THE LATTICE AND SEMIGROUP STRUCTURE OF MULTIPERMUTATIONS

CATARINA CARVALHO AND BARNABY MARTIN

Abstract. We study the algebraic properties of binary relations whose underlying digraph is smooth, that is has no source or sink. Such objects have been studied as surjective hyper-operations (shops) on the corresponding vertex set, and as binary relations that are defined everywhere and whose inverse is also defined everywhere. In the latter formulation, they have been called multipermutations.

We study the lattice structure of sets (monoids) of multipermutations over an n-element domain. Through a Galois connection, these monoids form the algebraic counterparts to sets of relations closed under definability in positive first-order logic without equality. We show one side of this Galois connection, and give a simple dichotomy theorem for the evaluation problem of positive first-order logic without equality on the class of structures whose preserving multipermutations form a monoid closed under inverse. These problems turn out either to be in Logspace or to be Pspace-complete. We go on to study the monoid of all multipermutations on an n-element domain, under usual composition of relations. We characterize its Green relations, regular elements and show that it does not admit a generating set that is polynomial on n.

1. Introduction

A *multipermutation* is a binary relation ϕ over a set $[n] = \{1, \ldots, n\}$ so that: for all $x \in [n]$ there exists $y \in [n]$ such that $(x, y) \in \phi$; and for all $y \in [n]$ there exists $x \in [n]$ such that $(x, y) \in \phi$. The term multipermutation originates with Schein in [36] but they were studied independently as *surjective hyper-operations* (shops) in [26, 28, 27].

In Universal Algebra there is a family of Galois connections that links relational expressivity in fragments of first-order logic with closure operators that generate particular types of algebra. For example, expressivity in the fragment of first-order logic containing $\{\exists, \wedge, =\}$ (called *primitive positive*, or pp-logic) is linked with superpositional closure of sets of finite arity operations (called *clones*). A survey of these Galois connections can be found in [6] (see Table 1) and a survey more oriented towards Computer Scientists containing much of the same material is [4] (see Tables 1 and 2).

The model-checking problem for primitive positive logic on a fixed relational structure $\mathcal{B}$ is known as the *Constraint Satisfaction Probem* $\mathrm{CSP}(\mathcal{B})$. The relevant Galois connection just noted above gave rise to the so-called

algebraic approach to the computational complexity of CSP($\mathcal{B}$). This approach culminated in the proof of the Feder-Vardi Conjecture, showing that such problems for finite $\mathcal{B}$ are either in P or are NP-complete [10, 40]. One side of the Galois connection we discuss in this paper played a similar role in resolving the computational complexities of the corresponding model-checking problems for the fragment of first-order logic containing $\{\forall, \exists, \wedge, \vee\}$, denoted by $\{\exists, \forall, \wedge, \vee\}$-FO($\mathcal{B}$) for a fixed finite relational structure $\mathcal{B}$ [27]. A complete Galois connection has two sides and it is the other side of this connection that we prove in this paper.

Galois connections have been leveraged in a variety of contexts related to the CSP in order to aid in classifications of computational complexity, where they have played, or continue to play, a key part in those projects. In the case of the *Quantified CSP*, the relevant connection is noted in [5] and involves surjective operations that preserve the corresponding relations (known in this case as well as the non-surjective case as *polymorphisms*). The complexity classification for *Quantified CSP* is famously wide open [41]. Another relative of the CSP, where the complexity classification is now known, is the *Valued CSP*. Here the corresponding "logic" is no longer a fragment of first-order logic. The corresponding Galois connection was discovered gradually, culminating in the notion of *weighted clones* in [14]. The algebraic approach was pivotal in the final complexity classification for Valued CSPs [37, 22], though the full power of weighted clones turned out not to be necessary (the more restricted notion of *fractional polymorphism* was enough). A final relative of the CSP, where the complexity classification is still open, is the *Promise CSP*. Again, the corresponding "logic" is not a fragment of first-order logic. The Galois connection here first appeared in [31] and was used subsequently in [7]. The algebraic approach here is ongoing and, indeed, promising (see [11]).

The Galois connection that we prove in this paper, related with the complexity of $\{\exists, \forall, \wedge, \vee\}$-FO($\mathcal{B}$), deals with sets of multipermutations ϕ over the set B under which the relational $\mathcal{B}$ (whose domain is B) is *invariant*, in the following sense. For a k-ary relation R of $\mathcal{B}$ and $(x_1, \ldots, x_k) \in R$, always $(y_1, \ldots, y_k) \in R$, if $(x_1, y_1), \ldots, (x_k, y_k) \in \phi$. To these sets, always containing the identity and closed under composition and subrelations (that are themselves also multipermutations), we will call *down shop-monoids* (DSMs). In this paper we study the structure of the lattice of DSMs on a k-element domain. We give a full Galois connection proving an isomorphism between the lattice of DSMs (over a k-element domain) and the lattice of k-element structures closed under definabilty in positive first-order logic without equality. We study in particular the automorphism born of the inverse operation on multipermutations. DSMs that are closed under inverse have a fundamentally group-like structure – what we call *blurred permutation subgroups* (BPSs). Using this characterization, we prove a dichotomy for our evaluation problem on structures that we term *she-complementative*, i.e. whose monoid of multipermutations under which they are invariant, is closed under

inverse. Specifically, these problems are either in Logspace or are Pspace-complete. This complexity classification follows from the general result of [27] but our proof here is simpler.

Multipermutations have been studied earlier as monoids of binary relations, when considered closed only under composition of relations (not also subrelations). Schein [36] looked at sets Φ of binary relations ϕ defined everywhere (i.e. where every element of the domain appears in the first component) that are closed under inverses (i.e. $\phi^{-1} \in \Phi$ for all $\phi \in \Phi$), so both the domain and range of these relations are the full domain. Having termed these objects multipermutations, he went on to characterize involutive semigroups of multipermutations. Furthermore, he proved that every involutive semigroup of difunctional multipermutations is an inverse semigroup, and every inverse semigroup is isomorphic to an involutive semigroup of difunctional multipermutations. Ten years later McKenzie and Schein [29], after showing that every semigroup is isomorphic to a transitive semigroup of binary relations, leave as an open problem the question "Which semigroups are isomorphic to transitive semigroups of multipermutations?" As far as we know this question is still open.

Bredikhin [8] studied the monoid of all difunctional multipermutations on a k-element domain. The operation he considered was not the usual composition of operations, since the composition of two difunctional relations is not necessarily difunctional. His idea on studying these monoids seemed to be to present a unification of the theories of inverse semigroups and lattices, see also [9]. These are, as far as we are aware, the only articles mentioning multipermutations. With their reappearance in the context mentioned above, we believe it is time to restart the study of these structures. With this in mind, we look at structural properties of the monoid of all multipermutations on a k-element domain.

The monoid of (all) binary relations on a k-element domain has been widely studied since the 60s, as have some of its subsemigroups like the full transformation monoid, Hall monoid and, more recently, diagram semigroups. The fact that binary relations can also be represented as boolean square matrices and as graphs allows us to use techniques from different areas of mathematics to study these monoids. Drawing on similarities with previously studied monoids, we look at some structural properties of the monoid of multipermutations. We characterize its Green's relations, give an algorithm to compute regular elements, and show that this monoid, unlike the symmetric group, does not admit a generating set that is of size polynomial in k. Finally we prove that blurred permutations are the completely regular difunctional multipermutations. There are still many questions to answer about the monoid of all multipermutations, e.g. What are its maximal subgroups? Is this semigroup better behaved in any way than the semigroup of all binary relations?

This paper is, partially, based on [28]. Some of the content from [28] is now obsolete and has been removed, other parts appear here (with minor issues)

corrected. The section on the monoid of multipermutations, Section 4, is new to this paper.

Presentation. The paper is organized as follows. In Section 2 we give the necessary preliminaries and introduce the Galois connection. In Section 3, we discuss the structure of our lattices, with particular emphasis on an automorphism born of an inverse operation. We go on to prove the characterization theorem that allows us to derive the complexity dichotomy for she-complementative structures. In Section 4 we study the monoid of all multipermutations on a k-element domain.

2. Preliminaries

Let $\mathcal{B}$ be a structure, always with finite domain B, over an at most countable relational signature σ. Let $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ be the positive fragment of first-order (fo) logic without equality. An *extensional* relation is (the interpretation in a structure of) a relation of the signature σ. We will usually denote extensional relations of $\mathcal{B}$ by R and other relations by S (or by some formula that defines them). In $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$, the atomic formulae are exactly substitution instances of extensional relations. The problem $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ has:

- Input: a sentence $\varphi \in \{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$.
- Question: does $\mathcal{B} \models \varphi$?

QCSP($\mathcal{B}$) is the restriction of this problem to formulae involving no disjunction, what in our notation would be $\{\exists, \forall, \wedge\}$-$\mathsf{FO}$. When $\mathcal{B}$ is of size one, the evaluation of any FO sentence may be accomplished in $\mathsf{Logspace}$ (essentially, the quantifiers are irrelevant and the problem amounts to the *boolean sentence value problem*, see [24]). In this case, it follows that $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ is in $\mathsf{Logspace}$. Furthermore, by inward evaluation of the quantifiers, $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ is readily seen to always be in Pspace.

For a structure $\mathcal{B}$ define the complement structure $\overline{\mathcal{B}}$ to be over the same domain B with relations which are the set-theoretic complements of those of $\mathcal{B}$. That is, for each r-ary relation R, $R^{\overline{\mathcal{B}}} = B^r \setminus R^{\mathcal{B}}$. Similarly, for a relation $R \subseteq B^r$, let $\overline{R}$ denote $B^r \setminus R$.

Consider the finite set $X = [n] := \{1, \ldots, n\}$ and its power set $\mathcal{P}(X)$. A *hyper-operation* on X is a function $f : X \to \mathcal{P}(X) \setminus \{\emptyset\}$ (that the image may not be the empty set corresponds to the hyper-operation being *total*, following [3]). If the hyper-operation f has the additional property that

- for all $y \in X$, there exists $x \in X$ such that $y \in f(x)$,

then we designate (somewhat abusing terminology) f *surjective*. A surjective hyper-operation in which each element is mapped to a singleton set is identified with a *permutation* (bijection). Instead of operations we can think of these hyper-operations as being binary relations. Given an hyper-operation f on X, we can construct the binary relation $\{(x, f(x)) : x \in X\}$, thus surjective hyper-operations can be thought of as binary relations $f \subseteq X \times X$

that satisfy

$$\forall x \in X \ \exists y_1, y_2 \in X \text{ s.t. } (x, y_1), (y_2, x) \in f.$$

Following the work of Schein [35], we denote these *multipermutations*, and will keep this terminology for both the relations and hyper-operations.

