Ranks of ideals in inverse semigroups of difunctional binary relations

James East* and Alexei Vernitski†

Abstract

The set $\mathcal{D}_n$ of all difunctional relations on an n element set is an inverse semigroup under a variation of the usual composition operation. We solve an open problem of Kudryavtseva and Maltcev (2011), which asks: What is the rank (smallest size of a generating set) of $\mathcal{D}_n$? Specifically, we show that the rank of $\mathcal{D}_n$ is $B(n) + n$, where $B(n)$ is the nth Bell number. We also give the rank of an arbitrary ideal of $\mathcal{D}_n$. Although $\mathcal{D}_n$ bears many similarities with families such as the full transformation semigroups and symmetric inverse semigroups (all contain the symmetric group and have a chain of $\mathscr{J}$-classes), we note that the fast growth of $\mathrm{rank}(\mathcal{D}_n)$ as a function of n is a property not shared with these other families.

Keywords: Semigroups, binary relations, ideals, generators, rank.

MSC: 20M20; 20M18.

1 Introduction

Fix a positive integer n, write $\mathbf{n} = \{1, \ldots, n\}$, and denote by $\mathcal{B}_n$ the set of all binary relations on $\mathbf{n}$. For $\alpha \in \mathcal{B}_n$ and for $x \in \mathbf{n}$, write $x\alpha = \{y \in \mathbf{n} : (x, y) \in \alpha\}$ and $\alpha x = \{y \in \mathbf{n} : (y, x) \in \alpha\}$. The set $\mathcal{B}_n$ forms a semigroup under the composition operation $\circ$ defined by $\alpha \circ \beta = \{(x, y) \in \mathbf{n} \times \mathbf{n} : x\alpha \cap \beta y \neq \varnothing\}$. In [17], the second author introduced and studied an alternative operation $\diamond$ on $\mathcal{B}_n$, defined by

$$\alpha \diamond \beta = \{(x, y) \in \mathbf{n} \times \mathbf{n} : x\alpha = \beta y \neq \varnothing\}.$$

It was shown in [17] that the operation $\diamond$ is not associative on $\mathcal{B}_n$, but that it is associative on the subset $\mathcal{D}_n$ of $\mathcal{B}_n$ consisting of all *difunctional* relations on $\mathbf{n}$; see Section 2 for the definition of difunctionality. The semigroup $(\mathcal{D}_n, \diamond)$ was shown to be an inverse semigroup in [17], and further properties of this semigroup were investigated in [12], including Green's relations, ideals, maximal subsemigroups and congruences. It was left as an open problem in [12] to determine the *rank* of $\mathcal{D}_n$: that is, the minimal size of a (semigroup) generating set for $\mathcal{D}_n$.[1] In this note, we solve this problem; see Theorem 2.3. In fact, we solve a more general problem, and calculate the rank of each ideal of $\mathcal{D}_n$; see Proposition 2.2. This being trivial for $n = 1$, we assume $n \geq 2$ for the remainder of the article.

2 Preliminaries and statement of the main results

Recall from [16] that a relation α on $\mathbf{n}$ is *difunctional* if $\alpha = \alpha \circ \alpha^{-1} \circ \alpha$, where $\alpha^{-1} = \{(y, x) : (x, y) \in \alpha\}$ is the inverse relation of α. There are many equivalent formulations of the difunctionality property. To describe the one that is most convenient for our purposes, we first introduce some notation. For a set X, we write $\mathscr{P}(X)$ for the set of all set partitions of X. For $1 \leq k \leq |X|$, we write $\mathscr{P}(X, k)$ for the set of all set partitions of X into k blocks. By convention, we also define $\mathscr{P}(\varnothing) = \mathscr{P}(\varnothing, 0) = \{\varnothing\}$.

A binary relation $\alpha \in \mathcal{B}_n$ is difunctional if and only if it is of the form $\alpha = (A_1 \times B_1) \cup \cdots \cup (A_r \times B_r)$, for some subsets $A, B \subseteq \mathbf{n}$ and some partitions $\{A_1, \ldots, A_r\} \in \mathscr{P}(A, r)$ and $\{B_1, \ldots, B_r\} \in \mathscr{P}(B, r)$. We

*Centre for Research in Mathematics, School of Computing, Engineering and Mathematics, Western Sydney University, Locked Bag 1797, Penrith NSW 2751, Australia. *Email:* `j.east@westernsydney.edu.au`

†Department of Mathematical Sciences, University of Essex, Colchester, United Kingdom. *Email:* `asvern@essex.ac.uk`

[1] We note that Proposition 7 in an earlier version of [12], available at `arxiv.org/pdf/math/0602623v1.pdf`, leads to a lower bound for $\mathrm{rank}(\mathcal{D}_n)$ that is fairly close to the precise value.

denote α as above by $\left[\begin{smallmatrix} A_1 & \cdots & A_r \\ B_1 & \cdots & B_r \end{smallmatrix}\right]$. We write

$$\begin{aligned} \operatorname{rank}(\alpha) &= r, & \operatorname{dom}(\alpha) &= A_1 \cup \cdots \cup A_r, & \ker(\alpha) &= \{A_1, \ldots, A_r\}, & \operatorname{def}(\alpha) &= |\mathbf{n} \setminus \operatorname{dom}(\alpha)|, \\ & & \operatorname{codom}(\alpha) &= B_1 \cup \cdots \cup B_r, & \operatorname{coker}(\alpha) &= \{B_1, \ldots, B_r\}, & \operatorname{codef}(\alpha) &= |\mathbf{n} \setminus \operatorname{codom}(\alpha)|, \end{aligned}$$

and we call these parameters the *rank*, *domain*, *codomain*, *kernel*, *cokernel*, *defect* and *codefect* of α, respectively. Note that the empty relation $\varnothing$ is difunctional, corresponding to the $r = 0$ case above.

