

# Computing with semigroups in GAP

**James D. Mitchell**

# Outline

## Part I - Getting started

- Semigroups in GAP
  - creating semigroups
    - \* by generators: transformations, matrices...
    - \* free semigroups and finitely presented semigroups
    - \* by multiplication table
    - \* by construction: Rees matrix semigroups
  - ideals, congruences and quotients
  - Green's relations
- The MONOID package
  - what it does
  - where to obtain it

## Part II - Applications

- Computing automorphisms of semigroups
  - an algorithm
  - some examples
- Largest subsemigroups
  - completely simple in  $\mathcal{T}_X$
  - inverse in  $\mathcal{T}_X$
  - 2-generated in  $\mathcal{I}_X$
- What do you want?
  - proposed and upcoming features
  - is there anything you want?
- Some exercises.

# Semigroups in GAP

Let  $S$  be a semigroup defined by a concrete set of generators  $A$ , i.e. mappings, matrices, etc.

GAP uses the **Froidure-Pin** Algorithm to compute:

- the elements of  $S$
- the left and right Cayley graphs of  $S$
- a semigroup presentation defining  $S$

All this for the same, or less, effort than the original method used to enumerate  $S$  in GAP.

## Green's relations

$s\mathcal{R}t$  if and only if  $s$  and  $t$  are in the same strongly connected component of the right Cayley graph of  $S$

$s\mathcal{L}t$  if and only if  $s$  and  $t$  are in the same strongly connected component of the left Cayley graph of  $S$

There are very efficient methods for finding the strongly connected components of a directed graph (implemented in the kernel of GAP).

$\mathcal{H}$ - and  $\mathcal{D}$ -classes can be easily calculated from the  $\mathcal{L}$ -classes and  $\mathcal{R}$ -classes.

# The MONOID package

The first versions of MONOID in GAP 3 by

S. Linton, G. Pfeiffer, E. F. Robertson, and N. Ruškuc

MONOID v3 for GAP 4 has efficient methods for:

- $|M|$  -  $M$  a finite transformation semigroup
- $\mathcal{R}$ ,  $\mathcal{D}$ ,  $\mathcal{L}$  and  $\mathcal{H}$
- fast membership test for  $M$
- local calculations of  $\mathcal{R}$ -,  $\mathcal{L}$ -, &  $\mathcal{D}$ -classes
- property testing of semigroups
- constructions of special types of semigroups

The most basic functions in MONOID replaces the existing methods for computing transformation semigroups.

For these functions the same commands are used in GAP when the MONOID loaded and when it is not.

## Property testing

**Result 1.** Let  $\Omega \subseteq \mathcal{T}_X$  and  $U = \langle \Omega \rangle$ . Then  $U$  is a **left zero semigroup** if and only if for all  $\alpha, \beta \in \Omega$ ,  $\text{im}(\alpha) = \text{im}(\beta)$  and  $\alpha^2 = \alpha$ .  
On the other hand,  $U$  is a **right zero semigroup** if and only if for all  $\alpha, \beta \in \Omega$ ,  $\text{ker}(\alpha) = \text{ker}(\beta)$  and  $\alpha^2 = \alpha$ .

**Result 2.** Let  $\Omega \subseteq \mathcal{T}_X$  and  $U = \langle \Omega \rangle$ . Then  $U$  is **completely simple** if and only if for all  $\alpha, \beta \in \Omega$ ,  $\text{im}(\alpha)$  is a transversal of  $\text{ker}(\beta)$ .

If  $X = \{1, 2, \dots, n\}$ , then

$$\text{Cone}_U(X) = \{ X\alpha : \alpha \in U^1 \}.$$

**Result 3.** Let  $\Omega \subseteq \mathcal{T}_X$  and  $U = \langle \Omega \rangle$ . Then  $U$  is **completely regular** if and only if for all  $\alpha \in \Omega$ ,  $\text{Cone}_U(\text{im}(\alpha))$  consists of partial transversals of  $\ker(\alpha)$ .

There is no 'cheap' way to determine if  $U$  is regular.

**Result 4.** Let  $U$  be a regular semigroup. Then  $U$  is **inverse** if and only if  $|\text{Ims}(U)| = |\text{Kers}(U)|$  and for each  $I \in \text{Ims}(U)$  there exists a unique  $K \in \text{Kers}(U)$  such that  $I$  is a transversal of  $K$ .

