A quasigroup is a group-like structure 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.
Two Quasigroup Elements Can Commute With Any Positive Rational Probability

A quasigroup is a group-like structure with the property that both left and right division are unique. 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 a finite group is the probability that two of its elements, chosen independently and uniformly at random, will commute. This is equivalent to the probability that a randomly chosen element in the Cayley table will be unchanged after a transposition. The commuting probability has been generalized to other automorphisms of groups ([1], [2]), and to other group-like structures, such as semigroups ([3], [5], [6]). It is well-known that the commuting probability of a non-abelian group is at most $\frac{2}{3}$ ([4]). 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 [5] involved four families of semigroups, and a construction involving a single family was later given in [6]. 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.** For $a, b \in \mathbb{N}$, we define $f(a, b) = \frac{a(a-1)}{2} + b$. We also define $F_k = \{(a, b) \in \mathbb{N}^2 : (a > b) \wedge (f(a, b) < k)\}$.

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

**Proof.** For $k \in \mathbb{N}$, let $a \in \mathbb{N}$ 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 $f(a, b) = \frac{a(a-1)}{2} + k - \frac{a(a-1)}{2} = k$. $\blacksquare$

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

We now use the above function to construct our two-parameter family of quasigroups. For $n \in \mathbb{N} \setminus \{0, 1\}$, we define $+_n$ and $-_n$ to be the addition and subtraction operators modulo $n$. We then let $G_n = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that $|G_n| = 4n^2$. For $k \in \mathbb{N}$ where $k < \frac{n(n+1)}{2}$, we define $*_k$ on $G_n$ as follows:

- if $(a, c) \in F_k$, then $(a, b) *_k (c, d) = (a +_n c, b +_n d +_n 1)$,
- otherwise, $(a, b) *_k (c, d) = (a +_n c, b +_n d)$.

Finally, we let $Q_{n, k} = (G_n, *_k)$. As an example of this construction, we have shown the Cayley table for $Q_{3, 2}$.

**Theorem 1.** $Q_{n, k}$ is a quasigroup with commuting probability $\frac{n^2 - 2k}{n^2}$. 
Let $Q_{n,k}$ be a quasigroup on $Q = \{0, 1, \ldots, n\}$ with $k$ columns. The commuting probability $\pi^c_{n,k}$ is given by 

$$\pi^c_{n,k} = \frac{1}{4n^2} \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} x + y \mod n.$$ 

Now suppose that $(a, b)\in\mathbb{Z}/n\mathbb{Z}$ does not commute, or $(c, d)\in\mathbb{Z}/n\mathbb{Z}$. By the corollary, there are exactly $k$ choices for $a$ and $c$ such that $(a, b)$ and $(c, d)$ do not commute. Additionally, there are $k$ ways to choose $b$ and $d$ for a given $a$ and $c$, so we see that there are $8k$ elements of $Q_n$ which do not commute. Therefore the commuting probability of $Q_{n,k}$ is 

$$\pi^c_{n,k} = 1 - \frac{8k}{4n^2} = \frac{n^2 - 2k}{n^2}.$$ 

**Theorem 2.** For all $a, b \in \mathbb{N} \setminus \{0\}$, there exists a quasigroup with commuting probability $\frac{a}{b}$. 

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

$$\pi^c_{n,k} = \frac{4b^2 - 4b^2 + 4ab}{4b^2 + 4ab} = \frac{a}{b}.$$ 

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 $(\mathbb{Z}/3\mathbb{Z}, -3)$. Further research on this topic may involve finding the smallest quasigroups with particular commuting probabilities.

**Summary.** A quasigroup is a group-like structure 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**


© THE MATHEMATICAL ASSOCIATION OF AMERICA