Denote by $\mathcal{I}_n$ the subset of $\mathcal{D}_n$ consisting of all difunctional relations $\left[\begin{smallmatrix} A_1 & \cdots & A_r \\ B_1 & \cdots & B_r \end{smallmatrix}\right]$ for which $|A_i| = |B_i| = 1$ for each $1 \leq i \leq r$. It was shown in [17] that $(\mathcal{I}_n, \diamond)$ is a subsemigroup of $(\mathcal{D}_n, \diamond)$; in fact, it was shown that the operations $\diamond$ and $\circ$ coincide on $\mathcal{I}_n$, so that $\mathcal{I}_n$ is precisely the *symmetric inverse monoid* on $\mathbf{n}$. In particular, the *symmetric group* $\mathcal{S}_n = \{\alpha \in \mathcal{D}_n : \operatorname{rank}(\alpha) = n\}$ is contained in $\mathcal{D}_n$. We note that the identity element of $\mathcal{S}_n$ is not an identity element of $\mathcal{D}_n$. In fact, $\mathcal{D}_n$ does not have an identity element, but it does have a zero element, namely the empty relation, $\varnothing$.

Let S be a semigroup, and write S^1 for the monoid obtained by adjoining an identity element to S if necessary. Recall that *Green's preorders* $\leq_{\mathscr{R}}$, $\leq_{\mathscr{L}}$, $\leq_{\mathscr{J}}$ are defined, for $a, b \in S$ by

$$a \leq_{\mathscr{R}} b \ \Leftrightarrow\ a \in bS^1, \quad a \leq_{\mathscr{L}} b \ \Leftrightarrow\ a \in S^1 b, \quad a \leq_{\mathscr{J}} b \ \Leftrightarrow\ a \in S^1 b S^1,$$

and that Green's relations $\mathscr{R}$, $\mathscr{L}$, $\mathscr{J}$ are defined by $\mathscr{R} = {\leq_{\mathscr{R}}} \cap {\geq_{\mathscr{R}}}$, $\mathscr{L} = {\leq_{\mathscr{L}}} \cap {\geq_{\mathscr{L}}}$, $\mathscr{J} = {\leq_{\mathscr{J}}} \cap {\geq_{\mathscr{J}}}$. Green's relation $\mathscr{H}$ is defined by $\mathscr{H} = \mathscr{R} \cap \mathscr{L}$. For more on Green's relations, and (inverse) semigroups more generally, the reader is referred to [9, 13]. The next result describes Green's relations and preorders on $\mathcal{D}_n$; its proof is routine, and is ommitted. (Parts (iv)–(vi) may be found in [12], in slightly different language, without proof.)

Lemma 2.1. *Let $\alpha, \beta \in \mathcal{D}_n$. Then*

(i) $\alpha \leq_{\mathscr{R}} \beta$ *if and only if* $\ker(\alpha) \subseteq \ker(\beta)$,

(ii) $\alpha \leq_{\mathscr{L}} \beta$ *if and only if* $\operatorname{coker}(\alpha) \subseteq \operatorname{coker}(\beta)$,

(iii) $\alpha \leq_{\mathscr{J}} \beta$ *if and only if* $\operatorname{rank}(\alpha) \leq \operatorname{rank}(\beta)$,

(iv) $\alpha \mathscr{R} \beta$ *if and only if* $\ker(\alpha) = \ker(\beta)$,

(v) $\alpha \mathscr{L} \beta$ *if and only if* $\operatorname{coker}(\alpha) = \operatorname{coker}(\beta)$,

(vi) $\alpha \mathscr{J} \beta$ *if and only if* $\operatorname{rank}(\alpha) = \operatorname{rank}(\beta)$. □

It follows from parts (iii) and (vi) of Lemma 2.1 that the $\mathscr{J}$-classes of $\mathcal{D}_n$ are the sets

$$J_r = \{\alpha \in \mathcal{D}_n : \operatorname{rank}(\alpha) = r\} \qquad \text{for } 0 \leq r \leq n,$$

and that these form a chain under the usual ordering on $\mathscr{J}$-classes: $J_0 < J_1 < \cdots < J_n$. That is, $J_r \subseteq \mathcal{D}_n \diamond J_s \diamond \mathcal{D}_n$ for any $0 \leq r \leq s \leq n$. Note also that $J_n = \mathcal{S}_n$ and $J_0 = \{\varnothing\}$. In any semigroup in which the $\mathscr{J}$-classes form a chain, the ideals form a chain under inclusion. So the ideals of $\mathcal{D}_n$ are the sets

$$I_r = J_0 \cup \cdots \cup J_r = \{\alpha \in \mathcal{D}_n : \operatorname{rank}(\alpha) \leq r\} \qquad \text{for } 0 \leq r \leq n.$$

Our main results calculate the *ranks* of these ideals, including that of $I_n = \mathcal{D}_n$ itself. Recall that the rank of a semigroup S is defined to be $\operatorname{rank}(S) = \min\big\{|A| : A \subseteq S,\ S = \langle A \rangle\big\}$, the least cardinality of a generating set for S. The rank of a semigroup should not be confused with the rank of a difunctional relation.

