The Lattice and Semigroup structure of Multipermutations

Catarina Carvalho
University of Hertfordshire

York Semigroup Seminar

joint work with B. Martin

What and Why

Study of a new-ish monoid of binary relations (or $\{0, 1\}$ square matrices, or ....) appearing from the study of the

Complexity of evaluating positive equality-free sentences of first order logic over a fixed finite structure $\mathcal{B}$

$$\{\exists,\ \forall,\ \wedge,\ \vee\} - \mathrm{FO}(\mathcal{B})$$

Logical setting

The evaluation problem under a logic $\mathcal{L}$, takes as input a structure (model) $\mathcal{B}$ and a sentence φ of $\mathcal{L}$, and asks whether $\mathcal{B} \models \varphi$.

Example

$$\{\exists,\ \wedge\} - \mathrm{FO}$$

is the equivalent of the CSP

$$\{\exists,\ \forall,\ \wedge\} - \mathrm{FO}$$

is the equivalent of the QCSP, quantified CSP

Complexity

- Complexity of CSP uses polymorphisms;
- Complexity of QCSP uses surjective polymorphisms;
- Complexity of positive first order logic without equality uses Shops: surjective hyper-operations.

Shops

0	1, 2
1	0
2	3, 4
3	3
4	1

0	0
1	0
2	0
3	0
4	0, 1, 2, 3, 4

0	4
1	1
2	3
3	2
4	0

not shops

0	0
1	1, 2
2	–
3	3, 4
4	3, 4

0	0, 1
1	0, 1
2	2, 4
3	0, 4
4	1, 2

Disclaimer

The Galois Connection that appears with this logic asks for closure under "sub-shops", down-closure, but we first want to understand the monoids in its simplest form.

Although it is still unclear if it makes a massive difference...

Madeleine & Martin 2015

Semigroup of binary relations

Let $X = \{1, 2, \ldots, n\}$ and $\mathcal{B}_n = \mathcal{B}_X$ be the semigroup of binary relations on the set X, with multiplication

$$\alpha\beta = \{(a, b) : (a, c) \in \alpha, (c, b) \in \beta \text{ for some } c \in X\}.$$

It was widely studied under several representations (tuples, matrices, lattice isomorphisms), as were some of its subsemigroups.

Shops

Are subsemigroups of B_n, whose relations ρ satisfy

- $\forall a \in X \ \ \exists b \in X \ \ (a, b) \in \rho$
- $\forall b \in X \ \ \exists a \in X \ \ (a, b) \in \rho$

Considered in one paper by B. Schein ('87), named them multipermutations

Acknowledgments

This paper was written in 1977 in Russian and submitted to a Soviet mathematical journal in January 1978. It had been accepted for publication but, in the fall of 1979, when I was about to leave the USSR, the manuscript was returned to me by the publisher without any explanations. I was not allowed to take it with me or to mail it abroad. It took five years and the efforts of four mathematicians from four countries to rescue the manuscript. I am very grateful to all of them, and I am sorry that I cannot give their names here without hurting some of them.

This paper is a slightly changed translation of the original Russian manuscript.

Multigroups: Journal of Algebra 1987

Multipermutations

Theorem (B. Schein '63)

Every semigroup is isomorphic to a semigroup of multipermutations.

He then studied semigroups of multipermutations that satisfy the extra identities

$$(x^{-1})^{-1} = x, \quad (xy)^{-1} = y^{-1}x^{-1}$$

which he called *multigroups*, and proved that

- The class of all multigroups do not form a variety (not closed under homomorphisms
- The class of all multigroups is not finitely axiomatizable
- Every inverse semigroup is a multigroup

Monois of multipermutations

Let $\mathcal{M}_n$ denote the monoid of all multipermutations on $X = \{1, 2, \ldots, n\}$

monoid of all $n \times n$ binary matrices with at least one 1 in every row and every column,

$$1 + 1 = 1, 0 + 1 = 1 + 0 = 1, 0 + 0 = 0$$

so, square matrices over the Boolean semi-ring $\{0, 1\}$, without 0 row or column

- S_n (symmetric group) is a submonoid of $\mathcal{M}_n$;
- T_n (transformation semigroup, all maps from X to X) is not a submonoid of $\mathcal{M}_n$, since not all transformations are surjective.
- H_n (Hall monoid, every relation contains a permutation) is a submonoid of $\mathcal{M}_n$

started looking at it from a semigroup theory point of view

Green's equivalences

In a semigroup S we have

- $a\mathcal{R}b \;\Leftrightarrow\; aS^1 = bS^1$, is a right congruence
- $a\mathcal{L}b \;\Leftrightarrow\; S^1a = S^1b$, is a left congruence
- $\mathcal{H} = \mathcal{R} \cap \mathcal{L}$
- $\mathcal{D} = \mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$
- $a\mathcal{J}b \;\Leftrightarrow\; S^1aS^1 = S^1bS^1$, for finite semigroups $\mathcal{J} = \mathcal{D}$

Example

In a group G we have $\mathcal{R} = \mathcal{L} = \mathcal{H} = \mathcal{D} = \mathcal{J} = G \times G$

