Computing with finite semigroups: part I

J. D. Mitchell

School of Mathematics and Statistics, University of St Andrews

November 20th, 2015

What is this talk about?

Given:

- a finite semigroup S; and
- a question about S.

Aim:

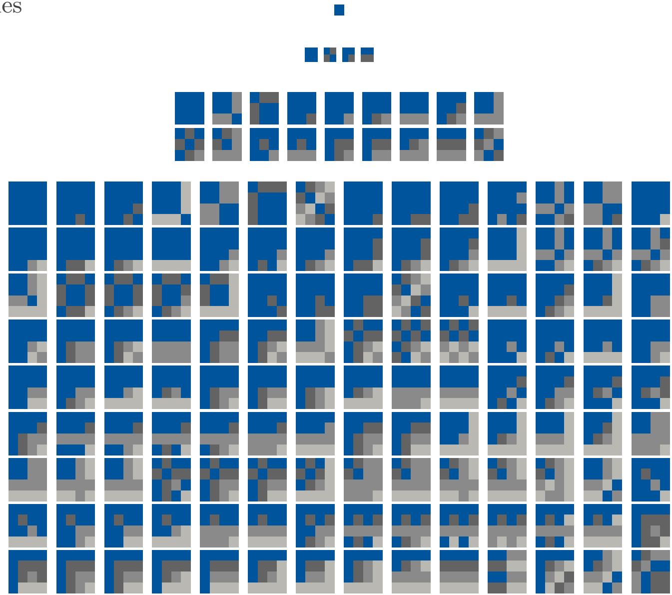
- to describe how to answer your question using a computer
- describe the state of the art.

Why?

- perform low-level calculations such as multiplication, inversion, ...
- suggests new theoretical results
- obtain counter-examples
- gain more detailed understanding
- perform more intricate calculations.

Insert semigroup into computer . . . number 1

Cayley tables



Insert semigroup into computer ... number 1

Reasons not to:

- Too many! 12 418 001 077 381 302 684 semigroups up to isomorphism and anti-isomorphism with 10 elements (Distler-Kelsey '13);
- Complexity! $O(|S|^3)$ just to verify associativity;
- Hard to input! A semigroup with 1000 elements has 1 million entries in the Cayley table;
- Requires nearly complete knowledge!

Insert semigroup into computer … number 2

Presentations

Words in generators and relations:

$$\langle a, b \mid a^2 = a,\ aba = ba,\ b^2a = ba,\ b^3 = b,\ bab^2 = ba \rangle.$$

Reasons not to:

- Relatively difficult to find! given a semigroup S it can be difficult to find a presentation for S;
- Undecidability! almost every meaningful question is undecidable, i.e. word problem, isomorphism problem, …

Insert semigroup into computer . . . number 3

Generators

Specify generators of a particular type.

Definition

A transformation is a function f from $\{1, \ldots, n\}$ to itself written:

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

A transformation semigroup is just a semigroup consisting of a set of transformations under composition of functions.

Theorem (Cayley's theorem)

Every semigroup is isomorphic to a permutation transformation semigroup.

Fundamental tasks

Input: generators A (transformations, partial perms, matrices, binary relations, partitions, ...) for a semigroup S.

Output:

- the size of S
- membership in S
- factorise elements over the generators
- the number of idempotents ($x^2 = x$)
- the maximal sub(semi)groups
- the ideal structural of S (i.e. Green's relations)
- is S a group? an inverse semigroup? a regular semigroup?
- the automorphism group of S
- the congruences of S...

An algorithm

S acting on itself by right multiplication

Input: a set A of generators (transformations, partial perms, matrices, binary relations, partitions, ...) for a semigroup S.

Output: the elements X of S.

Assumes: we can multiply and check equality.

Supposing the generators are distinct.

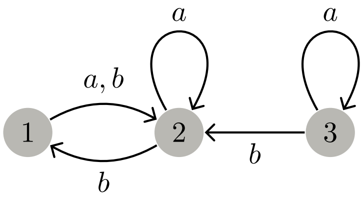
$X := A$
for $x \in X$ **do**
  for $a \in A$ **do**
    if $xa \notin X$ **then**
      append xa to X
return X

An example

Let S be the semigroup generated by the transformations

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix} \qquad \text{and} \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix}.$$

The graph of the actions of a and b:

