Commuting probabilities of quasigroups

STEPHEN M. BUCKLEY

Abstract. We show that there exist quasigroups, and even loops, whose commuting probability equals any specified rational value $r \in (0, 1]$. We also characterize all possible orders of quasigroups with commuting probability r.

1. Introduction

Suppose F is an finite algebraic system (meaning an algebraic system of finite cardinality), closed with respect to a multiplication operation denoted by juxtaposition. The set of commuting pairs in F is

$$\mathrm{Comm}(F) := \{(x, y) \in F \times F \mid xy = yx\}.$$

and the *commuting probability of* F is

$$\Pr(F) := \frac{|\mathrm{Comm}(F)|}{|F|^2}.$$

Here and always, $|A|$ denotes the cardinality of a set A.

There are some obvious restrictions on $\Pr(F)$: since every element commutes with itself, $1/|F| \le \Pr(F) \le 1$, and so $\Pr(F) \in (0, 1] \cap \mathbb{Q}$. In the case of groups or rings, the possible values of $\Pr(F)$ are much more restricted than this. In particular, the following results hold:

- If $\Pr(F) < 1$, then $\Pr(F) \le 5/8$; see [9] for groups and [10] for rings.
- The set of values in both cases has only one accumulation point exceeding $11/32$; see [15] for groups and [4] for rings.

By contrast, for semigroups, there are only the trivial restrictions. MacHale [11] showed that if S is a semigroup, then $\Pr(S)$ can attain values arbitrarily close to 1 (and also arbitrarily close to 0). Givens [8] later showed that the set of values of $\Pr(S)$ is dense in $[0, 1]$. Ponomarenko and Selinski [14] showed that $\Pr(S)$ can attain every value in $(0, 1] \cap \mathbb{Q}$. Subsequently, we gave an explicit formula for the minimal order of a semigroup having any specified commuting probability [2, Theorem 1].

Here, we examine the corresponding questions for quasigroups, and to a lesser extent for loops. We first show that, as for semigroups, there are no nontrivial restrictions on the possible commuting probabilities of loops (and, *a fortiori*, the same is true for quasigroups).

2010 *Mathematics Subject Classification.* 20N05, 05B15.

Key words and phrases. quasigroup, loop, Latin square, commuting deficiency, commuting probability.

Theorem 1.1. *For every $r \in (0,1] \cap \mathbb{Q}$, there exists a finite loop L with $\Pr(L) = r$.*

We also characterize all values attained by the *(commuting) deficiency*

$$\delta(Q) := \frac{|Q|^2 - |\operatorname{Comm}(Q)|}{2}$$

as Q ranges over $\mathcal{Q}_n$, the set of quasigroups of order n.

Theorem 1.2.

(a) If $Q \in \mathcal{Q}_n$, then $\delta(Q)$ is an integer, $0 \le \delta(Q) \le n(n-1)/2$, and $\delta(Q)$ is not equal to either 1 or 2.

(b) The values attained by $\delta(Q)$ as Q ranges over $\mathcal{Q}_n$ include all numbers satisfying the conditions in (a), with two exceptions: $\delta(Q) \ne 3$ if $n = 4$, and $\delta(Q) \ne 4$ if $n = 5$.

Since $\Pr(Q)$ is easily obtained from $\delta(Q)$ and n, the above result allows us to calculate the minimum order—and indeed all possible orders–of a quasigroup attaining any given (rational) commuting probability $0 < r \le 1$: see Theorem 3.10.

After dealing with some preliminary material in Section 2, we prove the above theorems in Section 3.

I wish to thank Des MacHale for suggesting this topic of research.

2. Preliminaries

A *quasigroup* $(Q, *)$ is a nonempty set Q with a binary operation $* : Q \times Q \to Q$ such that, for each $x, y \in Q$, there exist unique elements $l, r \in Q$ such that $l * x = y$ and $x * r = y$. We will usually denote multiplication in a quasigroup by juxtaposition.

A *loop* is a quasigroup Q with a two-sided identity, i.e. an element $e \in Q$ such that $ex = xe = x$ for all $x \in Q$. We denote by $\mathcal{Q}_n$ and $\mathcal{L}_n$ the classes of all quasigroups and loops, respectively, of order $n \in \mathbb{N}$.

An *isotopy* from one quasigroup Q to another Q' is a triple (α, β, γ) of bijections from Q to Q' such that

$$\alpha(x)\beta(y) = \gamma(xy)\,. \tag{2.1}$$

Note that if Q is a quasigroup, and (α, β, γ) is a triple of bijections from Q to a set Q', then (2.1) uniquely defines a quasigroup structure on Q'. An *isotopy of type* $(\mathrm{Id}, \mathrm{Id}, \gamma)$ will refer to such an isotopy where α and β in (2.1) are the identity maps. In a similar fashion, we define *isotopies of type* (α, α, γ) or *of type* $(\alpha, \mathrm{Id}, \mathrm{Id})$.

It is convenient to associate a linear order $<$ to the elements of $Q \in \mathcal{Q}_n$ by writing the elements as $x_1 < \cdots < x_n$. We can then define the *multiplication table* $T(Q, <)$ *of Q with respect to the linear order* $<$ by the rule that the (i,j)th entry of $T(Q)$ is $x_i x_j$. We will usually simply write $T(Q)$ in place of $T(Q, <)$ because we are interested only in $\delta(Q)$, and this is independent of the choice of linear order. (Put another way, changing the linear order is equivalent to applying an

isotopy of type $(\alpha, \alpha, \mathrm{Id})$ between two quasigroups on the same set, $(Q, *)$ and $(Q, \circ)$, and such isotopies preserve $\delta(\cdot)$.)

The multiplication table $T(Q)$ of an ordered quasigroup Q, with $n = |Q| < \infty$, is an *order n Latin square on the symbol set Q*, i.e. it is an $n \times n$ array of symbols using the symbol set Q, where each element of Q occurs exactly once in each row and exactly once in each column. Conversely, every order n Latin square $T = (T_{i,j})_{i,j=1}^n$ on a set Q of n symbols can (in a non-unique way) be viewed as $T(Q)$, where $Q \in \mathcal{Q}_n$. Thus, the determination of the possible values of $\Pr(Q)$ is effectively a problem concerning only Latin squares, so it suffices to write down such Latin squares rather than the associated quasigroups. However, it is often convenient to use the language of quasigroups. In particular, we often make use of C_n, the cyclic group of order n.

A *cell* of a Latin square $T = (T_{i,j})_{i,j=1}^n$ is just a position (i, j), and we say that a symbol a *is in cell* (i, j) if $T_{i,j} = a$.

A *Latin rectangle* is an $r \times s$ block of symbols, for some $r, s \in \mathbb{N}$, where no symbol appears twice in the same row or column. A Latin rectangle is *row (or column) balanced* if the same set of symbols appear in each row (or column) of the rectangle. Thus, for an $r \times s$ Latin rectangle to be a Latin square we must have $r = s$ and it must also be row balanced (or equivalently, column balanced).

A *partial Latin rectangle* P is like a Latin rectangle, except that we allow certain cells to be unspecified or *empty*. Of those that are specified or *filled*, no symbol appears twice in the same row or column. We denote empty entries in P by $*$. For instance, the following partial Latin rectangle, with six filled cells that each contain one of two distinct symbols a and b, will be useful later.

$$P_3 = \begin{array}{|ccc|}\hline * & a & b \\ b & * & a \\ a & b & * \\ \hline \end{array}$$

We say that a Latin rectangle R is *consistent* with a partial Latin rectangle P of the same size if the same symbol appears in each filled cell of P as in the corresponding cell of R.

An $r \times r$ Latin rectangle $T = (T_{i,j})$ is said to be *symmetric* if $T_{i,j} = T_{j,i}$ for all $1 \le i, j \le r$, and T is said to be *asymmetric* otherwise. A quasigroup Q is *commutative* if $xy = yx$ for all $x, y \in Q$, or equivalently if its multiplication table $T(Q)$ is symmetric, and otherwise it is said to be non-commutative.

If Q is a quasigroup, then the *centralizer* of $x \in Q$ is the set $C(x)$ of all $y \in Q$ such that $xy = yx$, and the *centrum* $C(Q)$ of Q is $\bigcap_{x \in Q} C(x)$.

When we talk of a *Latin subsquare* or *(partial) Latin subrectangle*, we just mean a Latin square or (partial) Latin rectangle that is contained in another Latin square/rectangle. We are particularly interested in *diagonal Latin subrectangles* of a Latin square T: these are the ones whose top left cell within T is (i, i) for some i. If in fact the top left cell of a Latin subrectangle S of T is $(1, 1)$, we call S a *corner Latin subrectangle* of T.

The *commuting deficiency*

$$\delta(Q) := \frac{|Q|^2 - |\operatorname{Comm}(Q)|}{2}$$

of a finite quasigroup Q is half the number of non-commuting pairs in Q. If T is a Latin square, we define $\delta(T) = \delta(Q)$, where Q is any quasigroup whose multiplication table is T; this is well defined. If $\mathcal{C}$ is a class of quasigroups or Latin squares, then we define

$$\delta(\mathcal{C}) = \{\delta(A) \mid A \in \mathcal{C}\}.$$

We are interested in $\delta(\mathcal{C})$ for the classes $\mathcal{C} = \mathcal{Q}_n$ and $\mathcal{C} = \mathcal{L}_n$, $n \in \mathbb{N}$. Studying $\delta(Q)$ is essentially equivalent to studying $\Pr(Q)$ because

$$\Pr(Q) = 1 - \frac{2\delta(Q)}{|Q|^2}. \tag{2.2}$$

An isotopy class can be defined for Latin squares in a manner consistent with its definition for quasigroups: the maps (α, β, γ) used in (2.1) tell us that two Latin squares are isotopy equivalent if one can be obtained from the other by some combination of permutations of rows (α), columns (β), and symbols (γ).

Quasigroup isotopies do not in general preserve the commuting probability, but they do if $\alpha = \beta$ in (2.1). We therefore define an *invariance class (of quasigroups, or of Latin squares)* to be an equivalence class with respect to isotopies of type (α, α, γ), i.e. two Latin squares are invariant equivalent if one can be obtained from the other by matched permutations of rows and columns, and a permutation of symbols.

It follows that, to obtain representatives of all invariance classes associated with a fixed isotopy class, it suffices to apply isotopies of type $(\alpha, \mathrm{Id}, \mathrm{Id})$ to a single representative of the isotopy class; the use of such isotopies will be useful for creating quasigroups Q of a given order with certain desired values of $\Pr(Q)$ or $\delta(Q)$.

