega$, in one design, yields a set of matrices which may be put in 1–1 correspondence with equivalent matrices in the other design (cf. Definition 1).

All design isomorphisms permute the elements of $\Upsilon_q$ and constitute a group [11, p. 28]. Such permutation groups are denoted $\mathscr{W}_q$, with $q$ a power of an odd prime. By definition, the $\mathscr{W}_q$-orbits on $\Upsilon_q$ represent the nonisomorphic designs.

Some elements of $\mathscr{W}_q$ are easily accommodated by the theory of Section 2. Others, notably those which map a specified nontrivial matrix onto $\mathbf{T}_q$, are not inducible by letter-identity and letter-position permutations because their action is $\upsilon$ dependent. As will be seen, however, the foregoing enumerations lead to simplifications in the enumeration of nonisomorphic designs.

### 3.2. $\mathscr{W}_q$: the group of constructed-design isomorphisms

We begin by specifying the "elemental" elements of $\mathscr{W}_q$. These elemental elements yield, by their combination, all its elements. Throughout, the action of a product of elements is taken to be from right to left: the rightmost acts first, etc.

A first class of elemental elements of $\mathscr{W}_q$ independently modifies individual nontrivial matrices, hence individual 4-sequence blocks in (5). These elements correspond to implementable equivalence transformations of individual matrices: cyclic row and column permutations and transposition about the main diagonal. These elements are of two types, depending on whether or not they involve transposition:

$$\lambda_\ell(u_{\rho_\ell}, u_{\chi_\ell}) : \Upsilon_q \to \Upsilon_q : u_{a_\ell}\ u_{b_\ell}\ u_{c_\ell}\ u_{d_\ell} \mapsto u_{\rho_\ell}u_{a_\ell}\ u_{\chi_\ell}u_{b_\ell}\ u_{\rho_\ell}u_{c_\ell}\ u_{\chi_\ell}u_{d_\ell}$$

and

$$\gamma_\ell\lambda_\ell(u_{\rho_\ell}, u_{\chi_\ell}) : \Upsilon_q \to \Upsilon_q : u_{a_\ell}\ u_{b_\ell}\ u_{c_\ell}\ u_{d_\ell} \mapsto u_{\rho_\ell}u_{b_\ell}\ u_{\chi_\ell}u_{a_\ell}\ u_{\rho_\ell}u_{d_\ell}\ u_{\chi_\ell}u_{c_\ell}.$$

Here, $\ell \in [(q-1)/2]$; $u_{\rho_\ell}$ and $u_{\chi_\ell}$ are any nonzero marks; and both mappings fix the remaining blocks: $u_{a_k}\, u_{b_k}\, u_{c_k}\, u_{d_k}$; $1 \leqslant k \neq \ell \leqslant (q-1)/2$. (They plainly also fix $\{u_{a_\ell}/u_{c_\ell}, u_{b_\ell}/u_{d_\ell}\}$).

A second class of elemental elements of $\mathscr{W}_q$ maps $\mathbf{T}_q$ onto an equivalent matrix by implementable collineations: mappings of its rows and columns to its rows and columns. These maps are also of two types, depending on whether or not they involve transposition of $\mathbf{T}_q$:

$$\Lambda(u_\rho) : \Upsilon_q \to \Upsilon_q : u_{a_k}u_{b_k}u_{c_k}u_{d_k} \mapsto u_\rho u_{a_k}\ u_\rho u_{b_k}\ u_{c_k}\ u_{d_k};\ \ \forall k \in [(q-1)/2]$$

and

$$\Gamma\Lambda(u_\rho) : \Upsilon_q \to \Upsilon_q : u_{a_k}u_{b_k}u_{c_k}u_{d_k} \mapsto u_\rho u_{c_k}\ u_\rho u_{d_k}\ u_{a_k}\ u_{b_k};\ \ \forall k \in [(q-1)/2].$$

Here, $u_\rho$ is any nonzero mark, and all blocks of $\upsilon$ are similarly modified. Thus, $\Gamma$ interchanges the $u_{a_k}$'s with the respective $u_{c_k}$'s and the $u_{b_k}$'s with the respective $u_{d_k}$'s. (The reason for not also including elements multiplying the $u_{c_k}$'s and $u_{d_k}$'s by a nonzero mark is because $\Lambda$, $\Gamma$ and elements of the first class engender such mappings.)