In the semigroup of transformations T_n, we have

- $\alpha \mathcal{L} \beta \ \Leftrightarrow im\alpha = im\beta$
- $\alpha \mathcal{R} \beta \ \Leftrightarrow ker\alpha = ker\beta$
- $\alpha \mathcal{D} \beta \ \Leftrightarrow |im\alpha| = |im\beta|$

$$ker\phi = \phi \circ \phi^{-1} = \{(a, b) : \phi(a) = \phi(b)\}$$

For B_n it is not as simple, the relations were characterized by

- Zaretskii ('62, '63) in terms of lattices;
- Plemmons and West ('70) in terms of boolean matrices
- Adu ('86) using direct composition (and skeletons of the relations)

Given $\alpha \in \mathcal{B}_n$, let $V(\alpha)$ be the row space of α, i.e. the set of all sums of rows of α, with 0 vector

$W(\alpha)$ be the column space of α

Lemma (Zaretskii)

For any $\alpha, \beta \in B_n$

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

Green's relations for multipermutations

Given $\alpha \in \mathcal{M}_n$, let $R(\alpha)$ to be the set of rows of α,

$$\langle R(\alpha)\rangle = \{\rho \in V(\alpha)\backslash\{0\} : \exists \alpha_j \in R(\alpha) : \rho \leq \alpha_j\}$$

$C(\alpha)$ the set of columns of α

Lemma

For any $\alpha, \beta \in M_n$ we have

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

Examples

$$\begin{array}{c|c} 0 & 0 \\ \hline 1 & 0 \\ \hline 2 & 0,1,2 \end{array} \quad \mathcal{L} \quad \begin{array}{c|c} 0 & 0 \\ \hline 1 & 0,1,2 \\ \hline 2 & 0,1,2 \end{array} \quad \mathcal{R} \quad \begin{array}{c|c} 0 & 0,1 \\ \hline 1 & 0,1,2 \\ \hline 2 & 0,1,2 \end{array}$$

multipermutations that are $\mathcal{L}$ related in $\mathcal{B}_n$ but not in $\mathcal{M}_n$

$$\begin{array}{c|c} 0 & 0 \\ \hline 1 & 1,2 \\ \hline 2 & 0,1,2 \end{array} \quad \text{and} \quad \begin{array}{c|c} 0 & 0 \\ \hline 1 & 1,2 \\ \hline 2 & 1,2 \end{array}$$

example

Claim

$\alpha \mathcal{D} \beta \;\Leftrightarrow\; \langle \mathsf{R}(\alpha) \rangle \cong \langle \mathsf{R}(\beta) \rangle$ and $\langle \mathsf{C}(\alpha) \rangle \cong \langle \mathsf{C}(\beta) \rangle$

joint work with M. Hughes

Several people worked on binary relations....

Kim

Hang Kim was born in Anju, North Korea in 1936, the oldest son of a small independent farmer. He grew up within a loving family stressing strict Confucian values and the

importance of education. By age 12, Kim already knew some Chinese, Japanese, English and Russian, and had skipped a couple grades of school.

These were hard times in Korea. Japan ruled Korea 1910–1945. In Kim's childhood,

and South Korean forces. In October 1950, China entered the war, and those forces withdrew. Kim had acted as an informal interpreter for American troops. Several friendly U.S. airmen invited Kim to occupy an empty U.S. Air Force plane seat, and leave with them for the south. At age 14, Kim had six hours to decide. His father urged him to go. Kim took the plane. He would not see his mother and siblings for 30 years, and he would never see his father again.

Commander. As the war's end approached, the Colonel and his family offered to bring Kim to the United States and provide for an education. With difficulty, a passport was secured.

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.

Lemma (Schein)

Let ρ be a binary relation. Then ρ is regular iff $\rho \subseteq \rho \circ (\rho^{-1} \circ \rho^{c} \circ \rho^{-1})^{c} \circ \rho$.

Example

0	0, 1
1	2
2	0, 1, 2

is regular as a binary relation, but not as a multipermutation

Algorithm (Kim & Roush)

Let $A \in \mathcal{B}_n$ be a matrix

- $V(A)$ is the row space of A
- $r(A)$ the basis for $V(A)$
- $I(v) = \{u : u \leq w \;\Leftrightarrow\; v \leq w, \text{ for } w \in r(A)\}$ vectores u have exactly one 1
- A_{i*} denotes the i^{th} row of A
- $p(t) = \{\inf w \in V(A) : t \leq w\}$.

Lemma (Kim& Roush)

Matrix A has an inverse iff $I(v) \neq \emptyset$ for each $v \in r(A)$.

Algorithm for multipermutations

1. find $r(A)$;
2. find $I(v)$ for each $v \in r(A)$;
3. for each $v \in r(A)$, choose a vector $u \in I(v)$;
4. for each u, choose a vector s s.t. $s_i = 1$ only if $A_{i*} \leqslant v$ and such that $s_i = 1$ for at least one i s.t. $A_{i*} = v$;
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 s.t. $b_i = 1$ only if $A_{i*} \leqslant p(t)$;
6. write the vectors s and b in the order of the u's and t.