A *surjective hyper-endomorphism* (she) of a set of relations (forming the finite-domain structure) $\mathcal{B}$ over X is a multipermutation f on X that satisfies, for all relations R of $\mathcal{B}$,

- if $(x_1, \ldots, x_i) \in R$ then, for all $y_1 \in f(x_1), \ldots, y_i \in f(x_i)$, $(y_1, \ldots, y_i) \in R$.

More generally, for $r_1, \ldots, r_k \in X$, we say f is *a she from* $(\mathcal{B}; r_1, \ldots, r_k)$ to $(\mathcal{B}; r'_1, \ldots, r'_k)$ if f is a she of $\mathcal{B}$ and $r'_1 \in f(r_1), \ldots, r'_k \in f(r_k)$. A she may be identified with a *surjective endomorphism* if each element is mapped to a singleton set. On finite structures surjective endomorphisms are necessarily automorphisms.

2.1. **Galois Connections.**

2.1.1. *Relational side.* For a set F of multipermutations on the finite domain B, let $\mathsf{Inv}(F)$ be the set of relations on B of which each $f \in F$ is a she (when these relations are viewed as a structure over B). We say that $S \in \mathsf{Inv}(F)$ is invariant or is *preserved* by (the multipermutations in) F. Let $\mathsf{shE}(\mathcal{B})$ be the set of shes of $\mathcal{B}$. Let $\mathsf{Aut}(\mathcal{B})$ be the set of automorphisms of $\mathcal{B}$.

Let $\langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-}\mathsf{FO}}$ and $\langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee,=\}\text{-}\mathsf{FO}}$ be the sets of relations that may be defined on $\mathcal{B}$ in $\{\exists, \forall, \wedge, \vee\}$-FO and $\{\exists, \forall, \wedge, \vee, =\}$-FO, respectively.

Lemma 1 ([25])**.** *Let* $\mathbf{r} := (r_1, \ldots, r_k)$ *be a* k*-tuple of elements of the finite-signature* $\mathcal{B}$*. There exists:*

(*i*). *a formula* $\theta_{\mathbf{r}}(u_1, \ldots, u_k) \in \{\exists, \forall, \wedge, \vee, =\}$-FO *such that* $(\mathcal{B}, r'_1, \ldots, r'_k) \models \theta_{\mathbf{r}}(u_1, \ldots, u_k)$ *iff there is an automorphism from* $(\mathcal{B}, r_1, \ldots, r_k)$ *to* $(\mathcal{B}, r'_1, \ldots, r'_k)$.

(*ii*). *a formula* $\theta_{\mathbf{r}}(u_1, \ldots, u_k) \in \{\exists, \forall, \wedge, \vee\}$-FO *such that* $(\mathcal{B}, r'_1, \ldots, r'_k) \models \theta_{\mathbf{r}}(u_1, \ldots, u_k)$ *iff there is a she from* $(\mathcal{B}, r_1, \ldots, r_k)$ *to* $(\mathcal{B}, r'_1, \ldots, r'_k)$.

The following is the main theorem of [25].

Theorem 1 ([25])**.** *For a finite-signature structure* $\mathcal{B}$ *we have*

(*i*). $\langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee,=\}\text{-}\mathsf{FO}} = \mathsf{Inv}(\mathsf{Aut}(\mathcal{B}))$ *and*

(*ii*). $\langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-}\mathsf{FO}} = \mathsf{Inv}(\mathsf{shE}(\mathcal{B}))$.

We will need a countable-signature version of this theorem for our final lattice isomorphism.

Theorem 2. *For a countable-signature structure* $\mathcal{B}$ *we have*

(*i*). $\langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee,=\}\text{-}\mathsf{FO}} = \mathsf{Inv}(\mathsf{Aut}(\mathcal{B}))$ *and*

(*ii*). $\langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-}\mathsf{FO}} = \mathsf{Inv}(\mathsf{shE}(\mathcal{B}))$.

Proof. Part (i) is well-known [20, 2] and may be proved in a similar, but simpler, manner to Part (ii), which we now prove. The direction $[\varphi(\mathbf{v}) \in \langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-FO}} \Rightarrow \varphi(\mathbf{v}) \in \mathsf{Inv}(\mathsf{shE}(\mathcal{B}))]$ is proved as before.

For $[S \in \mathsf{Inv}(\mathsf{shE}(\mathcal{B})) \Rightarrow S \in \langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-FO}}]$, we proceed similarly to before, but using finiteness of the domain B, which will rescue us from the pitfalls of an infinite signature. Let $\mathbf{r}_1, \ldots, \mathbf{r}_m$ enumerate the tuples of S. Consider the following finite disjunction:

$$\theta_S(u_1, \ldots, u_k) := \theta_{\mathbf{r}_1}(u_1, \ldots, u_k) \vee \ldots \vee \theta_{\mathbf{r}_m}(u_1, \ldots, u_k).$$

Let $R_1, R_2, \ldots$ be an enumeration of the extensional relations of $\mathcal{B}$. Let $\mathcal{B}_i$ be the reduct of $\mathcal{B}$ to the signature $\langle R_1, \ldots, R_i\rangle$. For $j \in [m]$ let $\theta^i_{\mathbf{r}_j}(u_1, \ldots, u_k)$ be built as in Lemma 1, but on the reduct $\mathcal{B}_i$. The relations $\theta^1_{\mathbf{r}_j}(u_1, \ldots, u_k)$, $\theta^2_{\mathbf{r}_j}(u_1, \ldots, u_k)$, ... are monotone decreasing on B^k – the shes must preserve an increasing number of extensional relations – and therefore reach a limit l_j such that $\theta^{l_j}_{\mathbf{r}_j}(u_1, \ldots, u_k) = \theta_{\mathbf{r}_j}(u_1, \ldots, u_k)$. Let $l := \max\{l_1, \ldots, l_m\}$ and build $\theta_S(u_1, \ldots, u_k)$ over the finite-signature reduct $\mathcal{B}_l$. The result follows. □

In the following, $\leq_{\mathsf{Logspace}}$ indicates the existence of a logspace many-to-one reduction.

Theorem 3. *Let $\mathcal{B}$ and $\mathcal{B}'$ be structures over the same domain B such that $\mathcal{B}'$ is finite-signature.*

(i). *If* $\mathsf{Aut}(\mathcal{B}) \subseteq \mathsf{Aut}(\mathcal{B}')$ *then* $\{\exists,\forall,\wedge,\vee,=\}\text{-FO}(\mathcal{B}') \leq_{\mathsf{Logspace}} \{\exists,\forall,\wedge,\vee,=\}\text{-FO}(\mathcal{B})$.

(ii). *If* $\mathsf{shE}(\mathcal{B}) \subseteq \mathsf{shE}(\mathcal{B}')$ *then* $\{\exists,\forall,\wedge,\vee\}\text{-FO}(\mathcal{B}') \leq_{\mathsf{Logspace}} \{\exists,\forall,\wedge,\vee\}\text{-FO}(\mathcal{B})$.

Proof. Part (i) is well-known [20, 2] and the proof is similar to that of Part (ii), which we give. If $\mathsf{shE}(\mathcal{B}) \subseteq \mathsf{shE}(\mathcal{B}')$, then $\mathsf{Inv}(\mathsf{shE}(\mathcal{B}')) \subseteq \mathsf{Inv}(\mathsf{shE}(\mathcal{B}))$. From Theorem 1, it follows that $\langle\mathcal{B}'\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-FO}} \subseteq \langle\mathcal{B}\rangle_{\{\exists,\forall,\wedge,\vee\}\text{-FO}}$. Recalling that $\mathcal{B}'$ contains only a finite number of extensional relations, we may therefore effect a logspace reduction from $\{\exists,\forall,\wedge,\vee\}\text{-FO}(\mathcal{B}')$ to $\{\exists,\forall,\wedge,\vee\}\text{-FO}(\mathcal{B})$ by substitution of predicates by formulas. That is, we reduce ϕ', an instance of $\{\exists,\forall,\wedge,\vee\}\text{-FO}(\mathcal{B}')$, to ϕ, an instance of $\{\exists,\forall,\wedge,\vee\}\text{-FO}(\mathcal{B})$, by substituting instances of R' in ϕ' by their $\{\exists,\forall,\wedge,\vee\}\text{-FO}$ definition over $\mathcal{B}$. □

2.1.2. *Down-shop-monoids and the functional side.* Consider the finite domain X. The *identity* multipermutation id_X is defined by $x \mapsto \{x\}$. Given multipermutations f and g, define the *composition* $g \circ f$ by $x \mapsto \{z : \exists y\ z \in g(y) \wedge y \in f(x)\}$. We say that f is a *sub-multipermutation* of g, denoted $f \subseteq g$, if $f(x) \subseteq g(x)$ for all x, and f is a multipermutation. A set of multipermutations on a finite set B is a *down-shop-monoid* (DSM), if it contains id_B, and is closed under composition and sub-multipermutations[1]. The multipermutation id_B is a she of all structures with domain B, and, if

[1]Closure under sub-multipermutations is termed *down closure* in [3], hence the D in DSM.

f and g are shes of $\mathcal{B}$, then so is $g \circ f$. Further, if g is a she of $\mathcal{B}$, then so is f for all sub-multipermutations $f \subseteq g$. It follows that $\mathsf{shE}(\mathcal{B})$ is always a DSM. If F is a set of permutations, then we write $\langle F \rangle_G$ to denote the group generated by F. If F is a set of multipermutations on B, then let $\langle F \rangle_{DSM}$ denote the minimal DSM containing the multipermutations of F. If F is the singleton $\{f\}$, then, by abuse of notation, we write $\langle f \rangle$ instead of $\langle \{f\} \rangle$. For multipermutations on small domains we will represent it by listing all elements of the domain on the left and their images on the right, e.g. the multipermutation $1 \mapsto \{1,2\}$, $2 \mapsto \{2\}$, $3 \mapsto \{1,3\}$ will be represented by $\begin{smallmatrix} 1 & 1,2 \\ 2 & 2 \\ 3 & 1,3 \end{smallmatrix}$. Also, if the multipermutation is a permutation we will keep the usual cycle notation.