The third, and final, class of elemental elements of $\mathscr{W}_q$ arises as follows. For designs to maintain the parameterized form (5), acceptable, additional permutations of the elements of $\Omega$ must yield a matrix equivalent to $\mathbf{T}_q$ from a nontrivial matrix. We may use such a permutation to map the $k$th nontrivial matrix onto $\mathbf{T}_q$, with $1 \leqslant k \leqslant (q-1)/2$. The mapping taking the $k$th matrix to $\mathbf{T}_q$ is denoted $\varepsilon_k$:

$$\varepsilon_k : \Omega \to \Omega : u_{a_k}u_i + u_{b_k}u_j\, u_{c_k}u_i + u_{d_k}u_j \mapsto u_iu_j;\ 0 \leqslant i, j < q;\ \ k \in [(q-1)/2]$$

or, equivalently,

$$\varepsilon_k : \Omega \to \Omega : u_\alpha\ u_\gamma \mapsto \frac{u_{d_k}u_\alpha - u_{b_k}u_\gamma}{\Delta_k}\ \frac{u_{a_k}u_\gamma - u_{c_k}u_\alpha}{\Delta_k}, \qquad k \in [(q-1)/2]. \tag{6}$$

Here $\Delta_k$ denotes $u_{a_k}u_{d_k} - u_{b_k}u_{c_k}$ ($\neq u_0$ for admissible sequences, from Theorem 2). In particular, $\varepsilon_k$ induces

$$[u_i\, u_j] = \mathbf{T}_q \mapsto \left[\frac{u_{d_k}u_i - u_{b_k}u_j}{\Delta_k}\ \frac{u_{a_k}u_j - u_{c_k}u_i}{\Delta_k}\right]\ \ (0 \leqslant i, j < q). \tag{7}$$

It is reasonable to replace the $k$th block with the foregoing. The induced action of $\varepsilon_k$ on elements of $\Upsilon_q$ will be denoted $\mu_k$; $k \in [(q-1)/2]$. It follows that

**Definition 3.**

$$\mu_k : \Upsilon_q \to \Upsilon_q : u_{a_k}\ u_{b_k}\ u_{c_k}\ u_{d_k} \mapsto u_{d_k}/\Delta_k - u_{b_k}/\Delta_k - u_{c_k}/\Delta_k\ u_{a_k}/\Delta_k;\ \ k \in [(q-1)/2]$$

and for all $\ell : 1 \leqslant \ell \neq k \leqslant (q-1)/2$, $u_{a_\ell}\ u_{b_\ell}\ u_{c_\ell}\ u_{d_\ell} \mapsto$

$$(u_{d_k}u_{a_\ell} - u_{b_k}u_{c_\ell})/\Delta_k\, (u_{d_k}u_{b_\ell} - u_{b_k}u_{d_\ell})/\Delta_k\, (u_{a_k}u_{c_\ell} - u_{c_k}u_{a_\ell})/\Delta_k\, (u_{a_k}u_{d_\ell} - u_{c_k}u_{b_\ell})/\Delta_k.$$

The action of $\mu_k$ on a given mark will, therefore, vary depending upon on $\upsilon$ and its $k$th 4-sequence block. Thus, the $\mu$'s are insubordinate to the theory of Section 2.

### 3.3. Characteristics of $\mathscr{W}_q$

The foregoing elements yield two key subgroups of $\mathscr{W}_q$: generating $\mathscr{W}_q$ as an extension group thereof. These subgroups are characterized as follows.

