Transformation semigroups & minimal ideals

Wilf Wilson

31st March 2015

Computational semigroup theory

- We want to store semigroups and calculate facts about them without needing a list of all the elements to hand.
- Specifying a semigroup by a generating set of transformations is a good way.

Transformations (of a finite set)

What are transformations, and what are they like?

A $\mathbf{transformation}$ of a finite set Ω is a function $f : \Omega \to \Omega$.

We may as well insist that $\Omega = \{1, 2, \ldots, n\}$.
We call a transformation of $\{1, 2, \ldots, n\}$ a *transformation on n points*.

Semigroups

In group theory we have permutation groups.

- e.g. S_n.

In semigroup theory we have transformation semigroups.

- e.g. T_n.

Permutations vs. transformations

We can write permutations in two-line notation:

- e.g. $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$

And we can do the same for transformations:

- e.g. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 3 & 1 \end{pmatrix}$

Permutations vs. transformations

For permutations we have the *order* of a permutation.

- i.e. the least positive integer n such that $g^n = \text{id}$.
- $\langle g \rangle = \{g, g^2, \dots, g^{n-1}, g^n\}$.

For transformations we have the *index* and the *period* of a transformation.

- i.e. the least positive integers m, r such that $f^m = f^{m+r}$.
- $\langle f \rangle = \{f, f^2, \dots, \underbrace{f^m, f^{m+1}, \dots, f^{m+r-1}}_{\text{A cyclic group of order } r}\}$.

The kernel and the image of a transformation

Let f be a transformation on n points.

The **image** of f, $\mathrm{im}(f)$, is the set $\{(i)f : i \in \{1, 2, \ldots, n\}\}$.

The **kernel** of f, $\ker(f)$, is the equivalence relation on $\{1, 2, \ldots, n\}$ which relates i and j whenever $(i)f = (j)f$.

The kernel and the image of a transformation

Let f be a transformation on n points.

The **image** of f, $\mathrm{im}(f)$, is the set $\{(i)f : i \in \{1, 2, \ldots, n\}\}$.

The **kernel** of f, $\ker(f)$, is the equivalence relation on $\{1, 2, \ldots, n\}$ which relates i and j whenever $(i)f = (j)f$.

For a permutation g, $\mathrm{im}(g) = \{1, 2, \ldots, n\}$ and $\ker(g)$ is equality.

Composition of transformations

The operation in a transformation semigroup is *composition of functions*. The composition $f \circ g$ of two transformations f and g is defined by:

$$(x)f \circ g = ((x)f)g \text{ for all } x \in \{1, 2, \ldots, n\}.$$

$$\begin{aligned} \text{Note that } \mathsf{im}(fg) &= \{((x)f)g : x \in \{1, 2, \ldots, n\}\} \\ &= \{(i)g : i \in \mathsf{im}(f)\} \\ &= \mathsf{im}(f) \cdot g \end{aligned}$$

The kernel and image of a transformation: an example

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 2 & 1 & 6 & 1 & 7 & 6 & 2 \end{pmatrix}$

The kernel and image of a transformation: an example

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 2 & 1 & 6 & 1 & 7 & 6 & 2 \end{pmatrix}$

- Then $\mathrm{im}(f) = \{1, 2, 5, 6, 7\}$.

The kernel and image of a transformation: an example

Let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 2 & 1 & 6 & 1 & 7 & 6 & 2 \end{pmatrix}$

- Then $\mathrm{im}(f) = \{1, 2, 5, 6, 7\}$.
- $\ker(f)$ has equivalence classes:

$$\begin{aligned} \{4, 6\} &= (1)f^{-1}, \\ \{1, 3, 9\} &= (2)f^{-1}, \\ \{2\} &= (5)f^{-1} \\ \{5, 8\} &= (6)f^{-1}, \\ \text{and } \{7\} &= (7)f^{-1}. \end{aligned}$$

The rank of a transformation

Let f be a transformation.

