Minimal order semigroups with specified commuting probability

STEPHEN M. BUCKLEY

Abstract. We determine the minimal order of a semigroup whose commuting probability equals any specified rational value in $(0, 1]$.

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

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

and the *commuting probability of* F is

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

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 $\Pr(F) \in (0, 1] \cap \mathbb{Q}$. However 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 [5] for groups and [6] for rings.
- The set of values in both cases has only one accumulation point exceeding $11/32$; see [9] for groups and [2] for rings.

By contrast for semigroups, there are only the obvious restrictions. MacHale [7] showed that if S is a semigroup, then $\Pr(S)$ can attain values arbitrarily close to 1 (and also arbitrarily close to 0), and a more elaborate recent proof of this result can be found in [1]. Givens [4] later showed that the set of values of $\Pr(S)$ is dense in $[0, 1]$, and finally Ponomarenko and Selinski [8] showed that $\Pr(S)$ can attain every value in $(0, 1] \cap \mathbb{Q}$.

In this paper, we determine the minimal order of a semigroup S satisfying $\Pr(S) = r$; we denote this minimal order by $\mathrm{Ord}(j, k)$ whenever $r = j/k$, $j, k \in \mathbb{N}$. Our characterization involves the well-known *p-adic valuation function* $\nu_p : \mathbb{Q}^* \to \mathbb{Z}$, as defined in Section 2. We also need the function $\alpha : \mathbb{N} \to \mathbb{N}$, where $\alpha(n)$ is the smallest number m with the property that n divides m^2. Explicitly $\alpha(p)$ is the positive integer satisfying $\nu_p(\alpha(n)) = \lceil \nu_p(n)/2 \rceil$ for all primes p, so $1 \le m \le n$, and m has the same prime factors as n.

Date: 04.03.2013.
2010 *Mathematics Subject Classification.* 20M99.

Theorem 1. *Suppose $j,k \in \mathbb{N}$ are coprime, and $1 \le j \le k$. Let $t \in \mathbb{N}$ be defined by*

$$t = \begin{cases} 2\alpha(k)j, & \text{if } j \text{ is even,} \\ & \qquad \text{or if } k \text{ and } \nu_2(k) \text{ are both even,} \\ \alpha(k)j, & \text{otherwise,} \end{cases}$$

and let r be the unique integer in $[0,t)$ such that $k = qt - r$ for some $q \in \mathbb{N}$. Then $\operatorname{Ord}(j,k) = (k+r)/j$.

The proofs in [1] and [8] are fairly elaborate. In particular, Ponomarenko and Selinski use four different families of semigroups to prove their result, and ask if a single family could suffice. Before our proof of Theorem 1, we answer this question in the affirmative using a certain easily constructed family of nilpotent semigroups. To prove Theorem 1, however, we need a different construction.

After some preliminaries in Section 2, we prove Theorem 1 in Section 3.

We wish to thank a referee for pointing out an error in the original version of Theorem 1.

2. Preliminaries

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 $r,s \in \mathbb{Q}^*$.

Suppose S is a semigroup. A *left zero* in S is an element $z \in S$ satisfies the identity $zx = z$, while a *right zero* satisfies the identity $xz = z$. An element is a zero if it is a left and right zero. A *left zero semigroup* is a semigroup satisfying the identity $xy = x$; similarly a *right zero semigroup* satisfies the identity $xy = y$.

If S is finite, then $\#_{\mathrm{CP}}(S) := |\operatorname{CP}(S)|$ and $\#_{\mathrm{NCP}}(S) := |S|^2 - \#_{\mathrm{CP}}(S)$ are the number of commuting and noncommuting pairs, respectively.

Note that two elements of a semigroup direct product $S = S_1 \times S_2$ commute if and only if their respective S_i-components commute for $i = 1,2$. This implies the following lemma.

Lemma 2. *If a semigroup S is the direct product of two finite semigroups S_1 and S_2, then $\Pr(S) = \Pr(S_1)\Pr(S_2)$.*

The next well-known lemma says that we can adjoin a zero to any semigroup. We omit the proof, which is trivial.