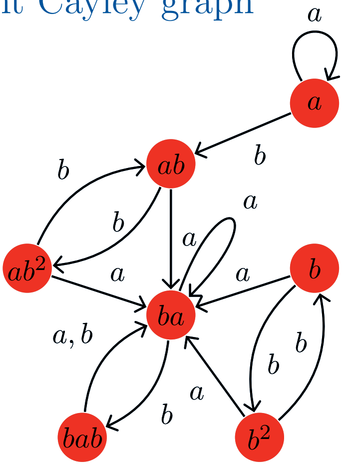


forth

The elements and the right Cayley graph

Edges of the form: $x \xrightarrow{y} xy$

	1	2	3	
a	2	2	3	
b	2	1	2	
ab	1	1	2	*
ba	2	2	2	*
b^2	1	2	1	*
ab^2	2	2	1	*
bab	1	1	1	*



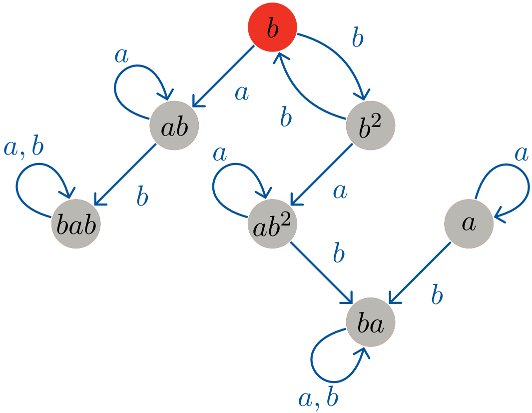
$a^2 = a$, $aba = ba$, $ba^2 = ba$, $b^2a = ba$, $b^3 = b$, $ab^2a = ba$, $ab^3 = ab$, $baba = ba$, $bab^2 = ba$

back forth

The left Cayley graph

Edges of the form $x \xrightarrow{y} yx\ldots$

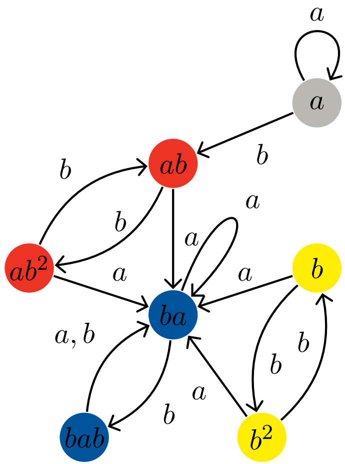
	1	2	3	
a	2	2	3	
b	2	1	2	
ab	1	1	2	$*$
ba	2	2	2	$*$
b^2	1	2	1	$*$
ab^2	2	2	1	$*$
bab	1	1	1	$*$



$a^2 = a$, $aba = ba$, $ba^2 = ba$, $b^2a = ba$, $b^3 = b$, $ab^2a = ba$, $ab^3 = ab$, $baba = ba$, $bab^2 = ba$

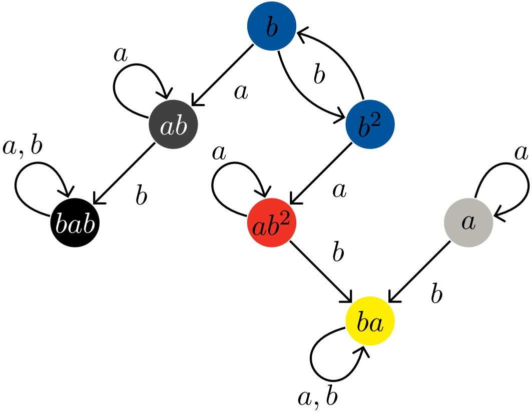
back forth

$\mathscr{R}$-classes



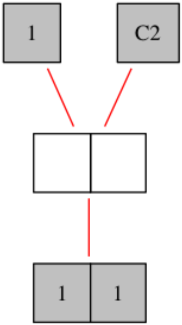
The $\mathscr{R}$-classes are the strongly connected components of the right Cayley graph.

$\mathscr{L}$-classes



The $\mathscr{L}$-classes are the strongly connected components of the left Cayley graph.

The Green's structure



The $\mathscr{D}$-classes are the strongly connected components of the union of the left and right Cayley graphs.

The partial order of the $\mathscr{D}$-classes is the transitive reflexive closure of the quotient of the union of the left and right Cayley graphs by its strongly connected components.