For a multipermutation f, define its inverse f^{-1} by $x \mapsto \{y : x \in f(y)\}$. Note that f^{-1} is also a multipermutation and $(f^{-1})^{-1} = f$, though $f \circ f^{-1} = id_B$ only if f is a permutation. For a set of multipermutation F, let $F^{-1} := \{f^{-1} : f \in F\}$.

A *permutation group* on a finite set B is a set of permutations of B closed under composition. It may easily be verified that such a set contains the identity and is closed under inverse. A permutation group may be identified with a particular type of DSM in which all multipermutations have only singleton sets in their range.

Theorem 4. *Let X be a finite set.*

(*i*) *Let F be a set of permutations on X. Then$\langle F \rangle_G = \mathsf{Aut}(\mathsf{Inv}(F))$.*
(*ii*) *Let F be a set of multipermutations on X. Then $\langle F \rangle_{DSM} = \mathsf{shE}(\mathsf{Inv}(F))$.*

Proof. Part (*i*) is well-known but we give a proof for illustrative purposes.

[$\langle F \rangle_G \subseteq \mathsf{Aut}(\mathsf{Inv}(F))$.] By induction. One may easily see that if $f, g \in \mathsf{Aut}(\mathsf{Inv}(F))$ then $f \circ g \in \mathsf{Aut}(\mathsf{Inv}(F))$. Further, if $f \in \mathsf{Aut}(\mathsf{Inv}(F))$ then $f^{-1} \in \mathsf{Aut}(\mathsf{Inv}(F))$ as the set of automorphisms is closed under inverse.

[$\mathsf{Aut}(\mathsf{Inv}(F)) \subseteq \langle F \rangle_G$.] Let $|X| = n$. One may easily see that $\mathsf{Inv}(F) = \mathsf{Inv}(\langle F \rangle_G)$ (for the forward containment, note that inverse follows from the fact that F is a set of bijections on a finite set). Let R be the n-ary relation that lists the permutations in $\langle F \rangle_G$ (e.g., the identity appears as $(1, 2, \ldots, n)$); R is preserved by $\langle F \rangle_G$. We will prove $\mathsf{Aut}(\mathsf{Inv}(\langle F \rangle_G)) \subseteq \langle F \rangle_G$ by contraposition. If g is a permutation not in $\langle F \rangle_G$, then $g \notin R$ and g does not preserve R as it maps the identity to g. Therefore $g \notin \mathsf{Aut}(\mathsf{Inv}(\langle F \rangle_G))$ and the result follows.

[Part (*ii*).]

[$\langle F \rangle_{DSM} \subseteq \mathsf{shE}(\mathsf{Inv}(F))$.] By induction. One may easily see that if $f, g \in \mathsf{shE}(\mathsf{Inv}(F))$ then $f \circ g \in \mathsf{shE}(\mathsf{Inv}(F))$. Similarly for sub-multipermutations and the identity.

[$\mathsf{shE}(\mathsf{Inv}(F)) \subseteq \langle F \rangle_{DSM}$.] Let $|D| = n$. One may easily see that $\mathsf{Inv}(F) = \mathsf{Inv}(\langle F \rangle_{DSM})$. Let R be the n^2-ary relation that lists the shes of $\langle F \rangle_{DSM}$ in the following manner. Consider the n^2 positions enumerated in n-ary, i.e. by (i, j) s.t. $i, j \in [n]$. Each she f gives rise to many tuples in which the

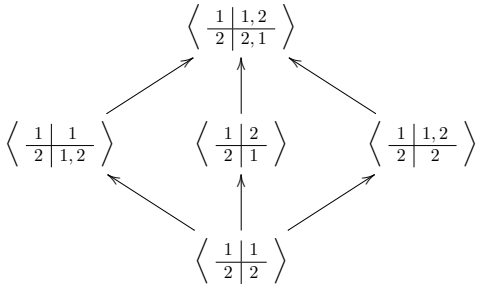

FIGURE 1. The lattice $\mathscr{F}_2$.

positions $(i,1),\ldots,(i,n)$ are occupied in all possible ways by the elements of $f(i)$. Thus, $f_0 := \begin{smallmatrix}1&|&1,2\\2&|&2\\3&|&3\end{smallmatrix}$ generates the following eight tuples

$$\begin{array}{c}(1,1,1,2,2,2,3,3,3)\\(1,1,2,2,2,2,3,3,3)\\(1,2,1,2,2,2,3,3,3)\\(1,2,2,2,2,2,3,3,3)\\(2,1,1,2,2,2,3,3,3)\\(2,1,2,2,2,2,3,3,3)\\(2,2,1,2,2,2,3,3,3)\\(2,2,2,2,2,2,3,3,3)\end{array}$$

Let $p_{i,j} \in [n]$ be the element at position (i,j). We describe as a *full coding* of f any such tuple s.t., for all i, $\{p_{i,1},\ldots,p_{i,|D|}\} = f(i)$. In our example, all tuples except the first and last are full codings of f_0. Note that R is preserved by $\langle F\rangle_{DSM}$. We will prove that $\mathsf{shE}(\mathsf{Inv}(\langle F\rangle_G)) \subseteq \langle F\rangle_{DSM}$ by contraposition. If g is a shop not in $\langle F\rangle_{DSM}$, then g does not appear fully coded in R and g does not preserve R as it maps the identity to all tuples that are full codings of g. Therefore $g \notin \mathsf{shE}(\mathsf{Inv}(\langle F\rangle_{DSM}))$ and the result follows. □

2.2. **Lattice isomorphism.** Consider sets of relations Γ on the domain $D = [n]$, closed under $\{\exists,\forall,\wedge,\vee\}$-FO-definability (such sets may be seen as countable signature structures $\mathcal{D}$). Let $\mathscr{R}_n$ be the lattice of such sets ordered by inclusion. Let the lattice $\mathscr{F}_n$ be of DSMs on the set $[n]$, again ordered by inclusion.

Corollary 2. *The lattices $\mathscr{R}_n$ and $\mathscr{F}_n$ are isomorphic and the operators* Inv *and* shE *induce isomorphisms between them.*

Proof. From the second parts of Theorems 2 and 4. □

The permutation groups form a lattice under inclusion whose minimal element contains just the identity and whose maximal element is the symmetric group (on the size of the domain). As per Theorem 3, this lattice classifies

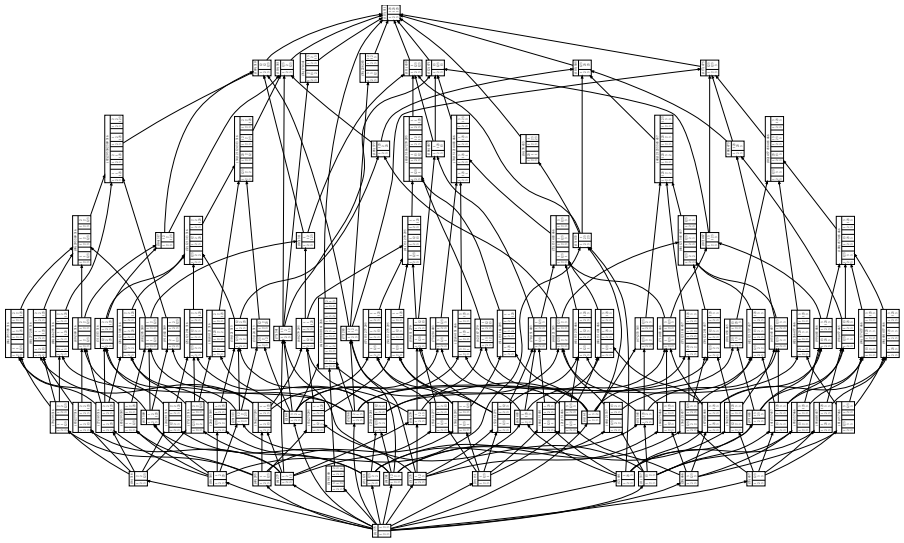

FIGURE 2. The lattice $\mathscr{F}_3$. The authors are grateful to Jos Martin for calculating and drawing $\mathscr{F}_3$.

the complexities of $\{\exists, \forall, \wedge, \vee, =\}$-$\mathsf{FO}(\mathcal{B})$ (again there is an isomorphism between this lattice and sets of relations closed under positive fo-definability). In the lattice of DSMs, $\mathscr{F}_n$, the minimal element still contains just the identity, but the maximal element contains all multipermutations. However, the lattice of permutation subgroups always appears as a sub-lattice within the lattice of DSMs. In the case of $\mathscr{F}_2$, Figure 1, we have 5 DSMs, two of which are the subgroups of S_2. In the case of $\mathscr{F}_3$, Figure 2, we have 115 DSMs, only six of which are the subgroups of S_3 – so the lattice complexity jumps very quickly.

3. The structure of $\mathscr{F}_n$

3.1. **Blurred permutation subgroups and symmetric multipermutations.** Many of the DSMs of $\mathscr{F}_n$ are reminiscent of subgroups of the symmetric group S_m for some $m \leq n$. We say that a multipermutation f on the domain $[n]$ is a *blurred permutation* if it may be built from (the multipermutation associated with) the permutation g on the domain $[m]$ ($m \leq n$) in the following manner:

(*) for $P_1, \ldots, P_m$ a partition of $[n]$, set $f(k) = P_{g(i)}$ for all $k \in P_i$, $i = 1, \ldots, m$.

We note that if f is a blurred permutation obtained as above with partition $P_1, \ldots, P_m$ and permutation g, then f^{-1} is also a blurred permutation

obtained with the same partition and permutation g^{-1}. This is easy to see if we think of $f^{-1}(k)$ as the set of elements that get mapped to k under f.