Lemma 3. *Suppose S is a semigroup and $S' := S \cup \{z\}$, where $z \notin S$. If we extend multiplication from S to S' by the equations $zz = zx = xz = z$ for all $x \in S$, then S' is also a semigroup.*

The following observation is based on the fact that all diagonal elements (x,x) of $S \times S$ lie in $\operatorname{CP}(S)$, and all other elements of $\operatorname{CP}(S)$ occur as pairs of the form $\{(x,y),(y,x)\}$.

Observation 4. If S is a finite semigroup, then $\#_{\mathrm{CP}}(S) - |S|$ is even and non-negative.

For $r \in \mathbb{R}$, we define $\lceil r \rceil$ to be the least integer no less than r.

3. Constructions and proofs

Suppose S is a nonempty set equipped with a binary operation $(x, y) \mapsto xy$. We say that S is 3-*nilpotent* if it has a distinguished element z such that all products of three elements equal z, i.e. both $u(vw)$ and $(uv)w$ equal z, regardless of the choice of u, v, w. An analogous concept could be defined with the parameter 3 replaced by a positive integer k, but it is $k = 3$ that is useful to us: it forces S to be a semigroup, but allows enough freedom for us to construct useful examples.

We are interested in one specific family $\mathcal{F} = \bigcup_{n>1} \mathcal{F}_n$ of 3-nilpotent semigroups. Here, $\mathcal{F}_n$ is the collection of semigroups S with n distinct elements $u_1, \dots, u_n$, whose multiplication satisfies the following constraints ($1 \le i, j \le n$ in all cases):

(a) $u_i u_j = u_1$ if $\{i, j\} \cap \{1, 2\}$ is nonempty, and also if $i \le j$.
(b) $u_i u_j \in \{u_1, u_2\}$ if $j < i$ ("subdiagonal products").

The distinguished element z is of course u_1.

The value of $\#_{\mathrm{CP}}(S)$ above depends only on the number of subdiagonal products that equal u_1. At one extreme, if all subdiagonal products equal u_2, then $\#_{\mathrm{CP}}(S) = (4n - 4) + (n - 2) = 5n - 6$, since the only commuting pairs are those with $\{i, j\} \cap \{1, 2\}$ nonempty, and those with $i = j$. At the other extreme, if all subdiagonal products equal u_1, then $\#_{\mathrm{CP}}(S) = n^2$. By considering all intermediate choices, we get a semigroup $S \in \mathcal{F}_n$ with $\#_{\mathrm{CP}}(S)$ equal any number between $5n - 6$ and n^2 inclusive that has the same parity as $5n - 6$, and hence the same parity as n.

Bearing in mind Observation 4, we have proved the following result.

Theorem 5. *Suppose $n, m \in \mathbb{N}$. If there is a semigroup S of order n with $\#_{\mathrm{CP}}(S) = m$, then $m - n$ is even. For $n > 1$, the converse holds with $S \in \mathcal{F}_n$ if $5n - 6 \le m \le n^2$.*

In particular, if n is even, then there exists $S \in \mathcal{F}_n$ with $\#_{\mathrm{CP}}(S) = in$ for each $5 \le i \le n$. Thus for given positive integers $j, k \in \mathbb{N}$, $j \le k$, there exists a 3-nilpotent semigroup $S \in \mathcal{F}_{6k}$ with $\#_{\mathrm{CP}}(S) = 36jk$, and so $\Pr(S) = j/k$. Consequently $\mathcal{F}$ is the desired family of semigroups that attains every rational probability, answering the question of Ponomarenko and Selinski [8] mentioned in the introduction.

The proof of Theorem 1 will follow easily from the following improvement of Theorem 5.

Theorem 6. *Suppose $n, m \in \mathbb{N}$. There is a semigroup S of order n with $\#_{\mathrm{CP}}(S) = m$ if and only if $n \le m \le n^2$ and $m - n$ is even.*

To prove Theorem 6, we will use the process of adjoining a zero to a semigroup, but we also need what we call noncommuting sums.

Definition 7. Suppose $\{S_i\}_{i \in I}$ is a collection of semigroups for some nonempty index set such that each S_i is a semigroup possesses a zero element z_i. The *noncommuting sum of S_i, $i \in I$*, denoted $\sum_{i \in I} S_i$, is a semigroup S with the following properties:

(a) As a set, S is the *disjoint union* $\coprod_{i \in I} S_i$. (Thus we may need to first replace each S_i by an isomorphic copy of itself to ensure pairwise disjointness.)