Semigroupe

- V. Froidure and J.-E. Pin, Algorithms for computing finite semigroups, in Foundations of Computational Mathematics, F. Cucker et M. Shub (eds), Berlin, 1997, pp. 112–126, Springer.
- J.-E. Pin, Algorithmic aspects of finite semigroup theory, a tutorial, www.liafa.jussieu.fr/∼jep/PDF/Exposes/StAndrews.pdf
- J.-E. Pin, Semigroupe, C programme, available at www.liafa.jussieu.fr/∼jep/Logiciels/Semigroupe2.0/semigroupe2.html
- The Semigroups package for GAP version 3.0 (not yet released)

GAP and Semigroupe

Pros and Cons

Pros: only requires:

- equality tester
- multiplication

then we can run the algorithm!

Does not use the representation of the semigroup!

Cons:

- has complexity $O(|S||A|)$
- it can be costly to multiply elements
- it can be costly to check if we've seen an element before
- all the elements are stored, which uses lots of memory

Does not use the representation of the semigroup!

The limitations of exhaustive enumeration

n	# transformations	memory	unit
1	1	16	bits
2	4	16	bytes
3	27	162	bytes
4	256	2	kb
5	3 125	~ 30	kb
6	46 656	~ 546	kb
7	823 543	~ 10	mb
8	16 777 216	~ 256	mb
9	387 420 489	~ 6	gb
10	10 000 000 000	~ 186	gb
11	285 311 670 611	~ 6	tb
12	8 916 100 448 256	~ 194	tb
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	n^n	$n^n \cdot n \cdot 16$	bits

Storing the elements of a semigroup is impractical.

Back to semigroups...

Suppose we want to compute the transformation semigroup S generated by:

$$a = (2\ 3), \quad b = (1\ 2\ 3)(4\ 5), \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 2 & 2 \end{pmatrix}.$$

We want to use algorithms from computational group theory.

We do not want to find or store the elements of S.

Schreier's Lemma for semigroups

Suppose that $S = \langle\, A \,\rangle$ acts on the right on a set Ω.

If $\Sigma \subseteq \Omega$, then we denote by S_Σ the group of permutations of Σ induced by elements of the stabiliser of Σ in S.

If $s \in S$ is such that $\Sigma \cdot s = \Sigma$, then s induces a permutation of Σ, denote by $s|_\Sigma$.

Proposition (Linton-Pfeiffer-Robertson-Ruškuc '98)

Let $\{\Sigma_1, \ldots, \Sigma_n\}$ be a s.c.c. of the action of S on $\mathcal{P}(\Omega)$. Then:

(i) *for every $i > 1$, there exist $u_i, v_i \in S$ such that $\Sigma_1 \cdot u_i = \Sigma_i$, $\Sigma_i \cdot v_i = \Sigma_1$, $(u_i v_i)|_{\Sigma_1} = \mathrm{id}_{\Sigma_1}$ and $(v_i u_i)|_{\Sigma_i} = \mathrm{id}_{\Sigma_i}$*

(ii) $S_{\Sigma_1} = \langle\, (u_i a v_j)|_{\Sigma_1} : 1 \leq i, j \leq n,\ a \in A,\ \Sigma_i \cdot a = \Sigma_j \,\rangle$.

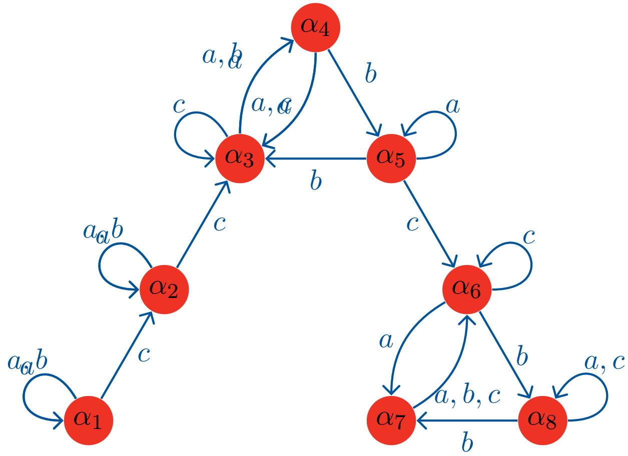
forth

Stabilisers

Let S be the semigroup generated by:

$$a = (2\ 3), \quad b = (1\ 2\ 3)(4\ 5), \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 2 & 2 \end{pmatrix}.$$

α_1	$1, 2, 3, 4, 5$
α_2	$1, 2, 3$
α_3	$1, 3$
α_4	$1, 2$
α_5	$2, 3$
α_6	3
α_7	2
α_8	1



