Semigroups of order-preserving transformations

Young researchers in mathematics
3rd August 2017

Wilf Wilson
University of St Andrews

What are semigroups and monoids?

Informally, a **binary operation** is a way of combining two elements to give a third, such as $+ \; - \; \times \; \div$ in $\mathbb{R}$.

A binary operation is **associative** if $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all possible x, y, z.

Definition (Semigroup)

A *semigroup* is a set with an associative binary operation.

Definition (Monoid)

A *monoid* is a semigroup with an identity element, 1. i.e. $1 \cdot x = x \cdot 1 = x$, for all elements x.

What are semigroups and monoids?

Informally, a **binary operation** is a way of combining two elements to give a third, such as $+ \; - \; \times \; \div$ in $\mathbb{R}$.

A binary operation is **associative** if $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all possible x, y, z.

Definition (Semigroup)

A *semigroup* is a set with an associative binary operation.

Definition (Monoid)

A *monoid* is a semigroup with an identity element, 1. i.e. $1 \cdot x = x \cdot 1 = x$, for all elements x.

What are semigroups and monoids?

Informally, a **binary operation** is a way of combining two elements to give a third, such as $+ \ - \ \times \ \div$ in $\mathbb{R}$.

A binary operation is **associative** if $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all possible x, y, z.

Definition (Semigroup)

A *semigroup* is a set with an associative binary operation.

Definition (Monoid)

A *monoid* is a semigroup with an identity element, 1.
i.e. $1 \cdot x = x \cdot 1 = x$, for all elements x.

Semigroups and monoids can be formed of. . .

- Square matrices over a ring R, with multiplication.
- Binary relations, with composition.
- Subsets of $\mathbb{N}$, with addition.
- Endomorphisms of a structure, with composition.
- If $A = \{a_1, \ldots, a_m\}$, then:
  - $A^* = \{\text{all strings over } A\}$ is the *free monoid* over A.
  - $A^+ = A^* \setminus \{\text{empty string}\}$ is the *free semigroup* over A.

(With the operation of concatenation.)

Semigroups and monoids can be formed of. . .

- Square matrices over a ring R, with multiplication.
- Binary relations, with composition.
- Subsets of $\mathbb{N}$, with addition.
- Endomorphisms of a structure, with composition.

- If $A = \{a_1, \ldots, a_m\}$, then:
  - $A^* = \{\text{all strings over } A\}$ is the *free monoid* over A.
  - $A^+ = A^* \setminus \{\text{empty string}\}$ is the *free semigroup* over A.

(With the operation of concatenation.)

How to specify a semigroup

- Multiplication table:

$\cdot$	a	b	c
a	a	a	a
b	a	b	b
c	a	c	c

- Generating set:

$$S = \langle 13,\ 8 \rangle \leqslant \mathbb{N}$$

- Semigroup presentation:

$$\langle x_1, x_2 \mid x_1^4 = x_2 x_1 \rangle$$

- . . . and all sorts of algebraic ways.

What do I do?

- Computational methods for finite semigroups.

Given a generating set, you might want to:

- Compute the size of the semigroup.
- Test membership in the semigroup.
- Describe maximal subgroups/subsemigroups.
- Calculate ideals.
- Compute congruences.
- Find the idempotents.
- Work out whether there is an identity/zero.

Algorithms typically have bad worst-case complexity.

Transformations

Definition (Transformation)

A *transformation* is a map from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$.

$$\text{We can write } f = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1f & 2f & \cdots & nf \end{pmatrix}.$$

Definition (Partial transformation)

A *partial transformation* is a *partial* map on $\{1, \ldots, n\}$.

$$\text{We can write } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ - & 4 & 1 & - & 4 \end{pmatrix}, \text{ for example.}$$

Definition (Partial permutation)

A *partial permutation* is an injective partial transformation.

Transformations

Definition (Transformation)

A *transformation* is a map from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$.

$$\text{We can write } f = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1f & 2f & \cdots & nf \end{pmatrix}.$$

Definition (Partial transformation)

A *partial transformation* is a *partial* map on $\{1, \ldots, n\}$.

$$\text{We can write } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ - & 4 & 1 & - & 4 \end{pmatrix}, \text{ for example.}$$

Definition (Partial permutation)

A *partial permutation* is an injective partial transformation.

Transformations

Definition (Transformation)

A *transformation* is a map from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$.

$$\text{We can write } f = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1f & 2f & \cdots & nf \end{pmatrix}.$$

Definition (Partial transformation)

A *partial transformation* is a *partial* map on $\{1, \ldots, n\}$.

$$\text{We can write } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ - & 4 & 1 & - & 4 \end{pmatrix}, \text{ for example.}$$

Definition (Partial permutation)

A *partial permutation* is an injective partial transformation.