We say that a DSM N over domain $[n]$ is a *blurred permutation subgroup* (BPS) if one may build it from (the DSM associated with) a subgroup M of S_m, $m \leq n$ by replacing each permutation $g \in M$ by the blurred permutation f created as in $(*)$, and then taking the closure under sub-multipermutations. For the example, the group $M := \langle \begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix} \rangle$

- becomes the BPS $N := \langle \begin{smallmatrix} 1 & 2,3,4 \\ 2 & 1 \\ 3 & 1 \\ 4 & 1 \end{smallmatrix} \rangle$ when $P_1 := \{1\}$ and $P_2 := \{2,3,4\}$, and
- becomes the BPS $N := \langle \begin{smallmatrix} 1 & 2,4 \\ 2 & 1,3 \\ 3 & 2,4 \\ 4 & 1,3 \end{smallmatrix} \rangle$ when $P_1 := \{1,3\}$ and $P_2 := \{2,4\}$,

and the permutation $\begin{smallmatrix} 1 & 1 \\ 2 & 3 \\ 3 & 2 \end{smallmatrix}$ becomes the blurred permutation $\begin{smallmatrix} 1 & 1 \\ 2 & 3,4 \\ 3 & 2 \\ 4 & 2 \end{smallmatrix}$ when $P_1 := \{1\}$, $P_2 := \{2\}$ and $P_3 := \{3,4\}$. A *blurred symmetric group* is a BPS built in the manner described from a symmetric group.

With an arbitrary multipermutation f on D, we may associate the digraph $\mathcal{G}_f$ on D in which there is an edge (x,y) if $f(x) \ni y$. The condition of totality ensures $\mathcal{G}_f$ has no sinks and the condition of surjectivity ensures $\mathcal{G}_f$ has no sources. f contains the identity as a sub-multipermutation iff $\mathcal{G}_f$ is reflexive. There is an edge from a to some y in $\mathcal{G}_g$ and an edge from y to b in $\mathcal{G}_f$ iff there is an edge from a to b in $\mathcal{G}_{f \circ g}$. In this fashion, it is easy to verify that there is a directed path of length n from a to b in $\mathcal{G}_f$ iff $b \in f^n(a)$.

A binary relation (and consequently a multipermutation) f is *symmetric* if, for all a and b, we have $a \in f(b)$ iff $b \in f(a)$, and it is *reflexive* if $a \in f(a)$ for all $a \in D$. Examples of symmetric multipermutations are id_D and $\begin{smallmatrix} 1 & 1,2 \\ 2 & 1,2 \\ 3 & 3 \end{smallmatrix}$. It not hard to see that f is symmetric iff $f = f^{-1}$ iff $\mathcal{G}_f$ is undirected.

Lemma 3. *The reflexive blurred permutations are the ones built in the manner $(*)$ from an identity multipermutation. Furthermore, they are symmetric.*

Proof. Let f be a reflexive blurred permutation obtained as in $(*)$ from the permutation σ with partition $P_1, \ldots, P_m$, $m \leq n$. We have, for any $i \in [m]$, $f(P_i) = P_{\sigma(i)}$. Since f is reflexive, for every $k \in P_i$ we have $k \in P_{\sigma(i)}$, so that $P_i = P_{\sigma(i)}$, implying $i = \sigma(i)$. Thus σ is the identity permutation. Recall that f^{-1} is obtained from σ^{-1} with the same partition. Since $\sigma = \sigma^{-1}$, it follows that $f = f^{-1}$, hence f is symmetric. □

We note that not all reflexive or symmetric multipermutations are blurred permutations.

Example 4. *The multipermutation* $\begin{smallmatrix} 1 & 1,2 \\ 2 & 1,2,3 \\ 3 & 2,3 \end{smallmatrix}$ *is symmetric and reflexive but is not a blurred permutation.*

Lemma 5. *For all multipermutations f, $f \circ f^{-1}$ and $f^{-1} \circ f$ are symmetric and reflexive multipermutations.*

Proof. It is sufficient to prove that $f \circ f^{-1}$ is symmetric. Let $a \in f \circ f^{-1}(b)$. Then there exists y s.t. $b \in f^{-1}(y)$ and $y \in f(a)$. Thus, $y \in f(b)$ and $a \in f^{-1}(y)$, i.e. $b \in f \circ f^{-1}(a)$. The fact that they are reflexive is easy to see. □

Let f and g be symmetric multipermutations on the domain D. The minimal symmetric multipermutation h containing both f and g as a sub-multipermutation is said to be the *join* of f and g. The *union* $(f \cup g)$ of f and g is the multipermutation given by, for all $x \in D$, $(f \cup g)(x) := f(x) \cup g(x)$.

Lemma 6. *Let f and g be symmetric and reflexive multipermutations on the domain $[n]$. The join of f and g is $(f \cup g)^n = (f \circ g)^n = (g \circ f)^n$.*

Proof. Consider the union $f \cup g$. Since f and g are both reflexive, we can see that $f \cup g \subseteq f \circ g \subseteq (f \cup g)^2$ and $f \cup g \subseteq g \circ f \subseteq (f \cup g)^2$. The join h of f and g contains exactly those $a \in h(b)$ and $b \in h(a)$ for which there is a path in $f \cup g$ from a to b (and b to a). By reflexivity of $f \cup g$ this is equivalent to there being an n-path between a and b in $(f \cup g)$, which is equivalent to there being an edge in $(f \cup g)^n$. Noting $(f \cup g)^n = (f \cup g)^{n+1}$, the result follows. □

Lemma 7. *In each DSM there is a unique maximal reflexive and symmetric multipermutation g. Furthermore g is a blurred permutation.*

Proof. Since each DSM contains the id_n we know that all DSMs contain at least one reflexive and symmetric multipermutation. Suppose, for a contradiction that there exist two maximal reflexive and symmetric multipermutations, f, g, on a DSM M. Then, by Lemma 6 the join of f, g also belongs to M, which contradicts the maximality of f and g. Thus in each DSM there exists a unique maximal reflexive and symmetric multipermutation. We now need to show that it is a blurred permutation. Since for any multipermutation f we have $f \subseteq f^2$, given g the maximal reflexive and symmetric multipermutation on a DSM M with domain $[n]$, we have $g^n = g$ (since g is maximal). To then see that g is a blurred permutation we can think of the graph $\mathcal{G}_g$ that is the union of disjoint reflexive cliques. □

Let g be a blurred permutation on the domain $[n]$ with associated partition $P_1, \ldots, P_m$. We say that a multipermutation f *respects* g if **neither**

- (i) exist a, b and c, d such that a, b are in the same set P_i and c, d are in distinct sets P_j, P_k, respectively, and $c \in f(a)$ and $d \in f(b)$, **nor**
- (ii) exist a, b and c, d such that a, b are in distinct sets P_j, P_k, respectively, and c, d are in the same set P_i and $c \in f(a)$ and $d \in f(b)$.

Lemma 8. *If the multipermutation f does not respect the blurred permutation g, then either $(f \circ g) \circ (g^{-1} \circ f^{-1})$ or $(f^{-1} \circ g^{-1}) \circ (g \circ f)$ is a reflexive and symmetric multipermutation that is not a sub-multipermutation of g.*

Proof. If f does not respect g because of Item (i) above, noting that $g(a) = g(b)$, then $h := (f \circ g) \circ (f \circ g)^{-1}$ satisfies $h(c) \supseteq \{c, d\}$. So $h \not\subseteq g$, and the result follows from Lemma 5 as $(f \circ g) \circ (f \circ g)^{-1} = (f \circ g) \circ (g^{-1} \circ f^{-1})$.

If f does not respect g because of Item (ii) above, then f^{-1} does not respect g because of Item (i) above. The result follows. □

Lemma 9. *If g is the maximal reflexive and symmetric multipermutation in a DSM M and f is a blurred permutation that respects g, then $f \in M$ iff there exists $f' \subseteq f$ s.t. $f' \in M$.*

Proof. The forward direction is trivial since M is closed under sub-multipermutations. Assume now that there exists $f' \subseteq f$ s.t. $f' \in M$. Since f is a blurred permutation that respects g we can see that the partition of f must be a refinement of the partition of g, i.e. if $P_1, \ldots, P_m$ is the partition of f and $Q_1, \ldots, Q_l$ is the partition of g we have for each $i \in [m]$, $P_i \subseteq Q_j$ for some $j \in [l]$. Now, applying the multipermutations right to left, we have for any $a \in [n]$ $g \circ f'(a) = g(T)$ with $f'(a) = T \subseteq f(a) = P_i \subseteq Q_j$ for some $i \in [m]$ and $j \in [l]$, with $g(a) = g(Q_j)$. By Lemmas 3 and 7 it follows that g is a blurred permutation obtained from the identity permutation, so $g(Q_j) = Q_j$. Then $f(a) = P_i \subseteq Q_j = g(f'(a)) = g(T) = g(Q_j)$. Hence $f \subseteq g \circ f'$, so $f \in M$. □

3.2. **Automorphisms of $\mathscr{F}_n$.** The lattice $\mathscr{F}_n$ has a collection of very obvious automorphisms corresponding to the permutations of S_n, in which one transforms a DSM M to M' by the uniform relabelling of the elements of the domain according to some permutation. For example, $M := \langle \begin{smallmatrix} 1 & 1,2 \\ 2 & 2 \\ 3 & 3 \end{smallmatrix} \rangle$ maps to $M' := \langle \begin{smallmatrix} 1 & 1 \\ 2 & 2 \\ 3 & 2,3 \end{smallmatrix} \rangle$ under the permutation $\{1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1\}$.

There is another, more interesting, automorphism of $\mathscr{F}_n$, which we will call the *inverse* automorphism. We do not close our DSMs under inverse because they were defined in order that the given Galois connections held. It is not hard to verify that if M is a DSM, then $\{f^{-1} : f \in M\}$ is also a DSM, which we call the *inverse* and denote M^{-1}. It is also easy to see that $f = (f^{-1})^{-1}$ and $M = (M^{-1})^{-1}$, from where it follows that inverse is an automorphism of $\mathscr{F}_n$.

3.3. **Properties of inverse.** Call a structure $\mathcal{B}$ *she-complementative* if $\mathsf{shE}(\mathcal{B}) = \mathsf{shE}(\mathcal{B})^{-1}$. Note that, if F is a DSM, then so is F^{-1}. In fact, this algebraic duality resonates with the de Morgan duality of $\exists$ and $\forall$, and the complexity-theoretic duality of NP and $\mathsf{co\text{-}NP}$ [25].