Suppose T is a Latin square on the symbols $x_1, \ldots, x_n$. We say that T is a *normalized Latin square* if the first row consists of the symbols in their chosen order $x_1, \ldots, x_n$, or a *reduced Latin square* if its first row and column are both in this chosen order.

An invariance class of Latin squares always has a normalized Latin square representative (just permute the symbols), and an isotopy class always has a reduced Latin square representative (apply a row permutation to a normalized Latin square). This leads us to the following observation.

Observation 2.1. If S is a set of Latin squares containing a representative of every isotopy class of order n Latin squares—for instance the set of all reduced order n Latin squares has this property—then to obtain $\delta(\mathcal{Q}_n)$, it suffices to compute $\delta(Q)$ for all Latin squares obtained from elements of S by row permutations.

Suppose $T = (T_{i,j})_{i,j=1}^n$ is an order n Latin square, and let $A = \{1, \ldots, n\}$. A *partial transversal* of T is a subset S of $A \times A$ such that no two cells are in

the same row or column, and the elements $T_{i,j}$, $(i,j) \in S$ are all distinct. A *transversal of* T is a partial transversal S with $|S| = n$. Thus, a transversal is a set of n cells in T, each containing a distinct symbol, and no two occupying the same row or column.

The *(standard) prolongation* $\mathrm{Prol}(T,S)$ *of a Latin square* $T = (T_{i,j})_{i,j=1}^n$ *by a transversal* $S = \{T_{i,j_i}\}_{i=1}^n$ is the order $(n+1)$ Latin square $T' = (T'_{i,j})_{i,j=1}^n$ obtained by adding an extra row at the bottom of T and an extra column to the right of T according to the following rules:

- $T'_{i,n+1} = T'_{n+1,j_i} = T_{i,j_i}$;
- $T'_{i,j_i} = T'_{n+1,n+1} = \omega$, where ω is the symbol in T' that is not in T;

A special case of prolongation goes back to a paper of Bruck [1], while the more general situation defined here goes back to Dénes and Pásztor [6]. We write $T' = \mathrm{Prol}(T,S)$ if T' is the prolongation of T via S.

Note that the four cells $(i,n+1)$, (i,j_i), $(n+1,j_i)$, and $(n+1,n+1)$ form a Latin subsquare of T' as defined above. It follows that if we interchange the two rows of this subsquare, and leave the rest of T' unchanged, then we get a new Latin square T''. We call T'' the *i-variant prolongation* of the Latin square T by the transversal S, and denote it by $\mathrm{Prol}(T,S;i)$.

It is sometimes convenient to define prolongations and (partial) transversals in terms of quasigroups Q. A partial transversal is a subset S of $Q \times Q$ such that the first and second coordinates of distinct elements are distinct, and such that the products xy are distinct for each pair (x,y). A transversal is a partial transversal such that the coordinate maps $\pi_i : S \to Q$, $i = 1,2$, and the product map $P : S \to Q$, $P(x,y) = xy$, are all surjective. The (standard) prolongation $P := \mathrm{Prol}(Q,S)$ is then a quasigroup such that as a set, P is the disjoint union $S \sqcup \{\omega\}$, and where multiplication $\circ$ is defined as follows, denoting multiplication in Q by juxtaposition:

$$x \circ y = \begin{cases} \omega, & (x,y) \in S \cup \{(\omega,\omega)\}\,, \\ uy, & (u,y) \in S,\ x = \omega\,, \\ xu, & (x,u) \in S,\ y = \omega\,, \\ xy, & \text{otherwise}\,. \end{cases}$$

Given $x_0 \in Q$, and y_0 such that $(x_0,y_0) \in S$, we write $S' = S \setminus \{(x_0,y_0)\}$, and define the *$x_0$-variant prolongation* $P = \mathrm{Prol}(Q,S;x_0)$ to be the quasigroup which as a set is the same as $\mathrm{Prol}(Q,S)$, but has multiplication $\circ$ defined by

$$x \circ y = \begin{cases} \omega, & (x,y) \in S' \cup \{(x_0,\omega),(\omega,y_0)\}\,, \\ uy, & (u,y) \in S',\ x = \omega\,, \\ xu, & (x,u) \in S',\ y = \omega\,, \\ x_0y_0, & (x,y) = (\omega,\omega)\,, \\ xy, & \text{otherwise}\,. \end{cases}$$

If $|Q| < \infty$—the only situation that interests us in this paper!—it is clear that these definitions for quasigroups are consistent with the corresponding concepts for an associated Latin square $T(Q)$.

Suppose $T = (T_{i,j})_{i,j=1}^n$ is an order n Latin square with an order m Latin subsquare S'. If $S = (S_{i,j})_{i,j=1}^m$ is another order m Latin square involving the same symbols as S', then we define the *patched Latin square* $\mathrm{Patch}(T, S; S')$ to be the order n Latin square obtained by putting the elements of S in place of those of S' in the natural manner, i.e. if the top left entry of S' in T is $T_{p,q}$, then we replace $T_{p+i-1,q+j-1}$ by $S_{i,j}$ for $1 \le i, j \le m$, and we leave all other entries in T unchanged. When S' is a diagonal subsquare of T, it is clear that

$$\delta(\mathrm{Patch}(T, S; S')) = \delta(T) + \delta(S) - \delta(S')\,. \tag{2.3}$$

Whenever we talk of a Latin square $\mathrm{Patch}(T, S; S')$, it is implicitly assumed that S and S' are of the same size, and contain the same symbols.

We will need a twisted variant of the usual direct product construction: a *twisted product of quasigroups Q_1 and Q_2* is any quasigroup on the Cartesian product $Q_1 \times Q_2$ where multiplication has the form

$$(x_1, x_2)(y_1, y_2) = (x_1 \circ_{x_2,y_2} y_1,\ x_2 y_2)\,.$$

Here, $(Q_1, \circ_{x_2,y_2})$ is a quasigroup for each $x_2, y_2 \in Q_2$. We denote any such twisted product Q as $Q_1 \mathbin{\widetilde{\times}} Q_2$, although we instead write $Q = Q_1 \times Q_2$ in the direct product case in which $\circ_{x,y}$ is the quasigroup operation of Q_1 for all $x, y \in Q_2$. A twisted product $Q_1 \mathbin{\widetilde{\times}} Q_2$ can of course be obtained from $Q_1 \times Q_2$ by making n^2 patches if $n = |Q_2| < \infty$.

The *p-adic valuation function* $\nu_p : \mathbb{Q}^* \to \mathbb{Z}$ is defined for each prime p and $r \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ by the equation $\nu_p(r) = k$, where k is the unique integer with the property that $r = p^k m/n$ for some integers m, n coprime to p. It has the property that $\nu_p(rs) = \nu_p(r) + \nu_p(s)$ for all $r, s \in \mathbb{Q}^*$.

Lastly in this section, let us state a theorem of Cruse.

Theorem 2.2 ([5, Theorem 1])**.** *Let T_r be an $r \times r$ symmetric Latin rectangle based on the symbols $1, ..., n$, where $n > r$. Denote by $N(i)$ the number of occurrences of the symbol i in T_r. In order for T_r to be extendible to an order n symmetric Latin square T_n based on $1, ..., n$, it is necessary and sufficient that the following pair of conditions both hold:*

(a) $N(i) \ge 2r - n$ for every $1 \le i \le n$, and
(b) $n - N(i)$ is even for at least r of the symbols i.

In the above theorem, T_r being *extendible* to T_n means that T_r is a corner Latin subrectangle of T_n. In particular, if T_r is actually a Latin subsquare of T_n, and $T' = \mathrm{Patch}(T_n, S; T_r)$, then $\delta(T')$ can be computed using (2.3).

3. Constructions and proofs

We begin with a lemma that sets the stage for our subsequent analysis.

Lemma 3.1. *For $n \in \mathbb{N}$, let*

$$\pi(\mathcal{Q}_n) = \{i \in \mathbb{N} \mid 0 \leq i \leq n(n-1)/2,\ i \neq 1, 2\}\,.$$
$$\pi(\mathcal{L}_n) = \{i \in \mathbb{N} \mid 0 \leq i \leq (n^2 - 3n + 2)/2,\ i \neq 1, 2\}\,.$$

Then $\delta(\mathcal{Q}_n) \subseteq \pi(\mathcal{Q}_n)$ and $\delta(\mathcal{L}_n) \subseteq \pi(\mathcal{L}_n)$.

Proof. The result is immediate verified when $n = 1, 2$, so we suppose that $n > 2$ and that $Q \in \mathcal{Q}_n$, $L \in \mathcal{L}_n$. First, observe that all diagonal elements (x, x) of $Q \times Q$ lie in $\mathrm{Comm}(Q)$, and all other elements of $\mathrm{Comm}(Q)$ occur in pairs of the form $\{(x, y), (y, x)\}$. Similarly, there are $3|L| - 2$ pairs guaranteed to lie in $\mathrm{Comm}(L)$, namely (x, x), $(1, x)$, and $(x, 1)$, for all $x \in L$. It follows readily that

$$\delta(\mathcal{Q}_n) \subseteq \pi(\mathcal{Q}_n) \cup \{1, 2\}\,,$$
$$\delta(\mathcal{L}_n) \subseteq \pi(\mathcal{L}_n) \cup \{1, 2\}\,.$$

It remains only to show that $\delta(Q) \notin \{1, 2\}$. Suppose Q is noncommutative, and let us choose u not in the centrum of Q. There must be at least two distinct elements v, w that fail to commute with u: if we had $ux = xu$ for all $x \in Q \setminus \{v\}$, then we would also have $uv = vu$ because of the fact that the maps $x \mapsto xu$ and $x \mapsto ux$ are bijections. By using the same argument with v or w in place of u, we conclude that for each $x \in \{u, v, w\}$, there exist at least two distinct elements y such that (x, y) is a non-commuting pair. Thus, $\delta(Q) \geq 3$, as required. □

For the rest of this paper, we denote by Γ the set of all $n \in \mathbb{N}$ that satisfy the equation $\delta(\mathcal{Q}_n) = \pi(\mathcal{Q}_n)$. To prove Theorem 1.2, we need to show in particular that $\Gamma = \mathbb{N} \setminus \{4, 5\}$. We start by showing that $4, 5 \notin \Gamma$.

Theorem 3.2.