**Result 5.** Let  $\Omega \subseteq \mathcal{T}_X$  and  $U = \langle \Omega \rangle$ . Then  $U$  is a **Clifford** semigroup if and only if for all  $\alpha, \beta \in \Omega$

- (i)  $\alpha|_{\text{im}(\alpha)}$  is a permutation of  $\text{im}(\alpha)$ ;
- (ii)  $\alpha e_\beta = e_\beta \alpha$ .

## Where to get MONOID

The current release version of MONOID is 3.0.1 available from:

`www-groups.mcs.st-and.ac.uk/~jamesm/semigroups/`

MONOID works with GAP 4.4.8 which is going to be released soon...

`http://www.gap-system.org/Download/index.html`

## Part II - Applications

### Computing Automorphisms

(joint work with J. Araújo and P. v Bunäü)

Let  $S$  be a finite semigroup. Then the most naïve approach is to:

- for every bijection  $\phi : S \rightarrow S$  test if

$$(x)\phi(y)\phi = (xy)\phi$$

for all  $x, y \in S$ ;

Even for small examples this calculation exceeds human patience.

As the examples grow in size it exceeds the patience of the computer too.

## Better?

Automorphisms preserve:

- Green's  $\mathcal{D}$ -relation
- the poset of  $\mathcal{D}$ -classes
- if  $D_1\phi = D_2$ , then  $D_1 \cong D_2$  (as principal factors)

The search space is **reduced** using these restrictions.

Require prior methods to compute:

- the  $\mathcal{D}$ -classes of  $S$  (using Froidure-Pin or MONOID)
- the partial order  $P$  of  $\mathcal{D}$ -classes (using MONOID)
- the automorphism group of  $P$  (using nauty through GRAPE);
- the isomorphisms between principal factors of  $\mathcal{D}$ -classes (see next slide).

# Automorphisms of Rees matrix semigroups

Let  $D$  be a  $\mathcal{D}$ -class of  $S$ . Then form a new semigroup  $D^* = D \cup \{0\}$  with multiplication  $*$  defined by

$$x * y = \begin{cases} xy & \text{if } xy \in D \\ 0 & \text{if } xy \notin D. \end{cases}$$

if  $\phi$  is an automorphism of  $S$ , then  $D^* \cong (D\phi)^*$

$D^*$  is the **principal factor** of  $D$

$D^*$  is a Rees matrix semigroup with zero

Let  $M = \mathcal{M}^0[G; I, J; P]$  be a regular Rees matrix semigroup over the group  $G$ , index sets  $I$  and  $J$ , and sandwich matrix  $P = (p_{ji})_{j \in J, i \in I}$ .

Define a bipartite graph  $\Gamma(M)$  with vertices  $I \cup J$  and edge  $(i, j)$  whenever  $p_{ji} \neq 0$ .

Let  $\text{Aut } \Gamma(M)$  denote the set of all  $I$  and  $J$  preserving automorphisms of  $\Gamma(M)$ .

**Result 6.** *Let  $\lambda \in \text{Aut } \Gamma(M)$ ,  $\gamma \in \text{Aut } G$ , and  $f : I \cup J \rightarrow G$ . Then the mapping*

$$\alpha : (i, g, j) \mapsto (i\lambda, (if)(g\gamma)(jf)^{-1}, j\lambda) \quad (1)$$

*is an automorphism if and only if  $p_{ji} = (jf)(p_{j\lambda^{-1}i\lambda^{-1}})\gamma(if)^{-1}$  for all  $p_{ji} \neq 0$ .*

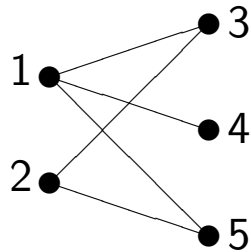
*Furthermore, every automorphism of  $M$  can be described in this way.*

## An example & a non-example

**Example.** Let  $M = \mathcal{M}^0[\mathbb{Z}_3; \{1, 2\}, \{3, 4, 5\}; P]$  where  $\mathbb{Z}_3 = \{x, x^2, x^3\}$  &

$$P = \begin{pmatrix} x^3 & x^3 \\ x^3 & 0 \\ x^3 & x \end{pmatrix}.$$

The graph  $\Gamma(M)$ :



$$\text{Aut } \Gamma(M) = \langle (35) \rangle.$$

The automorphism group of  $\mathbb{Z}_3$  is  $\text{Aut } \mathbb{Z}_3 = \langle x \mapsto x^2 \rangle \cong \mathbb{Z}_2$ .