To state our main results, we recall the definition of the Stirling and Bell numbers. For non-negative integers n and k, the *Stirling number of the second kind* $S(n,k)$ denotes the number of partitions of a set of size n into k (nonempty) subsets. The *Bell number* $B(n) = S(n,1) + \cdots + S(n,n)$ denotes the total number of partitions of a set of size n into any number of subsets. Note that $S(0,0) = 1$, and $S(n,k) = 0$ if $k > n$. The Stirling and Bell numbers are listed as Sequences A008277 and A000110, respectively, on [1].

Proposition 2.2. *Let $n \geq 2$ and $0 \leq r \leq n$. Then the rank of the ideal $I_r = \{\alpha \in \mathcal{D}_n : \operatorname{rank}(\alpha) \leq r\}$ of $\mathcal{D}_n$ is given by*

$$\operatorname{rank}(I_r) = \begin{cases} \rho_{nr} & \text{if } r = 0 \text{ or } r \geq 3 \\ \rho_{nr} - 1 & \text{if } 1 \leq r \leq 2, \end{cases}$$

where $\rho_{nr} = r + (r+1)S(n, r+1) + \displaystyle\sum_{k=1}^{r} S(n,k)$.

Proposition 2.2 yields a formula for the rank of $\mathcal{D}_n$ itself, upon putting $r = n$. This formula may be simplified, noting that $S(n, n+1) = 0$, and that $\sum_{k=1}^{n} S(n,k) = B(n)$:

Theorem 2.3. *If $n \geq 3$, then* $\operatorname{rank}(\mathcal{D}_n) = B(n) + n$. □

For completeness, we note that $\operatorname{rank}(\mathcal{D}_2) = B(2) + 1 = 3$. We end this section with a simple combinatorial lemma.

Lemma 2.4. *Let $0 \leq r \leq n$. Then*

(i) *J_r contains $(r+1)S(n,r+1) + S(n,r)$ $\mathscr{R}$-classes (and the same number of $\mathscr{L}$-classes), and*

(ii) *the $\mathscr{H}$-class of any idempotent from J_r is isomorphic to the symmetric group $\mathcal{S}_r$.*

Proof. By Lemma 2.1(iv), an $\mathscr{R}$-class in J_r is uniquely determined by the kernel of each of its elements. This is a partition $\mathbf{A} = \{A_1, \ldots, A_r\}$ of some subset A of $\mathbf{n}$ for which $|A| \geq r$. The number of such partitions with $|A| = n$ is equal to $S(n,r)$. The number of such partitions with $|A| < n$ is $(r+1)S(n,r+1)$; indeed, to specify such a partition, we first partition $\mathbf{n}$ into $r+1$ blocks and choose one of these not to include as a block of $\mathbf{A}$. This completes the proof of (i).

By Lemma 2.1(iv) and (v), it is clear that the $\mathscr{H}$-class of the idempotent $\left[\begin{smallmatrix} 1 & \cdots & r \\ 1 & \cdots & r \end{smallmatrix}\right] \in J_r$ consists of all permutations of the set $\{1, \ldots, r\}$, so that part (ii) of the current lemma is true of this idempotent. But all group $\mathscr{H}$-classes in J_r are isomorphic; see [9, Proposition 2.3.6]. □

Remark 2.5. An alternative way of counting the $\mathscr{R}$-classes in J_r involves (in the notation of the proof of Lemma 2.4) first choosing the subset A and then the partition $\mathbf{A} \in \mathscr{P}(A, r)$. This leads to the alternative expression of $\sum_{k=r}^{n} \binom{n}{k} S(k,r)$ for the number of such $\mathscr{R}$-classes.

3 Proof of the main result

Note that Proposition 2.2 is trivial for $r = 0$, since $I_0 = \{\varnothing\}$ and $\rho_{n0} = 1$, so for the duration of this section, we fix $n \geq 2$ and some $1 \leq r \leq n$.

Recall from [9, Section 3.1] that the *principal factor* of a $\mathscr{J}$-class J in a semigroup S is the semigroup J^* with underlying set $J \cup \{0\}$, where 0 is a symbol not in J, and with product $*$ defined by

$$a * b = \begin{cases} ab & \text{if } a, b, ab \in J \\ 0 & \text{otherwise.} \end{cases}$$

Recall from [11] that the *relative rank* of a semigroup S with respect to a subset $A \subseteq S$, denoted $\operatorname{rank}(S : A)$, is the smallest cardinality of a subset $B \subseteq S$ such that $S = \langle A \cup B \rangle$. The proof of the next result is routine, but is included for convenience.

Lemma 3.1. *Let S be a finite semigroup with a single maximal $\mathscr{J}$-class J that is not a subsemigroup of S. Then* $\operatorname{rank}(S) = \operatorname{rank}(J^*) + \operatorname{rank}(S : J)$.