Lemma 10. *For all $\mathcal{B}$, $\mathsf{shE}(\mathcal{B}) = \mathsf{shE}(\overline{\mathcal{B}})^{-1}$.*

Proof. It follows from the definition of she that f is a she of $\mathcal{B}$ iff f^{-1} is a she of $\overline{\mathcal{B}}$. □

We are now in a position to derive the following classification theorem.

Theorem 5. *A DSM N is a BPS iff $N = N^{-1}$.*

Proof. It is straightforward to see that a BPS N is such that $N = N^{-1}$. Specifically, if $f \in N$ then f is derived from a multipermutation g of a permutation in a group M. The inverse f^{-1} may be derived in the same manner from the inverse g^{-1} of g.

Now suppose N is such that $N = N^{-1}$. Let g be the maximal reflexive and symmetric multipermutation in N. Let $P_1, \ldots, P_m$ be the associated partition of g in the manner previously discussed. Let M be the blurred symmetric group formed from S_m by the sets $P_1, \ldots, P_m$. We claim $N \subseteq M$. This follows from Lemmas 6 and 8, since, if $N \not\subseteq M$, then some multipermutation $f \in N$ fails to respect g, contradicting the maximality of g. This shows that all multipermutations $f \in N$ can be extended to a blurred permutation with partition $P_1, \ldots, P_m$.

Let f be a multipermutation in N and f' be a blurred permutation with partition $P_i, \ldots, P_m$ such that $f \subseteq f'$. By Lemma 9 $f' \in N$. Thus N is generated by precisely the blurred permutations f', with partition $P_1, \ldots, P_m$, that contain the multipermutations $f \in N$. Thus we see that N is a BPS. □

Corollary 11. *A DSM N is a BPS iff the maximal elements in N are blurred permutations.*

Proof. Forward is trivial. Assume now that all maximal elements of N are blurred permutations. By Theorem 5, it is enough to show that $N^{-1} = N$. Let $f \in N$ be arbitrary, $f \subseteq g$, with g a maximal blurred permutation of N with partition $P_1, \ldots, P_m$. Then there exists $k \in \mathbb{N}$ such that g^k acts as the identity on the sets of the partition, i.e. $g^k(P_i) = P_i$ for all $i = 1, \ldots, m$. Hence g generates its inverse, i.e $g^{-1} = g^l$ for some $l < k$. We can then obtain f^{-1} as a submultipermutation of g^l. Thus $f^{-1} \in N$, and we can conclude that $N = N^{-1}$. □

We may now give a complexity classification for she-complementative structures based on the following result of [25].

Lemma 12 ([25])**.** *If* $\mathsf{shE}(\mathcal{B})$ *is a BPS derived from* S_m*, for* $m \geq 2$*, then* $\{\exists, \forall, \wedge, \vee\}$ -$\mathsf{FO}(\mathcal{B})$ *is* Pspace*-complete.*

Corollary 13. *If* $\mathcal{B}$ *is she-complementative then* $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ *is either in* Logspace *or is* Pspace*-complete.*

Proof. We know from Theorem 5 that $\mathsf{shE}(\mathcal{B})$ is a BPS. If it is a BPS formed from the trivial group S_1, then $\mathsf{shE}(\mathcal{B})$ contains all multipermutations. It follows that $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ is in Logspace (indeed one may evaluate the quantified variables in an instance arbitrarily - for more details see [25]). If $\mathsf{shE}(\mathcal{B})$ is a BPS formed from S_m, with $m \geq 2$, then $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ is Pspace-complete by Lemma 12. □

4. The structure of $\mathscr{M}_n$

Let $\mathscr{M}_n$ denote the monoid of all multipermutations on $[n]$ with the binary operation of composition of relations. In this section we study the structure of $(\mathscr{M}_n, \circ)$ from a semigroup point of view.

Several well studied monoids are associated with $\mathscr{M}_n$: the symmetric group S_n is a submonoid of $\mathscr{M}_n$; the Hall monoid H_n (where every relation contains a permutation, see for example [12]) is also a submonoid of $\mathscr{M}_n$; while the transformation semigroup T_n (all maps from $[n]$ to $[n]$) is not contained in $\mathscr{M}_n$ since not all transformations are surjective. Let $\mathcal{B}_n$ be the semigroup of all $n \times n$ matrices over the boolean semiring $\{0, 1\}$. This semigroup is isomorphic, in a natural way, to the semigroup of all binary relations on $[n]$, where the operation is the usual composition of relations, and $\mathscr{M}_n$ is (isomorphic to) a submonoid of $\mathcal{B}_n$. We can then think of $\mathscr{M}_n$ as the submonoid of $\mathcal{B}_n$ composed of all boolean matrices with at least one 1 in every row and every column. We will slightly abuse notation and use $\mathcal{B}_n$ to denote both this monoid and the monoid of all binary relations on $[n]$.

4.1. **Green's relations.** Green's relations for T_n and S_n are trivial and can be found in any book on Semigroup Theory. In contrast, for the semigroup of all binary relations $\mathcal{B}_n$ no simple, direct, charaterization is known. They were characterized, possibly among others, by Zaretskii [38, 39] in terms of lattices; Plemmons and West [32] in terms of boolean matrices, and by Adu [1] using direct composition (and skeletons of the relations). Similarly, for $\mathscr{M}_n$ a simple characterization has so far eluded us. In this section, to keep our results matching the current literature, we will multiply matrices left to right (i.e. compose multipermutations left to right).

We can think of the rows and columns of an $n \times n$ boolean matrix from $\mathcal{B}_n$ as vectors on $\{0, 1\}^n$, so these can be, naturally, added and compared coordinate-wise using boolean operations.

Let $\alpha \in \mathcal{B}_n$. The *row space* of α, $V(\alpha)$, is the set of all possible sums of rows of α, including the zero vector. Analogously, the *column space* of α, $W(\alpha)$, is the set of all possible sums of columns of α, including the zero vector.

Lemma 14 (Zaretskii)**.** *For any $\alpha, \beta \in \mathcal{B}_n$:*

(1) $\alpha \mathcal{L} \beta \;\Leftrightarrow\; V(\alpha) = V(\beta)$;
(2) $\alpha \mathcal{R} \beta \;\Leftrightarrow\; W(\alpha) = W(\beta)$.

Following this characterization given by Zarestkii [39] for Green's relations in $\mathcal{B}_n$, which can also be found in [32, Lemma 1.2], we obtained the following characterization for $\mathscr{M}_n$:

Theorem 6. *Given $\alpha \in \mathscr{M}_n$ let $R(\alpha)$ be the set of rows and $C(\alpha)$ the set of columns, respectively, of α. Define $\langle R(\alpha)\rangle = \{\rho \in V(\alpha)\backslash\{0\} : \exists \alpha_j \in R(\alpha) : \rho \leq \alpha_j\}$ and $\langle C(\alpha)\rangle$ analogously. For any $\alpha, \beta \in M_n$, we have*

(1) $\alpha \mathcal{L} \beta \;\Leftrightarrow\; \langle R(\alpha)\rangle = \langle R(\beta)\rangle$,

(2) $\alpha\mathcal{R}\beta \Leftrightarrow \langle C(\alpha)\rangle = \langle C(\beta)\rangle$,
(3) $\alpha\mathcal{H}\beta \Leftrightarrow \langle R(\alpha)\rangle = \langle R(\beta)\rangle$ *and* $\langle C(\alpha)\rangle = \langle C(\beta)\rangle$.

Proof. For each $\gamma \in \mathscr{M}_n$ denote by γ_i the i^{th} row of γ (when γ is in matrix form).

Let $\alpha, \beta \in \mathscr{M}_n$ be such that $\langle R(\alpha)\rangle = \langle R(\beta)\rangle$. Since $R(\alpha) \subseteq \langle R(\alpha)\rangle$, for all $i \in [n]$ there exist $j_1, \ldots, j_l \in [n]$ such that $\alpha_i = \beta_{j_1} + \cdots + \beta_{j_l}$, we can then define $\rho \in \mathscr{M}_n$ by the rule ρ_i has a 1 in exactly all places $j_1, \ldots, j_l$ (and zeros everywhere else). It is then easy to see that $\rho \circ \beta = \alpha$. In a similar way we can define $\delta \in \mathscr{M}_n$ such that $\delta \circ \alpha = \beta$. It follows that $\alpha\mathcal{L}\beta$.

Let us assume now that $\alpha, \beta \in \mathscr{M}_n$ are such that $\alpha\mathcal{L}\beta$. By Lemma 14 we know that $V(\alpha) = V(\beta)$, so, for all $i \in [n]$, $\alpha_i \in V(\beta)$ which implies that $\alpha_i = \beta_{j_1} + \cdots + \beta_{j_l}$ for some $\beta_{j_1}, \ldots, \beta_{j_l} \in R(\beta)$, since $\alpha_i \neq 0$. Since there exists $\rho \in \mathscr{M}_n$, so that i appears in the image of ρ (i.e. ρ has at least one 1 in column i), such that $\rho\alpha = \beta$, we have that $\alpha_i \leq \beta_j$ for some $j = 1, \ldots, n$. Hence $\alpha_i \in \langle R(\beta)\rangle$, and so $R(\alpha) \subseteq \langle R(\beta)\rangle$. It the follows, by definition of $\langle R(\alpha)\rangle$, that $\langle R(\alpha)\rangle \subseteq \langle R(\beta)\rangle$. Analogously, we can show that $\langle R(\beta)\rangle \subseteq \langle R(\alpha)\rangle$. Thus $\langle R(\alpha)\rangle = \langle R(\beta)\rangle$.

In a similar way, reversing rows and columns, we can show that $\alpha\mathcal{R}\beta$ if and only if $\langle C(\alpha)\rangle = \langle C(\beta)\rangle$. And, as a consequence of both these facts we have that $\alpha\mathcal{H}\beta$ if and only if $\langle R(\alpha)\rangle = \langle R(\beta)\rangle$ and $\langle C(\alpha)\rangle = \langle C(\beta)\rangle$. □

Example 15. *We have* $\begin{array}{c|c} 1 & 1 \\ \hline 2 & 1 \\ \hline 3 & 1,2,3 \end{array}$ $\mathcal{L}$ $\begin{array}{c|c} 1 & 1 \\ \hline 2 & 1,2,3 \\ \hline 3 & 1,2,3 \end{array}$ $\mathcal{R}$ $\begin{array}{c|c} 1 & 1,2 \\ \hline 2 & 1,2,3 \\ \hline 3 & 1,2,3 \end{array}$.