Image, domain, kernel

Let α be a partial transformation on the set $\{1, \ldots, n\}$.

- $\text{im}(\alpha) = \big\{i\alpha : i \in \{1, \ldots, n\}\big\}$.
- $\text{dom}(\alpha) = \big\{i \in \{1, \ldots, n\} : i\alpha \text{ is defined}\big\}$.
- $\ker(\alpha)$ is the partition of $\text{dom}(\alpha)$ into parts with equal image.

Example: if $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ - & 4 & 1 & - & 4 \end{pmatrix}$, then

- $\text{im}(\alpha) = \{1, 4\}$,
- $\text{dom}(\alpha) = \{2, 3, 5\}$,
- $\ker(\alpha) = \big\{\{2, 5\}, \{3\}\big\}$.

These attributes are often useful for computations.

Image, domain, kernel

Let α be a partial transformation on the set $\{1,\ldots,n\}$.

- $\operatorname{im}(\alpha) = \big\{i\alpha : i \in \{1,\ldots,n\}\big\}$.
- $\operatorname{dom}(\alpha) = \big\{i \in \{1,\ldots,n\} : i\alpha \text{ is defined}\big\}$.
- $\ker(\alpha)$ is the partition of $\operatorname{dom}(\alpha)$ into parts with equal image.

Example: if $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ - & 4 & 1 & - & 4 \end{pmatrix}$, then

- $\operatorname{im}(\alpha) = \{1,4\}$,
- $\operatorname{dom}(\alpha) = \{2,3,5\}$,
- $\ker(\alpha) = \big\{\{2,5\},\{3\}\big\}$.

These attributes are often useful for computations.

Image, domain, kernel

Let α be a partial transformation on the set $\{1, \ldots, n\}$.

- $\operatorname{im}(\alpha) = \big\{i\alpha : i \in \{1, \ldots, n\}\big\}$.
- $\operatorname{dom}(\alpha) = \big\{i \in \{1, \ldots, n\} : i\alpha \text{ is defined}\big\}$.
- $\ker(\alpha)$ is the partition of $\operatorname{dom}(\alpha)$ into parts with equal image.

Example: if $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ - & 4 & 1 & - & 4 \end{pmatrix}$, then

- $\operatorname{im}(\alpha) = \{1, 4\}$,
- $\operatorname{dom}(\alpha) = \{2, 3, 5\}$,
- $\ker(\alpha) = \big\{\{2, 5\}, \{3\}\big\}$.

These attributes are often useful for computations.

Transformation semigroups

Composition of functions is associative!

A *transformation semigroup* is any semigroup of transformations, with composition of functions.

- $\mathcal{PT}_n$, the *partial transformation semigroup of degree n*, is the semigroup consisting of all partial transformations on $\{1, \ldots, n\}$.
- $\mathcal{T}_n$, the *full transformation semigroup of degree n*, is the semigroup consisting of all transformations on $\{1, \ldots, n\}$.

There's an analogue of **Cayley's theorem** here.

Transformation semigroups

Composition of functions is associative!

A *transformation semigroup* is any semigroup of transformations, with composition of functions.

- $\mathcal{PT}_n$, the *partial transformation semigroup of degree* n, is the semigroup consisting of all partial transformations on $\{1, \ldots, n\}$.
- $\mathcal{T}_n$, the *full transformation semigroup of degree* n, is the semigroup consisting of all transformations on $\{1, \ldots, n\}$.

There's an analogue of **Cayley's theorem** here.

Inverse semigroups

Definition (Inverse semigroup)

A semigroup S is *inverse* if all for $x \in S$, there is a **unique** $x' \in S$ such that $x = xx'x$ and $x' = x'xx'$.

- $\mathcal{I}_n$, the *symmetric inverse monoid of degree* n, is the semigroup consisting of all partial permutations on $\{1, \ldots, n\}$.

There's another analogue of **Cayley's theorem**.

Inverse semigroups

Definition (Inverse semigroup)

A semigroup S is *inverse* if all for $x \in S$, there is a **unique** $x' \in S$ such that $x = xx'x$ and $x' = x'xx'$.

- $\mathcal{I}_n$, the *symmetric inverse monoid of degree* n, is the semigroup consisting of all partial permutations on $\{1, \ldots, n\}$.