The **rank** of f, rank(f), is equal to $|\text{im}(f)|$.

Equivalently:

The **rank** of f is the number of equivalence classes of ker(f).

The rank of a transformation

Let f be a transformation.

The **rank** of f, rank(f), is equal to $|\mathrm{im}(f)|$.

Equivalently:

The **rank** of f is the number of equivalence classes of ker(f).

$$\text{i.e. } \mathrm{rank}(f) = \left| \frac{\{1, 2, \ldots, n\}}{\ker(f)} \right| = |\mathrm{im}(f)|$$

The rank of a transformation

A very important rule to consider when composing transformations is:

$$\mathsf{rank}(xy) \leq \min\{\mathsf{rank}(x), \mathsf{rank}(y)\}$$

The rank of a transformation

A very important rule to consider when composing transformations is:

$$\mathsf{rank}(xy) \leq \min\{\mathsf{rank}(x), \mathsf{rank}(y)\}$$

Proof.

- $\mathsf{rank}(xy) = |\mathsf{im}(xy)| = |\mathsf{im}(x) \cdot y| \leq |\mathsf{im}(x)| = \mathsf{rank}(x)$
- $\mathsf{rank}(xy) = |\mathsf{im}(xy)| = |\mathsf{im}(x) \cdot y| \leq |\{1, 2, \ldots, n\} \cdot y| = \mathsf{rank}(y)$

□

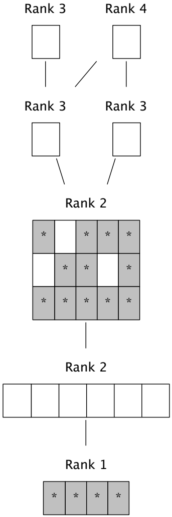
Composition of transformations

Our old example: let $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 2 & 1 & 6 & 1 & 7 & 6 & 2 \end{pmatrix}$

Let g be another transformation.

- Consider two distinct points $i, j \in \mathrm{im}(f)$.
- If $(i)g = (j)g$ then we say that g *collapses the pair* $\{i, j\}$.
  - g collapses some pair in $\mathrm{im}(f)$ if and only if $\mathrm{rank}(fg) < \mathrm{rank}(f)$.

Semigroup diagram: rank



If you have been to a talk about semigroups before, you might recognise these semigroup diagrams.

Notice that rank decreases as you move further down the diagram.

Ideals

Let $S = (S, \cdot)$ be a semigroup and let $I \subseteq S$ be a non-empty subset of S.

Then I is an *ideal* if:

$$I \cdot S \subseteq I \text{ and } S \cdot I \subseteq I.$$

Equivalently:

$$is \in I \text{ and } si \in I \text{ for all } i \in I, s \in S.$$

Ideals

Let $S = (S, \cdot)$ be a semigroup and let $I \subseteq S$ be a non-empty subset of S.

Then I is an *ideal* if:

$$I \cdot S \subseteq I \text{ and } S \cdot I \subseteq I.$$

Equivalently:

$$is \in I \text{ and } si \in I \text{ for all } i \in I, s \in S.$$

I like to think of ideals as **black holes**.

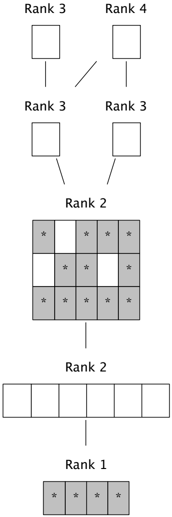
Principal ideals

For a semigroup S and an element $x \in S$ the set:

$$S^1 x S^1$$

is an ideal of S and is called *the principal ideal generated by* x.

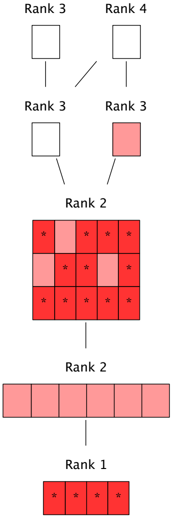
Semigroup diagram: principal ideal



Two elements lie in the same grid if they generate the same principal ideal.