(a) A Latin square T satisfies $\delta(T) = 3$ if and only if it is invariant equivalent to a Latin square T' whose only non-commuting pairs are given by a partial diagonal subrectangle P_3 of the form

$$P_3 = \begin{array}{|ccc|}\hline * & a & b \\ b & * & a \\ a & b & * \\ \hline\end{array}$$

(b) A Latin square T satisfies $\delta(T) = 4$ if and only if it is invariant equivalent to a Latin square T' whose only non-commuting pairs are given by a partial diagonal subrectangle P_4 of the form

$$P_4 = \begin{array}{|cccc|}\hline * & * & a & b \\ * & * & b & a \\ b & a & * & * \\ a & b & * & * \\ \hline\end{array}$$

(c) $4, 5 \notin \Gamma$. In fact, $3 \notin \delta(\mathcal{Q}_4)$ and $4 \notin \delta(\mathcal{Q}_5)$.

Proof. Suppose Q is a quasigroup. For each $x \in Q$, let L_x and R_x be the bijections from Q to Q defined by $L_x(y) = xy$ and $R_x(y) = yx$, let $D(x) = Q \setminus C(x)$, and let $D(Q) = Q \setminus C(Q)$. Note that y is a fixed point of the bijection $g_x = L_x^{-1} \circ R_x$ if and only if $y \in C(x)$. Thus for all $x \in D(Q)$,

- $g_x|_{C(x)}$ is the identity map;
- $g_x|_{D(x)}$ is a fixed-point-free bijection;
- $|D(x)| \geq 2$.

We also define the bijection $h_x = L_x \circ R_x^{-1}$, noting that $h_x(yx) = xy$ for all $y \in Q$. Writing $C'(x) = R_x(C(x))$ and $D'(x) = R_x(D(x))$, the above conditions can also be written as

- $h_x|_{C'(x)}$ is the identity map;
- $h_x|_{D'(x)}$ is a fixed-point-free bijection;
- $|D'(x)| \geq 2$.

Given a Latin square $T = (T_{i,j})_{i,j=1}^n$ on the symbol set $Q = \{x_1, \ldots, x_n\}$, we make Q into a quasigroup by defining $x_i x_j = T_{i,j}$ for $1 \leq i, j \leq n$. Define $D(x)$ and $D(Q)$ as above, and let $m = |D(Q)|$. Since $|D(x)| \geq 2$ for all $x \in D(Q)$, it follows that $\delta(Q) \geq m$. On the other hand, $\delta(T)$ cannot be larger than $m(m-1)/2$, half the number of off-diagonal elements in $D(Q)$. It follows that if $m = 3$, then $\delta(T) = 3$; if $m = 4$, then $4 \leq \delta(T) \leq 6$; and if $m > 4$, then $\delta(T) > 4$. In particular, $\delta(T) = 3$ implies $m = 3$ and $\delta(T) = 4$ implies $m = 4$.

Suppose now that $\delta(T) = 3$, and so $m = 3$. Writing $D(Q) = \{x, y, z\}$ and defining a new linear order $\prec$ with $x \prec y \prec z \prec w$ for all $w \in C(Q)$, gives a new Latin square $T' = T(Q, \prec)$ that is invariant equivalent to T, and has a 3×3 corner Latin subrectangle corresponding to the elements of $D(Q)$. Here, each of the three elements must fail to commute with the other two elements of $D(Q)$, so this subrectangle is consistent with the following partial Latin subrectangle

$$Q_3 = \begin{array}{|ccc|}\hline * & a & b \\ b' & * & c \\ a' & c' & * \\ \hline \end{array}$$

where $a, b, c, a', b', c' \in Q$. Now, $a \neq b$ and, because h_x is a fixed-point free bijection from $D'(x) = \{a', b'\}$ to itself, we see that $b' = b$ and $a' = a$. Similarly, since h_y is a bijection from $D'(y) = \{a, c'\}$ to itself, we must have $a = c$ and $b = c'$. It follows that $Q_3 = P_3$, as required in (a). Note that we describe P_3 as a Latin subrectangle rather than a Latin subsquare because there is no reason that the missing entries in Q_3 should all be the same as each other.

We next prove (b). Suppose that $\delta(T) = 4$, let Q be an associated quasigroup, and let m and $D(Q)$ be as before. We already know that $m = 4$ in this case, so $D(Q) = \{x, y, z, w\}$. Each of these elements must fail to commute with exactly two others lest the deficiency be too large, so we assume that x fails to commute only with z and w. Thus, y must also fail to commute with z and w, and so by imposing a new order $x \prec y \prec z \prec w \prec u$ for all $u \in C(Q)$, the new Latin square $T' = T(Q, \prec)$ that is invariant equivalent to T contains a partial corner

subrectangle of the form

$$Q_4 = \begin{array}{|cccc|}\hline * & * & a & b \\ * & * & c & d \\ b' & d' & * & * \\ a' & c' & * & * \\ \hline\end{array},$$

where the noncommuting cells of T are precisely the filled cells of Q_4.

Now, $a \neq b$ and, because $h_u : D'(u) \to D'(u)$ is a fixed-point-free bijection for $u = x$, we see that $b' = b$ and $a' = a$. Since it is a bijection for $u = y$, we have $d' = d$ and $c' = c$. Since it is a bijection for $u = z$, we see that $\{b, d\} = \{a, c\}$, so $b = c$ and $a = d$, as required.

Finally, we prove (c). If $3 \in \delta(\mathcal{Q}_4)$, then the following partial Latin rectangle could be completed to form an order 4 Latin square:

$$\begin{array}{|cccc|}\hline * & a & b & * \\ b & * & a & * \\ a & b & * & * \\ * & * & * & * \\ \hline\end{array}$$

There are only two other symbols to fit into the missing spots in the top three rows, so the last column must repeat one of them. Thus, no such Latin square exists.

Similarly if $4 \in \delta(\mathcal{Q}_5)$, then the following partial Latin rectangle could be completed to form an order 5 Latin square:

$$\begin{array}{|ccccc|}\hline * & * & a & b & * \\ * & * & b & a & * \\ b & a & * & * & * \\ a & b & * & * & * \\ * & * & * & * & * \\ \hline\end{array}$$

There are only three other symbols to fit into the missing spots in the top four rows, so the last column must repeat one of them. Thus, no such Latin square exists. □

The following lemma does part of the work involved in an inductive proof of Theorem 1.2(b): for large enough n, it will show that $\delta(\mathcal{Q}_n)$ contains "small" target values. We will need other techniques to get larger values.

Lemma 3.3. *Suppose $j \in \mathbb{N}$. Then*

$$\delta(\mathcal{Q}_n) \supseteq \begin{cases} \bigcup_{1 \leq i \leq j} \delta(\mathcal{Q}_i), & n = 2j, \\ \bigcup_{1 \leq i < j/2} \delta(\mathcal{Q}_{2i+1}), & n = 2j+1. \end{cases}$$

Proof. Suppose $n = 2j$ and $i \le j$. We apply Theorem 2.2 with $r = i$ to embed an order r symmetric Latin square T_r in an order n symmetric Latin square T_n. Condition (a) in that theorem is trivially satisfied since $2r - n \le 0$. Condition (b) also holds because $n - N(k) = n$ is even for all $j < k \le n$. Thus, such an embedding is indeed possible.

Let $S \in \mathcal{Q}_i$ be such that it contains the same symbols as T_i and satisfies $\delta(S) = m$. By (2.3), $\delta(\mathrm{Patch}(T_n, S; T_i)) = m$, as required. Since we can do this for all $m \in \delta(\mathcal{Q}_i)$, we get the desired containment in this case.

The case $n = 2j+1$ is similar except that the parity condition (b) requires that we extend only Latin squares of odd order $r = 2i+1$, and then $n - N(k) = n - r$ is even for $1 \le i \le r$. □

One of our main methods for finding values in $\delta(\mathcal{Q}_n)$ and $\delta(\mathcal{L}_n)$ is to examine twisted products $Q = C_j \mathbin{\widetilde{\times}} C_k$, where $j, k > 1$. Writing $X = (u, x)$, $Y = (v, y)$, $u, v \in C_j$, $x, y \in C_k$, we have

$$\delta(Q) = \delta_{\mathrm{on}}(Q) + \delta_{\mathrm{off}}(Q)\,,$$

where $\delta_{\mathrm{on}}(Q)$ is the *on-diagonal contribution*, counting only $(X, Y) \in \mathrm{Comm}(Q)$ with $x = y$, and $\delta_{\mathrm{off}}(Q)$ is the *off-diagonal contribution* counting only $(X, Y) \in \mathrm{Comm}(Q)$ with $x \ne y$. Whenever $\mathcal{C}$ is a class of quasigroups, we also define $\delta_{\mathrm{on}}(\mathcal{C})$ and $\delta_{\mathrm{off}}(\mathcal{C})$ in a manner analogous to $\delta(\mathcal{C})$, i.e. these are the set of possible on- and off-diagonal contributions of quasigroups in these classes. Since the on- and off-diagonal contributions are dependent on disjoint parts of the twisted product construction, it follows that $\delta(\mathcal{C})$ is the sum of all numbers $a + b$, $a \in \delta_{\mathrm{on}}(\mathcal{C})$, $b \in \delta_{\mathrm{off}}(\mathcal{C})$, and so it makes sense to analyze these contributions separately.

We now give a pair of lemmas that give information about possible off- and on-diagonal contributions of certain types of twisted products.

Lemma 3.4. *Suppose $j > 1$. Then we have the following:*

(a) For all $k \ge 2$, there exists a twisted product quasigroup Q of the form $C_j \mathbin{\widetilde{\times}} C_k$ with $\delta_{off}(Q)$ equal to any number in the set

$$A_{j,k} = \begin{cases} \{\, ji \mid 0 \le i \le j(k^2 - k)/2,\ i \ne 1 \,\}, & j > 2, \\ \{\, 4i \mid 0 \le i \le (k^2 - k)/2 \,\}, & j = 2. \end{cases}$$

(b) For all $k \ge 3$, there exists a twisted product loop L of the form $C_j \mathbin{\widetilde{\times}} C_k$ with $\delta_{off}(L)$ equal to any number in the set

$$A'_{j,k} = \begin{cases} \{\, ji \mid 0 \le i \le j(k^2 - 3k + 2)/2,\ i \ne 1 \,\}, & j > 2, \\ \{\, 4i \mid 0 \le i \le (k^2 - 3k + 2)/2 \,\}, & j = 2. \end{cases}$$

Proof. We first prove (a). Associate some linear order, $<$, to the elements of C_k; the choice of order is irrelevant. The twisted product operation $\circ_{x,y}$, $x, y \in C_k$, will be defined as follows:

- For all $x > y$, $\circ_{x,y}$ equals $*$, the group operation of C_j.

- For all $x < y$, $\circ_{x,y}$ is obtained from $*$ by applying an isotopy of type $(\mathrm{Id}, \mathrm{Id}, \gamma_{x,y})$. (Thus, $\gamma_{x,y}$ is an arbitrary permutation of $\{1, \ldots, j\}$.)
- For $x = y$, $\circ_{x,y}$ is any commutative quasigroup operation (such as that of C_j).

