Two Quasigroup Elements Can Commute With Any Positive Rational Probability

A quasigroup is a set Q with a binary operation $*$ such that Q is closed under $*$ and for all elements a, b of Q, the equations $a * x = b$ and $x * a = b$ both have unique solutions for x. This property is commonly referred to as uniqueness of left and right “division”, although the quasigroup operation may not be multiplicative in nature. From this property it follows that each row and column in the Cayley table is a permutation of the quasigroup elements. The solved states of many well-known puzzles, such as Latin squares and sudoku, also satisfy this permutation property, and can therefore be viewed as quasigroup tables without headings.

The commuting probability of an algebraic structure is the probability that two of its elements, chosen independently and uniformly at random, will commute. For finite structures, this is equivalent to the probability that a randomly chosen element in the Cayley table will be unchanged after a transposition of the rows and columns. Commuting probabilities of groups have been studied extensively, as has the notion of an element being unchanged by an arbitrary automorphism of a group ([1], [2]). It is well-known that the commuting probability of a non-abelian group is at most $\frac{5}{8}$ ([3]). As for semigroups, it has been shown that a finite semigroup may have any positive rational commuting probability. The original proof of this fact in [4] involved four families of semigroups, and a construction involving a single family was later given in [5]. Here we will show a similar result for quasigroups; that is, we will construct a single family of finite quasigroups whose commuting probabilities cover all rationals in $(0, 1]$. In preparation, we first define the following function:

Definition. *Let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $a, b \in \mathbb{N}_0$, we define $f(a, b) = \frac{a(a-1)}{2} + b$. We also define $F_k = \{(a, b) \in \mathbb{N}_0^2 : (a > b) \wedge (f(a, b) < k)\}$.*

Taking $k = 4$ as an example, we see that $f(1, 0) = 0, f(2, 0) = 1, f(2, 1) = 2, f(3, 0) = 3$, but $f(3, 1) = 4$. So $F_4 = \{(1, 0), (2, 0), (2, 1), (3, 0)\}$.

Lemma 1. *For each $k \in \mathbb{N}_0$, there is a unique pair $(a, b) \in \mathbb{N}_0^2$ such that both $a > b$ and $f(a, b) = k$.*

Proof. For $k \in \mathbb{N}_0$, let $a \in \mathbb{N}_0$ be maximal such that $\frac{a(a-1)}{2} \leq k$. Then a exists and is unique. Now let $b = k - \frac{a(a-1)}{2}$. Suppose by way of contradiction that $a \leq b$. Then we have $k = b + \frac{a(a-1)}{2} \geq a + \frac{a(a-1)}{2} = \frac{a(a+1)}{2}$, which violates our assumption that a was maximal. So $a > b$. Finally, we see that $f(a, b) = \frac{a(a-1)}{2} + k - \frac{a(a-1)}{2} = k$. ■

Corollary. *Let F_k be defined as above. Then $|F_k| = k$.*

We now use the above function to construct a two-parameter family of quasigroups. We define our ground set G_n to be $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Now if the elements of G_n are combined with the usual addition operations, this will divide the Cayley table into n^2 two-by-two “blocks” based on a shared first element of the ordered pairs within each block. The second elements of each pair within these blocks will be arranged like so:

$\begin{vmatrix}0 & 1\\ 1 & 0\end{vmatrix}$ (see also the unshaded blocks in Table). However, under the usual addition operations, the commuting probability will always be 1. We will instead define an operation that “flips” the second entries of some blocks to the opposite values, *i.e.* $\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix}$ (see also the shaded blocks in Table). If a block is flipped, and its counterpart on the opposite side of the main diagonal is not flipped, then the pairs of elements which combine to give those entries in the table will not commute. We will choose to only flip blocks which appear below the main diagonal of the Cayley table, which are arranged in a triangular formation. In examining the construction of F_k, we see that the ordered pairs in F_k correspond exactly to the “coordinates” of the blocks below the main diagonal in the table, indexed by the first components of the elements of G_n which give rise to these entries (*i.e.* the $\mathbb{Z}/n\mathbb{Z}$ components). Specifically, the elements of F_k index the first k blocks encountered by traversing the sub-diagonal blocks first from left-to-right, then from top-to-bottom. Hence we will choose which blocks to flip using F_k, which will allow us to vary the commuting probability by changing the value of k.