If  $\lambda \in \text{Aut } \Gamma(M)$ ,  $\gamma \in \text{Aut } \mathbb{Z}_3$ , and  $1f \in \mathbb{Z}_3$ , then:

$$\begin{aligned} 3f &= p_{3\lambda 1\lambda} \cdot 1f \cdot (p_{31}\gamma)^{-1}, & 4f &= p_{4\lambda 1\lambda} \cdot 1f \cdot (p_{41}\gamma)^{-1}, \\ 5f &= p_{5\lambda 1\lambda} \cdot 1f \cdot (p_{51}\gamma)^{-1}, & 2f &= p_{3\lambda 2\lambda}^{-1} \cdot 3f \cdot p_{32}\gamma. \end{aligned}$$

Thus  $[\lambda, \gamma, f]$  is an automorphism of  $M$  if

$$2f = p_{5\lambda 2\lambda}^{-1} \cdot 5f \cdot (p_{52})\gamma.$$

If  $\lambda = (3\ 5)$ ,  $\gamma : x \mapsto x$ , and  $1f = x$ , then  $3f = 4f = 5f = 1f = x$  but

$$p_{5\lambda 2\lambda}^{-1} \cdot 5f \cdot (p_{52})\gamma = p_{32}^{-1} \cdot x \cdot p_{52} = x \cdot x \neq x^{-1} \cdot x = 2f.$$

If  $\lambda = 1_{\Gamma(M)}$ ,  $\gamma : x \mapsto x$ , and  $1f = x$ , then  $1f = 2f = 3f = 4f = 5f$  and

$$p_{52}^{-1} \cdot x \cdot (p_{52})\gamma = x^{-1} \cdot x \cdot x = 2f.$$

# The algorithm

## Algorithm 1.

**A1.1. partition the  $\mathcal{D}$ -classes:** *so that  $D \sim D'$  if:*

- $|D| = |D'|$ ;
- *the number of  $\mathcal{L}$ -classes and  $\mathcal{R}$ -classes in  $D$  and  $D'$  are equal*
- *both  $D$  and  $D'$  are regular or nonregular*
- *the number of idempotents is equal*

**A1.2. compute automorphisms  $G$  of  $P$  that preserve  $\sim$**

**A1.3. inside each orbit under  $G$  determine  $\mathcal{D}$ -classes that are isomorphic**

**A1.4 restrict  $G$  according to A1.3.**

## The algorithm

**A1.5. find possible images of generators** by finding isomorphisms between principal factors of  $\mathcal{D}$ -classes

**A1.6. test the possible maps:** if  $A\alpha$  generates  $S$  and satisfies  $R$ , then  $\alpha$  is an automorphism

## Largest subsemigroups

**Question 7.** If  $\mathfrak{X}$  is a class of semigroups, then what is the largest size that a subsemigroup of  $\mathcal{T}_X$  belonging to  $\mathfrak{X}$  can have?

**Example.** The largest proper subsemigroup of  $\mathcal{T}_X$  is

$$U = A_n \cup K(n, n-1) = \{\alpha \in \mathcal{S}_X : \alpha \text{ is even}\} \cup \{\alpha \in \mathcal{T}_X : |\text{im}(\alpha)| \leq n-1\}.$$

Thus the largest proper subsemigroup of  $\mathcal{T}_X$  has size

$$n^n - (n!/2).$$

$U$  is regular, and so the largest regular subsemigroup of  $\mathcal{T}_X$  also has size

$$n^n - (n!/2).$$

## Left & right zero semigroups

**Result 8.** If  $U$  is a left zero subsemigroup of  $\mathcal{T}_X$  where the rank of the elements is  $r$ , then

$$|U| \leq r^{n-r}.$$

**Proof.** It suffices to find the largest set of idempotents with a common image of size  $r$ . The size of this set is  $r^{n-r}$ . ■

**Result 9.** If  $U$  is a right zero subsemigroup of  $\mathcal{T}_X$  where the rank of the elements is  $r$  and  $n \equiv t \pmod{r}$ , then

$$|U| \leq \lceil n/r \rceil^t \lfloor n/r \rfloor^{r-t} \leq \lfloor (n/r)^r \rfloor.$$

**Result 10.** The largest size of a right zero subsemigroup of  $\mathcal{T}_X$  is

$$\begin{array}{ll} 3^{(n/3)} & \text{if } n \equiv 0 \pmod{3} \\ 2^2 \cdot 3^{(n-4)/3} & \text{if } n \equiv 1 \pmod{3} \\ 2 \cdot 3^{(n-2)/3} & \text{if } n \equiv 2 \pmod{3}. \end{array}$$