The subgroup $\mathscr{M}_q$ is generated by $\mu_k$; $1 \leqslant k \leqslant (q-1)/2$. $\mathscr{M}_q$ will be seen to have order $((q+1)/2)!$ and to contain the elements $\sigma$ and $\sigma\mu_k$; $1 \leqslant k \leqslant (q-1)/2$, with $\sigma \in \mathscr{S}_{(q-1)/2}$—the symmetric group of order $(q-1)/2$—permuting the 4-sequence blocks.

To establish these results, we employ the following consequences of Definition 3:

$$\mu_k^2 = \imath;\ 1 \leqslant k \leqslant (q-1)/2$$

and

$$\mu_k \mu_\ell = (k\ell)\mu_k;\ 1 \leqslant k, \ell \leqslant (q-1)/2;\ k \neq \ell.$$

Here, $\imath$ denotes the group identity; as always, group operations on the right are applied first; and $(k\ell) \in \mathscr{S}_{(q-1)/2}$ denotes transposition of the 4-sequence block $k$ with the 4-sequence block $\ell$. It is easily established that $\mu_k \sigma = \sigma \mu_{\sigma^{-1}(k)}$; $1 \leqslant k \leqslant (q-1)/2$, and, furthermore, $\mathscr{M}_q \cong \mathscr{S}_{(q+1)/2}$.

The remaining elements of $\mathscr{W}_q$ generate $\mathscr{N}_q$, a subgroup of order $2^{(q+1)/2}(q-1)^q$, with the following specifications. It is generated by two groups: (i) a dihedral group $\mathscr{D}_{q-1}$, of order $2(q-1)$ and (ii) the direct product of $(q-1)/2$ copies of a Z-metacyclic group $\mathscr{C}_{q-1}$, each of order $2(q-1)^2$. The individual groups of (ii) correspond to the admissible equivalence transformations of individual matrices: $\lambda_k(u_{\rho_k}, u_{\chi_k})$ and $\gamma_k \lambda_k(u_{\rho_k}, u_{\chi_k})$, with $1 \leqslant k \leqslant (q-1)/2$. The $\mathscr{D}_{q-1}$ incorporates the actions of the second class of elemental elements: $\Lambda(u_\rho)$ and $\Gamma\Lambda(u_\rho)$.

Although $\mathscr{N}_q$ is not Abelian, the elements of $\mathscr{D}_{q-1}$ commute with those of $\mathscr{C}_{q-1}^{(q-1)/2}$. (Thus $\mathscr{N}_q$ is an extension of $\mathscr{C}_{q-1}^{(q-1)/2}$ by $\mathscr{D}_{q-1}$.) Collecting the foregoing notation, the elements of $\mathscr{N}_q$ are denoted

$$\Gamma^j \Lambda(u_\rho) \prod_{\ell=1}^{(q-1)/2} \gamma_\ell^{i_\ell} \lambda_\ell(u_{\rho_\ell}, u_{\chi_\ell})$$

with $i_\ell$ and $j \in \{0,1\}$, $1 \leqslant \ell \leqslant (q-1)/2$, and with all of the $\rho$'s and $\chi$'s arbitrary elements of $\{1,2,\ldots,q-1\}$. For future reference, note that

$$\Lambda(u_\rho)\Gamma \prod_{\ell=1}^{(q-1)/2} \gamma_\ell^{i_\ell} \lambda_\ell(u_{\rho_\ell}, u_{\chi_\ell}) = \Gamma\Lambda(u_\rho^{-1}) \prod_{\ell=1}^{(q-1)/2} \gamma_\ell^{i_\ell} \lambda_\ell(u_{\rho_\ell}u_\rho, u_{\chi_\ell}u_\rho), \tag{8}$$

where $\gamma^0 = \imath$.