Proof. To avoid confusion during the proof, if $X \subseteq J$, we will write $\langle X \rangle$ for the subsemigroup of S generated by X, and $\langle X \rangle^*$ for the subsemigroup of J^* generated by X.

First, suppose $J^* = \langle A \rangle^*$ and $S = \langle J \cup B \rangle$, with $|A| = \operatorname{rank}(J^*)$ and $|B| = \operatorname{rank}(S : J)$. Since J is not a subsemigroup of S, we have $A \subseteq J$. Then $\langle A \cup B \rangle = \langle \langle A \rangle \cup B \rangle = \langle J \cup B \rangle = S$, so that $\operatorname{rank}(S) \leq |A \cup B| \leq |A| + |B| = \operatorname{rank}(J^*) + \operatorname{rank}(S : J)$.

Conversely, suppose $S = \langle C \rangle$, and put $A = C \cap J$ and $B = C \setminus J$. Let $x \in J$, and consider an expression $x = c_1 \cdots c_k$, where $c_1, \ldots, c_k \in C$. Since $S \setminus J$ is a (nonempty) ideal of S, each factor c_i must belong to J; that is $c_i \in A$. It follows that $J \subseteq \langle A \rangle$, and so $J^* = \langle A \rangle^*$; note that $0 \in \langle A \rangle^*$ because J is not a subsemigroup of S. In particular, $|A| \geq \operatorname{rank}(J^*)$. But also $S = \langle A \cup B \rangle = \langle \langle A \rangle \cup B \rangle \supseteq \langle J \cup B \rangle \supseteq S$, so it follows that $S = \langle J \cup B \rangle$, giving $|B| \geq \operatorname{rank}(S : J)$. Thus, $|C| = |A| + |B| \geq \operatorname{rank}(J^*) + \operatorname{rank}(S : J)$. Since this is true for any generating set C for S, it follows that $\operatorname{rank}(S) \geq \operatorname{rank}(J^*) + \operatorname{rank}(S : J)$. □

In the case that S is the ideal I_r of $\mathcal{D}_n$, it follows that $\operatorname{rank}(I_r) = \operatorname{rank}(J_r^*) + \operatorname{rank}(I_r : J_r)$. We give the values of $\operatorname{rank}(J_r^*)$ and $\operatorname{rank}(I_r : J_r)$ in Lemmas 3.2 and 3.3, respectively.

Lemma 3.2. *If* $1 \leq r \leq n$, *then* $\operatorname{rank}(J_r^*) = \operatorname{rank}(\mathcal{S}_r) - 1 + (r+1)S(n, r+1) + S(n, r)$.

Proof. Since $\mathcal{D}_n$ is an inverse semigroup, J_r^* is a *Brandt semigroup*. More specifically, by Lemma 2.4(ii), J_r^* is a Brandt semigroup over the symmetric group $\mathcal{S}_r$. By [7, Corollary 9], it follows that $\operatorname{rank}(J_r^*) = \operatorname{rank}(\mathcal{S}_r) - 1 + q$, where q is the number of $\mathscr{R}$-classes in J_r. The result now follows from Lemma 2.4(i). □

In light of Lemmas 3.1 and 3.2, and the fact [14] that

$$\operatorname{rank}(\mathcal{S}_r) = \begin{cases} 1 & \text{if } r \leq 2 \\ 2 & \text{if } r \geq 3, \end{cases}$$

the proof of Proposition 2.2 will be complete if we can prove the following.

Lemma 3.3. *If* $1 \leq r \leq n$, *then* $\operatorname{rank}(I_r : J_r) = r - 1 + \sum_{k=1}^{r-1} S(n, k)$.

To prove Lemma 3.3, we will first need to prove a number of intermediate results. Consider a partition $\mathbf{A} = \{A_1, \ldots, A_k\} \in \mathscr{P}(\mathbf{n})$ with $\min(A_1) < \cdots < \min(A_k)$. We define the difunctional relations

$$\lambda_{\mathbf{A}} = \left[\begin{smallmatrix} A_1 & \cdots & A_k \\ 1 & \cdots & k \end{smallmatrix}\right] \qquad \text{and} \qquad \rho_{\mathbf{A}} = \left[\begin{smallmatrix} 1 & \cdots & k \\ A_1 & \cdots & A_k \end{smallmatrix}\right].$$

Here and elsewhere, we use an obvious shorthand notation: for example, $\left[\begin{smallmatrix} A_1 & \cdots & A_k \\ 1 & \cdots & k \end{smallmatrix}\right]$ is an abbreviation for $\left[\begin{smallmatrix} A_1 & \cdots & A_k \\ \{1\} & \cdots & \{k\} \end{smallmatrix}\right]$. For $1 \leq k \leq n$, put

$$\mathcal{L}_k = \{\lambda_{\mathbf{A}} : \mathbf{A} \in \mathscr{P}(\mathbf{n}),\ |\mathbf{A}| \leq k\} \qquad \text{and} \qquad \mathcal{R}_k = \{\rho_{\mathbf{A}} : \mathbf{A} \in \mathscr{P}(\mathbf{n}),\ |\mathbf{A}| \leq k\}.$$

Recall that the symmetric inverse monoid $\mathcal{I}_n$ is a subsemigroup of $\mathcal{D}_n$.