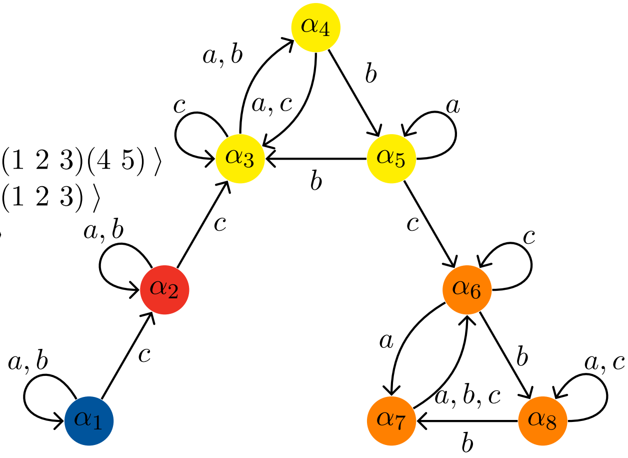
Stabilisers

Let S be the semigroup generated by:

$$a = (2\ 3), \quad b = (1\ 2\ 3)(4\ 5), \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 2 & 2 \end{pmatrix}.$$

α_1	$1, 2, 3, 4, 5$
α_2	$1, 2, 3$
α_3	$1, 3$
α_6	3

$$\begin{aligned} S_{\{1,2,3,4,5\}} &= \langle\, (2\ 3), (1\ 2\ 3)(4\ 5)\,\rangle \\ S_{\{1,2,3\}} &= \langle\, (2\ 3), (1\ 2\ 3)\,\rangle \\ S_{\{1,3\}} &= \langle\, (1\ 3)\,\rangle \\ S_{\{3\}} &= \langle\, \mathrm{id}\,\rangle \end{aligned}$$



Relating the action and the $\mathscr{R}$-classes

Proposition

Let S be a transformation semigroup, let $x \in S$, and let R be the $\mathscr{R}$-class of x in S. Then:

(i) $\{\, \operatorname{im}(y) \,:\, y \in R \,\}$ *is a s.c.c. of the action of* S

(ii) $\{\, y \in R \,:\, \operatorname{im}(y) = \operatorname{im}(x) \,\}$ *is a group isomorphic to the stabiliser* $S_{\operatorname{im}(x)}$

(iii) *if* $\operatorname{im}(y)$ *belongs to the s.c.c. of* $\operatorname{im}(x)$, *then* $S_{\operatorname{im}(x)} \cong S_{\operatorname{im}(y)}$.

An $\mathscr{R}$-class R can be represented by a triple consisting of

- the representative x
- the s.c.c. of $\operatorname{im}(x)$
- the stabiliser $S_{\operatorname{im}(x)}$.

forth

The structure of an $\mathscr{R}$-class

Proposition

Let S be a transformation semigroup, let $x \in S$, and let R be the $\mathscr{R}$-class of x in S. Then:

(i) $\{\, \operatorname{im}(y) \,:\, y \in R \,\}$ *is a s.c.c. of the action of* S

(ii) $\{\, y \in R \,:\, \operatorname{im}(y) = \operatorname{im}(x) \,\}$ *is a group isomorphic to the stabiliser* $S_{\operatorname{im}(x)}$

(iii) *if* $\operatorname{im}(y)$ *belongs to the s.c.c. of* $\operatorname{im}(x)$, *then* $S_{\operatorname{im}(x)} \cong S_{\operatorname{im}(y)}$.

The $\mathscr{R}$-class R_{c^2} of c^2 can be represented by the triple:

- the representative
$$c^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 3 & 3 \end{pmatrix}$$
- the s.c.c. $\{\{1,3\},\{1,2\},\{2,3\}\}$ of $\operatorname{im}(c^2)$
- the stabiliser $S_{\operatorname{im}(c^2)} = S_{\{1,3\}} = \langle\, (1\ 3)\,\rangle$

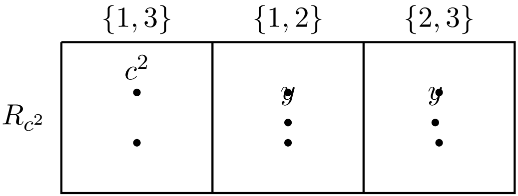
The structure of an $\mathscr{R}$-class

Proposition

(i) $\{\, \mathrm{im}(y) \,:\, y \in R \,\}$ *is a s.c.c. of the action of* S

(ii) $\{\, y \in R \,:\, \mathrm{im}(y) = \mathrm{im}(x) \,\}$ *is a group isomorphic to the stabiliser* $S_{\mathrm{im}(x)}$

(iii) *if* $\mathrm{im}(y)$ *belongs to the s.c.c. of* $\mathrm{im}(x)$, *then* $S_{\mathrm{im}(x)} \cong S_{\mathrm{im}(y)}$.