**Theorem 3.** *$\mathscr{W}_q$ is a normal extension of $\mathscr{N}_q$ by $\mathscr{M}_q$.*

**Proof.** $\mathscr{W}_q$ is generated by $\mathscr{M}_q$ and $\mathscr{N}_q$. The commutation of $\sigma \in \mathscr{S}_{(q-1)/2}$ with elements of $\mathscr{N}_q$ is as follows:

$$\sigma\Gamma^j\Lambda(u_\rho) \prod_{\ell=1}^{(q-1)/2} \gamma_\ell^{i_{\sigma^{-1}(\ell)}} \lambda_\ell(u_{\rho_{\sigma^{-1}(\ell)}}, u_{\chi_{\sigma^{-1}(\ell)}}) = \Gamma^j\Lambda(u_\rho) \prod_{\ell=1}^{(q-1)/2} \gamma_\ell^{i_\ell} \lambda_\ell(u_{\rho_\ell}, u_{\chi_\ell})\sigma. \tag{9}$$

Commutation of the $\mu$'s with elements of $\mathscr{N}_q$ is as follows:

$$\begin{aligned}
&\mu_k\Gamma^j\Lambda(u_\rho) \prod_{\ell=1}^{(q-1)/2} \gamma_\ell^{i_\ell} \lambda_\ell(u_{\rho_\ell}, u_{\chi_\ell}) \\
&\quad = \Lambda(u_{\chi_k}/u_{\rho_k})\Gamma^{i_k}\gamma_k^j \lambda_k(u_{\chi_k}^{-1}u_\rho^{j-1}, u_{\chi_k}^{-1}u_\rho^{-j}) \left( \prod_{\ell=1}^{(q-1)/2'} \gamma_\ell^{i_\ell} \lambda_\ell(u_{\rho_\ell}/u_{\chi_k}, u_{\chi_\ell}/u_{\chi_k}) \right) \mu_k,
\end{aligned} \tag{10}$$

where $1 \leqslant k \leqslant (q-1)/2$; where the prime on the product symbol indicates that the term with $\ell = k$ is omitted; where, as above, $i_k$, $i_\ell$ and $j \in \{0,1\}$; and where $\Gamma^0 = \imath$. Transposition of $\Lambda$ and $\Gamma$, on the right-hand side ($i_k = 1$), may be effected by (8).

As all elements of $\mathscr{M}_q$ may be written either as $\sigma$ or as $\sigma\mu_k$; $1 \leqslant k \leqslant (q-1)/2$, it follows from (9) and (10) that $\mathscr{N}_q \triangleleft \mathscr{W}_q$. Because $\mathscr{M}_q \cap \mathscr{N}_q = \imath$, $\mathscr{W}_q$ is an *internal semidirect product* of $\mathscr{M}_q$ and $\mathscr{N}_q$ [16, p. 27]. □

**Corollary 1.** *The order of $\mathscr{W}_q$ is $2^{\frac{q+1}{2}}(q-1)^q\left(\frac{q+1}{2}\right)!$.*

### 3.4. Collineation groups

Because all the designs of Theorem 2 contain the same lines, all isomorphisms are collineations. Furthermore, $\mathscr{W}_q$, through its actions upon $\upsilon \in \Upsilon_q$, is primitive on blocks consisting either of rows or of columns from individual matrices, engendering new matrices by re-matching these blocks. These collineations are, in general, distinct from those in the respective group of isomorphisms of affine planes, $A\Gamma L_3(q)$ [1, p. 98] [3, Chapter XII], as may be further appreciated by means of the following example.