Example 16. *The following multipermutations are* $\mathcal{L}$ *related in* $\mathcal{B}_n$ *but not in* $\mathscr{M}_n$

$$\begin{array}{c|c} 1 & 1 \\ \hline 2 & 2,3 \\ \hline 3 & 1,2,3 \end{array} \quad \textit{and} \quad \begin{array}{c|c} 1 & 1 \\ \hline 2 & 2,3 \\ \hline 3 & 2,3 \end{array}$$

.

Example 17. *The following multipermutations are* $\mathcal{L}$ *related in* $\mathscr{M}_n$ *but do not have the same set of rows*

$$\begin{array}{c|c} 1 & 1,3 \\ \hline 2 & 1 \\ \hline 3 & 3 \\ \hline 4 & 2,4 \\ \hline 5 & 1,3,5 \end{array} \quad \text{and} \quad \begin{array}{c|c} 1 & 1 \\ \hline 2 & 3 \\ \hline 3 & 2,4 \\ \hline 4 & 2,4 \\ \hline 5 & 1,3,5 \end{array}.$$

4.2. **Regular elements.** An element a of a semigroup S is called *regular* if there exists $x \in S$ s.t. $a = axa$, x is called an inverse of a. Schein [34] gave us a way of checking if a binary relation is regular in the semigroup of all binary relations.

Lemma 18 ([34])**.** *Let* $\rho \in \mathcal{B}_n$ *be a binary relation. Then* ρ *is regular (in* $\mathcal{B}_n$*) iff* $\rho \subseteq \rho \circ (\rho^{-1} \circ \rho^c \circ \rho^{-1})^c \circ \rho$.

Here ρ^{-1} is the inverse relation, as defined earlier on for multipermutations $\rho^{-1} = \{(y, x) : (x, y) \in \rho\}$, and ρ^c is the complement relation $\rho^c = \{(x, y) \in X \times X : (x, y) \notin \rho\}$. Since we are here using the word inverse for distinct things we will use just inverse for semigroup inverse and

will call inverse relation as ρ^{-1} to avoid confusion. In the same paper he showed that the relation

$$(\rho^{-1} \circ \rho^c \circ \rho^{-1})^c \circ \rho \circ (\rho^{-1} \circ \rho^c \circ \rho^{-1})^c$$

is the greatest (relatively to containment of relations) inverse of ρ.

Using Schein's condition we can check if a multipermutation ρ has an inverse, by checking if this greatest inverse is also a multipermutation, but it is not enough to check the regularity condition presented in the lemma above.

Example 19. *The multipermutation* $\begin{array}{c|c} 1 & 1,2 \\ \hline 2 & 3 \\ \hline 3 & 1,2,3 \end{array}$ *is regular as a binary relation, but not as a multipermutation, since all inverses of it are binary relations that are not multipermutations.*

Even though this greatest inverse is computable in polynomial time it is not always simple to check. We adapted an algorithm by Kim & Roush [21] to compute inverses for multipermutations, in particular we keep the notation used in that article for easier comparison.

Let V_n be the set of all n-tuples of elements of $\{0,1\}$. A subset W of V_n is called a *subspace* of V_n if it contains the zero vector and $u+v \in W$ for all $u, v \in W$. The *subspace spanned* by W is the smallest subspace that contains W, we denote it by $\langle W \rangle$. A vector v is said to be *dependent* on W if $v \in \langle W \rangle$. A set W is said to be *independent* if for all $v \in W$, v is not dependent on $W \backslash \{v\}$. A subset S is said to be a *basis* for a subspace W if $W = \langle S \rangle$ and S is an independent set.

If $v \in V_n$ we denote by v_i the element of $\{0,1\}$ occurring in position i of v. For $u, v \in V_n$ we say that $u \leqslant v$ if $u_i = 1$ only if $v_i = 1$ for all $i = 1, \ldots, n$. Given α, a boolean square matrix, let α_{i^*} denote the i^{th} row of α.

By the row space of α we mean the subspace spanned by the set of rows of α, and denote it by $R(\alpha)$. We denote by $b(\alpha)$ the basis for $R(\alpha)$ and call it the *row basis* of α.

For each $v \in b(\alpha)$ a vector u with one 1 is called an *identification vector* of v if and only if: $u \leqslant w$ holds if and only if $v \leqslant w$ for $w \in b(\alpha)$.

Let $I(v)$ denote the set of identification vectors of a basis vector v of α. Finally, set $p(t) = \inf\{w \in R(\alpha) : t \leq w\}$, where the infimum is taken in the lattice $V(\alpha)$.

Algorithm for binary relations: Kim & Roush [21]
Input $\alpha \in \mathcal{B}_n$,

(1) find $b(\alpha)$;
(2) find $I(v)$ for each $v \in b(\alpha)$;
(3) for each $v \in b(\alpha)$, choose a specific identification vector $u \in I(v)$;
(4) for each such chosen u, choose a vector s such that $s_i = 1$ if $\alpha_{i^*} \leqslant v$ and such that $s_i = 1$ for at least one i such that $\alpha_{i^*} = v$;
(5) choose any vector t with exactly one 1 entry other than the u's chosen in Step (3), if t is not less than any row vector, send t to an

arbitrary vector. Otherwise send t to a vector b such that $b_i = 1$ only if $\alpha_{i^*} \leqslant p(t)$;

(6) linearly order the set of vectors with only one 1 in such a way that the mapping $i \mapsto (\delta_{i1}, \delta_{i2}, \ldots, \delta_{in})$ is an order isomorphism. Write the vectors s and b in the order of the u's and t.

Algorithm for multipermutations:
Input $\alpha \in \mathscr{M}_n$,

(1) find $b(\alpha)$;
(2) find $I(v)$ for each $v \in b(\alpha)$;
(3) for each $v \in b(\alpha)$, choose a specific identification vector $u \in I(v)$;
(4) for each such chosen u, choose a vector s such that $s_i = 1$ if $\alpha_{i^*} \leqslant v$;
(5) choose any vector t with exactly one 1 entry other than the u's chosen in Step (3), and send t to a vector b such that $b_i = 1$ only if $\alpha_{i^*} \leqslant p(t)$;
(6) linearly order the set of vectors with only one 1 in such a way that the mapping $i \mapsto (\delta_{i1}, \delta_{i2}, \ldots, \delta_{in})$ is an order isomorphism. Write the vectors s and b in the order of the u's and t.

The resulting matrix will be an inverse of α, that will also be a multipermutation when the conditions presented in Theorem 7 are satisfied. We note that this algorithm differs from the one above in Step (5) since for the case of multipermutations all columns of the matrix have a 1.

Example 20. *Let* $\alpha = \begin{array}{c|c} 1 & 2 \\ \hline 2 & 2,3 \\ \hline 3 & 1 \end{array} \in \mathscr{M}_n$, *in matrix form we have* $\alpha = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$

Following the steps above we get:

(1) $b(\alpha) = \{(0\ 1\ 0), (0\ 1\ 1), (1\ 0\ 0)\}$ *which we note is equal to* $R(\alpha)$*;*
(2) $I((0\ 1\ 0)) = \{(0\ 1\ 0)\}; I((0\ 1\ 1)) = \{(0\ 0\ 1)\}; I((1\ 0\ 0)) = \{(1\ 0\ 0)\}$*;*
(3) the u's are clearly defined, no choice needs to be made;
(4) For $u = (0\ 1\ 0)$*,* s *must be* $(1\ 0\ 0)$*; for* $u = (0\ 0\ 1)$ *the vector* s *can be* $(1\ 1\ 0)$ *or* $(0\ 1\ 0)$*; for* $u = (1\ 0\ 0)$*,* s *must be* $(0\ 0\ 1)$*;*
(5) no choice for t;
(6) there are two inverses of α *in* $\mathscr{M}_n$*, they are*

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Lemma 21. *Let* $\alpha \in \mathscr{M}_n$ *be arbitrary. If* $b(\alpha) \neq R(\alpha)$ *then* α *has no inverse in* $\mathscr{M}_n$*.*

Proof. Suppose that $\alpha_1 \neq b(\alpha)$, so that α_1 can be written as the sum of other rows of α. We show that all inverses of α in $\mathcal{B}_n$ will have only zeros in the first column. Following the algorithm above, we know that $\alpha_1 \neq v$ for all $v \in b(\alpha)$, so no vector s, produced by the algorithm, will have a 1 in

the first component. Since t contains a unique 1 we know that $p(t) \neq \alpha_1$, it follows that b will not contain 1 in its first component. □

Lemma 22. *Let $\alpha \in \mathscr{M}_n$ be arbitrary. If $p(t) = 0$, for any possible t, then α has no inverse in $\mathscr{M}_n$.*

Proof. If $p(t) = 0$ then, from the above algorithm we get $b = 0$, since no row of α is the zero row, so all inverses of α will have a zero row, thus they will not be multipermutations. □

Theorem 7. *A multipermutation α has an inverse, in $\mathscr{M}_n$, iff $b(\alpha) = R(\alpha)$, $I(v) \neq \emptyset$ for each $v \in b(\alpha)$, and $p(t) \neq 0$ (for some t).*

Proof. ($\Rightarrow$.) Follows from [21, Lemma 1] and Lemmas 21 and 22.

($\Leftarrow$.) Assume that $b(\alpha) = R(\alpha)$, $I(v) \neq \emptyset$ for each $v \in r(\alpha)$, and $p(t) \neq 0$ (for some t). By [21, Lemma 1] we know that α has an inverse in $\mathcal{B}_n$. Since $p(t) \neq 0$ for some t we know that α will have an inverse with no zero row. We now just need to show that one of the inverses with no zero row also has no zero column.