If $X = (u, x)$ and $Y = (v, y)$ are elements of Q with $x < y$, then $XY = (\gamma_{x,y}(uv), xy)$, while $YX = (vu, yx) = (uv, xy)$ (since C_j and C_k are commutative!). Thus, $XY = YX$ if and only if uv is a fixed point of $\gamma_{x,y}$. Now, each element of C_j equals uv for j choices of (u, v) as u, v range over C_j, so we get a total contribution of js to $\delta_{\text{off}}(Q)$ by all elements of $Q \times Q$ having the form (X, Y) or (Y, X), where $X = (u, x)$, $Y = (v, y)$, x, y is fixed with $x < y$, and s is the number of non-fixed points of the permutation $\gamma_{x,y}$. Thus, this contribution can be any number in the set

$$A_j = \{ji \mid 0 \leq i \leq j,\ i \neq 1\},$$

and $\delta_{\text{off}}(Q)$ can equal any sum of $(k^2 - k)/2$ numbers selected from A_j (allowing repetitions). By taking all except one such number equal to either 0 or j^2, and allowing the last number to range over A_j, we get all numbers in $A_{j,k}$ except those that are equivalent to j mod j^2. When $j = 2$ or when $k = 2$, there are no such exceptional numbers in $A_{j,k}$, so we are already done.

Suppose instead that $j, k \geq 3$. To get the missing numbers, just take a sum of the form $\sum_{m=1}^{k(k-1)/2} a_m$, where $a_1 = 2j$, $a_2 = j(j-1)$, and $a_m \in \{0, j^2\}$ for $m > 1$. Here, we are implicitly using the inequalities $a_1 \leq j^2$, $a_2 \geq 2j$, and $k(k-1)/2 \geq 2$, but these all hold for $j, k \geq 3$.

For part (b), we simply insist that, in the above constructions, $\circ_{e,x} = \circ_{x,e} = *$, and that $\circ_{x,x}$ is a loop operation, for all $x \in C_k$. There remain $(k-2)(k-1)/2$ choices of $(x, y) \in C_j \times C_k$ with $x < y$, and for each such choice, we get a contribution to $\delta_{\text{off}}(Q)$ of some number in A_j as above. The proof that the total off-diagonal contribution can be any number in $A'_{j,k}$ then proceeds as before. □

Remark 3.5. The *intersection number* of a pair of order n Latin squares $T = (T_{i,j})$ and $T' = (T'_{i,j})$ that both use the same symbol set is the number of cells (i, j) such that $T_{i,j} = T'_{i,j}$. Arguing as in the above proof, we see that if Q is of the form $C_j \mathbin{\tilde{\times}} C_k$, then $\delta_{\text{off}}(Q)$ can equal any sum of $k(k-1)/2$ numbers, each of which has the form $j^2 - i$ for some $i \in I(j)$, where $I(j)$ is the set of all possible intersection numbers of order j Latin squares.

$I(j)$ has been characterized by Fu [7] as follows:

$$\begin{aligned}
I(1) &= \{1\}, \\
I(2) &= \{0, 4\}, \\
I(3) &= \{0, 3, 9\}, \\
I(4) &= \{0, 1, 2, 3, 4, 6, 8, 9, 12, 16\}, \\
I(n) &= \{0 \leq k \leq n^2\} \setminus \{n^2 - 1, n^2 - 2, n^2 - 3, n^2 - 5\}.
\end{aligned}$$

Using this result, we can improve Lemma 3.4 when $j \geq 4$ by replacing $A_{j,k}$ and $A'_{j,k}$ by the larger sets $\widetilde{A}_{j,k}$ and $\widetilde{A}'_{j,k}$, respectively, where

$$\widetilde{A}_{j,k} = \begin{cases} \{\, i \mid 0 \leq i \leq j^2(k^2-k)/2,\ i \neq 1,2,3,5 \,\}, & j > 4, \\ \{\, i \mid 0 \leq i \leq j^2(k^2-k)/2,\ i \neq 1,2,3,5,6,9 \,\}, & j = 4, \end{cases}$$

$$\widetilde{A}'_{j,k} = \begin{cases} \{\, i \mid 0 \leq i \leq j^2(k^2-3k+2)/2,\ i \neq 1,2,3,5 \,\}, & j > 4, \\ \{\, i \mid 0 \leq i \leq j^2(k^2-3k+2)/2,\ i \neq 1,2,3,5,6,9 \,\}, & j = 4. \end{cases}$$

The restrictions on k remain unchanged, so $k \geq 2$ and $k \geq 3$ in the strengthened versions of parts (a) and (b), respectively. The straightforward modifications for these improved versions are left to the reader. We gave the weaker Lemma 3.4 because it is sufficient for our purposes, and its proof is self-contained.

Our next lemma, concerning the possible on-diagonal contributions of twisted products, has a rather more complex statement than its off-diagonal cousin in order to maximize its utility.

Lemma 3.6. *Suppose that $j \geq 4$, $k > 1$, and that*

$$\delta(\mathcal{Q}_j) \supseteq \{i \mid (j^2-j)/4 \leq i \leq (j^2-j)/2\}\,. \tag{3.1}$$

Then we have the following:

(a) There exists a twisted product quasigroup Q of the form $C_j \mathbin{\widetilde{\times}} C_k$ with $\delta_{on}(Q)$ equal to any number in the set

$$B_{j,k} = \delta(\mathcal{Q}_j) \cup \{i \mid (j^2-j)/2 < i \leq (j^2-j)k/2\}\,.$$

In particular, if $j \in \Gamma$, then

$$B_{j,k} = \{i \mid 0 \leq i \leq (j^2-j)k/2,\ i \neq 1,2\}\,.$$

(b) There exists a twisted product loop L of the form $C_j \mathbin{\widetilde{\times}} C_k$ with $\delta_{on}(L)$ equal to any number in the set

$$B'_{j,k} = \delta(\mathcal{Q}_j) \cup \{i \mid (j^2-j)/2 < i \leq (j^2-j)(k-1)/2\}\,.$$

In particular, if $j \in \Gamma$, then

$$B'_{j,k} = \{i \mid 0 \leq i \leq (j^2-j)(k-1)/2,\ i \neq 1,2\}\,.$$

(c) Similar but weaker conclusions can be reached if (3.1) is replaced by the weaker assumption

$$\{i \mid (j^2-j)/4 < i \leq (j^2-j)/2\} \subseteq \delta(\mathcal{Q}_j)\,. \tag{3.2}$$

Specifically, the conclusions remain true if we adjust the definitions of $B_{j,k}$ and $B'_{j,k}$ by removing the element $(j^2-j)/2+1$.

Proof. We first prove (a), with Q of the form $C_j \mathbin{\widetilde{\times}} C_k$. We label the elements of C_k as $x_1, \ldots, x_k$. For $i \neq i'$, the definition of $\circ_{x_i,x_{i'}}$ is unimportant, so we simply choose it to be the group operation of C_j in all cases. Pick the twisted product operations $\circ_i := \circ_{x_i,x_i}$ so that the contribution to $\delta_{\mathrm{on}}(Q)$ corresponding to each $x_i \in C_k$ is $(j^2-j)/2$. Summing these yields $\delta_{\mathrm{on}}(Q) = (j^2-j)k/2$; this is the largest value in $B_{j,k}$.

By hypothesis (3.1), we can alter $\circ_1$ so as to decrease its contribution by increments of 1 until its contribution is just $s := \lceil j(j-1)/4 \rceil$. Now, leave $\circ_1$ fixed, and alter $\circ_2$ so as to decrease its contribution by increments of 1 until its contribution is also s. Next, change $\circ_1$ to a commutative operation (such as that of C_j), and simultaneously change $\circ_2$ back so that its contribution is $(j^2-j)/2$.

If $k = 2$, then this set of alterations has given quasigroups $Q \in \mathcal{Q}_{2j}$ with $\delta_{\mathrm{on}}(Q)$ equal to all numbers between $(j^2-j)/2$ and j^2-j, inclusive. By varying $\circ_2$ and keeping $\circ_1$ commutative, we get all remaining numbers in $B_{j,2}$.

If $k > 2$, then we need to repeat the above procedure, but using $\circ_r$ and $\circ_{r+1}$ for $r = 2$ in place of $\circ_1$ and $\circ_2$. If $k > 3$, we then do the same with $r = 3$. Continuing in this fashion, we get quasigroups $Q \in \mathcal{Q}_{jk}$ with $\delta_{\mathrm{on}}(Q)$ equal to any number between $(j^2-j)/2$ to $k(j^2-j)/2$, inclusive. The only remaining numbers in $B_{j,k}$ are elements of $\delta(\mathcal{Q}_j)$, and we obtain these values by taking $\circ_r$ to be commutative for all $r < k$, and $\circ_k$ to be an appropriate quasigroup operation. It is clear that $B_{j,k}$ has the indicated form when $j \in \Gamma$.

We now prove (b) with L of the form $C_j \mathbin{\widetilde{\times}} C_k$. We choose $\circ_{x,y}$ to be the group operation $*$ on C_j for all $x, y \in C_k$, $x \neq y$, and also for $x = y = e$, where e is the identity of C_k. These choices give no contribution towards $\delta_{\mathrm{on}}(L)$ but, ensure that L is a loop. Since $\circ_{x,x}$ can be any quasigroup operation, for all other $x \in C_k$, the rest of the argument proceeds as in (a).

Finally, we suppose that (3.1) is replaced by the weaker (3.2). We assume that $(j^2-j)/4$ is an integer, since otherwise the result follows a fortiori from (a) and (b). By using the argument of (a), we can construct a quasigroup Q in which $\delta_{\mathrm{on}}(Q)$ attains any value in $B_{j,k}$ except values exceeding $(j^2-j)/2$ that are equivalent to 1 mod $(j^2-j)/2$. The smallest of these numbers, $(j^2-j)/2+1$, is given as an exception in the statement of (c), so it remains to show that $\delta_{\mathrm{on}}(Q)$ can attain the value $l(j^2-j)/2+1$ for $2 \leq l < k$. We choose $\circ_{x_i,x_i}$ to give a contribution of $(j^2-j)/4+1$ for $i = 1, 2$; a contribution of $(j^2-j)/2-1$ for $i = 3$; a contribution of $(j^2-j)/2$ for $3 \leq i \leq l+1$; and a contribution of zero for $l+1 \leq i \leq k$. The proof for the (b) variant is similar. □

Our first application of the above pair of lemmas is the following useful corollary.