(We call these grids $\mathscr{J}$-classes - this is how they are defined).

Semigroup diagram: principal ideal



Two elements lie in the same grid if they generate the same ideal.

(We call these $\mathscr{D}$- or $\mathscr{J}$-classes - this is how they are defined).

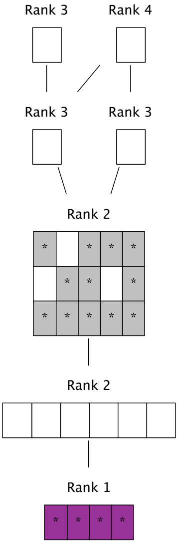
An element in the upper pink $\mathscr{D}$-class generates this ideal.

The minimal ideal

- A finite semigroup has a finite number of ideals.
- The intersection of two ideals is an ideal.

Therefore a finite semigroup has a *minimal ideal* (w.r.t. containment).

Semigroup diagram: minimal ideal



Minimal ideal $\leftrightarrow$ minimal rank

Let S be a finite transformation semigroup, and let $x \in S$.

$$x \text{ is in the minimal ideal of } S \Leftrightarrow \text{rank}(x) \text{ is smallest possible in } S.$$

That is, the minimal ideal is precisely the set of elements of minimal rank.

Aim

For various reasons, we wish to be able to quickly get hold of an element of the minimal ideal of a transformation semigroup.

Aim

For various reasons, we wish to be able to quickly get hold of an element of the minimal ideal of a transformation semigroup.

For example:

Aim

For various reasons, we wish to be able to quickly get hold of an element of the minimal ideal of a transformation semigroup.

For example:

- To see if the semigroup is synchronising.

Aim

For various reasons, we wish to be able to quickly get hold of an element of the minimal ideal of a transformation semigroup.

For example:

- To see if the semigroup is synchronising.
- To calculate the zero of a semigroup (or prove it doesn't exist).

Aim

For various reasons, we wish to be able to quickly get hold of an element of the minimal ideal of a transformation semigroup.

For example:

- To see if the semigroup is synchronising.
- To calculate the zero of a semigroup (or prove it doesn't exist).
- To calculate all the *other* elements of the minimal ideal.

Ways of calculating

- **BAD**: getting all of the elements and looking at them in turn.
  - Exponential complexity in n.
- **BETTER**: using the ideas I'm about to share.
  - Quadratic complexity in n.
  - Joint work with James Mitchell.

An example

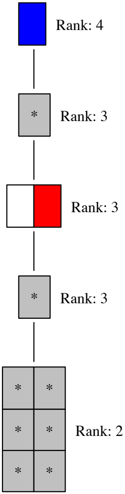
Let $S = \langle \sigma, \tau \rangle$ where:

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

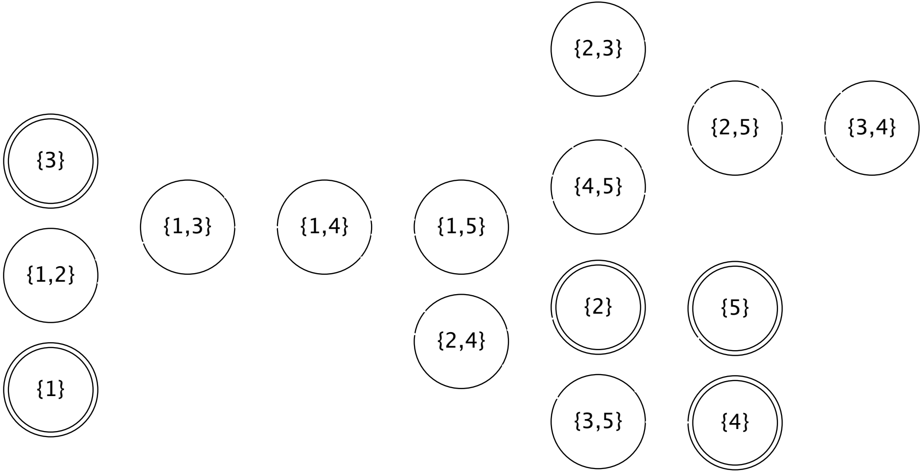
and

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

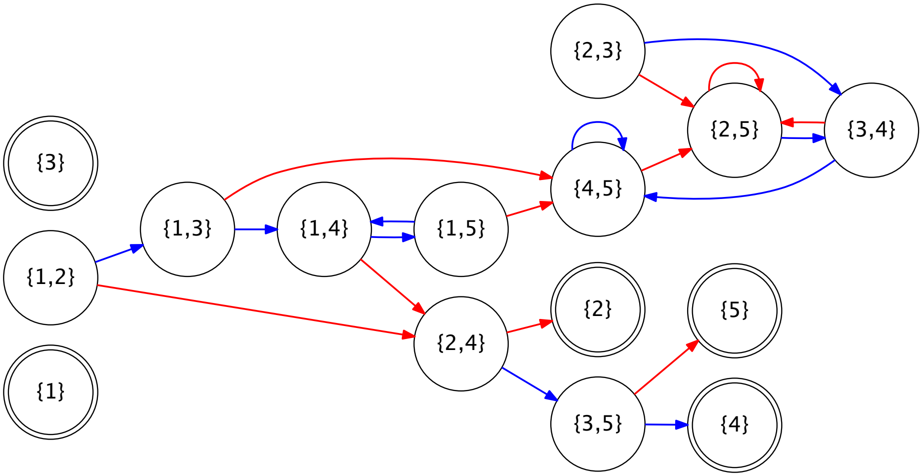
are transformations on 5 points.



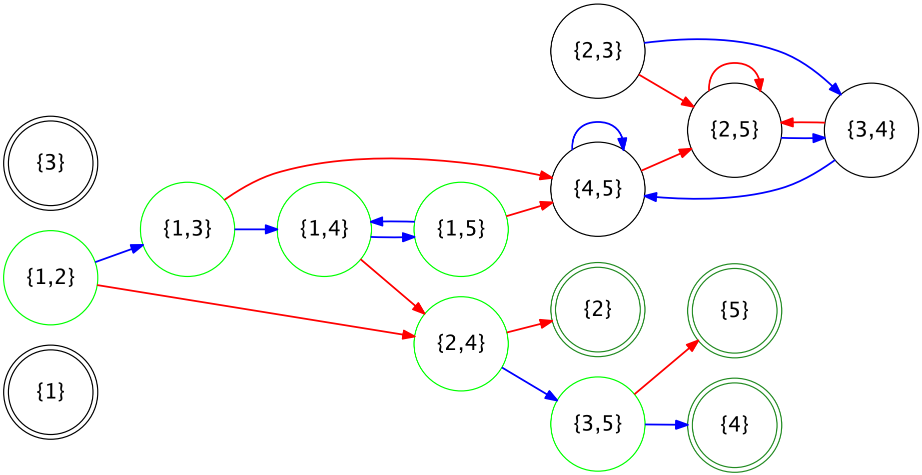
The graph: the $\binom{5}{2} + 5$ vertices



The graph: the $\binom{5}{2} \cdot 2$ edges



The graph: the 6 collapsible pairs



The two types of pairs

The $\binom{5}{2} = 10$ pairs fall into two types: those which can be collapsed, and those which can not.

The two types of pairs

The $\binom{5}{2} = 10$ pairs fall into two types: those which can be collapsed, and those which can not.

Our collapsible pairs:

$$\begin{aligned} \{3,5\}\sigma &= \{4\} \\ \{2,4\}\tau &= \{2\} \\ \{1,2\}\tau^2 &= \{2\} \\ \{1,4\}\tau^2 &= \{2\} \\ \{1,3\}\sigma\tau^2 &= \{2\} \\ \{1,5\}\sigma\tau^2 &= \{2\} \end{aligned}$$

The other pairs:

$$\begin{gathered} \{2,3\} \\ \{2,5\} \\ \{3,4\} \\ \{4,5\} \end{gathered}$$

Every element in S must have different images for i and j if $\{i,j\}$ is not collapsible.