We know, by assumption, that α_1^* (the first row of α) belongs to $b(\alpha)$, hence, when we are at Step (3) of the algorithm and $v = \alpha_1^*$ we will choose s such that $s_1 = 1$. Thus the first column of the inverse of α will be non zero. Since all rows of α belong to $b(\alpha)$ it follows that we can choose an inverse with non zero columns. Thus α has an inverse in $\mathscr{M}_n$. □

Example 23. $\begin{array}{c|c} 1 & 1,2,3 \\ \hline 2 & 2,3 \\ \hline 3 & 1 \end{array}$ *has inverses in $\mathcal{B}_n$ but not in $\mathscr{M}_n$. Using the algorithm above for binary relations, we can check that all its inverses are*

$$\begin{array}{c|c} 1 & 3 \\ \hline 2 & 2 \\ \hline 3 & \end{array}, \quad \begin{array}{c|c} 1 & 3 \\ \hline 2 & 2 \\ \hline 3 & 2 \end{array}, \quad \text{and} \quad \begin{array}{c|c} 1 & 3 \\ \hline 2 & \\ \hline 3 & 2 \end{array},$$

none being a multipermutation. This follows from the fact that its row basis does not include all its rows.

4.3. **Generators.** It is known that, unlike S_n that is generated by two elements, $\mathcal{B}_n$ does not admit a polynomial (on n) generating set. This was mentioned by Devadze [16] and more recently proved by Konieczny [23].

In this section we show that $\mathscr{M}_n$ also does not admit a polynomial generating set, and does indeed need more elements to be generated than $\mathcal{B}_n$.

Using Devadze's set of generators, and the proof provided by Konieczny, we show that any set of generators of $\mathscr{M}_n$ must include the two permutations that generate S_n and a set of representatives of the prime $\mathcal{D}$-classes of $\mathscr{M}_n$. To obtain a generating set we add a few more multipermutations to the set mentioned above.

Let $\alpha, \beta, \gamma \in \mathcal{B}_n$, the monoid of binary relations. We say that α is *prime* if it is not a permutation and if $\alpha = \beta \circ \gamma$ implies that either β or γ are a permutation.

De Caen and Gregory [15] showed that if $\alpha \in \mathcal{B}_n$ is prime then no column of α can contain another column, and no row of α can contain another row. In particular if $\alpha \in \mathcal{B}_n$ is prime then α has no zero row or column and no row

or column with all entries equal to 1. This means that all prime elements of $\mathcal{B}_n$ are multipermutations. In the same paper they also show that prime multipermutations are not regular, and if a $\mathcal{D}$-class of $\mathcal{B}_n$ contains a prime relation then all relations in that class are prime. We will call these classes *prime $\mathcal{D}$-classes*, and they are $\mathcal{D}$-classes of $\mathscr{M}_n$ that are located just below the group of units S_n in the partial order of $\mathcal{D}$-classes of $\mathscr{M}_n$. This can also be found in [23] without mentioning multipermutations.

We are now trying to build a generating set for $\mathscr{M}_n$, and it follows from Konieczny's result, adapted to multipermutations, that any set of generators must contain a set of generators of S_n and a set of representatives of the prime $\mathcal{D}$-classes of $\mathscr{M}_n$. The following is the equivalent of [23, Lemma 4.2].

Lemma 24. *Let D be a prime $\mathcal{D}$-class of $\mathscr{M}_n$ and let T be a set of generators of $\mathscr{M}_n$. Then $D \cap T \neq \emptyset$.*

Proof. Assume, for a contradiction, that $D \cap T = \emptyset$. Let

$$m = \min\{k : \alpha = t_1 \circ \cdots \circ t_k \text{ for some } \alpha \in D \text{ and } t_1, \ldots, t_k \in T\}.$$

Choose some $\alpha \in D$ such that $\alpha = t_1 \circ \cdots \circ t_k$ for some $t_1, \ldots, t_m \in T$. Since $\alpha \notin T$ we have $m \geq 2$. Note that $t_1 \notin S_n$ since otherwise $t_1^{-1}\alpha = t_2 \circ \cdots \circ t_m \in D$, which would contradict the minimality of m. Similarly, $t_m \notin S_n$. Since t_m is a multipermutation we must have that $|t_m(i)| \geq 2$ (or when in matrix form, there is a row of t_m with at least two 1s) for some $i = 1, \ldots, n$, it follows that $|t_2 \circ \cdots \circ t_m(j)| \geq 2$ for some $j = 1, \ldots, m$ (note that we apply the relations left to right). Hence $t_2 \circ \cdots \circ t_m \notin S_n$, and since $t_1 \notin S_n$, and $\alpha = t_1 \circ (t_2 \circ \cdots \circ t_m)$, which is a contradiction since α is prime. Thus $D \cap T \neq \emptyset$.

□

The number of prime $\mathcal{D}$-classes grows faster than a polynomial on n, so we won't be able to find a minimal generating for $\mathscr{M}_n$ that is polynomial. A minimal generating set for it will contain a set of representatives of the prime $\mathcal{D}$-classes, the two permutations that generate S_n, the multipermutation (in matrix form)

$$\pi = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

and a few more multipermutations. This will be the subject of future work, and we leave here a few examples that were tested using GAP [19, 30]:

Example 25. *The only prime element in $\mathscr{M}_3$ (up to equivalence) is* $\begin{array}{c|c}1&1,2\\\hline 2&2,3\\\hline 3&1,3\end{array}$ [15, Example 2.3]. *A generating set for $\mathscr{M}_3$ is the given by the permutations* $(1\ 2), (1\ 2\ 3)$*, the prime multipermutation, the multipermutation* $\begin{array}{c|c}1&1\\\hline 2&1,2\\\hline 3&3\end{array}$ *(called π above) and* $\begin{array}{c|c}1&1\\\hline 2&1\\\hline 3&2,3\end{array}$.

Example 26. *The prime elements in $\mathscr{M}_4$ (up to equivalence) are* [15, Example 2.5]

$$\begin{bmatrix}0&1&1&1\\1&1&0&0\\1&0&1&0\\1&0&0&1\end{bmatrix} \quad \textit{and} \quad \begin{bmatrix}1&0&0&1\\1&1&0&0\\0&1&1&0\\0&0&1&1\end{bmatrix}$$

and they belong to different $\mathcal{D}$-classes. A generating set for $\mathscr{M}_4$ is given by the $(1\ 2), (1\ 2\ 3\ 4)$*, the prime multipermutations above, the multipermutation* $\begin{array}{c|c}1&1\\\hline 2&1,2\\\hline 3&3\\\hline 4&4\end{array}$ *(called π above), together with the multipermutations* $\begin{array}{c|c}1&1\\\hline 2&2\\\hline 3&2\\\hline 4&3,4\end{array}$, $\begin{array}{c|c}1&1,2\\\hline 2&1,3\\\hline 3&2,3\\\hline 4&4\end{array}$.

4.4. **Blurred permutations.** A multipermutation, or more generally binary relation, f, is called *difunctional* if it satisfies $f \circ f^{-1} \circ f \subseteq f$. Schein [36] showed that every inverse semigroup is isomorphic to an appropriate inverse semigroup of full difunctional binary relations (here the operation is not usual composition since the composition of two difunctional binary relations is not necessarily difunctional). In this subsection we relate blurred permutations with difunctional relations. It is worth noting that in some articles these are named bifunctional, e.g. [17][2], and that in that article difunctional multipermutations are called biequivalences or block bijections.

Lemma 27. *Every blurred permutation is difunctional.*

Proof. Let f be a blurred permutation obtained from the permutation σ with partition $P_1, \ldots, P_m$, then f^{-1} is obtained from σ^{-1} with partition $P_{\sigma(1)}, \ldots P_{\sigma(m)}$. For any $i = 1, \ldots, m$ and any $k \in P_i$ we have $f(k) = f(P_i) = P_{\sigma(i)}$, and $f \circ f^{-1} \circ f(k) = f \circ f^{-1}(P_{\sigma(i)}) = f(P_i) = P_{\sigma(i)}$. Thus $f \circ f^{-1} \circ f = f$, and it follows that f is difunctional. □

It is also clear from this proof that blurred permutations are all regular and the inverse multipermutation is also an inverse (in the sense of regular element). We note that the reverse of this lemma is not true.

Example 28. *The multipermutation* $\begin{array}{c|c}1&1,3\\\hline 2&1,3\\\hline 3&2,4\\\hline 4&2,4\end{array}$ *is difunctional but not a blurred permutation.*

Theorem 8. *Blurred permutations are the difunctional multipermutations f that satisfy $f \circ f^{-1} = f^{-1} \circ f$. Hence they can be defined exactly by*

[2]The dual terminology of difunctional and bifunctional may have arisen from translation of the French *difonctionelle* from [33].

the rules $f \circ f^{-1} \circ f = f$ *and* $f \circ f^{-1} = f^{-1} \circ f$*, or equivalently are full total binary relations on* X *of the form* $(A_1 \times B_1) \cup \cdots \cup (A_k \times B_k)$*, with* $\{A_1, \ldots A_k\} = \{B_1, \ldots, B_k\}$ *partitions of* X*.*

Proof. We can see in [36] a result attributed to J. Riguet that says that a binary relation is difunctional if and only if it is of the form $(A_1 \times B_1) \cup \cdots \cup (A_k \times B_k)$, with $A_1, \ldots, A_k$ all distinct and $B_1, \ldots, B_k$ all distinct. So we can say that a multipermutation on $[n]$ is difunctional if and only if it is of the form $(A_1 \times B_1) \cup \cdots \cup (A_k \times B_k)$, with $\{A_1, \ldots A_k\}, \{B_1, \ldots, B_k\}$ partitions of $[n]$. We now need to show that $\{A_1, \ldots A_k\} = \{B_1, \ldots, B_k\}$.

Let f be a blurred permutation. Since it is difunctional it satisfies $f \circ f^{-1} \circ f = f$, so we just need to show it satisfies $f \circ f^{-1} = f^{-1} \circ f$. Suppose that f is obtained from permutation σ and partition $A_1, \ldots, A_m$, then $f^{-1} \circ f(A_i) = f^{-1}(A_{\sigma(i)}) = A_{\sigma^{-1}\sigma(i)} = A_i$ and $f \circ f^{-1}(A_i) = f(A_{\sigma^{-1}(i)}) = A_{\sigma\sigma^{-1}(i)} = A_i$. Thus $f \circ f^{-1} = f^{-1} \circ f$.

From this we can also see that the $(A_1 \times B_1) \cup \cdots \cup (A_k \times B_k)$ can be rewritten as $(A_1 \times A_{\sigma(1)}) \cup \cdots \cup (A_k \times A_{\sigma(k)})$, so it follows that $\{A_1, \ldots A_k\} = \{B_1, \ldots, B_k\}$.