Corollary 3.7. *Suppose $k \in \mathbb{N}$.*

(a) If $s \in \mathbb{N}$, $0 \leq s \leq (k^2-k)/2$, then there exists a quasigroup Q of order $2k$ such that $\delta(Q) = 4s$. Moreover, if $s \leq (k^2-3k+2)/2$, then Q can be taken to be a loop.

(b) If $s \in \mathbb{N}$, $0 \le s \le (3k^2-k)/2$, then there exists a quasigroup Q of order $3k$ such that $\delta(Q) = 3s$. Moreover, if $s \le (3k^2-7k+4)/2$, then Q can be taken to be a loop.

Proof. Let Q be a quasigroup Q of the form $C_2 \mathbin{\widetilde{\times}} C_k$. Lemma 3.4(a) with $j = 2$ tells us that $\delta_{\text{off}}(Q)$ can be any multiple of 4 between 0 and $2(k^2-k)$, inclusive. There is no on-diagonal contribution to $\delta_{\text{on}}(Q)$, so we immediately deduce the first statement of (a). If we wish the twisted product Q to be a loop, Lemma 3.4(b) with $j = 2$ says that $\delta_{\text{off}}(Q)$ can be any multiple of 4 between 0 and $2(k^2-3k+2)$, inclusive. Together with the equation $\delta_{\text{on}}(Q) = 0$, we immediately deduce the second statement of (a).

We next prove (b). First, note that $\delta(C_3) = 0$, and if we apply an isotopy of the form $(\alpha, \mathrm{Id}, \mathrm{Id})$ to C_3, where α is a transposition of two elements of $\{1,2,3\}$, then we get a quasigroup Q with $\delta(Q) = 3$. Thus, $3 \in \Gamma$, and this already proves (b) for $k = 1$. We assume that $k > 1$ from now on. Lemma 3.4(a) tells us that $\delta_{\text{off}}(Q)$ can be any multiple of 3 between 0 and $9(k^2-k)/2$, inclusive, with the exception of 3 itself. It is also clear that $\delta_{\text{on}}(Q)$ can be any number $3i$, $0 \le i \le k$: just pick the on-diagonal operations $\circ_{x,x}$ to be non-commutative for i elements $x \in C_k$, and commutative for the remaining $k-i$ elements. Putting together the possible values for $\delta_{\text{off}}(Q)$ and $\delta_{\text{on}}(Q)$, the first statement of (b) follows readily.

The second statement of (b) follows similarly, except now $\delta_{\text{off}}(Q)$ is bounded above by $9(k^2-3k+2)/2$ when we appeal to Lemma 3.4(b), and the on-diagonal contribution is bounded by $3(k-1)$ because we insist that $\circ_{e,e}$ is the group operation of C_k. □

The above corollary is already enough to prove Theorem 1.1.

Proof of Theorem 1.1. Let $r = i/j$, where $i, j \in \mathbb{N}$ are coprime. We may assume that $r < 1$ since any commutative group G satisfies $\Pr(G) = 1$. Let m be any positive integer such that j divides m^2, and let

$$q = \left\lceil \frac{3}{2rm} \right\rceil , \qquad k = 2mq\,, \qquad s = k^2(1-r)/2\,.$$

Now, $m^2 r \in \mathbb{N}$ and $q \in \mathbb{N}$, so $s = 2q^2(m^2 - m^2 r) \in \mathbb{N}$. We claim that $s \le (k^2-3k+2)/2$. Assuming this claim, it follows from Corollary 3.7(a) that there exists $L \in \mathcal{L}_{2k}$ such that $\delta(L) = 4s$. By (2.2),

$$\Pr(L) = 1 - \frac{\delta(L)}{2k^2} = r\,,$$

as required.

As for the claim, because $s = k^2(1-r)/2$, the claim is equivalent to the inequality $k^2 r/2 \ge (3k-2)/2$, which is in turn implied immediately by the inequality $kr \ge 3$. But this last inequality follows from the definition of k, and so we are done. □

Remark 3.8. If we only wanted Q to be a quasigroup in the above proof, then it would have sufficed to take $q = \lceil 1/(2rm) \rceil$ there. Since every element commutes with itself, we have $\Pr(Q) \geq 1/|Q|$ for every quasigroup Q, and it is then straightforward to deduce that the minimal order of a quasigroup Q satisfying $\Pr(Q) = r$ is at least $m\lceil 1/(rm) \rceil$, where m is now the *minimal* positive integer such that j divides m^2. We have thus found to within a factor 2 the minimum value of $|Q|$ among quasigroups Q satisfying $\Pr(Q) = r$. However, we will later find the precise minimum value.

The next lemma allows for a significant reduction in the proof of Theorem 1.2.

Lemma 3.9. *If $n = jk$ for some $j \in \Gamma$, $j \geq 4$, $k \in \mathbb{N}$, then $n \in \Gamma$.*

Proof. Suppose $k \geq 2$, and $j \in \Gamma$ for some $j \geq 4$. It follows from Lemmas 3.4 and 3.6 that there exist quasigroups Q of the form $C_j \mathbin{\tilde{\times}} C_k$ with $\delta_{\text{off}}(Q)$ taking on any of the values in $A_{j,k}$, and $\delta_{\text{on}}(Q)$ taking on any of the values in $B_{j,k}$. Taking the off-diagonal contribution to be any number $0 \leq a \leq j^2(k^2 - k)/2$ which is divisible by j^2 (noting that all such numbers lie in $A_{j,k}$), and taking the on-diagonal contribution to be any number in $B_{j,k}$, we claim that we already obtain all values in $\pi(\mathcal{Q}_n)$ in the case $k > 2$. In fact, any target value of at least 3 can be obtained by adding an off-diagonal contribution that is divisible by j^2 to an on-diagonal contribution lying between 3 and $(j^2 - j)k/2$; all such values are possible by Lemma 3.6(a); we are implicitly using the inequality $(j^2 - j)k/2 - 3 \geq j^2 - 1$. The only remaining target value is 0, which we obtain as $\delta(C_j \times C_k)$.

Suppose instead that $k = 2$. The argument for $k > 2$ still produces all target values except $j^2 + 1$ and $j^2 + 2$. To obtain these, it suffices to note that $2j \in A_{j,k}$ and $\{j^2 + 1 - 2j, j^2 + 2 - 2j\} \subseteq B_{j,k}$; here, we are implicitly using the inequalities $2j \leq j^2$ and $j^2 + 1 - 2j \geq 3$, both of which are true for $j \geq 4$. □

We are now ready to prove Theorem 1.2. The Latin squares needed in Part 1 of the proof can be found in the support document [3]. These examples give all values of $\delta(\mathcal{Q}_n)$ for $3 \leq n \leq 7$ (Tables 1–5), and for $n = 9$ (Tables 6–8).

Before we give the proof, let us comment on the methods used to find these examples. Using Observation 2.1, we see that the computation of $\delta(\mathcal{Q}_n)$ reduces to the computation of $\delta(T)$ for $n!$ Latin squares T obtained by row permutations from representatives of every isotopy class of order n Latin squares. This renders trivial the computation of $\delta(\mathcal{Q}_n)$ for $n \leq 3$, since in each case there is a unique reduced Latin square up to relabeling of the symbols. (This unique reduced Latin square coincides with the multiplication table of C_n once we write the identity element in the first position.) As for $n = 4$, it is straightforward to find by hand Latin squares with deficiencies 0, 4, 5, and 6, and this determines $\delta(\mathcal{Q}_4)$ because of Theorem 3.2(c).

For larger n, we wrote a computer program to investigate matters. Isotopy class representatives were in all cases obtained by following links on a webpage of Brendan McKay [12]. For $n \in \{5, 6, 7\}$, the computer programme quickly obtained all possible deficiencies. Analyzing the cases $n \in \{5, 6, 7\}$ by hand also

proved feasible but not easy: we do not reproduce the calculations involved since the computer-generated examples in the support document were found with less effort.

We were able to conclude the computer searches when $n \in \{6, 7\}$ before all isotopy classes of Latin squares had been examined because all possible values of $\delta(Q)$ showed up among the first thirteen of 22 isotopy class representatives for $n = 6$, and among the first eight of 564 isotopy class representatives for $n = 7$.

These efficiencies for $n = 6, 7$ were of no great significance, but a similar efficiency is essential for $n = 9$. Since there are more than 10^{11} isotopy classes of order 9 Latin squares [13, Theorem 3], and 9! row permutations to be checked for each, a successful brute force computer search for $n = 9$ is feasible only if all possible deficiencies show up after examining just a small fraction of the total number of isotopy classes. Working from McKay's first partial list of *Isotopy classes with nontrivial groups*, this did indeed occur. However, examples for small positive deficiencies tended to take longer to appear, and we needed to examine almost 29 500 isotopy classes (and so about 10.6 billion Latin squares) before finding an example with $\delta(Q) = 5$.

The search difficulties for $n = 9$ hint at a limitation of such brute force methods. Since the number of isotopy classes of Latin squares grows quickly, and one must examine $n!$ row-permuted Latin squares associated with each isotopy class representative, an examination of all Latin squares by computer is infeasible for $n \geq 9$.

Searching only a sample of the Latin squares of a given order in hopes of finding all deficiencies can of course be tried. However, heuristically, one expects small deficiencies to become quite rare compared with large deficiencies as n becomes large, and so such a partial search is likely to end in failure for orders in excess of 9 even if billions of row-permuted Latin squares are examined.

Fortunately, 9 is a threshold value of sorts: for $n > 9$, we have more room to maneuver, and various constructions will allow us to find all possible deficiency values. Similar constructions almost work for $n = 9$. In fact, by such methods, we can construct all deficiencies except $\delta(Q) = 5$ (which, coincidentally, was also the most time-consuming deficiency for the computer search).

Proof of Theorem 1.2.
The proof is broken into parts depending on the value of n. In view of Lemma 3.9, it suffices to prove the following.

(a) $\{1, 2, 3, 6, 7, 9\} \subseteq \Gamma$.
(b) A characterization of $\delta(\mathcal{Q}_n)$ for the exceptional values $n \in \{4, 5\}$.
(c) $5k \in \Gamma$ for $k > 1$.
(d) $4k \in \Gamma$ for $k > 1$.
(e) $p \in \Gamma$ if $p > 11$ is a prime equivalent to 3 mod 4.
(f) $p \in \Gamma$ if $p > 17$ is a prime equivalent to 1 mod 4.
(g) $\{11, 13, 17\} \subseteq \Gamma$.

We prove (a) and (b) in Part 1 of the proof, and we prove (c) and (d) in Parts 2 and 3, respectively. We then prove weaker versions of (e) and (f) in Parts 4 and 5, respectively: in both cases, we add the extra assumption that a certain odd number less than p is in Γ. Finally, we prove (g) in Part 6, and also fill the remaining gaps in the proofs of (e) and (f). The order of proof is chosen because later parts generally involve the ideas used in earlier parts plus some additional ideas.

