The Probability that Two Semigroup Elements Commute Can Be Anything

Vadim Ponomarenko

Department of Mathematics and Statistics, San Diego State University, 5500 Campanile Drive, San Diego CA 92182-7720
E-mail: vadim@sciences.sdsu.edu

Natalie Selinski

San Diego State University

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

We begin by recalling Lagrange's celebrated four-square theorem (found in, e.g., [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 $4^k(8m + 7)$.

The proof proceeds with four constructions; it is unknown if a single semigroup family can answer this question.

Claim 1 *Every rational in* $(0, 1/3]$ *is an achievable commuting probability.*

Proof. For positive integers a, b, c and nonnegative integer k, we consider the family of semigroups $S(a, b, c, k)$, as defined subsequently. The ground set is $A \cup B \cup C \cup D_1 \cup D_2 \cup \cdots \cup D_k$, where $|A| = a, |B| = b, |C| = c, |D_1| = |D_2| = \cdots = |D_k| = 2$. Let $\alpha \in A, \beta \in B, \gamma \in C, \delta_1 \in D_1, \ldots, \delta_k \in D_k$. We define f on our semigroup via $f(x) = \begin{cases} \alpha & x \in A \\ \beta & x \in B \\ \gamma & x \in C \\ \delta_i & x \in D_i \end{cases}$.

We define the semigroup operation as $x \star y = f(x)$; it is routine to check that this is associative, and that the commuting probability is $\frac{a^2+b^2+c^2+4k}{(a+b+c+2k)^2}$.

Let the desired commuting probability be $\frac{p}{q}$. Set $M = 16pq - 8q + 3 = 8q(2p-1)+3$; this is a natural number not of the form $4^k(8m+7)$ and hence by Lagrange's four-square theorem we can find natural 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 $k = \frac{4q-a-b-c}{2}$. Note that 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 in 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 $a+b+c \leq 3(1+\sqrt{M/3})$. We now prove this is at most $4q$ (and hence k is nonnegative); otherwise $3(1+\sqrt{M/3}) > 4q$, which simplifies to $16q(3p-q) > 0$, a contradiction since $\frac{p}{q} \leq \frac{1}{3}$. The commuting probability of $S(a,b,c,k)$ is $\frac{a^2+b^2+c^2+4k}{(a+b+c+2k)^2} = \frac{(a-1)^2+(b-1)^2+(c-1)^2+2(a+b+c)-3+4k}{(4q)^2} = \frac{(16pq-8q+3)+2(4q-2k)-3+4k}{16q^2} = \frac{16pq}{16q^2} = \frac{p}{q}$, as desired. ▮

Claim 2 *Every rational in* $(2/3, 1]$ *is an achievable commuting probability.*

Proof. For positive integers a, b, c and nonnegative integer k, we consider the family of semigroups $T(a,b,c,k)$, as defined subsequently. The ground set is $A \cup B \cup C \cup D_1 \cup D_2 \cup \cdots \cup D_k$, where $|A| = a, |B| = b, |C| = c, |D_1| = |D_2| = \cdots = |D_k| = 2$. We define f on our semigroup 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 define $x \star y = y \star x = x$. If $f(x) = f(y)$, we define $x \star y = x$. It is routine to check that this is associative, and that the commuting probability is $\frac{(a+b+c+2k)^2+(a+b+c+2k)-a^2-b^2-c^2-4k}{(a+b+c+2k)^2}$.

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 $4^k(8m+7)$ and hence by Lagrange's four-square theorem we can find natural 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 $k = \frac{4q-a-b-c}{2}$. Note that 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. As before, $x+y+z$ is maximized for $x = y = z = \sqrt{M/3}$. Hence $a+b+c \leq 3(1+\sqrt{M/3})$. We now prove this is at most $4q$ (and hence k is nonnegative); otherwise $3(1+\sqrt{M/3}) > 4q$, which simplifies to $4q(4(2q-3p)+3) > 0$, a contradiction since $2q - 3p \leq -1$. The commuting probability of $T(a,b,c,k)$ is $\frac{(a+b+c+2k)^2+(a+b+c+2k)-a^2-b^2-c^2-4k}{(a+b+c+2k)^2} = \frac{16q^2+4q-(a-1)^2-(b-1)^2-(c-1)^2-2(a+b+c)+3-4k}{(4q)^2} = \frac{16q^2+4q-M-2(4q-2k)+3-4k}{16q^2} = \frac{16pq}{16q^2} = \frac{p}{q}$, as desired. ▮

Claim 3 *Every rational in* $(1/2, 2/3]$ *is an achievable commuting probability.*

Proof. Let S be a semigroup on $\{1, 2, \dots, n\}$, with operation $\star$ and commuting probability $\frac{m}{n^2}$. We define a new semigroup on $\{1, 2, \dots, n\} \cup \{-1, -2, \dots, -n\}$, 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; its commuting probability is $\frac{2m+2n^2}{(2n)^2} = \frac{m+n^2}{2n^2} = (\frac{m}{n^2}+1)/2$. We now apply this construction to the semigroup family in Claim 1, and observe that $y = (x+1)/2$ is a bijection between the rationals in $(0, 1/3]$ and the rationals in $(1/2, 2/3]$. ▮

Claim 4 *Every rational in* $(1/3, 1/2]$ *is an achievable commuting probability.*

Proof. Let S be a semigroup on $\{1, 2, \dots, n\}$, with operation $\star$ and commuting probability $\frac{m}{n^2}$. We define a new semigroup on $\{1, 2, \dots, n\} \cup \{-1, -2, \dots, -n\}$, 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; its commuting probability is $\frac{2m}{(2n)^2} = (\frac{m}{n^2})/2$. We now apply this construction to the semigroup family in Claim 2, 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 Torchbooks/The Science Library. Harper & Brothers, New York, 1960.
2. Berit Givens. The probability that two semigroup elements commute can be almost anything. *College Math. J.*, 39(5):399–400, 2008.