There's another analogue of **Cayley's theorem**.

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n.$
- All transformations: $|\mathcal{T}_n| = n^n.$
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n.$
- All transformations: $|\mathcal{T}_n| = n^n.$
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

The sizes of these semigroups

- All permutations: $|\mathcal{S}_n| = n!$
- Partial transformations: $|\mathcal{PT}_n| = \sum_{k=0}^{n} \binom{n}{k} n^k = (n+1)^n$.
- All transformations: $|\mathcal{T}_n| = n^n$.
- All partial permutations: $|\mathcal{I}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 k!$

Order-preserving transformations

A partial transformation α is

- **order-preserving** if $i \leqslant j \;\Rightarrow i\alpha \leqslant j\alpha$
- **order-reversing** if $i \leqslant j \;\Rightarrow i\alpha \geqslant j\alpha$

for all $i, j \in \mathrm{dom}(\alpha)$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & - & 2 & - & 5 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 2 & 1 \end{pmatrix}.$$

Which permutations are order-preserving/reversing?

Order-preserving transformations

A partial transformation α is

- **order-preserving** if $i \leqslant j \Rightarrow i\alpha \leqslant j\alpha$
- **order-reversing** if $i \leqslant j \Rightarrow i\alpha \geqslant j\alpha$

for all $i, j \in \mathrm{dom}(\alpha)$.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & - & 2 & - & 5 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 2 & 1 \end{pmatrix}.$$

Which permutations are order-preserving/reversing?

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Sizes of the order-preserving monoids

- Partial: $|\mathcal{PO}_n| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k-1}{k}$
- Total: $|\mathcal{O}_n| = \binom{2n-1}{n}$
- Partial injective: $|\mathcal{POI}_n| = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Green's relations

Let S be a monoid and let $x, y \in S$.

- $x \mathscr{L} y$ if and only if $Sx = Sy$.
- $x \mathscr{R} y$ if and only if $xS = yS$.
- $x \mathscr{J} y$ if and only if $SxS = SyS$.

For the monoids defined today:

- $x \mathscr{L} y$ if and only if $\mathrm{im}(x) = \mathrm{im}(y)$.
- $x \mathscr{R} y$ if and only if $\ker(x) = \ker(y)$.
- $x \mathscr{J} y$ if and only if $|\mathrm{im}(x)| = |\mathrm{im}(y)|$.

Green's relations are really useful for computations!

Green's relations

Let S be a monoid and let $x, y \in S$.

- $x \mathscr{L} y$ if and only if $Sx = Sy$.
- $x \mathscr{R} y$ if and only if $xS = yS$.
- $x \mathscr{J} y$ if and only if $SxS = SyS$.

For the monoids defined today:

- $x \mathscr{L} y$ if and only if $\mathrm{im}(x) = \mathrm{im}(y)$.
- $x \mathscr{R} y$ if and only if $\ker(x) = \ker(y)$.
- $x \mathscr{J} y$ if and only if $|\mathrm{im}(x)| = |\mathrm{im}(y)|$.

Green's relations are really useful for computations!

Green's relations

Let S be a monoid and let $x, y \in S$.

- $x \mathscr{L} y$ if and only if $Sx = Sy$.
- $x \mathscr{R} y$ if and only if $xS = yS$.
- $x \mathscr{J} y$ if and only if $SxS = SyS$.

For the monoids defined today:

- $x \mathscr{L} y$ if and only if $\mathrm{im}(x) = \mathrm{im}(y)$.
- $x \mathscr{R} y$ if and only if $\ker(x) = \ker(y)$.
- $x \mathscr{J} y$ if and only if $|\mathrm{im}(x)| = |\mathrm{im}(y)|$.

Green's relations are really useful for computations!

http://gap-packages.github.io/Semigroups

Semigroups

Download .tar.gz

View On GitHub

Version 3.0.4

This project is maintained by
J. D. Mitchell

GAP Package Semigroups

The Semigroups package is a GAP package containing methods for semigroups, monoids, and inverse semigroups. There are particularly efficient methods for semigroups or ideals consisting of transformations, partial permutations, bipartitions, partitioned binary relations, subsemigroups of regular Rees 0-matrix semigroups, and matrices of various semirings including boolean matrices, matrices over finite fields, and certain tropical matrices.

Semigroups contains efficient methods for creating semigroups, monoids, and inverse semigroup, calculating their Green's structure, ideals, size, elements, group of units, small generating sets, testing membership, finding the inverses of a regular element, factorizing elements over the generators, and so on. It is possible to test if a semigroup

The end.