Finding the $\mathscr{R}$-classes…

Input: a set A of transformations generating a semigroup S.

Output: the $\mathscr{R}$-classes of S.

find the action of S on $\{1, \ldots, n\}$ ▷ the orbit algorithm
find the s.c.c.s of the action ▷ standard graph algorithms
$\mathfrak{R} := \{1\}$ ▷ $\mathscr{R}$-class reps
for $x \in \mathfrak{R}$ **do**
    for $a \in A$ **do**
        if $(ax, y) \notin \mathscr{R}$ for any $y \in \mathfrak{R}$ **then** ▷ see the next slide
            append ax to $\mathfrak{R}$
            return $\mathfrak{R}$.

Validity

Suppose that $S = \langle\, a, b \,\rangle$. If $s \in S$, then write

$$|s| = \text{min. length of a word in } a \text{ and } b \text{ equal to } s.$$

Then

- $a = a \cdot 1 \in \mathfrak{R}$
- $b = b \cdot 1 \in \mathfrak{R}$ if and only if $(a, b) \notin \mathscr{R}$
- $\ldots$
- Suppose $\mathfrak{R} = \{r_1 = a, r_2, \ldots, r_k\}$ contains representatives of $\mathscr{R}$-classes of elements $s \in S$ with $|s| < N$ for some N (and maybe more elements).
- if $s \in S$ and $|s| = N$, then $s = at$ or $s = bt$ for some $t \in S$ with $|t| = N - 1$.
- $(t, r_i) \in \mathscr{R}$ for some i, and so $(s, ar_i) = (at, ar_i) \in \mathscr{R}$ ($\mathscr{R}$ is a left congruence)

The previous algorithm is valid!

Testing membership in an $\mathscr{R}$-class - I

If $x, y \in S$, then $x \mathscr{R} y$ implies that $\ker(x) = \ker(y)$.

For example,

$$bc^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 3 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 3 & 1 & 3 & 3 \end{pmatrix} \notin R_{c^2}$$

since

$$\ker(c^2) = \{\{1\}, \{2, 3, 4, 5\}\} \neq \{\{1, 2, 4, 5\}, \{3\}\} = \ker(bc^2).$$

forth

Testing membership in an $\mathscr{R}$-class - II

Is

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 2 & 2 & 2 \end{pmatrix} \in R_{c^2}?$$

$$S_{\{1,3\}} = \langle\, (1\ 3)\, \rangle$$

	$\{1,3\}$	$\{1,2\}$	$\{2,3\}$
R_{c^2}	c^2 $\vdots$ $c^2(1\ 3)$	c^2b $\vdots$ $c^2(1\ 3)b$	c^2b^2 $\vdots$ $c^2(1\ 3)b^2$

b b b

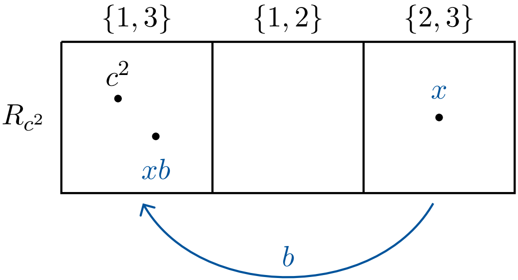
Every element of R_{c^2} is of the form: c^2gb^i where $g \in S_{\{1,3\}}$.