Consider $q=3$: $|\mathscr{W}_3|=64$ and $|A\Gamma L_3(3)|=432$, so the latter contains collineations not induced by the former. $A\Gamma L_3(3)$ acts primitively on blocks consisting of the four parallel classes containing three lines each. Its actions may be contrasted with those of the elements of $\mathscr{W}_3$, acting on the design's lines: the rows and columns of $\mathbf{T}_3$ and of the nontrivial matrix. Note that the elements of $\mathscr{N}_3$ interchange rows and columns within matrices, and there are 144 elements of $A\Gamma L_3(3)$ which effect such permutations, with some of the latter common to both groups. The cycle-index polynomial for $\mathscr{N}_3$'s action on twelve lines (rows and columns) equals

$$\frac{1}{32}(x_1^6+x_1^4x_2+x_2^3+x_2x_4)(x_1^6+2x_1^4x_2+2x_1^2x_2^2+2x_2^3+2x_2x_4).$$

The left parenthesis indicates actions on the rows and columns of $\mathbf{T}_3$, and the right parenthesis indicates actions on the rows and columns of the nontrivial matrix. Focusing on terms corresponding to the stabilizing of $\mathbf{T}_3$, only the identity occurs in $A\Gamma L_3(3)$—because the latter's non-identity elements fix at most four lines. Thus, collineations induced by elements of $\mathscr{W}_3$ may be absent from $A\Gamma L_3(3)$.

### 3.5. Enumerating the orbits of $\mathscr{W}_q$

There are numerous approaches for finding the $\mathscr{W}_q$-orbits on the sequences of (5). An elementary method would model the problem by a simple graph—whose vertices correspond to the sequences and whose edges represent equivalences. The connected components would then represent the desired equivalence classes. One could superimpose $\mathscr{W}_q$'s equivalencings upon matchings and, presumably, resolve the situation for larger $q$ than is achieved herein. At the other end of the spectrum, as illustrated through the model enumerations of Section 2.1, the Burnside Lemma could be directly applied to $\mathscr{W}_q$, acting on $\Upsilon_q$ [10], provided one knew the respective cycle-index polynomials. Herein, an intermediate course is pursued: we use numerical group-theory methods for orbit construction.

Provisionally removing the $\mu$'s from $\mathscr{W}_q$, its remaining elements are easily seen to generate a group of order $2^{(q+1)/2}(q-1)^q((q-1)/2)!$. This group has a natural matrix representation. Multiplicative factors $u_{\rho_\ell}$ and $u_{\chi_\ell}$, from $\lambda_\ell(u_{\rho_\ell},u_{\chi_\ell})$; $1\leqslant \ell \leqslant (q-1)/2$, yield that potentially distinct, constructed designs could be parameterized by a $(q-1)$-sequence of distinct, nonzero marks:

$$v = u_{\alpha_1}u_{\beta_1}u_{\alpha_2}u_{\beta_2}\cdots u_{\alpha_{(q-1)/2}}u_{\beta_{(q-1)/2}}. \tag{11}$$

We denote the set of all admissible $v$'s by $N_q$. Here, each $u_\alpha$ results from a ratio $u_a/u_c$ and each $u_\beta$ results from a ratio $u_b/u_d$. Then the actions of the $\gamma$'s, along with those of $\mathscr{S}_{(q-1)/2}$, would constitute the actions, on letter positions, of $\mathscr{B}_{q-1}$. Thus, potentially nonisomorphic, constructed designs would be parameterized by the perfect matchings of the elements of $GF(q)-u_0$:

$$\left\{\{u_{\alpha_1},u_{\beta_1}\},\{u_{\alpha_2},u_{\beta_2}\},\ldots,\{u_{\alpha_{(q-1)/2}},u_{\beta_{(q-1)/2}}\}\right\}. \tag{12}$$

$\Lambda(u_\rho)$ multiplies all marks in each $v$ by $u_\rho \neq u_0$. $\Gamma$ inverts all the marks in each $v$. Recalling that $u_\ell$ equals $\zeta^{\ell-1}$, $1\leqslant \ell \leqslant q-1$, with $\zeta$ a primitive root, the latter two classes of permutations of marks' identities constitute an action of $\mathscr{D}_{q-1}$ on matchings (cf. the generators given in Section 2.1). Therefore, the nonisomorphic designs would correspond to orbits of the group $\mathscr{B}_{q-1}\otimes\mathscr{D}_{q-1}$, with the appropriate actions on the set of arrangements of the nonzero marks of $GF(q)$. Thus, the results of Section 2 have the following implication.