Lemma 3.4. *Let* $\alpha \in I_{r-1}$. *Then* $\alpha = \beta \diamond \gamma \diamond \delta$ *for some* $\beta \in \mathcal{L}_r$, $\gamma \in \mathcal{I}_n$, $\delta \in \mathcal{R}_r$ *with* $\operatorname{rank}(\gamma) = \operatorname{rank}(\alpha)$.

Proof. Write $\alpha = \left[\begin{smallmatrix} A_1 & \cdots & A_k \\ B_1 & \cdots & B_k \end{smallmatrix}\right]$, noting that $k \leq r - 1$. Put $A_{k+1} = \mathbf{n} \setminus \operatorname{dom}(\alpha)$ and $B_{k+1} = \mathbf{n} \setminus \operatorname{codom}(\alpha)$, and let

$$\mathbf{A} = \begin{cases} \{A_1, \ldots, A_k\} & \text{if } A_{k+1} = \varnothing \\ \{A_1, \ldots, A_k, A_{k+1}\} & \text{if } A_{k+1} \neq \varnothing \end{cases} \qquad \text{and} \qquad \mathbf{B} = \begin{cases} \{B_1, \ldots, B_k\} & \text{if } B_{k+1} = \varnothing \\ \{B_1, \ldots, B_k, B_{k+1}\} & \text{if } B_{k+1} \neq \varnothing. \end{cases}$$

Then it is easy to see that $\alpha = \lambda_{\mathbf{A}} \diamond \gamma \diamond \rho_{\mathbf{B}}$, where $\gamma = \rho_{\mathbf{A}} \diamond \alpha \diamond \lambda_{\mathbf{B}} \in \mathcal{I}_n$ with $\operatorname{rank}(\gamma) = k$. □

Lemma 3.5. *We have* $I_r = \langle J_r \cup \mathcal{L}_r \cup \mathcal{R}_r \rangle$.

Proof. We must consider two separate cases. Suppose first that $r < n$. Note that J_r contains the set $\Omega = \{\alpha \in \mathcal{I}_n : \operatorname{rank}(\alpha) = r\}$. It is well known that $\langle \Omega \rangle = \{\alpha \in \mathcal{I}_n : \operatorname{rank}(\alpha) \leq r\}$; see for example [19, Lemma 4.7]. The result now follows from Lemma 3.4.

Suppose now that $r = n$, so $J_r = \mathcal{S}_n$. By Lemma 3.4, it suffices to show that $\mathcal{I}_n \subseteq \langle \mathcal{S}_n \cup \mathcal{L}_n \cup \mathcal{R}_n \rangle$. For this, let $\mathbf{A} \in \mathscr{P}(\mathbf{n}, n-1)$ be arbitrary, and put $\alpha = \rho_{\mathbf{A}} \diamond \lambda_{\mathbf{A}} \in \langle \mathcal{L}_n \cup \mathcal{R}_n \rangle$, noting that $\alpha = \left[\begin{smallmatrix} 1 & \cdots & n-1 \\ 1 & \cdots & n-1 \end{smallmatrix}\right] \in \mathcal{I}_n$ and $\operatorname{rank}(\alpha) = n - 1$. It then follows from the proof of [6, Theorem 3.1] (see also [15]) that $\mathcal{I}_n = \langle \mathcal{S}_n \cup \{\alpha\} \rangle$. □

Let $\mathbf{A}, \mathbf{B} \in \mathscr{P}(\mathbf{n}, r)$, and write $\mathbf{A} = \{A_1, \ldots, A_r\}$ and $\mathbf{B} = \{B_1, \ldots, B_r\}$ with $\min(A_1) < \cdots < \min(A_r)$ and $\min(B_1) < \cdots < \min(B_r)$. We define $\phi_{\mathbf{A},\mathbf{B}} = \left[\begin{smallmatrix} A_1 & \cdots & A_r \\ B_1 & \cdots & B_r \end{smallmatrix}\right]$. In order to simplify notation in what follows, and since n is fixed, for each $1 \leq k \leq n$, we will write $p_k = S(n, k)$. For each $1 \leq k \leq n$, let us denote the elements of $\mathscr{P}(\mathbf{n}, k)$ by $\mathbf{A}_{k,1}, \ldots, \mathbf{A}_{k,p_k}$.

Lemma 3.6. *For each $1 \leq k \leq n-1$, let $\Sigma_k = \{\phi_{\mathbf{A}_{k,1},\mathbf{A}_{k,2}}, \ldots, \phi_{\mathbf{A}_{k,p_k-1},\mathbf{A}_{k,p_k}}\} \cup \{\lambda_{\mathbf{A}_{k,p_k}}, \rho_{\mathbf{A}_{k,1}}\}$. Then for any $1 \leq r \leq n$, $I_r = \langle J_r \cup \Sigma_1 \cup \cdots \cup \Sigma_{r-1}\rangle$.*

