Two Semigroup Elements Can Commute With Any Positive Rational Probability

Vadim Ponomarenko (vadim@sciences.sdsu.edu) and Natalie Selinski (selinski@rohan.sdsu.edu), San Diego State University, San Diego, CA 92182

In a recent article in this *Journal*, Givens [2] defined the *commuting probability* of a finite semigroup as the probability that $x \star y = y \star x$ when x and y are chosen independently and uniformly at random from the semigroup. She asked which commuting probabilities can be achieved, and partially answered this question by showing that they are dense in $(0, 1]$. We prove that *every* rational in $(0, 1]$ can be achieved.

We begin by recalling Lagrange's celebrated four-square theorem (found, e.g., in [1]). It states that every natural number can be expressed as the sum of four integer squares; furthermore, three squares suffice unless the number is of the form $4^k(8m + 7)$.

Our proof requires four constructions. It is unknown whether a single semigroup family might suffice.

RATIONALS IN $(0, 1/3]$

Given positive integers a, b, c and nonnegative integer k, we define the family of semigroups $S(a, b, c, k)$, as follows. The ground set is $A \cup B \cup C \cup$

$D_1 \cup D_2 \cup \cdots \cup D_k$, where $|A| = a, |B| = b, |C| = c$, and $|D_1| = |D_2| = \cdots = |D_k| = 2$. Let $\alpha \in A, \beta \in B, \gamma \in C, \delta_1 \in D_1, \ldots, \delta_k \in D_k$, and define f on our semigroup by

$$f(x) = \begin{cases} \alpha & x \in A \\ \beta & x \in B \\ \gamma & x \in C \\ \delta_i & x \in D_i \end{cases},$$

and define the semigroup operation itself as $x \star y = f(x)$; it is routine to check that this is associative with commuting probability

$$\frac{a^2 + b^2 + c^2 + 4k}{(a + b + c + 2k)^2}.$$

Suppose the desired commuting probability is $\frac{p}{q}$. Set $M = 16pq - 8q + 3 = 8q(2p - 1) + 3$. This is a natural number not of the form $4^k(8m + 7)$ and hence we can find natural numbers x, y, z satisfying $x^2 + y^2 + z^2 = M$. Set $a = x + 1, b = y + 1, c = z + 1$. These are positive integers. Set $k = \frac{4q-a-b-c}{2}$. Since M is odd, one or three of x, y, z are odd, hence zero or two of a, b, c are odd, hence k is an integer. It is a routine exercise using Lagrange multipliers to show that $x + y + z$ is maximized on the surface $x^2 + y^2 + z^2 = M$ for $x = y = z = \sqrt{M/3}$. Hence $a + b + c \leq 3(1 + \sqrt{M/3})$. This is at most $4q$ hence k is nonnegative. Otherwise $3(1 + \sqrt{M/3}) > 4q$, which simplifies to $16q(3p - q) > 0$, which contradicts $\frac{p}{q} \leq \frac{1}{3}$. The commuting probability of $S(a,b,c,k)$ is

$$\frac{a^2+b^2+c^2+4k}{(a+b+c+2k)^2} = \frac{(a-1)^2+(b-1)^2+(c-1)^2+2(a+b+c)-3+4k}{(4q)^2} =$$

$$= \frac{(16pq-8q+3)+2(4q-2k)-3+4k}{16q^2} = \frac{16pq}{16q^2} = \frac{p}{q}.$$

RATIONALS IN (2/3, 1]

For positive integers a, b, c and nonnegative integer k, we define the family of semigroups $T(a,b,c,k)$, as follows. The ground set is as before. We define f this time via

$$f(x) = \begin{cases} i & x \in D_i \\ k+1 & x \in C \\ k+2 & x \in B \\ k+3 & x \in A \end{cases}.$$

If $f(x) > f(y)$, we let $x \star y = y \star x = x$; if $f(x) = f(y)$, we define $x \star y = x$. It is routine to check that this is associative with commuting probability

$$\frac{(a+b+c+2k)^2 + (a+b+c+2k) - a^2 - b^2 - c^2 - 4k}{(a+b+c+2k)^2}.$$

Let the desired commuting probability be $\frac{p}{q}$. Set $M = 16q^2 - 16pq - 4q + 3 = 4q(4q-4p-1)+3$; this is a natural number not of the form $4^k(8m+7)$ hence we can find natural numbers x, y, z satisfying $x^2+y^2+z^2 = M$. Set $a = x+1, b = y+1, c = z+1$; these are positive integers. Set $k = \frac{4q-a-b-c}{2}$. As before k is an integer and $x+y+z$ is maximized for

$x = y = z = \sqrt{M/3}$. Hence $a + b + c \leq 3(1 + \sqrt{M/3})$. This is at most $4q$ (and hence k is nonnegative); otherwise $3(1+\sqrt{M/3}) > 4q$, which simplifies to $4q(4(2q - 3p) + 3) > 0$, contradicting $2q - 3p \leq -1$. The commuting probability of $T(a, b, c, k)$ is

$$\frac{(a + b + c + 2k)^2 + (a + b + c + 2k) - a^2 - b^2 - c^2 - 4k}{(a + b + c + 2k)^2} =$$

$$= \frac{16q^2 + 4q - (a - 1)^2 - (b - 1)^2 - (c - 1)^2 - 2(a + b + c) + 3 - 4k}{(4q)^2} =$$

$$= \frac{16q^2 + 4q - M - 2(4q - 2k) + 3 - 4k}{16q^2} = \frac{16pq}{16q^2} = \frac{p}{q}.$$

RATIONALS IN (1/2, 2/3]

Let S be a semigroup on $\{1, 2, \ldots, n\}$, with operation $\star$ and commuting probability $\frac{m}{n^2}$. We define a new semigroup on $\{1, 2, \ldots, n\} \cup \{-1, -2, \ldots, -n\}$, with operation

$$x \circledast y = \begin{cases} -(|x| \star |y|) & x, y < 0 \\ |x| \star |y| & \text{otherwise.} \end{cases}$$

It is routine to check that this is associative with commuting probability

$$\frac{2m + 2n^2}{(2n)^2} = \frac{m + n^2}{2n^2} = \left(\frac{m}{n^2} + 1\right)/2.$$

We apply this construction to the semigroups $S(a, b, c, k)$ and observe that $y = (x+1)/2$ is a bijection between the rationals in $(0, 1/3]$ and the rationals in $(1/2, 2/3]$.

RATIONALS IN $(1/3, 1/2]$

Let T be a semigroup on $\{1, 2, \ldots, n\}$, with operation $\star$ and commuting probability $\frac{m}{n^2}$. We define a new semigroup on $\{1, 2, \ldots, n\} \cup \{-1, -2, \ldots, -n\}$, with operation

$$x \circledast y = \begin{cases} -(|x| \star |y|) & x < 0 \\ \\ |x| \star |y| & x > 0. \end{cases}$$

It is routine to check that this is associative with commuting probability

$$\frac{2m}{(2n)^2} = \left(\frac{m}{n^2}\right)/2.$$

We apply this construction to $T(a, b, c, k)$ and observe that $y = x/2$ is a bijection between the rationals in $(2/3, 1]$ and the rationals in $(1/3, 1/2]$.

REFERENCES

1. H. Davenport. *The higher arithmetic: An introduction to the theory of numbers.* Harper, New York NY, 1960.

2. B. Givens, The probability that two semigroup elements commute can be almost anything. *College Math. J.* **39**, no. 5 (2008) 399–400.