(b) Multiplication in S is defined by the following requirements: it extends multiplication on each S_i, and the equation $xy = z_i$ holds for all $x \in S_i$, $y \in S_j$, $i \neq j$.

Lemma 8. *Suppose S_i is a semigroup with a zero for each i in a nonempty index set I. Then the noncommuting sum $\sum_{i\in I} S_i$ is a semigroup. If each S_i is finite and I is finite, then*

$$\#_{\mathrm{CP}}\left(\sum_{i\in I} S_i\right) = \sum_{i\in I} \#_{\mathrm{CP}}(S_i)\,. \tag{1}$$

Proof. From the definition, we see that each z_i is a left zero on S. We wish to prove that $u(vw) = (uv)w$ for all $u \in S_i$, $v \in S_j$, and $w \in S_k$. This follows from the semigroup property of S_i if $i = j = k$, so suppose this is not so. If $i \neq j$, then $vw \notin S_i$ and so $u(vw) = z_i$. Also, $uv = z_i$, and z_i is a left zero on S, so $(uv)w = z_i$. If instead $i = j$ but $k \neq i$, then $uv \in S_i$, so $(uv)w = z_i$. Also, $vw = z_i$, so $u(vw) = uz_i = z_i$, since z_i is the zero of S_i.

If $x \in S_i$ and $y \in S_j$ for some $i \neq j$, then $xy = z_i \neq z_j = yx$, so $\mathrm{CP}(S) = \coprod_{i\in I} \mathrm{CP}(S_i)$. This readily implies (1). □

Proof of Theorem 6. The proof is by induction on n. Let P_n be the proposition that there is a semigroup S of order n with $\#_{\mathrm{CP}}(S) = m$ for each $m \in \mathbb{N}$ for which $m - n$ is even and $n \leq m \leq n^2$. In fact it suffices to assume that $n + 2 \leq m \leq n^2 - 2$, since $\#_{\mathrm{CP}}(S) = n$ holds if S is the left zero semigroup of order n, and $\#_{\mathrm{CP}}(S) = n^2$ holds if S is a commutative semigroup of order n (and these exist for all n). In particular, we see that P_1 and P_2 are true.

Assume therefore that $n > 2$, and assume inductively that P_k is true for all $1 \leq k < n$. By adjoining a zero to a semigroup of order $k - 1$, we see that for $1 \leq k \leq n$, there exists a semigroup S of order k that contains a zero and satisfies $\#_{\mathrm{CP}}(S) = m$ for every $m \in [3k - 2, k^2]$ that has the same parity as k. In particular this is true for $k = n$, so in order to complete the inductive step, it suffices to show that there exists a semigroup S of order n with $\#_{\mathrm{CP}}(S) = m$ for every $m \in [n, 3n - 4]$ that has the same parity as n. Letting S be the semigroup of order n defined as the noncommuting sum of a semigroup S_k of order $k < n$ for which $\#_{\mathrm{CP}}(S_k) = 3k - 2$, and $n - k$ copies of the semigroup of order 1, we see from (1) that $\#_{\mathrm{CP}}(S) = n - k + (3k - 2) = n + 2k - 2$. By letting k range over all integers between 1 and $n - 1$, we get all required values of $\#_{\mathrm{CP}}(S)$. □

Proof of Theorem 1. Let w be the least integer not less than $k/j\alpha(k)$, and let e be the least even number not less than $k/j\alpha(k)$, so $e \in \{w, w + 1\}$. The claimed value of $\mathrm{Ord}(j, k)$ is $n_2 := e\alpha(k)$ if j is even, or if both k and $\nu_2(k)$ are even, and $n_1 := w\alpha(k)$ otherwise.