Proof. Put $\Omega = J_r \cup \Sigma_1 \cup \cdots \cup \Sigma_{r-1}$. By Lemma 3.5, to show that $I_r = \langle\Omega\rangle$, it suffices to show that $\langle\Omega\rangle$ contains both $\mathcal{L}_r$ and $\mathcal{R}_r$. Let $\mathbf{A} \in \mathscr{P}(\mathbf{n})$ with $|\mathbf{A}| \leq r$. We must show that $\lambda_{\mathbf{A}}, \rho_{\mathbf{A}} \in \langle\Omega\rangle$. If $|\mathbf{A}| = r$, then $\lambda_{\mathbf{A}}, \rho_{\mathbf{A}} \in J_r \subseteq \langle\Omega\rangle$, so suppose $\mathbf{A} \in \mathscr{P}(\mathbf{n}, k)$, where $1 \leq k \leq r-1$. Then $\mathbf{A} = \mathbf{A}_{k,l}$ for some $1 \leq l \leq p_k$. But then

$$\begin{aligned}
\lambda_{\mathbf{A}} = \lambda_{\mathbf{A}_{k,l}} &= (\phi_{\mathbf{A}_{k,l},\mathbf{A}_{k,l+1}} \diamond \cdots \diamond \phi_{\mathbf{A}_{k,p_k-1},\mathbf{A}_{k,p_k}}) \diamond \lambda_{\mathbf{A}_{k,p_k}}, \\
\rho_{\mathbf{A}} = \rho_{\mathbf{A}_{k,l}} &= \rho_{\mathbf{A}_{k,1}} \diamond (\phi_{\mathbf{A}_{k,1},\mathbf{A}_{k,2}} \diamond \cdots \diamond \phi_{\mathbf{A}_{k,l-1},\mathbf{A}_{k,l}}),
\end{aligned}$$

where the first bracketed expression is omitted if $l = p_k$, and the second if $l = 1$. □

Remark 3.7. We could not help noticing that the generating set used in Lemma 3.6 looks very similar to the construction of so-called *rainbow tables* in computer security [8]. This is perhaps not surprising, since both constructions have the purpose, broadly speaking, of reducing the total amount of memory used for storing given information.

Since $|\Sigma_k| = S(n, k) + 1$ for each k, it follows from Lemma 3.6 that $\operatorname{rank}(I_r : J_r) \leq r - 1 + \sum_{k=1}^{r-1} S(n, k)$. To complete the proof of Lemma 3.3, we must therefore show that this upper bound for $\operatorname{rank}(I_r : J_r)$ is also a lower bound. To do this, we will show in Lemmas 3.10 and 3.12 that if $\Sigma \subseteq I_r$ is such that $I_r = \langle J_r \cup \Sigma\rangle$, then Σ must include certain specified kinds of relations. First, we prove two intermediate lemmas. There are obvious dual versions of Lemmas 3.8 and 3.9, but we will not state them.

Lemma 3.8. *If $\alpha, \beta, \gamma \in \mathcal{D}_n$ are such that $\alpha = \beta \diamond \gamma$ and $\operatorname{dom}(\alpha) = \mathbf{n}$, then $\ker(\alpha) = \ker(\beta)$.*

Proof. Since $\alpha = \beta \diamond \gamma$, we have $\alpha \leq_{\mathscr{R}} \beta$, so Lemma 2.1(i) gives $\ker(\alpha) \subseteq \ker(\beta)$. Since $\operatorname{dom}(\alpha) = \mathbf{n}$, it is clear that $\ker(\alpha)$ is maximal, inclusion-wise, so we must in fact have $\ker(\alpha) = \ker(\beta)$. □

Lemma 3.9. *If $\alpha, \beta, \gamma \in \mathcal{D}_n$ are such that $\alpha = \beta \diamond \gamma$, $\ker(\alpha) = \ker(\beta)$ and $\operatorname{codom}(\beta) = \mathbf{n}$, then $\beta^{-1} \diamond \alpha = \gamma$.*

Proof. Since $\ker(\beta) = \ker(\alpha) = \ker(\beta \diamond \gamma)$, it follows that $\operatorname{coker}(\beta) \subseteq \ker(\gamma)$. Since $\operatorname{codom}(\beta) = \mathbf{n}$, $\operatorname{coker}(\beta)$ is maximal, inclusion-wise, so we must in fact have $\operatorname{coker}(\beta) = \ker(\gamma)$. But then $\beta^{-1} \diamond \beta = \gamma \diamond \gamma^{-1}$, which gives $\gamma = \gamma \diamond \gamma^{-1} \diamond \gamma = \beta^{-1} \diamond \beta \diamond \gamma = \beta^{-1} \diamond \alpha$. □

Lemma 3.10. *If $I_r = \langle J_r \cup \Sigma\rangle$, and if $1 \leq k \leq r-1$, then there exist $\sigma, \tau \in \Sigma$ with $\operatorname{dom}(\sigma) = \operatorname{codom}(\tau) = \mathbf{n}$, $\operatorname{rank}(\sigma) = \operatorname{rank}(\tau) = k$ and $\operatorname{codef}(\sigma), \operatorname{def}(\tau) > 0$.*

Proof. It suffices to prove the existence of σ, as the existence of τ will follow by a symmetrical argument (for which we need the duals of Lemmas 3.8 and 3.9). Let $1 \leq k \leq r-1$, and write

$$\Omega = \{\alpha \in \mathcal{D}_n : \operatorname{dom}(\alpha) = \mathbf{n},\ \operatorname{rank}(\alpha) = k,\ \operatorname{codef}(\alpha) > 0\}.$$