## Proof of Result 9

- $K$  is any partition of  $\{1, 2, \dots, n\}$  with classes  $A_1, A_2, \dots, A_r$ ;
- there are  $k = \prod_{i=1}^r |A_i|$  transversals of  $K$ ;
- there are  $k$  idempotents with kernel  $K$ ;
- must find  $M = \max\{a_1 \cdots a_r : n = a_1 + \cdots + a_r\}$ ;
- by the AM-GM inequality,  $M \leq \lfloor (n/r)^r \rfloor$ ;
- $\lfloor (n/r)^r \rfloor \in \mathbb{N}$  if and only if  $r|n$ ;
- if  $r \nmid n$ , then let  $b_1 + \cdots + b_r = M$ ;
- if  $b_1 > \lceil n/r \rceil$ , then  $b_2 < \lfloor n/r \rfloor$ ;
- thus  $(b_1 - 1)(b_2 + 1)b_3 \cdots b_r > b_1 b_2 \cdots b_r$ , a contradiction;
- $b_1, b_2, \dots, b_r \in \{\lceil n/r \rceil, \lfloor n/r \rfloor\}$ ;
- if  $n = x \lceil n/r \rceil + y \lfloor n/r \rfloor$ , then  $x = t$  and  $y = r - t$ . ■

## Completely simple semigroups

If  $U$  is a largest completely simple semigroup, then from the results about left and right zero semigroups:

$$r! r^{n-r} \leq |U| \leq r! r^{n-r} \lceil n/r \rceil^t \lfloor n/r \rfloor^{r-t}.$$

**Result 11.** If  $U$  is a completely simple subsemigroup of  $\mathcal{T}_X$  where the rank of the elements is  $r \geq 2$ , then

$$|U| \leq r! r^{n-r}.$$

**Example.** If  $U$  consists of all mappings  $\alpha$  with a given image, of size  $r$ , that satisfy  $\text{rank}(\alpha^2) = \text{rank}(\alpha)$ , then  $|U| = r! r^{n-r}$ .

Since

$$n! > (n-1)(n-1)! > (n-2)^2(n-2)! > \dots,$$

it follows that

**Result 12.** The largest completely simple subsemigroup of  $\mathcal{T}_X$  is  $\mathcal{S}_X$ .

## Inverse semigroups

**Result 13.** If  $U$  is an inverse subsemigroup of  $\mathcal{T}_X$  where the least rank of an element is  $r$ , then

$$|U| \leq r! + \sum_{m=1}^{n-r} \binom{n-r}{m}^2 (r-1)! m!.$$

**Where's this number come from?**

- The least  $\mathcal{D}$ -class  $D_r$  of  $U$  is a group;
- the size of  $D_r$  is at most  $r!$ ;
- every  $\alpha \in D_r$  has the same image  $I$  and kernel  $K$ ;
- every element of  $U$  preserves  $I$  and  $K$ ;
- a subgroup of elements with rank  $r + m$  has size  $\leq (r-1)! m!$ ;
- the number of  $\mathcal{H}$ -classes of elements with rank  $r + m$  is  $\leq \binom{n-r}{m}^2$ .

## 2-generator subsemigroups of $\mathcal{I}_X$

Joint work with Jorge and Vitor.

**Theorem 14.** If  $n \geq 3$  is odd, then the largest 2-generated subsemigroup of  $\mathcal{I}_X$  has size

$$\mathfrak{o}(n) = 2n - 4 + \frac{1}{4}(n^4 + 2n^3 - 23n^2 + 36n - 12)(n - 2)! \\ + \sum_{r=1}^{n-3} \binom{n}{r}^2 r!.$$

The permutation  $\alpha = (1\ 2\ \cdots\ n - 2)(n - 1\ n) \in \mathcal{S}_X$  and the partial bijection

$$\beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ - & 3 & 4 & \cdots & 2 \end{pmatrix}$$

generate an inverse subsemigroup of size  $\mathfrak{o}(n)$ .

## Upcoming features of MONOID

- the automorphism group algorithm outlined above
- Tietze transformations for f.p. semigroups
- functionality for partial mappings, bijections and binary relations
- specialised functions for computing with partial mappings, bijections and binary relations

### Proposed features

- efficient Todd-Coxeter type procedures for semigroups
- Reidemeister-Schreier methods for finding presentations for substructures (subgroups, ideals and subsemigroups)