Suppose $S \in \Sigma_n$, where Σ_n is the class of semigroups of order $n \in \mathbb{N}$. Suppose also that $\Pr(S) = j/k$, or equivalently $\#_{\mathrm{CP}}(S) = n^2 j/k$. Now $\#_{\mathrm{CP}}(S)$ must be an integer, so n must be divisible by $\alpha(k)$, and we can write $n = i\alpha(k)$. Observation 4 tells us that we can find $S \in \Sigma_n$ with $\#_{\mathrm{CP}}(S) = n^2 j/k$ if and only if $\#_{\mathrm{CP}}(S) \geq n$ and $\#_{\mathrm{CP}}(S)$ has the same parity as n. The inequality $\#_{\mathrm{CP}}(S) \geq n$ can be rewritten as $i \geq k/j\alpha(k)$, so $i \geq w$. We assume from now on that $i \geq w$, and so the existence of $S \in \Sigma_n$ with $\Pr(S) = j/k$ reduces to checking the parity condition.

If i is even, then n is also even. Also $m := (\alpha(k))^2 j/k$ is an integer, so $\#_{\mathrm{CP}}(S) = i^2 m$ is even and the parity condition is fulfilled. Thus there exists $S \in \Sigma_n$ with $\#_{\mathrm{CP}}(S) = n^2 j/k$, and so the minimal order is at most n_2. It remains only to decide if the minimal order is n_1 or n_2. In fact it equals n_1 if $n_1^2 j/k - n_1$ is even, and n_2 otherwise. Note that $n_1^2 j/k = w^2 jk'$ where $k' := (\alpha(k))^2/k \in \mathbb{N}$. We assume from now on that w is odd, since otherwise $n_1 = n_2$ and we are done.

Suppose j is even. Since j and k are coprime, k is odd, and so n_1 is also odd. But $w^2 jk'$ is even, so the parity condition is violated and the minimal order is n_2 in this case.

Suppose next that k and $\nu_2(k)$ are both even, and so j must be odd. Because $\nu_2(k)$ is even, k' is odd, and so $n_1^2 j/k$ is odd. But k is even, so $\alpha(k)$ and n_1 are even. Again the parity condition is violated, and the minimal order is n_2.

Finally suppose j is odd and either k or $\nu_2(k)$ is odd. If k is odd, then $\alpha(k)$ and n_1 are odd, as is $w^2 jk'$. Thus the parity condition is satisfied, and the minimal order is n_1. If instead $\nu_2(k)$ is odd (and so k is even), then $\alpha(k)$ and k' are even, so both n_1 and $w^2 jk'$ are even. Thus the parity condition is satisfied, and the minimal order is n_1. □

Finally, we give a simple alternative proof of the density of the values of $\Pr(S)$, exploiting the readily verified fact that $\#_{\mathrm{NCP}}(S') = \#_{\mathrm{NCP}}(S)$ in Lemma 3. If we start with a finite noncommutative semigroup S_0 of order n with $m > 0$ noncommuting pairs (x, y) of elements, and we adjoin a new zero N times for some $N \in \mathbb{N}$, then we get a semigroup S_N of order $N + n$ with $\#_{\mathrm{CP}}(S_N) = (N + n)^2 - m$. Thus $\Pr(S_N) = 1 - m/(N + n)^2$ gives probabilities arbitrarily close to 1 as $N \to \infty$.

Lemma 2 implies that $\Pr(S_n) = (\Pr(S_1))^n$ if S_n is the direct product of n copies of a finite semigroup S_1. By applying this fact with $\Pr(S_1)$ arbitrarily close to 1, we deduce that the values of $\Pr(S)$ are dense in $[0, 1]$.

References

[1] K. Ahmadidelir, C.M. Campbell, and H. Doostie, *Almost commutative semigroups*, Alg. Colloq. **18** (2011), 881–888.

[2] S.M. Buckley, D. MacHale, and Á. Ní Shé, *Finite rings with many commuting pairs of elements*, preprint.

[3] S.M. Buckley and D. MacHale, *Contrasting the commuting probabilities of groups and rings*, preprint.

[4] B. Givens, *The probability that two semigroup elements commute can be almost anything*, College Math. J. **39** (2008), 399–400.

[5] W.H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[6] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.

[7] D. MacHale, *Probability in finite semigroups*, Irish Math. Soc. Bull. **25** (1990), 64–68.

[8] V. Ponomarenko and N. Selinski, *Two semigroup elements can commute with any positive rational probability*, College Math. J. **43** (2012), 334–336.

[9] 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