For $\alpha \in \Omega$, write $\ell(\alpha)$ for the minimum value of m such that $\alpha = \beta_1 \diamond \cdots \diamond \beta_m$ for some $\beta_1, \ldots, \beta_m \in J_r \cup \Sigma$. Let $L = \min\{\ell(\alpha) : \alpha \in \Omega\}$. To establish the existence of σ, it suffices to prove that $L = 1$. To do this, suppose to the contrary that $L \geq 2$, and choose some $\alpha = \left[\begin{smallmatrix} A_1 & \cdots & A_k \\ B_1 & \cdots & B_k \end{smallmatrix}\right] \in \Omega$ with $\ell(\alpha) = L$. So we may write $\alpha = \beta_1 \diamond \beta_2 \diamond \cdots \diamond \beta_L$ for some $\beta_1, \beta_2, \ldots, \beta_L \in J_r \cup \Sigma$. For simplicity, put $\beta = \beta_1$ and $\gamma = \beta_2 \diamond \cdots \diamond \beta_L$, so $\alpha = \beta \diamond \gamma$. Lemma 3.8 gives $\ker(\beta) = \ker(\alpha)$, so we may write $\beta = \left[\begin{smallmatrix} A_1 & \cdots & A_k \\ C_1 & \cdots & C_k \end{smallmatrix}\right]$. If $\operatorname{codef}(\beta) > 0$, then we put

$\sigma = \beta$, and the proof of the lemma is complete. So suppose $\mathrm{codef}(\beta) = 0$. This means that $\mathrm{codom}(\beta) = \mathbf{n}$, and Lemma 3.9 then gives

$$\beta^{-1} \diamond \alpha = \gamma = \beta_2 \diamond \cdots \diamond \beta_L. \tag{3.11}$$

But $\beta^{-1} \diamond \alpha = \left[\begin{smallmatrix} C_1 & \cdots & C_k \\ A_1 & \cdots & A_k \end{smallmatrix}\right] \diamond \left[\begin{smallmatrix} A_1 & \cdots & A_k \\ B_1 & \cdots & B_k \end{smallmatrix}\right] = \left[\begin{smallmatrix} C_1 & \cdots & C_k \\ B_1 & \cdots & B_k \end{smallmatrix}\right]$. Consequently, $\mathrm{dom}(\beta^{-1} \diamond \alpha) = \mathrm{codom}(\beta) = \mathbf{n}$ and $\mathrm{codef}(\beta^{-1} \diamond \alpha) = \mathrm{codef}(\alpha) > 0$. Thus, $\beta^{-1} \diamond \alpha \in \Omega$. But $\ell(\beta^{-1} \diamond \alpha) \leq L - 1$, by (3.11), contradicting the minimality of L. This completes the proof. □

Lemma 3.12. *If $I_r = \langle J_r \cup \Sigma \rangle$, and if $\mathbf{A} \in \mathscr{P}(\mathbf{n})$ with $|\mathbf{A}| \leq r-1$, then there exist $\sigma, \tau \in \Sigma$ with $\ker(\sigma) = \mathbf{A}$ and $\mathrm{coker}(\tau) = \mathbf{A}$.*

Proof. Again, it suffices to demonstrate the existence of σ. Choose some $\alpha \in I_r$ with $\ker(\alpha) = \mathbf{A}$, noting that $\mathrm{dom}(\alpha) = \mathbf{n}$. Suppose $\alpha = \beta_1 \diamond \cdots \diamond \beta_k$ where $\beta_1, \ldots, \beta_k \in J_r \cup \Sigma$. If $k = 1$, then $\alpha = \beta_1 \in \Sigma$, and we are done, with $\sigma = \alpha$. If $k \geq 2$, then $\alpha = \beta_1 \diamond (\beta_2 \diamond \cdots \diamond \beta_k)$, and Lemma 3.8 gives $\ker(\beta_1) = \ker(\alpha) = \mathbf{A}$, and we are done with $\sigma = \beta_1$. □

Proof of Lemma 3.3. As noted after the proof of Lemma 3.6, it suffices to show that $\mathrm{rank}(I_r : J_r) \geq r - 1 + \sum_{k=1}^{r-1} S(n,k)$. Suppose $I_r = \langle J_r \cup \Sigma \rangle$. For each $1 \leq k \leq r-1$, let $\Sigma_k = \{\alpha \in \Sigma : \mathrm{rank}(\alpha) = k\}$, and fix some such k. It is enough to show that $|\Sigma_k| \geq 1 + S(n,k)$. By Lemma 3.10, there exists some $\tau \in \Sigma_k$ with $\mathrm{def}(\tau) > 0$. By Lemma 3.12, for any $\mathbf{A} \in \mathscr{P}(\mathbf{n}, k)$, there exists some $\sigma_{\mathbf{A}} \in \Sigma_k$ with $\ker(\sigma_{\mathbf{A}}) = \mathbf{A}$. Clearly these elements of Σ are all distinct, so $|\Sigma_k| \geq 1 + |\mathscr{P}(\mathbf{n}, k)| = 1 + S(n,k)$, as required. □

As noted before the statement of Lemma 3.3, this completes the proof of Proposition 2.2.