We now show the reverse implication. If $f = (A_1 \times B_1) \cup \cdots \cup (A_k \times B_k)$ with $\{A_1, \ldots A_k\} = \{B_1, \ldots, B_k\}$ we can see that it is a blurred permutation obtained from the permutation that sends A_i to B_i.

If we assume that f is a multipermutation that satisfies $f = f \circ f^{-1} \circ f$ and $f \circ f^{-1} = f^{-1} \circ f$, we know it is difunctional, so $f = A_1 \times B_1 \cup \cdots \cup A_k \times B_k$, then $f^{-1} \circ f = (B_1 \times B_1) \cup \cdots \cup (B_k \times B_k)$ and $f \circ f^{-1} = (A_1 \times A_1) \cup \cdots \cup (A_k \times A_k)$. It then follows that we must have $\{A_1, \ldots, A_k\} = \{B_1, \ldots, B_k\}$, so f is a blurred permutation.

□

In other words, blurred permutations are the completely regular difunctional multipermutations. For the definition of completely regular see for example [13].

Corollary 29. *For any difunctional multipermutation* f*, the multipermutations* $f \circ f^{-1}$ *and* $f^{-1} \circ f$ *are blurred permutations.*

Proof. Let f be an arbitrary difunctional multipermutation. Since $(f \circ f^{-1})^{-1} = f \circ f^{-1}$, we have

$$(f \circ f^{-1}) \circ (f \circ f^{-1})^{-1} = f \circ f^{-1} \circ f \circ f^{-1} = (f \circ f^{-1})^{-1} \circ (f \circ f^{-1}),$$

and

$$(f \circ f^{-1}) \circ (f \circ f^{-1})^{-1} \circ (f \circ f^{-1}) = f \circ f^{-1} \circ f \circ f^{-1} \circ f \circ f^{-1} = f \circ f^{-1}$$

due to the fact that $f \circ f^{-1}$ is idempotent, for f is difunctional. It follows from Theorem 8 that $f \circ f^{-1}$ is a blurred permutation. Similarly, we can show that $f^{-1} \circ f$ is a blurred permutation. □

In light of Corollary 13, and the connection between BPSs and blurred permutations given in Corollary 11, one might ask whether the more general

class of difunctional multipermutations are naturally associated with DSMs $M = \mathsf{shE}(\mathcal{B})$, where the complexity of $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ is only in Logspace or Pspace-complete (and cannot attain the complexities NP-complete and co-NP-complete). We do not know whether the set of DSMs whose maximal elements are difunctional is different from the set of DSMs whose maximal elements are blurred permutations. Indeed, we leave this as an interesting open question. However, it follows from the results in [27], that the multipermutations f associated with NP-completeness and co-NP-completeness are as far from difunctionality as possible since $f \circ f^{-1}$, and consequently $f \circ f^{-1} \circ f$, will always be the full multipermutation, i.e. the multipermutation that sends every element to the full domain. This would only satisfy difunctionality if f were itself the full multipermutation, in which case any corresponding $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$ would be in Logspace. It follows that the complexity of $\{\exists, \forall, \wedge, \vee\}$-$\mathsf{FO}(\mathcal{B})$, where $\mathsf{shE}(\mathcal{B}) = M$, all of whose maximal elements are difunctional, is either in Logspace or is Pspace-complete.

Another interesting class of multipermutations worth looking at in this context, is the factor power of the symmetric group, whose study was initiated in [18].

Acknowledgements

We are grateful for corrections and advice from several referees throughout the lifetime of this draft.

References

[1] Adu, D. I. Green's relations on the semigroup of binary relations. *Demonstratio Mathematica 19*, 4 (1986), 895–914.

[2] Bodnarčuk, V. G., Kalužnin, L. A., Kotov, V. N., and Romov, B. A. Galois theory for post algebras, part I and II. *Cybernetics 5* (1969), 243–539.

[3] Börner, F. Total multifunctions and relations. In *Contributions to general algebra, 13 (Velké Karlovice, 1999/Dresden, 2000)*. Heyn, Klagenfurt, 2001, pp. 23–35.

[4] Börner, F. Basics of Galois connections. In *Complexity of Constraints - An Overview of Current Research Themes [Result of a Dagstuhl Seminar]* (2008), pp. 38–67.

[5] Börner, F., Bulatov, A. A., Chen, H., Jeavons, P., and Krokhin, A. A. The complexity of constraint satisfaction games and QCSP. *Inf. Comput. 207*, 9 (2009), 923–944.

[6] Börner, F., Pöschel, R., and Sushchansky, V. Boolean systems of relations and Galois connections. *Acta Sci. Math. 68* (2002), 293–302.

[7] Brakensiek, J., and Guruswami, V. Promise constraint satisfaction: Structure theory and a symmetric boolean dichotomy. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2018, New Orleans, LA, USA, January 7-10, 2018* (2018), pp. 1782–1801.

[8] Bredikhin, D. A. Representations of inverse semigroups by difunctional multipermutations. In *Transformation Semigroups: Proceedings of the International Conference held at the University of Essex, Colchester, England, August 3 rd-6th* (1993), pp. 1–10.

[9] Bredikhin, D. A. How can representation theories of inverse semigroups and lattices be united? *Semigroup Forum 53*, 2 (1996), 184–193.

[10] Bulatov, A. A. A dichotomy theorem for nonuniform CSPs. In *58th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2017*. IEEE Computer Soc., Los Alamitos, CA, 2017, pp. 319–330.

[11] Bulín, J., Krokhin, A. A., and Oprsal, J. Algebraic approach to promise constraint satisfaction. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, STOC 2019, Phoenix, AZ, USA, June 23-26, 2019* (2019), pp. 602–613.

[12] Butler, K. K. H. The semigroup of Hall relations. *Semigroup Forum 9*, 3 (1974/75), 253–260.

[13] Clifford, A. Semigroups admitting relative inverses. *Annals of Mathematics* (1941), 1037–1049.

[14] Cohen, D. A., Cooper, M. C., Creed, P., Jeavons, P. G., and Zivný, S. An algebraic theory of complexity for discrete optimization. *SIAM J. Comput. 42*, 5 (2013), 1915–1939.

[15] De Caen, D., and Gregory, D. Primes in the semigroup of boolean matrices. *Linear Algebra and its Applications 37* (1981), 119–134.

[16] Devadze, H. Generating sets of the semigroup of all binary relations in a finite set. In *Dokl. Akad. Nauk BSSR* (1968), vol. 12, pp. 765–768.

[17] FitzGerald, D., and Lau, K. W. On the partition monoid and some related semigroups. *Bulletin of the Australian Mathematical Society 83*, 2 (2011), 273–288.

[18] Ganyushkin, A., and Mazorchuk, V. S. Factor-powers of finite symmetric groups. *Mathematical Notes 58*, 2 (1995), 794–802.

[19] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.0*, 2020.

[20] Geiger, D. Closed systems of functions and predicates. *Pacific Journal of Mathematics 27* (1968), 95–100.

[21] Kim, K. H., and Roush, F. W. Inverses of boolean matrices. *Linear Algebra and its Applications 22* (1978), 247–262.

[22] Kolmogorov, V., Krokhin, A. A., and Rolínek, M. The complexity of general-valued CSPs. *SIAM J. Comput. 46*, 3 (2017), 1087–1110.

[23] Konieczny, J. A proof of Devadze's theorem on generators of the semigroup of Boolean matrices. *Semigroup Forum 83*, 2 (2011), 281–288.

[24] Lynch, N. Log space recognition and translation of parenthesis languages. *J. ACM 24* (1977), 583–590.

[25] Madelaine, F., and Martin, B. The complexity of positive first-order logic without equality. *Logic in Computer Science, Symposium on* (2009), 429–438.

[26] Madelaine, F. R., and Martin, B. The complexity of positive first-order logic without equality. *ACM Trans. Comput. Log. 13*, 1 (2012), 5:1–5:17.

[27] Madelaine, F. R., and Martin, B. On the complexity of the model checking problem. *SIAM J. Comput. 47*, 3 (2018), 769–797.

[28] Martin, B. The lattice structure of sets of surjective hyper-operations. In *Principles and Practice of Constraint Programming - CP 2010 - 16th International Conference, St. Andrews, Scotland.* (2010), vol. 6308 of *Lecture Notes in Computer Science*, Springer, pp. 368–382.

[29] McKenzie, R., and Schein, B. Every semigroup is isomorphic to a transitive semigroup of binary relations. *Transactions of the American Mathematical Society 349*, 1 (1997), 271–285.

[30] Mitchell, J. D., et al. *Semigroups - GAP package, Version 3.3.1*, May 2020.

[31] Pippenger, N. Galois theory for minors of finite functions. *Discrete Mathematics 254*, 1 (2002), 405 – 419.

[32] Plemmons, R., and West, M. On the semigroup of binary relations. *Pacific Journal of Mathematics 35*, 3 (1970), 743–753.

[33] Riguet, J. Relations binaires, fermetures, correspondances de Galois. *Bulletin de la Société Mathématique de France 76* (1948), 114–155.
[34] Schein, B. M. Regular elements of the semigroup of all binary relations. *Semigroup Forum 13*, 2 (1976/77), 95–102.
[35] Schein, B. M. Representation of inverse semigroups by local automorphisms and multi-automorphisms of groups and rings. *Semigroup Forum 32*, 1 (1985), 55–60.
[36] Schein, B. M. Multigroups. *Journal of Algebra 111*, 1 (1987), 114–132.
[37] Thapper, J., and Zivný, S. The complexity of finite-valued CSPs. *J. ACM 63*, 4 (2016), 37:1–37:33.
[38] Zaretskii, K. Regular elements of the semigroup of binary relations. *Uspekhi Matematicheskikh Nauk 17*, 3 (1962), 177–179.
[39] Zaretskii, K. The semigroup of binary relations. *Matematicheskii Sbornik 103*, 3 (1963), 291–305.
[40] Zhuk, D. A proof of the CSP dichotomy conjecture. *J. ACM 67*, 5 (2020), Art. 30, 78.
[41] Zhuk, D., and Martin, B. QCSP monsters and the demise of the Chen conjecture. In *STOC '20—Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing* ([2020] ©2020), ACM, New York, pp. 91–104.