Inverses for multipermutations

Theorem

A multipermutation A has an inverse iff $r(A) = R(A)$, $I(v) \neq \emptyset$ for each $v \in r(A)$, and $p(t) \neq 0$.

Using Schein's condition we can also easily check if a multipermutation ρ has an inverse, just check if

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

the greatest inverse of ρ, is a multipermutation.

Generating sets

- S_n is generated by $(1\ 2)$ and $(1\ 2\ \ldots\ n)$;
- T_n is generated by $(1\ 2)$, $(1\ 2\ \ldots\ n)$ and any map with rank (image size) $n-1$;
- What about $\mathcal{M}_n$?

Not polynomially generated

The number of prime $\mathcal{D}$-classes grows exponentially with n

Generators of $\mathcal{B}_n$: 2 generators of S_n, +2 generators, to generate all regular binary relations, $+$ one representative of each *prime* $\mathcal{D}$-class;

Generators of $\mathcal{M}_n$: 2 generators of S_n, +1 generator from above, $+$ one representative of each *prime* $\mathcal{D}$-class, + k more.

And subclasses?

Are there natural subclasses (*) that are closed under composition and down-closure that might have this property of polynomial generation?
It holds for reflexive, symmetric multipermutations, any other interesting classes?

1. class of regular multipermutations is not closed under composition;
2. class of idempotent multipermutation is not closed under composition.

Open questions

- What are the maximal subgroups of the semigroup of multipermutations?
- Which semigroups are isomorphic to transitive semigroups of multipermutations? (McKenzie, Schein)

They prove that every semigroup is isomorphic to a semigroup of binary relations on a finite set.

A subset $\Phi \subset B_A$ is called transitive if $\bigcup \Phi = A \times A$, that is, for any $a, b \in A$ there exists $\phi \in \Phi$ with $(a, b) \in \phi$.

The lattice structure

We ask for down-closure here, i.e. closure under submultipermutations

Example

$\langle \begin{array}{c|c} 0 & 1,2 \\ \hline 1 & 0 \\ \hline 2 & 1 \end{array} \rangle_{DSM}$ is the monoid containing the following multipermutations

$\begin{array}{c|c} 0 & 1,2 \\ \hline 1 & 0 \\ \hline 2 & 1 \end{array}$, $\begin{array}{c|c} 0 & 2 \\ \hline 1 & 0 \\ \hline 2 & 1 \end{array}$, $\begin{array}{c|c} 0 & 0,1,2 \\ \hline 1 & 1,2 \\ \hline 2 & 0 \end{array}$, $\begin{array}{c|c} 0 & 1 \\ \hline 1 & 2 \\ \hline 2 & 0 \end{array}$, id, $\begin{array}{c|c} 0 & 0,1,2 \\ \hline 1 & 0,1,2 \\ \hline 2 & 0,1,2 \end{array}$

plus

Similar to the lattice of permutation groups (under inclusion), minimal element contains only the identity permutation, and maximal element contains all the multipermutations.

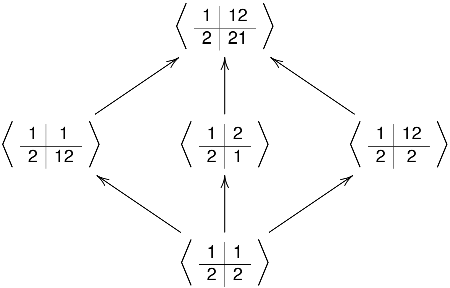

Figure: The lattice on 2 elements.

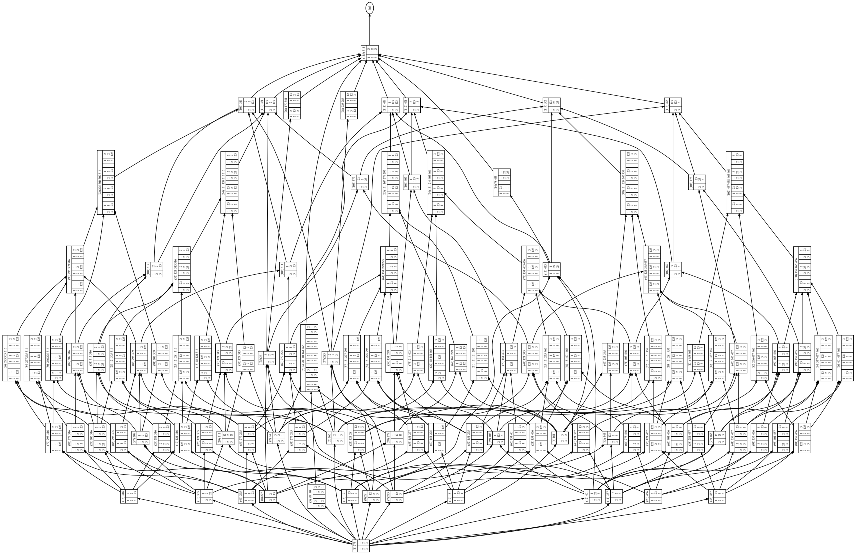

Figure: The lattice on 3 elements.