Remark 3.13. Finally, we note that $\mathcal{D}_n$ bears many similarities with several families of semigroups, such as the symmetric inverse monoids $\mathcal{I}_n$, the full and partial transformation monoids $\mathcal{T}_n$ and $\mathcal{PT}_n$, and certain diagram monoids such as the partition monoids $\mathcal{P}_n$. All these monoids have a chain of $\mathscr{J}$-classes, and have the symmetric group $\mathcal{S}_n$ as their (unique) maximal $\mathscr{J}$-class. However, the ranks of the monoids $\mathcal{I}_n$, $\mathcal{T}_n$, $\mathcal{PT}_n$ and $\mathcal{P}_n$ are constant and very small (all being equal to either 3 or 4, for $n \geq 3$), and each monoid may be generated by elements in its top two $\mathscr{J}$-classes; see [2, 3, 6, 18]. The proper ideals of these monoids are all generated by elements in a single $\mathscr{J}$-class; formulae for the ranks of the ideals of these monoids may be found in [4, 5, 10, 19]. By contrast, as we have seen, $\mathrm{rank}(\mathcal{D}_n) = B(n) + n$ grows rapidly with n, and any generating set for $\mathcal{D}_n$ or one of its proper ideals must contain elements from all $\mathscr{J}$-classes except the very bottom one. Calculated values of $\mathrm{rank}(I_r)$ and $\mathrm{rank}(\mathcal{D}_n)$ are given in Tables 1 and 2, respectively.

$n \setminus r$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	1	2									
2	1	3	3								
3	1	7	8	8							
4	1	15	27	21	19						
5	1	31	92	84	60	57					
6	1	63	303	385	266	213	209				
7	1	127	968	1768	1419	986	889	884			
8	1	255	3027	7901	8049	5446	4313	4154	4148		
9	1	511	9332	34364	45810	33883	23888	21405	21163	21156	
10	1	1023	28503	146265	256576	223439	150465	121186	116342	115993	115985

Table 1: Values of $\mathrm{rank}(I_r)$; see Proposition 2.2.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mathrm{rank}(\mathcal{D}_n)$	1	2	3	8	19	57	209	884	4148	21156	115985	678581	4213609	27644450

Table 2: Values of $\mathrm{rank}(\mathcal{D}_n)$; see Theorem 2.3.

References

[1] The On-Line Encyclopedia of Integer Sequences. Published electronically at `http://oeis.org/`, 2016.

[2] A. Ja. Aĭzenštat. Defining relations of finite symmetric semigroups (in Russian). *Mat. Sb. N.S.*, 45 (87):261–280, 1958.

[3] James East. Generators and relations for partition monoids and algebras. *J. Algebra*, 339:1–26, 2011.

[4] James East and Robert D. Gray. Diagram monoids and Graham–Houghton graphs: Idempotents and generating sets of ideals. *J. Combin. Theory Ser. A*, 146:63–128, 2017.

[5] G. U. Garba. Idempotents in partial transformation semigroups. *Proc. Roy. Soc. Edinburgh Sect. A*, 116(3-4):359–366, 1990.

[6] Gracinda Gomes and John M. Howie. On the ranks of certain finite semigroups of transformations. *Math. Proc. Cambridge Philos. Soc.*, 101(3):395–403, 1987.

[7] Robert D. Gray. The minimal number of generators of a finite semigroup. *Semigroup Forum*, 89(1):135–154, 2014.

[8] Martin Hellman. A cryptanalytic time-memory trade-off. *IEEE transactions on Information Theory*, 26(4):401–406, 1980.

[9] John M. Howie. *Fundamentals of semigroup theory*, volume 12 of *London Mathematical Society Monographs. New Series.* The Clarendon Press, Oxford University Press, New York, 1995. Oxford Science Publications.

[10] John M. Howie and Robert B. McFadden. Idempotent rank in finite full transformation semigroups. *Proc. Roy. Soc. Edinburgh Sect. A*, 114(3-4):161–167, 1990.

[11] John M. Howie, N. Ruškuc, and P. M. Higgins. On relative ranks of full transformation semigroups. *Comm. Algebra*, 26(3):733–748, 1998.

[12] Ganna Kudryavtseva and Victor Maltcev. Two generalisations of the symmetric inverse semigroups. *Publ. Math. Debrecen*, 78(2):253–282, 2011.

[13] Mark V. Lawson. *Inverse semigroups.* World Scientific Publishing Co., Inc., River Edge, NJ, 1998. The theory of partial symmetries.

[14] Eliakim Hastings Moore. Concerning the abstract groups of order $k!$ and $\frac{1}{2}k!$ holohedrically isomorphic with the symmetric and the alternating substitution-groups on k letters. *Proc. London Math. Soc.*, 28(1):357–366, 1897.

[15] L. M. Popova. Defining relations in some semigroups of partial transformations of a finite set (in Russian). *Uchenye Zap. Leningrad Gos. Ped. Inst.*, 218:191–212, 1961.

[16] J. Riguet. Relations binaires, fermetures, correspondances de Galois. *Bull. Soc. Math. France*, 76:114–155, 1948.

[17] Alexei Vernitski. A generalization of symmetric inverse semigroups. *Semigroup Forum*, 75(2):417–426, 2007.

[18] N. N. Vorob'ev. On symmetric associative systems. *Leningrad. Gos. Ped. Inst. Uč. Zap.*, 89:161–166, 1953.

[19] Ping Zhao and Vítor H. Fernandes. The ranks of ideals in various transformation monoids. *Comm. Algebra*, 43(2):674–692, 2015.