Part 1 *Characterization of $\delta(\mathcal{Q}_n)$ for $n \leq 9$, $n \neq 8$.*

Latin squares with all deficiencies that occur are given in [3, Tables 1–8] for orders $n \leq 7$ and $n = 9$. In view of Lemma 3.2(c), these examples finish the characterization of $\delta(\mathcal{Q}_n)$ for such n.

Part 2 *If $n = 5k$ for some $k > 1$, then $n \in \Gamma$.*

Suppose $n = 5k$, $k > 1$; the restriction $k > 1$ is needed because of Lemma 3.2(c). Let $Q = C_5 \mathbin{\widetilde{\times}} C_k$. Lemma 3.4 says that $\delta_{\text{off}}(Q)$ can take on any value in

$$A_{5,k} := \{\, 5i \mid 0 \leq i \leq 5(k^2-k)/2,\ i \neq 1 \,\}.$$

Next, note that (3.1) holds for $j = 5$, so Lemma 3.6 tells us that $\delta_{\text{on}}(Q)$ can take on any value in

$$B_{5,k} := \{i \mid 0 \leq i \leq 10k,\ i \neq 1, 2, 4\}.$$

Thus, $\delta(Q)$ can be any number of the form $a + b$, $a \in A_{j,k}$, $b \in B_{j,k}$. If $k > 2$, then every number in $\pi(\mathcal{Q}_n)$ that is not less than 5 can be obtained by taking some $0 \leq a \leq 25(k^2-k)/2$ that is divisible by 25 (noting that all such numbers lie in $A_{5,k}$) and $5 \leq b \leq 10k$; here, we are implicitly using the fact that $10k - 5 \geq 25 - 1$.

By taking $\delta_{\text{off}}(Q) = 0$ and $\delta_{\text{on}} \in \{0, 3\} \subset B_{5,k}$, we see that $\{0, 3\} \subset \delta(\mathcal{Q}_n)$. It remains only to get a quasigroup Q with $\delta(Q) = 4$. There are two cases: if k is even, then we appeal to Corollary 3.7(a), while if $k > 1$ is odd, we appeal to Lemma 3.3 to get that $4 \in \delta(\mathcal{Q}_7) \subseteq \delta(\mathcal{Q}_{5k})$, as required.

Suppose instead that $k = 2$. By adding a number in $A_{5,2} = \{0, 10, 15, 20, 25\}$ to a number in $B_{5,2} = \{0, 3\} \cup \{i \mid 5 \leq i \leq 20\}$, it is readily verified that we get all elements of $\pi(\mathcal{Q}_{10}) \setminus \{4\}$. But $4 \in \delta(\mathcal{Q}_{10})$ by Corollary 3.7(a), so we are done.

Part 3 *If $n = 4k$ for some $k > 1$, then $n \in \Gamma$.*

Suppose $n = 4k$, $k > 1$; the restriction $k > 1$ is needed because of Lemma 3.2(c). Most deficiencies can be obtained in a fashion similar to the proof for $5k$. Applying Lemmas 3.4 and 3.6(c), we see that $\delta_{\text{off}}(Q)$ can take on any value in

$$A_{4,k} := \{\, 4i \mid 0 \leq i \leq 2(k^2-k),\ i \neq 1 \,\},$$

while $\delta_{\text{on}}(Q)$ can take on any value in the (adjusted set) $B_{4,k}$ given by

$$B_{4,k} := \{i \mid 0 \leq i \leq 6k,\ i \neq 1, 2, 3, 7\}.$$

If $k \geq 3$, then every number in $\pi(\mathcal{Q}_{4k})$ other than 3 and 7 can be obtained as $\delta(Q)$, $Q \in \mathcal{Q}_{4k}$, by adding an off-diagonal contribution that is divisible by 8 and not exceeding $8(k^2-k)$ to an on-diagonal contribution lying in $B_{4,k}$; we are implicitly using the fact that $6k - 8 \geq 8 - 1$. There are two remaining target values when

$k \geq 3$, namely 3 and 7. To obtain these, we apply Lemma 3.3 with $j = 2k$ to get that $\{3, 7\} \subseteq \delta(\mathcal{Q}_6) \subseteq \delta(\mathcal{Q}_n)$, as required.

Suppose instead that $k = 2$. By adding a number in $A_{4,2} = \{0, 8, 12, 16\}$ to a number in $B_{4,2} = \{0, 4, 5, 6, 8, 9, 10, 11, 12\}$, it is readily verified that we get all elements of $\pi(\mathcal{Q}_8)$ except 3 and 7. To obtain the first of these, we apply Lemma 3.3 to get that $3 \in \delta(\mathcal{Q}_3) \subseteq \delta(\mathcal{Q}_8)$. To obtain $\delta(Q) = 7$, we first consider the following symmetric 5×5 Latin rectangle R, involving the symbols $1, \ldots, 8$:

$$R \quad = \quad \begin{array}{|ccc|cc|} \hline 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \\ \hline 3 & 1 & 2 & 6 & 7 \\ \hline 4 & 5 & 6 & 1 & 8 \\ 5 & 4 & 7 & 8 & 2 \\ \hline \end{array}$$

All eight symbols appear at least twice, and every symbol except 3 appears an even number of times. These conditions allow us to apply Theorem 2.2 with $r = 5$ and $n = 8$ to extend R to a symmetric order 8 Latin square T. Now, $\delta(T) = 0$, but T inherits a couple of useful features from R that allow us to obtain other deficiencies: as indicated for R above, T has an order 3 Latin subsquare S_3 in its top left corner, and an order 2 Latin subsquare S_2 (involving the symbols 4 and 5) immediately below this. If we swap any two rows of S_3, and the two rows of S_2, but make no other change to T, then we obtain a new order 8 Latin square T' satisfying $\delta(T') = 7$.

Part 4 *If $m = 2k + 1 \in \Gamma$ for some $k \geq 4$, then $n = 4k + 3 \in \Gamma$.*

By Lemma 3.3, the assumption $m \in \Gamma$ implies that all values in $\pi(\mathcal{Q}_n)$ no larger than $(m^2 - m)/2$ lie in $\delta(\mathcal{Q}_n)$. It remains to construct an order n Latin square P such that $\delta(P) = s$ for a fixed but arbitrary s satisfying $(m^2 - m)/2 < s \leq (n^2 - n)/2$. In all cases, we will construct P by prolongating Q, where Q is of the form $C_2 \mathbin{\widetilde{\times}} C_m$, and $m = 2k + 1$.

Most of the following argument works for $k \geq 2$ (and so $m \geq 5$). It will be useful for Part 6 to work in this generality where possible. However, we will need to assume that $k \geq 4$ at the very end of this part of the proof.

To begin with, we define the group $G = C_2 \times C_m$. For each $x, y \in C_m$, the (x, y)-*block* of $G \times G$ is the set of elements $(X, Y) \in G \times G$ such that $X = (u, x)$, $Y = (v, y)$, $u, v \in C_2$. Such an (x, y)-block is said to be *diagonal* or *off-diagonal*, depending on whether or not $x = y$.

G has many transversals, and the varying asymmetry of these transversals is the key to the construction. The map $x \mapsto x^2$ is a bijection of C_m, so the main diagonal

$$D = \{(g^i, g^i) \mid 1 \leq i \leq m\}$$

is a transversal of C_m; here, g is a generator of C_m. A second transversal is given by

$$D' = D(\sigma) = \{(g^i, g^{i+1}) \mid 1 \leq i \leq m\}.$$

The two disjoint transversals D and D' of C_m induce a transversal S of $C_2 \times C_m$ via a map of the form

$$\begin{aligned} D \cup D' &\to G \times G \\ (x, y) &\mapsto (X, Y)\,, \end{aligned}$$

where $X = (u_{x,y}, x)$, $Y = (v_{x,y}, y)$, and $u_{x,y}, v_{x,y} \in C_2$. Initially, we choose $u_{x,y} = v_{x,y}$ for all $(x, y) \in D$, thus ensuring that $Y = X$ for $(x, y) \in D$. To ensure that S is a transversal, we choose $u_{x,y} \neq v_{x,y}$ for all $(x, y) \in D'$.

It is clear that the above procedure gives a transversal of G. Let $P_0 = \mathrm{Prol}(G, S)$. Then $\delta(P_0) = 3m$ because there are six non-commuting pairs corresponding to each off-diagonal element (X, Y) in the transversal: (X, Y), (X, ω), (ω, Y), and the transposes of these pairs; here, ω is the single element in $P_0 \setminus G$.

Claim 1 *If $m = 2k+1 \geq 5$ (and so $n = 2m+1 \geq 11$), then by taking either P_0 or some related prolongation, we obtain a quasigroup P of order n whose deficiency equals any desired element of $\pi(\mathcal{Q}_n)$ greater than $3m - 2$, with the exception of $3m + 1$.*

There are various deficiency-changing ways to alter the construction of P_0 that together enable us to justify Claim 1. First, we can make diagonal alterations by changing the transversal: we choose $v_{x,x}$ different from $u_{x,x}$ for i elements $x \in G$, $0 \leq i \leq m$. To ensure that we still obtain a transversal, we need to take $u_{x,y} = v_{x,y}$ whenever $(x, y) \in D'$, $xy = ww$, and w is one of the i elements for which $v_{w,w} \neq u_{w,w}$. The changes for $(x, y) \in D'$ have no effect on the deficiency, but those on the diagonal increase the deficiency of the prolongated quasigroup by $3i$, for the same reason as above.

Independently of the diagonal alterations, we can increase the off-diagonal contributions by arguing as in the proof of Lemma 3.4(a) for $j = 2$. However, there are some differences that need to be mentioned. For each $x \neq y$, we "nominate" either the (x, y)- or the (y, x)-block as the one that may be changed. In the proof of Lemma 3.4(a), the implicit nomination consisted of all (x, y)-blocks with $x < y$ (for some linear order $<$). Here, we need to be more careful: we do not want to affect the transversals, so the nominations must avoid blocks containing elements of D'. Thus, we nominate all (x, y)-blocks with $x < y$, with the exception that if such a block contains an element of D', we instead nominate its *partner*, the (y, x)-block.