We now define our quasigroup operation. In doing so, we abuse notation slightly by considering the elements of the ordered pairs in F_k to be from $\mathbb{Z}/n\mathbb{Z}$, rather than $\mathbb{N}_0$ as they were defined. For instance, if $n = 5$, we will consider the element $(2, 1)$ of F_4 to correspond to the pair $([2], [1])$ where the congruence classes are taken modulo 5. Then, for $k \in \mathbb{N}_0$ where $k < \frac{n^2}{2}$, we define $(a, b) *_k (c, d)$ as $(a + c, b + d + 1)$ if $(a, c) \in F_k$ and $(a + c, b + d)$ otherwise. Note that since $a, c \in \mathbb{Z}/n\mathbb{Z}$ and $b, d \in \mathbb{Z}/2\mathbb{Z}$, the addition operations are performed modulo n and modulo 2 respectively. Finally, we let $Q_{n,k} = (G_n, *_k)$. As an example of this construction, we have shown the Cayley table for $Q_{3,2}$, separated into the two-by-two blocks mentioned earlier. Note that the number of elements in the Cayley table is $|G_n|^2 = 4n^2$, in this case 36.

$Q_{3,2}$	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)	(2, 1)	(2, 0)
(1, 0)	(1, 1)	(1, 0)	(2, 0)	(2, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 0)	(1, 1)	(2, 1)	(2, 0)	(0, 1)	(0, 0)
(2, 0)	(2, 1)	(2, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(2, 1)	(2, 0)	(2, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)

Table 1. The Cayley table for $Q_{3,2}$; cells for which $(a, c) \in F_k$ are shaded.

Theorem 1. *$Q_{n,k}$ is a quasigroup with commuting probability $\frac{n^2-2k}{n^2}$.*

Proof. Suppose that $(x_1, y_1) *_k (c, d) = (a, b)$ and $(x_2, y_2) *_k (c, d) = (a, b)$. Then $x_1 = x_2 = a - c$. Now if $(x_1, c) \in F_k$, then $y_1 = y_2 = b - d - 1$, and if not, then $y_1 = y_2 = b - d$. So $(x_1, y_1) = (x_2, y_2)$. Now suppose that $(a, b) *_k (x_1, y_1) = (c, d)$ and $(a, b) *_k (x_2, y_2) = (c, d)$. Then $x_1 = x_2 = c - a$. As before, if $(a, x_1) \in F_k$, then $y_1 = y_2 = d - b - 1$, and if not, then $y_1 = y_2 = d - b$. So $(x_1, y_1) = (x_2, y_2)$, and therefore $Q_{n,k}$ is a quasigroup.

Two elements $(a, b), (c, d)$ of $Q_{n,k}$ will not commute iff either (a, c) or $(c, a) \in F_k$. By the corollary, there are exactly $2k$ choices for the pair (a, c) such that (a, b) and (c, d) do not commute. Additionally, there are 4 ways to choose b and d for a given a and c, so we see that there are $8k$ pairs of elements of $Q_{n,k}$ which do not commute.

Since each pair of elements corresponds to an entry in the Cayley table, of which there are $4n^2$, we see that the commuting probability of $Q_{n,k}$ is $1 - \frac{8k}{4n^2} = \frac{n^2-2k}{n^2}$. ■

Theorem 2. *For all $a, b \in \mathbb{N}$ with $a \leq b$, there exists a quasigroup with commuting probability $\frac{a}{b}$.*

Proof. Let $n = 2b$, $k = 2b^2 - 2ab$. Note that $k < 2b^2 = \frac{n^2}{2}$. Then by Theorem 1, the commuting probability of $Q_{n,k}$ is $\frac{4b^2-4b^2+4ab}{4b^2} = \frac{a}{b}$. ■

While the above construction can generate quasigroups with any positive rational commuting probability, these quasigroups are not necessarily the smallest ones with that commuting probability. For $\frac{a}{b} = \frac{1}{3}$, this construction produces a quasigroup with order 12. However, there exist smaller quasigroups with commuting probability $\frac{1}{3}$, for example $(\mathbb{Z}/3\mathbb{Z}, -)$. Further research on this topic may involve finding the smallest quasigroups with particular commuting probabilities.

Summary. A quasigroup is a set with a binary operation in which both left and right division are unique. Equivalently, every row and column in a quasigroup table is a permutation of its elements. The commuting probability of a quasigroup is the probability that two of its elements, chosen at random, will commute. In this paper, we show that a quasigroup may have any rational number in $(0, 1]$ as a commuting probability.

References

1. Harsha Arora and Ram Karan, What is the probability an automorphism fixes a group element? *Communications in Algebra* **45.3** (2017) 1141–1150.
2. Parama Dutta and Rajat Kanti Nath, Autocommuting probability of a finite group, *Communications in Algebra* **46.3** (2018) 961–969.
3. W. H. Gustafson, What is the probability that two group elements commute? *American Mathematical Monthly* **80** (1973) 1031–1034.
4. Vadim Ponomarenko and Natalie Selinski, Two Semigroup Elements Can Commute With Any Positive Rational Probability, *College Mathematics Journal* **43.4** (2012) 334–336.
5. Michelle Soule, A Single Family of Semigroups with Every Positive Rational Commuting Probability, *College Mathematics Journal* **45.2** (2014) 136–139.