The idea

S must have an element x with minimal rank r.

- Take an element $f \in S$.
- Then $f \cdot x$ also has minimal rank.

$\Rightarrow$ We can right-multiply any f to obtain an element of minimal rank.
$\Rightarrow$ For any non-minimal f, there is a collapsible pair of points in im(f).

- Start with any $f \in S$, and collapse pairs until you can't.
- You now have an element of the minimal ideal.

Let's do it

Our collapsible pairs:

$$\{3,5\}\sigma = \{4\}$$
$$\{2,4\}\tau = \{2\}$$
$$\{1,2\}\tau^2 = \{2\}$$
$$\{1,4\}\tau^2 = \{2\}$$
$$\{1,3\}\sigma\tau^2 = \{2\}$$
$$\{1,5\}\sigma\tau^2 = \{2\}$$

Let's do it

Our collapsible pairs:

Let $r_0 = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 4 \end{pmatrix}$

$$\{3,5\}\sigma = \{4\}$$
$$\{2,4\}\tau = \{2\}$$
$$\{1,2\}\tau^2 = \{2\}$$
$$\{1,4\}\tau^2 = \{2\}$$
$$\{1,3\}\sigma\tau^2 = \{2\}$$
$$\{1,5\}\sigma\tau^2 = \{2\}$$

Let's do it

Our collapsible pairs:

$$\{3,5\}\sigma = \{4\}$$
$$\{2,4\}\tau = \{2\}$$
$$\{1,2\}\tau^2 = \{2\}$$
$$\{1,4\}\tau^2 = \{2\}$$
$$\{1,3\}\sigma\tau^2 = \{2\}$$
$$\{1,5\}\sigma\tau^2 = \{2\}$$

Let $r_0 = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 4 \end{pmatrix}$

Collapse pair $\{3,5\}$ in im(r_0):

$$r_1 := r_0\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 4 & 5 \end{pmatrix}$$

Let's do it

Our collapsible pairs:

$$\{3,5\}\sigma = \{4\}$$
$$\{2,4\}\tau = \{2\}$$
$$\{1,2\}\tau^2 = \{2\}$$
$$\{1,4\}\tau^2 = \{2\}$$
$$\{1,3\}\sigma\tau^2 = \{2\}$$
$$\{1,5\}\sigma\tau^2 = \{2\}$$

Let $r_0 = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 4 \end{pmatrix}$

Collapse pair $\{3,5\}$ in im(r_0):

$$r_1 := r_0\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 4 & 5 \end{pmatrix}$$

Collapse pair $\{1,4\}$ in im(r_1):

$$r_2 := r_1\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 5 & 2 & 5 \end{pmatrix}$$

Let's do it

Our collapsible pairs:

$$\begin{aligned}\{3,5\}\sigma &= \{4\}\\ \{2,4\}\tau &= \{2\}\\ \{1,2\}\tau^2 &= \{2\}\\ \{1,4\}\tau^2 &= \{2\}\\ \{1,3\}\sigma\tau^2 &= \{2\}\\ \{1,5\}\sigma\tau^2 &= \{2\}\end{aligned}$$

Let $r_0 = \sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 5 & 4\end{pmatrix}$

Collapse pair $\{3,5\}$ in $\text{im}(r_0)$:

$$r_1 := r_0\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 4 & 5 & 4 & 5\end{pmatrix}$$

Collapse pair $\{1,4\}$ in $\text{im}(r_1)$:

$$r_2 := r_1\tau^2 = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 2 & 5 & 2 & 5\end{pmatrix}$$

No collapsible pairs $\Rightarrow r_2$ minimal.

End.