This gives us a set of $(m^2 - m)/2$ nominated blocks. As before, multiplication in every (x, y)-block consists of defining $XY = (\gamma_{x,y}(uv), xy)$ for all $X = (u, x)$, $Y = (v, y)$, $u, v \in C_2$, where $\gamma_{x,y}$ is a permutation of C_2. For all except the nominated blocks, we take $\gamma_{x,y}$ to be the identity map. For nominated blocks, $\gamma_{x,y}$ may be either the identity map in C_2 ("no change") or the non-trivial permutation of C_2 ("change"). In either case, the change in the prolongated Latin square caused by a non-trivial $\gamma_{x,y}$ is restricted to the (x, y)-block, so we only need to examine this block and its partner block to determine what effect this block change has on the deficiency.

When we are computing the increase in the deficiency caused by each changed nominated block, we need to consider two kinds of blocks: the m nominated blocks whose partner block contains an element of D', and the $(m^2 - 3m)/2$ other nominated blocks. For both kinds of blocks, changing the block increases the *before-prolongation deficiency* by 4. If the partner block does not contain an element of D', then the block change also increases the *after-prolongation deficiency* by 4. However, if the partner block does contain an element of D', then the after-prolongation deficiency is only increased by 3. This last situation is illustrated below: the contribution towards $\delta(P)$ of the two blocks that are given in the diagram increases from 1 on the left (before the block change) to 4 on the right (after the block change).

$*$	$*$	a	b
$*$	$*$	b	a
a	ω	$*$	$*$
b	a	$*$	$*$

is changed to

$*$	$*$	b	a
$*$	$*$	a	b
a	ω	$*$	$*$
b	a	$*$	$*$

If we make all the diagonal and off-diagonal alterations as described above, then there are no commuting pairs left in the quasigroup, so these changes allow us to go from a deficiency of $3m$ to one of $(n^2 - n)/2$ in steps of 3 and 4, with at least $m \geq 5$ steps of each size. It is clear that this allows us to obtain all elements of $\pi(\mathcal{Q}_n)$ greater than $3m - 1$ with the exception of $3m + 1$, $3m + 2$, and $3m + 5$.

Now, $3m + 6$, $3m + 3$ and $3m$ can each be obtained as above by changing at most two nominated blocks. Since there are $m \geq 5$ off-diagonal blocks containing elements of S, we can in each case choose $X_0 = (u_0, x_0)$ such that $(X_0, Y_0) \in S$ and $Y_0 = (v, y_0)$, and the (y, x)-block is unchanged. If we now use a variant prolongation $\mathrm{Prol}(G, S; X_0)$, then the deficiency is lowered by one; this is because there are only four non-commuting pairs in P corresponding to (X_0, Y_0), namely (X_0, ω), (ω, Y_0), and the transposes of these pairs. Thus we obtain prolongated quasigroups with deficiencies $3m + 5$, $3m + 2$, and $3m - 1$. This finishes the proof of Claim 1.

Recall that we have already handled deficiencies of at most $(m^2 - m)/2$. Thus, we are done if $(m^2 - m)/2 \geq 3m + 1$. This holds when $k \geq 4$ (and $m \geq 9$).

Part 5 *If $2k - 1 \in \Gamma$ for some $k \geq 6$, then $n = 4k + 1 \in \Gamma$.*

The proof of this part is similar to the case $n = 4k + 3$, so we concentrate on the differences. Letting $m = 2k$, the main diagonal of C_m no longer provides a transversal of C_m: indeed, parity considerations imply that the main diagonal of any symmetric Latin square T of even order contains no more than half the elements of any transversal.

However, the set $T_m = D_m \cup E_m \subset C_m \times C_m$ forms a transversal of C_m, where

$$D_m = \{(g^i, g^i) \mid 1 \leq i \leq k\},$$
$$E_m = \{(g^i, g^{i+1}) \mid 1 \leq i \leq k\},$$

and g is a generator of C_m. We then obtain a transversal S of the group $G = C_2 \times C_m$ by taking two elements $(X, Y) \in G \times G$ corresponding to each $(x, y) \in T_m$: in both cases, the C_m-components of X and Y are x and y, respectively, but in one case, the C_2-components of X and Y are the same, while in the other, they are different.

Exactly k elements in S are of the form (X, X), so as in the previous part, we see that the resulting prolongation $P_1 = \mathrm{Prol}(G, S)$ satisfies $\delta(P_0) = 9k$. We then obtain the following claim. We omit the proof because it is so similar to that of Claim 1.

Claim 2 *If $m = 2k \geq 4$ (and so $n = 2m + 1 \geq 9$), then by taking either P_1 or some related prolongation, we obtain a quasigroup P of order n whose deficiency equals any element of $\pi(\mathcal{Q}_n)$ greater than $9k - 2$, with the exception of $9k + 1$.*

The assumption $2k - 1 \in \Gamma$ implies that all values in $\pi(\mathcal{Q}_n)$ that are no larger than $(2k-1)(k-1)$ lie in $\delta(\mathcal{Q}_n)$. This part of the proof is now complete because $(2k-1)(k-1) \geq 9k + 1$ for $k \geq 6$.

Part 6 *If $n \neq 4, 5$, then $n \in \Gamma$.*

We already know that all odd numbers $n \leq 9$, $n \neq 5$, lie in Γ, and we show below that $\{11, 13, 17\} \subset \Gamma$. Assuming this fact for now, we finish the proof for all other n, beginning with odd n. Assume that some odd number $n \neq 5$ is not in Γ, and that n is a minimal counterexample. Then $n \geq 15$. But we also know that such a number is in Γ if it is a multiple of 5 or 7, so we need to consider only numbers of the form $n = 4k + 3$ for $k \geq 4$ and $n = 4k + 1$ for $k \geq 7$. In the former case, we already know that $m = 2k + 1 \in \Gamma$ since $5 < m < n$. Similarly, in the latter case, we already know that $m = 2k - 1 \in \Gamma$. Thus, Part 4 or Part 5 give a contradiction to the minimality of n.

Suppose instead that $n = 2m$ is even. In view of Part 3, we may assume that m is of the form $2k + 1$ for some $k \geq 0$. If $k \geq 3$, then $m \in \Gamma$, and so $n \in \Gamma$ by Lemma 3.9. The cases $k = 0, 1$ follow from Part 1, while the case $k = 2$ follows from Part 2.

It remains to show that $\{11, 13, 17\} \subset \Gamma$. We first consider $n = 11$. Claim 1 in Part 4 for $m = 5$ provides us with all possible deficiencies larger than 13, except for 16. To obtain all remaining deficiencies, we begin with the following order 7 Latin rectangle:

$R =$

S_5				6	7
				7	6
				8	9
				9	10
				10	11
S_2	8	9	10	11	1
	9	10	11	1	10

Above, S_5 indicates any symmetric order 5 Latin subsquare involving the symbols $1, \dots, 5$, and S_2 indicates the order 2 Latin subsquare involving the symbols 6 and 7 that makes R symmetric. Note that all eleven symbols occur at least three times in R, and seven of them occur an odd number of times (namely $1, \dots, 5, 10, 11$). Therefore we can apply Theorem 2.2 with $r = 7$ and $n = 11$ to extend R to a symmetric order 11 Latin square T.

By construction, T contains the Latin subsquare S_5 in the top left position, and the Latin subsquare S_2 beneath it. The fact that T is a Latin square then implies that the part of T lying directly beneath S_2 is a column-balanced 4×2 Latin subrectangle $R_{4,2}$ (containing the symbols $8, 9, 10, 11$). Swapping the columns of either S_2 or $R_{4,2}$ gives a contribution of 4 or 8, respectively, to the deficiency of an altered order 11 Latin square, and replacing S_5 by an arbitrary order 5 Latin square (using the same symbols) gives a contribution equal to any desired element of $\delta(\mathcal{Q}_5)$. Each of these alterations can be done independently of each other, and the resulting Latin square T' has deficiency equal to the sum of the contributions corresponding to the replacements for S_5, S_2, and $R_{4,2}$. Consequently, we get as deficiencies all values in $\delta(\mathcal{Q}_5)$ incremented by 0, 4, 8, or 12. This set of values yields, in particular, all deficiencies less than 17, so we are done.

The last two numbers to be considered, 13 and 17, are of the form $n = 4k + 1$ for $k = 3, 4$. Claim 2 in Part 5 provides us with all possible deficiencies greater than $9k - 2$, except $9k + 1$. To obtain the remaining deficiencies, we begin with the following symmetric order $2k - 1$ Latin rectangle R.

$R =$

S_{2k-1}				$2k \quad 2k+1$ $2k+1 \quad 2k$
				$\vdots$
				$4k-4 \quad 4k-3$ $4k-3 \quad 4k-4$
				$4k-2 \quad 4k-3$
S_2^1	.....	S_2^{k-1}	...	$4k \quad 1$ $1 \quad 4k+1$

Within R, S_{2k-1} is any symmetric order $2k-1$ Latin square involving the symbols $1,\dots,2k-1$, and S_2^i is an order 2 Latin square containing the symbols $2(k+i)-2$ and $2(k+i)-1$ for $i=1,\dots,k-1$. Since R is symmetric, the entries in each S_2^i and the other two missing entries in the last two rows—all omitted to avoid clutter—can be read off from the last two columns of R.

Note that all $4k+1$ symbols occur at least once in R, and $2k+1$ of them occur an odd number of times (namely $1,\dots,2k-1,4k,4k+1$). Therefore we can apply Theorem 2.2 with $r=2k+1$ and $n=4k+1$ to extend R to a symmetric order $4k+1$ Latin square T. The fact that T is a Latin square then implies that the part of T lying directly beneath S_2^1 is a column-balanced $2k\times 2$ Latin subrectangle $R_{2k,2}$ (containing the symbols $2k+2,\dots,4k+1$).

Swapping the columns of any given S_2^i gives a contribution of 4 to the deficiency of an altered order $4k+1$ Latin square, and swapping the columns of $R_{2k,2}$ gives a contribution of $4k$. These alterations can be done independently of each other and the resulting Latin square T' has deficiency equal to the sum of the contributions, yielding a deficiency equal to any multiple of 4 between 0 and $8k-4$, inclusive. Independently of these alterations, we can replace S_{2k-1} by an arbitrary order $2k-1$ Latin square (using the same symbols), giving an additional contribution equal to any desired element of $\delta(\mathcal{Q}_{2k-1})\supseteq\pi(\mathcal{Q}_{2k-1})\setminus\{4\}$ for $k\geq 3$. This allows us to get a deficiency equal to any desired element in $\delta(\mathcal{Q}_{4k+1})$ that is no larger than $(2k-1)(k-1)+8k-4$; the assumption $k\geq 3$ is needed to ensure that $\pi(\mathcal{Q}_{2k-1})$ contains at least three consecutive integers, allowing us to span the gaps between multiples of 4. Since $(2k-1)(k-1)+8k-4>9k-2$ for $k\geq 3$, we are done. □

Finally, we return to our original motivation, which was to investigate commuting probabilities. The characterization of $\delta(\mathcal{Q}_n)$ will allow us to characterize in the following theorem the minimum order, and indeed all possible orders, of a quasigroup Q satisfying $\Pr(Q)=r$ for a given rational number r. However, this characterization is not as simple as that of $\delta(\mathcal{Q}_n)$, justifying the decision to concentrate on deficiencies in our above investigation. We use the p-adic valuation function $\nu_p:\mathbb{Q}^*\to\mathbb{Z}$ defined in Section 2.