back forth

Testing membership in an $\mathscr{R}$-class - III

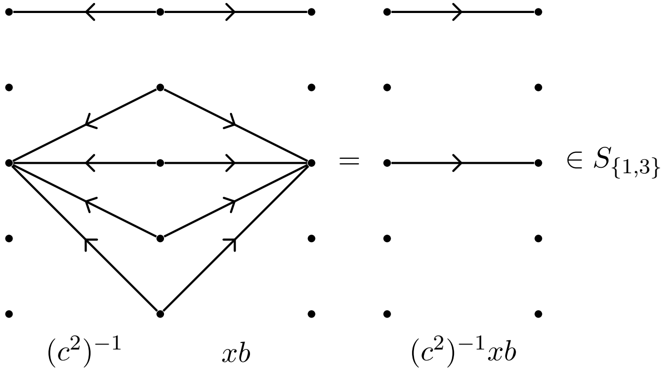
$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 2 & 2 & 2 \end{pmatrix}$$

$$\begin{aligned} x \in R_{c^2} \quad & \text{if and only if} \quad x = c^2 g b^2 \text{ for some } g \in S_{\{1,3\}} = \langle\, (1\ 3)\,\rangle \\ & \text{if and only if} \quad xb = c^2 g \text{ for some } g \in S_{\{1,3\}} = \langle\, (1\ 3)\,\rangle \end{aligned}$$



Testing membership in an $\mathscr{R}$-class - IV

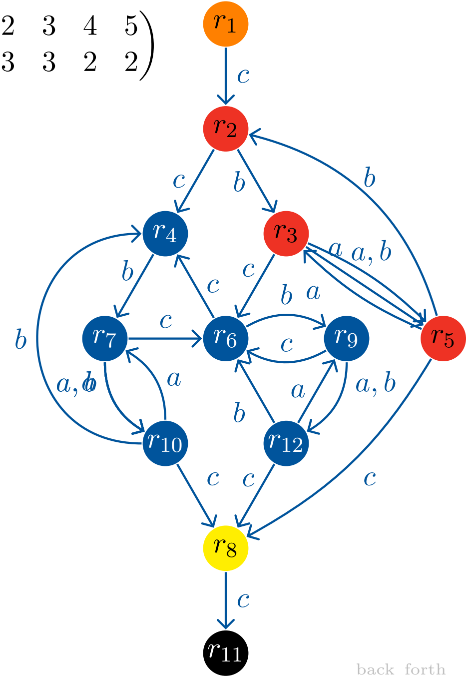
$$x \in R_{c^2} \quad \text{if and only if} \quad xb = c^2 g \text{ for some } g \in S_{\{1,3\}} = \langle\, (1\ 3)\, \rangle$$
$$\text{if and only if} \quad (c^2)^{-1} xb = g \in S_{\{1,3\}} = \langle\, (1\ 3)\, \rangle$$



forth

$$a = (2\ 3),\ b = (1\ 2\ 3)(4\ 5),\ c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 3 & 2 & 2 \end{pmatrix}$$

r_1	a	12345	$1\|2\|3\|4\|5$	$*$
r_2	c	123	$1\|23\|45$	$*$
r_3	bc	123	$12\|3\|45$	$*$
r_4	c^2	13	$1\|2345$	$*$
r_5	abc	123	$13\|2\|45$	$*$
r_6	cbc	13	$145\|23$	$*$
r_7	bc^2	13	$1245\|3$	$*$
r_8	$cabc$	13	$123\|45$	$*$
r_9	$(bc)^2$	13	$12\|345$	$*$
r_{10}	abc^2	13	$1345\|2$	$*$
r_{11}	c^2abc	3	12345	
r_{12}	$a(bc)^2$	13	$13\|245$	



$a \cdot a = \mathrm{id}\ \mathscr{R} a$

$b \cdot a = (1\ 3)(4\ 5)\ \mathscr{R} a$

$$c \cdot a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 2 & 3 & 3 \end{pmatrix}$$

back forth

Complexity

In the worst case the above algorithm has the same complexity as the Froidure-Pin Algorithm $O(|S| \cdot |A|)$ where $S = \langle\, A \,\rangle$. The worst case is realised when S is $\mathscr{J}$-trivial.

In the best case the complexity is the same as that of the Schreier-Sims Algorithm. The best case is realised when S happens to be a group (but maybe doesn't know it).

If $S = T_n$, i.e. S has lots of large subgroups and $\mathscr{R}$-classes, the complexity is $O(2^n)$ compared with $O(n^n)$ for the Froidure-Pin Algorithm.

More theory

It is possible to generalize the technique described above to arbitrary subsemigroups of a regular semigroup.

Examples include:

- semigroups of matrices over finite fields
- subsemigroups of the partition monoid
- semigroups and inverse semigroups of partial permutations
- subsemigroups of regular Rees 0-matrix semigroups
- ....

The theory is described in:

J. East, A. Egri-Nagy, J. D. Mitchell, and Y. Péresse, Computing finite semigroups, `http://arxiv.org/abs/1510.01868`, 45 pages.