**Corollary 2.** *$D_{q-1}$ constitutes an upper bound on the number of nonisomorphic lattice-square designs of order $q$.*

Reinstating the $\mu$'s, we employ the normality of $\mathscr{N}_q$ to facilitate the application of the Burnside Lemma to $\mathscr{W}_q$.

**Lemma 1** (Burnside). *Given a permutation group $\mathscr{G}$, acting on a set $U$, and $\mathscr{N}\triangleleft\mathscr{G}$, the number of $\mathscr{G}$-orbits of $U$ equals*

$$\frac{1}{[\mathscr{G}:\mathscr{N}]}\sum_{\xi}\psi_{\mathscr{N}}(\xi)$$

*with the summation over left coset representatives $\xi$ for cosets of $\mathcal{N}$, and with $\psi_{\mathcal{N}}(\xi)$ denoting the number of $\mathcal{N}$-orbits of $U$ fixed by $\xi$.*

For $\mathcal{W}_q$, the $\mathcal{N}_q$-orbits on sequences of (5) may first be found. These may clearly be taken to be orbits of $v$'s. The application of Lemma 1 is straightforward, after specifying the actions of coset representatives upon $\mathcal{N}_q$-orbits. These coset representatives may be taken to be (the subsequently defined) $\tilde{\sigma}$ and $\tilde{\sigma}\tilde{\mu}_k$, $1 \leqslant k \leqslant (q-1)/2$. These representatives may, for simplicity, taken to act upon $v$'s, from which the desired action upon $\mathcal{N}_q$-orbits may be inferred, orbits enumerated by $P_{q-1}$ (cf. (3)). It is easily seen that if one member of an orbit is transformed to another member of this orbit by an element of $\mathcal{G}/\mathcal{N}$, then all members of the orbit are so transformed by this element.

From the permutability of design matrices, $\tilde{\sigma} \in \mathcal{S}_{(q-1)/2}$ acts by permuting "blocks" of length two in (11) corresponding to individual matrices: e.g. interchanging $u_{\alpha_\ell}$ with $u_{\alpha_{\tilde{\sigma}(l)}}$ and $u_{\beta_\ell}$ with $u_{\beta_{\tilde{\sigma}(l)}}$; with $1 \leqslant \ell < m \leqslant (q-1)/2$. Also, (neglecting a factor of $-u_{d_k}/u_{c_k}$ because this is instantiated by "cyclic" actions of $\mathcal{N}_q$) $\tilde{\mu}_k$, derived from $\mu_k$, maps $N_q$ to itself; $\tilde{\mu}_k$ transforms $u_{\alpha_k}\ u_{\beta_k}$ into $u_1\ u_{\beta_k}/u_{\alpha_k}$ and transforms $u_{\alpha_\ell}\ u_{\beta_\ell}$ into $(u_{\beta_k}-u_{\alpha_\ell})/(u_{\alpha_k}-u_{\alpha_\ell})\ (u_{\beta_k}-u_{\beta_\ell})/(u_{\alpha_k}-u_{\beta_\ell})$; $1 \leqslant l \leqslant (q-1)/2$; $\ell \neq k \in [(q-1)/2]$.

Lemma 1 was evaluated using the program GAP [9] to effect construction of the orbits, yielding the following enumeration of $L_q$: the number of nonisomorphic designs of order $q$:

| $q$ | $L_q$ |
|---|---|
| 3 | 1 |
| 5 | 2 |
| 7 | 4 |
| 9 | 9 |
| 11 | 31 |
| 13 | 128 |

