Semigroups in GAP: an introduction and tutorial

Wilf Wilson
University of St Andrews

21 October 2016

Transformations in GAP

A transformation is a function on the set $\{1, \ldots, n\}$. Examples:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 1 & 5 & 3 & 3 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 2 & 1 & 4 \end{pmatrix}.$$

Composition of transformations: $fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 4 & 1 & 1 & 1 \end{pmatrix}.$

In GAP, a transformation is stored as a list:

$f =$ [4, 1, 1, 5, 3, 3], $g =$ [4, 5, 1, 2, 1, 4], etc.

```
gap> f := Transformation([4, 1, 1, 5, 3, 3]);
gap> S := Semigroup(f);
```

The definition of a semigroup

A semigroup is a set (S) with an associative binary operation $(*)$.

Associativity: $(x * y) * z = x * (y * z)$.

In GAP: `IsSemigroup = IsMagma and IsAssociative`.
In GAP: `IsMonoid = IsMagmaWithOne and IsAssociative`.
In GAP: `IsGroup = IsMagmaWithInverses and IsAssociative`.

We wish to compute with semigroups.

Specifying a semigroup by multiplication table

A finite semigroup can be specified by a multiplication table. An example:

	1	2	3	4
1	1	2	3	4
2	2	1	3	4
3	3	4	3	4
4	4	3	3	4

- The row and column labels are the elements.
- The entry in row i, column j defines the product $i \cdot j$.

Multiplication tables are abstract, but usually impractical.

An aside: counting multiplication tables

	1	2	3	4	n
All tables	1	16	19,683	4,294,967,269	n^{n^2}
Magmas	1	10	3,330	178,981,952	$\sim n^{n^2}/n!$
Semigroups	1	4	18	126	?
Groups	1	1	1	2	?

There are 12,418,001,077,381,302,684 semigroups of order 10.

Some examples of semigroups

Examples:

- Transformations, with composition of functions.
- Partial permutations, with composition of (partial) functions.
- $n \times n$ matrices, with matrix multiplication.
- Finite strings, with concatenation.
- Binary relations, with composition of relations.
- Subsets of a set, with union/intersection.

We can specify such a semigroup with reference only to its elements.

Semigroups by generating set

A semigroup can be specified by a set of generators.
The elements are all possible combinations of the generators. Example:

$$(\mathbb{N}, +) = \langle 1 \rangle.$$

Question: what is a generating set for $(\mathbb{N}, \times)$?

Theme: we try to compute *without* having to find all the elements.

What might we want to compute?

- Test commutativity.
- Test membership.
- Compute the (number of) elements.
- Count the idempotents.
- Find the maximal subgroups or subsemigroups.
- Find the Green's relations.

Green's equivalence relations $\mathscr{L}$, $\mathscr{R}$, and $\mathscr{H}$:

- $x \mathscr{L} y$ if and only if $x = ay$ and $y = bx$ (for some a, b).
- $x \mathscr{R} y$ if and only if $x = ya$ and $y = xb$ (for some a, b).
- $x \mathscr{H} y$ if and only if $x \mathscr{L} y$ and $x \mathscr{R} y$.

Finitely presented semigroups

Specify a semigroup by generators and relations. An example:

$$\langle x, y \mid xy = yx,\ x^3 = x^2,\ y^2 = y \rangle$$

- Works for finite semigroups, and many infinite semigroups.
- Difficult to write algorithms.
- Leads to problems of undecidability.

Often, we deal with semigroups that we *know* are finite.

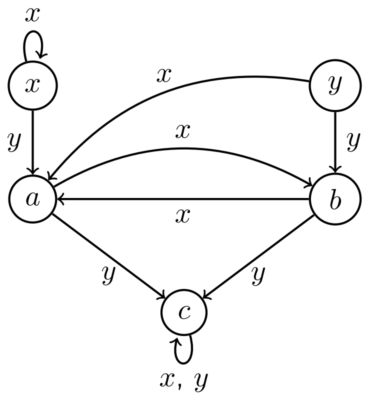
Naive exhaustive enumeration of a semigroup

Given a set of generators A of a finite semigroup S, we can find all the elements of S with the following procedure:

- Define $S = A$.
- For each $s \in S$, and for each $a \in A$:
  - if $sa \notin S$:
    - add a to S.
- Return S as the set of elements.

Requires $|S| \cdot |A|$ multiplications and searches.

The right Cayley graph for $S = \{x, y, a, b, c\}$; generating set $\{x, y\}$:



Associativity gives us left multiplication: $x(yzt) = (xyz)t$.

Thus we obtain the left Cayley graph and the Green's relations.

How can we avoid enumerating the semigroup?

A fundamental problem in computational semigroup theory.

- Use the generators.
- Use theory.
- Use the representation.
- Use the power of GAP!

Case study: commutative semigroups

Commutative semigroup: where $x * y = y * x$ for all x and y.

How do we test for commutativity?

Case study: counting idempotents

An *idempotent*: an element x where $x * x = x$.

- Some semigroups have no idempotents.
- Some semigroups consist only of idempotents.
- There exist semigroups at every point between these extremes.

How do we count the idempotents in a semigroup?

Using the representation of a semigroup

Full transformation semigroup:

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

Full matrix semigroup (over a field):

- $x \mathscr{L} y$ if and only if x and y have the same row space.
- $x \mathscr{R} y$ if and only if x and y have the same column space.

Partition monoid:

- $x \mathscr{L} y$ if and only if $x^* x = y^* y$.
- $x \mathscr{R} y$ if and only if $x x^* = y y^*$.

. . .

Using the representation: transformation semigroups

A transformation 'acts' on *points*: $i \mapsto (i)f$.

A transformation 'acts' on *sets of points*: $A \mapsto A \cdot f = \{(i)f : i \in A\}$.

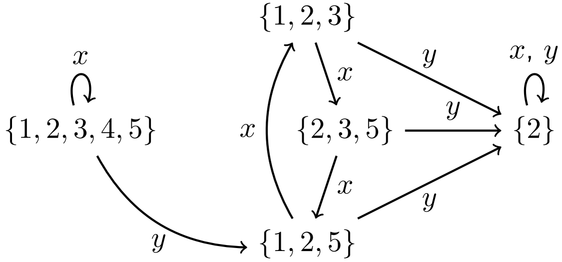
$$\text{Example :} \quad \{2,3\} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 5 & 3 \end{pmatrix} = \{1,5\}.$$

If $s = x_1 x_2 \cdots x_m$, then

$$\operatorname{im}(s) = \operatorname{im}(x_1 x_2 \cdots x_m) = \operatorname{im}(x_1) \cdot x_2 \cdots x_m.$$

Thus: every image which occurs can be found via an orbit-style algorithm.

Using the representation: 'orbit' graph



Roughly:

- $x\mathscr{R}y$ if $\ker(x) = \ker(y)$ and $\operatorname{im}(x) \sim \operatorname{im}(y)$ *(plus group theory)*.
- $x\mathscr{L}y$ if $\operatorname{im}(x) = \operatorname{im}(y)$ and $\ker(x) \sim \ker(y)$ *(plus group theory)*.

If there are fewer kernels/images than elements: net win!

Semigroups and Digraphs packages for GAP

- Semigroups package:
  gap-packages.github.io/Semigroups
- Digraphs package:
  gap-packages.github.io/Digraphs