Theorem 3.10. *Let $\mu_{\mathcal{Q}}(j,k)$ be the minimum order of a quasigroup with commuting probability j/k, where $j,k\in\mathbb{N}$ are coprime and $j\leq k$. Let m_0 be the smallest integer whose square is divisible by k, i.e. $\nu_p(m_0)=\lceil\nu_p(k)/2\rceil$ for all primes p, let*

$$m=\begin{cases}2m_0, & \text{if } k-j \text{ is odd and } \alpha_2(k) \text{ is even,}\\ m_0, & \text{otherwise,}\end{cases}$$

and let $M(j,k)=m\lceil k/mj\rceil$.

(a) If Q is a quasigroup with $\Pr(Q)=j/k$, then $|Q|$ is divisible by m.
(b) $\mu_{\mathcal{Q}}(j,k)$ is divisible by $M(j,k)$.

(c) In most instances, $\mu_{\mathcal{Q}}(j,k) = M(j,k)$*. The only exceptions are as follows:*

$$\begin{aligned} \mu_{\mathcal{Q}}(5,8) &= 8, \\ \mu_{\mathcal{Q}}(17,25) &= 10, \\ \mu_{\mathcal{Q}}(n^2-2i, n^2) &= 2n, \text{ for } i \in \{1,2\} \\ \mu_{\mathcal{Q}}(in^2-1, in^2) &= 4n, \text{ for } i \in \{1,2\}. \end{aligned}$$

Above, $n \in \mathbb{N}$ *is arbitrary, but subject to the conditions that* $j > 0$*, and* j, k *are coprime.*

(d) There exists a quasigroup Q *of order* N *with* $\Pr(Q) = j/k$ *if and only if* $N \geq \mu_{\mathcal{Q}}(j,k)$*, and* N *is divisible by* m*.*

Proof. In the case $j = k = 1$, we have $m = M(1,1) = 1$. Clearly, $\mu_{\mathcal{Q}}(1,1) = 1$, and there are commutative quasigroups of all orders. From now on, we may assume that $1 \leq j < k$.

We first prove part (a). For a quasigroup Q with $\Pr(Q) = j/k$, it follows immediately from (2.2) that $\delta(Q) = |Q|^2(k-j)/2k$. Since $\delta(Q)$ is an integer, and j is coprime to k, we see that k must be a divisor of $|Q|^2$, which implies that m_0 is a divisor of $|Q|$. For $|Q|^2(k-j)/2k$ to be an integer, we also need to cancel the factor 2 below the line. This is certainly possible if m_0^2/k is even, i.e. if $\nu_2(k)$ is odd, and it is also possible if $k-j$ is even. However, if $\nu_2(k)$ is even and $k-j$ is odd, then we need $|Q|$ to be divisible by $2m_0$ in order for $|Q|^2(k-j)/2k$ to be an integer. This finishes the proof of (a), but note conversely that *the desired deficiency value,* $|Q|^2(k-j)/2k$*, is an integer whenever* $|Q|$ *is divisible by* m*.*

We next establish the exceptional cases in (c). Suppose first that $(j,k) = (5,8)$, and so $m = 4$ and $M(5,8) = 4$. If $Q \in \mathcal{Q}_4$ and $\Pr(Q) = 5/8$, then we would have $\delta(Q) = 3$, contradicting Theorem 3.2(c). However, for $Q \in \mathcal{Q}_8$, $\Pr(Q) = 5/8$ implies $\delta(Q) = 12$. Since $12 \in \delta(\mathcal{Q}_8)$, we are done. The case $(j,k) = (17,25)$ similarly leads to $m = 5$ and $M(17,25) = 5$. However, $Q \in \mathcal{Q}_5$ satisfying $\Pr(Q) = 17/25$ would again contradict Theorem 3.2(c), but this probability arises for $Q \in \mathcal{Q}_{10}$.

Suppose next that $k = n^2 > 1$, and so $m = n$. Suppose also that $j = n^2 - 1$, and so $M(j,k) = 2n$. But if $\Pr(Q) = j/k$ for some quasigroup Q with $|Q| = 2n$, then it would follow that $\delta(Q) = 2$, contradicting Theorem 1.2(a). On the other hand, $|Q| = 4n$ leads to $\delta(Q) = 8$, and that is always possible. The other two exceptions for $k = n^2$, namely $j \in \{n^2-2, n^2-4\}$, lead to $M(j,k) = n$. For $|Q| = n$, we would need the impossible values $\delta(Q) \in \{1,2\}$, but for $|Q| = 2n$, we are looking for values $\delta(Q) \in \{4,8\}$; both these values are possible because $n \geq 3$ (since $k-j$ is even, forcing $k = n^2$ to be odd, and $n^2 - 2 > 0$).

The final exception is $(j,k) = (2n^2-1, 2n^2)$ for some $n > 1$. Thus, $m = 2n$ and $M(j,k) = 2n$. If $\Pr(Q) = j/k$ for some quasigroup $Q \in \mathcal{Q}_{2n}$, then it would follow that $\delta(Q) = 1$, contradicting Theorem 1.2. On the other hand, for $Q \in \mathcal{Q}_{4n}$, $\Pr(Q) = (2n^2-1)/2n^2$ implies $\delta(Q) = 4$, which is possible.

From now on, we assume that (j,k) is not one of the listed exceptions. We write $r = j/k$, and $M = M(j,k)$. As a first step towards proving that $\mu_{\mathcal{Q}}(j,k) = M(j,k)$, we claim that $d := M^2(k-j)/2k \geq 3$. Now, $M = sm_0$ and $m_0^2 = tk$ for some $s,t \in \mathbb{N}$, so $d = s^2t(k-j)/2$.

Suppose first that $t = 1$, and so $k = n^2$ is a perfect square. Suppose also that $k - j$ is odd. Thus, $j \leq k-3$, and $\alpha_2(k)$ is even. Consequently, $M \geq 2m_0$, and $d \geq 4(3)/2$. If instead $t = 1$, $k = n^2$, and $k - j$ is even, then $k - j \geq 6$, and so $d \geq 6/2$.

Next, suppose $t = 2$, and so $k = 2n^2$ for some $n \in \mathbb{N}$. In view of the fact that j and k are coprime, and $j < k - 1$, we again have $k - j \geq 3$, and so $d \geq 2(3)/2$, as required.

Next, suppose that $t = 3$, and so $k = 3n^3$ for some $n \in \mathbb{N}$. If $k - j$ is odd, then also $\alpha_2(k)$ is even, and so $M \geq 2m_0$ and $d \geq 2^2(3)/2$. Alternatively, if $t = 3$ and $k - j$ is even, then $d \geq (3)(2)/2$. The case $t = 4$ cannot arise, and $t = 5$ is similar to $t = 3$. Finally, if $t \geq 6$, then $d \geq 6/2$. This completes the proof of the claim.

For a quasigroup of a given order N and deficiency $\delta > 0$ to exist, δ must be an integer, it must be no less than 3, it must be no larger than $(N^2 - N)/2$ and, finally, there is a "missing deficiency" for $N \in \{4, 5\}$. The assumption that N is divisible by m is equivalent to δ being an integer, while the above claim established that $\delta \geq 3$. The missing deficiencies for $N \in \{4, 5\}$ are ruled out since they are covered by two of the exceptional values of (j,k) in (c). Thus, it follows that, as long as $N \geq M$ and N is divisible by m, the existence of a quasigroup Q of order N with $\Pr(Q) = r$ is equivalent to the inequality $N^2(1-r)/2 \leq (N^2 - N)/2$, or equivalently, $N \geq 1/r$. Since $M(j,k) \geq 1/r$ by definition, it follows that there exist quasigroups Q with $\Pr(Q) = j/k$ of every order $N \geq \mu(j,k)$, N divisible by m.

On the other hand, if $N < M(j,k)$ and N is a multiple of m, then $N < 1/r$ and so no quasigroup Q of order N with $\Pr(Q) = r$ can exist. This finishes the proof of (c) and (d). Part (b) follows immediately in the non-exceptional cases of (c), and our proof of the exceptional cases shows that it holds in those cases also. □

References

[1] R.H. Bruck, *Some results in the theory of quasigroups*, Trans. Amer. Math. Soc. **55** (1944), 19–52.

[2] S.M. Buckley, *Minimal order semigroups with specified commuting probability*, Semigroup Forum, to appear.

[3] S.M. Buckley, datafile associated with this paper; available at `http://archive.maths.nuim.ie/staff/sbuckley/Papers/qgp_data.pdf`.

[4] S.M. Buckley, D. MacHale, and Á. Ní Shé, *Finite rings with many commuting pairs of elements*, preprint; available at `http://archive.maths.nuim.ie/staff/sbuckley/Papers/bms.pdf`.

[5] A.B. Cruse, *On embedding incomplete symmetric Latin squares*, J. Combinatorial Theory Ser. A **16** (1974), 18–22.

[6] J. Dénes and E. Pásztor *Some problems on quasigroups* (Hungarian), Magyar Tud. Akad. Mat. Fiz. Oszt. Közl. **13** (1963), 109–118.
[7] H.-L. Fu, *On the constructions of certain types of Latin squares having prescribed intersections*, PhD thesis, Auburn University, 1980.
[8] B. Givens, *The probability that two semigroup elements commute can be almost anything*, College Math. J. **39** (2008), 399–400.
[9] W.H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.
[10] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.
[11] D. MacHale, *Probability in finite semigroups*, Irish Math. Soc. Bull. **25** (1990), 64–68.
[12] B.D. McKay, *Latin squares*, webpage available at `http://cs.anu.edu.au/~bdm/data/latin.html`; accessed 15 March 2014.
[13] B.D. McKay, A. Meynert, and W. Myrvold, *Small latin squares, quasigroups, and loops*, J. Combin. Des. **15** (2007), 98–119.
[14] V. Ponomarenko and N. Selinski, *Two semigroup elements can commute with any positive rational probability*, College Math. J. **43** (2012), 334–336.
[15] D.J. Rusin, *What is the probability that two elements of a finite group commute?*, Pac. J. Math. **82** (1979), 237–247.

Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.

E-mail address: `stephen.buckley@maths.nuim.ie`