For example, the following two pairs of matrices represent the nontrivial matrices from the two nonisomorphic lattice-square designs of order 5. Here, we index the pairs of marks: $[u_i u_j] \mapsto [5i+j]$; $0 \leqslant i,j \leqslant 4$. Therefore, $u_1u_2u_1u_1u_3u_4u_1u_1$ yields

$$\begin{bmatrix} 0 & 11 & 17 & 23 & 9 \\ 6 & 22 & 4 & 15 & 13 \\ 12 & 19 & 8 & 1 & 20 \\ 18 & 5 & 21 & 14 & 2 \\ 24 & 3 & 10 & 7 & 16 \end{bmatrix}, \quad \begin{bmatrix} 0 & 21 & 7 & 13 & 19 \\ 16 & 12 & 4 & 5 & 23 \\ 22 & 9 & 18 & 1 & 10 \\ 8 & 15 & 11 & 24 & 2 \\ 14 & 3 & 20 & 17 & 6 \end{bmatrix}$$

and $u_1u_3u_1u_1u_2u_4u_1u_1$ yields

$$\begin{bmatrix} 0 & 16 & 22 & 8 & 14 \\ 6 & 2 & 19 & 10 & 23 \\ 12 & 9 & 3 & 21 & 15 \\ 18 & 20 & 11 & 4 & 7 \\ 24 & 13 & 5 & 17 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 21 & 7 & 13 & 19 \\ 11 & 2 & 24 & 15 & 8 \\ 17 & 14 & 3 & 6 & 20 \\ 23 & 5 & 16 & 4 & 12 \\ 9 & 18 & 10 & 22 & 1 \end{bmatrix}.$$

Our method of enumeration is impractical for $q \geqslant 17$, indicating the need for better, general methodologies.

**Acknowledgements**

We are indebted to E. Lamken, of Caltech and C. Colbourn, of Arizona State University, for calling our attention to the existing connections to lattice-square designs and also to A. Bruen, of the University of Calgary, for suggesting various improvements. We thank A. Hulpke and R. Liebler, of Colorado State University, for sharing their insights and the referees for their indulgence. This work was supported by the USDOE under Contract #W-7405-ENG-36, to the University of California.

## References

[1] E.F. Assmus Jr., J.D. Key, Designs and their Codes, Cambridge University Press, Cambridge, MA, 1992.
[2] C. Berge, Principles of Combinatorics (translated by John Sheehan), Academic Press, New York, 1971, pp. 111,172.
[3] R.D. Carmichael, Introduction to the Theory of Groups of Finite Order, Ginn & Company, Boston, 1937.
[4] M.A. Chateauneuf, C.J. Colbourn, E. Lamken, D.R. Kreher, D.C. Torney, Pooling, Lattice Square, and Union Jack Designs, Ann. Combin. 3 (1999) 27–35.
[5] W.Y.C. Chen, Induced Cycle Structures of the Hyperoctahedral Group, SIAM J. Discrete Math. 3 (1993) 353–362.
[6] W.G. Cochran, G.M. Cox, Experimental Designs, Wiley, New York, 1950, pp. 346–369.
[7] C.J. Colbourn, J.H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[8] D.-Z. Du, F. Hwang, Combinatorial Group Testing and its Applications, World Scientific, Singapore, 2000.
[9] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.3 (http://www.gap-system.org), 2002.
[10] L.A. Goldberg, Automating Pólya theory: the computational complexity of the cycle index polynomial, Inform. and Comput. 105 (1993) 268–288.
[11] N. Jacobson, Basic Algebra I, 2nd Edition, W.H. Freeman & Co., New York, 1996.
[12] J.H. van Lint, R.M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, MA, 1993, p. 76.
[13] M. Lothaire, Combinatorics on Words, Cambridge University Press, Cambridge, MA, 1997.
[14] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und Chemische Verbindungen, Acta Math. 68 (1937) 145–254.
[15] D. Raghavarao, Constructions and Combinatorial Problems in the Design of Experiments, Wiley, New York, 1971.
[16] D.J.S. Robinson, A Course in the Theory of Groups, Springer, Berlin, 1996.
[17] H.J. Ryser, Combinatorial Mathematics, Quinn & Boden Co., Inc., Rahway, NJ, 1963.