Computing with finite semigroups

Wilf Wilson
University of St Andrews

2nd June 2015

Semigroup

Definition

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

Semigroup

Definition

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

The operation combines two elements a and b in S to give a third, $a * b$.
Associativity means that for any three elements, $a * (b * c) = (a * b) * c$.

Groups versus semigroups

- There are 2 groups of order 10.
- There are $12,418,001,077,381,302,684$ semigroups of order 10.

Simple example: $\mathbb{N}$

$\mathbb{N} = \{1, 2, 3, \ldots\}$ with addition.

- the sum of two natural numbers is a natural number
- addition is associative

Subsemigroups of $\mathbb{N}$ are called *numeric* semigroups.

A fundamental example: T_n

T_n, the *full transformation semigroup*: the set of all functions from $\{1, 2, \ldots, n\}$ to itself, with composition of functions.

T_n is analogous to the symmetric group S_n in group theory.

Subsemigroups of T_n are called *transformation* semigroups.

The motivation

People want to study algebra.

Given a semigroup S you might want to know some algebraic properties:

- How big is S?
- What are the congruences on S?
- Is S a group?
- Is the operation on S commutative?

This is well-developed for group theory.

Suitable types of semigroup for a computer

Suitable types of semigroup for a computer

- Semigroups of numbers
  - An element can be stored as a number.

Suitable types of semigroup for a computer

- Semigroups of numbers
  - An element can be stored as a number.
- Semigroups of transformations
  - An element can be stored as a list of numbers.
  - [1, 3, 2, 3] could represent $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 2$, $4 \mapsto 3$.

Suitable types of semigroup for a computer

- Semigroups of numbers
  - An element can be stored as a number.
- Semigroups of transformations
  - An element can be stored as a list of numbers.
  - `[ 1, 3, 2, 3 ]` could represent $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 2$, $4 \mapsto 3$.
- Semigroups of square matrices over a ring
  - An element can be stored as a list of lists of ring elements.
  - `[ [ 1, 0 ], [ 0, 1 ] ]` could be the identity matrix.

Suitable types of semigroup for a computer

- Semigroups of numbers
  - An element can be stored as a number.
- Semigroups of transformations
  - An element can be stored as a list of numbers.
  - `[ 1, 3, 2, 3 ]` could represent $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 2$, $4 \mapsto 3$.
- Semigroups of square matrices over a ring
  - An element can be stored as a list of lists of ring elements.
  - `[ [ 1, 0 ], [ 0, 1 ] ]` could be the identity matrix.
- Semigroups of binary relations
  - Stored as a list of pairs.
  - `[ [ 1, 1 ], [ 2, 2 ], [ 3, 3 ], [ 4, 4 ], [ 1, 2 ], [ 1, 3 ], [ 1, 4 ], [ 2, 4 ] ]` could represent the divisibility relation on $\{1, 2, 3, 4\}$.

The benefits

- Helps people learn about semigroups.
- Helps people test hypotheses, finding counter-examples, etc.
- Helps people notice patterns.
  - It can direct pure mathematics research.

The benefits

- Helps people learn about semigroups.
- Helps people test hypotheses, finding counter-examples, etc.
- Helps people notice patterns.
  - It can direct pure mathematics research.
- Leads to a lot of collaboration with the computer science.
- The ideas behind the algorithms might have application elsewhere.

The difficulty

T_{10} has 10^{10} elements.

If each element needs 100 bytes of memory, we'll need 10^{12} bytes in total.

- We need to calculate without having all the elements to hand.

If a calculation involves looking at all 10^{10} elements, that will be slow.

- We need to calculate without needing to look at every element.

Generators

We can define a semigroup by a *generating set*.
This saves us having to store all the elements.

e.g. $\mathbb{N}$ is generated by 1.

If a, b, c are three transformations in T_n then
$S = \langle a, b, c \rangle$ is the semigroup consisting of all products involving a, b, c.

Commutativity

A semigroup is commutative if $a * b = b * a$ for all $a, b \in S$.

Commutativity

A semigroup is commutative if $a * b = b * a$ for all $a, b \in S$.

Proposition

A semigroup S is commutative if and only if its generators commute.

A case study: commutativity of T_{10}

T_{10} has 10^{10} elements! But T_{10} is generated by 3 elements: $X = \{a, b, c\}$.

So we can determine whether T_{10} is commutative in ≤ 6 multiplications:

```
for { a, b } in X :
 if not a * b = b * a then :
  return false
return true
```

End.