Word Problems for Semigroups, Monoids and Groups
The Burn 2010

Markus Pfeiffer
markusp@mcs.st-and.ac.uk

University of St Andrews

2010-06-02
Motivation

- How to define basic algebraic structures
Motivation

- How to define basic algebraic structures
- How to define them in a potentially computing-device friendly way
Motivation

- How to define basic algebraic structures
- How to define them in a potentially computing-device friendly way
- ...and then let the computer help us
Motivation

- How to define basic algebraic structures
- How to define them in a potentially computing-device friendly way
- ...and then let the computer help us
- Today, we want Semigroups, Monoids and Groups
Motivation

- How to define basic algebraic structures
- How to define them in a potentially computing-device friendly way
- ... and then let the computer help us
- Today, we want Semigroups, Monoids and Groups
- Okay, I will be honest, I will mainly talk about Semigroups, Monoids and Groups are just special cases.
Semigroups, Monoids, Groups

Definition

Let $S$ be a set together with a binary operation $\circ : S \times S \to S$. 

$S$ is a semigroup, if for all $x, y, z$ in $S$

$$x \circ (y \circ z) = (x \circ y) \circ z$$

$S$ is a monoid, if additionally there exists some $e$ in $S$ such that for all $x$ in $S$

$$e \circ x = x \circ e = x$$

$S$ is a group, if additionally for all $x$ in $S$ there is $x'$ in $S$ such that

$$x \circ x' = x' \circ x = e$$

the inverse of $x$
Semigroups, Monoids, Groups

Definition
Let $S$ be a set together with a binary operation $\circ : S \times S \rightarrow S$.

- $S$ is a *semigroup*, if for all $x, y, z$ in $S$

  \[ x \circ (y \circ z) = (x \circ y) \circ z \]

  $\circ$ is *associative*
Semigroups, Monoids, Groups

Definition
Let $S$ be a set together with a binary operation $\odot : S \times S \to S$.

- $S$ is a **semigroup**, if for all $x, y, z$ in $S$
  \[ x \odot (y \odot z) = (x \odot y) \odot z \]

  $\odot$ is **associative**

- $S$ is a **monoid**, if additionally there exists some $e$ in $S$ such that for all $x$ in $S$
  \[ e \odot x = x \odot e = x \]

  $e$ is the **identity** of $S$
Semigroups, Monoids, Groups

Definition

Let \( S \) be a set together with a binary operation \( \circ : S \times S \rightarrow S \).

- \( S \) is a **semigroup**, if for all \( x, y, z \) in \( S \)
  \[ x \circ (y \circ z) = (x \circ y) \circ z \]
  \( \circ \) is **associative**

- \( S \) is a **monoid**, if additionally there exists some \( e \) in \( S \) such that for all \( x \) in \( S \)
  \[ e \circ x = x \circ e = x \]
  \( e \) is the **identity** of \( S \)

- \( S \) is a **group**, if additionally for all \( x \) in \( S \) there is \( x' \) in \( S \) such that
  \[ x \circ x' = x' \circ x = e \]
  \( x' \) the **inverse** of \( x \)
Better have some examples!

Example
Better have some examples!

Example

- \((\mathbb{N}, +)\) is a semigroup
Better have some examples!

Example

- $(\mathbb{N}, +)$ is a semigroup
- For any set $M$, $(P(M), \cup)$ is a monoid
...Better have some examples!

Example

- $(\mathbb{N}, +)$ is a semigroup
- For any set $M$, $(P(M), \cup)$ is a monoid
- Choose your favourite group
... Better have some examples!

Example

- \((\mathbb{N}, +)\) is a semigroup
- For any set \(M\), \((P(M), \cup)\) is a monoid
- Choose your favourite group

- groups are much more popular than monoids or semigroups
Better have some examples!

Example

- $(\mathbb{N}, +)$ is a semigroup
- For any set $M$, $(P(M), \cup)$ is a monoid
- Choose your favourite group

- groups are much more popular than monoids or semigroups
- And we seem to know how to work with our favourite algebraic structure,
...Better have some examples!

Example

- $(\mathbb{N}, +)$ is a semigroup
- For any set $M$, $(P(M), \cup)$ is a monoid
- Choose your favourite group

- groups are much more popular than monoids or semigroups
- And we seem to know how to work with our favourite algebraic structure,
- But we want computers to do the hard work.
How to tell your (theoretical) computer

- Finite Stuff, Naturals, Rationals, some Reals we get for “free”
- Groups: Permutations, Matrices
- Semigroups, Monoids: ?
Why strings are a natural representation for Semigroups, Monoids and Groups

Let $A$ be a finite set.

- A string is a finite sequence of elements of $A$
- $A^*$ the set of all strings over $A$
- $A^+$ the set of all nonempty strings over $A$

Example

Let $A := \{a, b\}$.

- $\epsilon$, $a$, $ab$, $ba$, $abaabaababaaabab$ are strings
- If $x$ and $y$ are strings, the concatenation $xy$ is a string.
- $A^+$ together with concatenation is a (very special!) semigroup.
- $A^*$ together with concatenation is a (very special!) monoid.
- We can do this for groups, but it is slightly more complicated.
So why are $A^+$ and $A^*$ special?

- Suppose $S$ is some semigroup.
- Take any map $f : A \rightarrow S$
- Then $f$ can be extended into a unique semigroup homomorphism
  \[ \varphi : A^+ \rightarrow S \]
- And in some cases we can choose $f$ such that all elements of $S$ can be represented by at least one string.
- Then we call $A$ a set of generators for $S$
- (Sets of) strings are something computers can deal with very nicely!
Finite State Automata \texttt{fsa}

\[ \mathcal{A} = \langle Q, A, q_0, F, \Delta \rangle \]

\[ L = \{ ac^i \mid i \in \mathbb{N} \} \cup \{ bc^k \mid k \equiv_3 0 \} \subseteq A^* \text{ (called language).} \]
Asynchronous (2-tape) Finite State Automata (afsa)

\[ \mathcal{A} = \langle Q, A, A, q_0, F, \Delta \rangle \]

\[ R = \{ (ac^i, ac^i) \mid i \in \mathbb{N} \} \cup \{ (ab^k, ac^{3k}) \mid k \in \mathbb{N} \} \subseteq A^+ \times A^+ , \]
rational relations.
The Word Problem

Definition
Let $S$ be a semigroup such that for some finite set $A$ and a choice for $f$, the homomorphism $\varphi : A^+ \rightarrow S$ is surjective. We call the set

$$WP(S, A) := \{(v, w) \mid \varphi(v) = \varphi(w)\} \subseteq A^+ \times A^+$$

the word problem of $S$ with respect to the set $A$. 
The Word Problem

Definition
Let $S$ be a semigroup such that for some finite set $A$ and a choice for $f$, the homomorphism $\varphi : A^+ \rightarrow S$ is surjective. We call the set

$$WP(S, A) := \{(v, w) | \varphi(v) = \varphi(w)\} \subseteq A^+ \times A^+$$

the *word problem* of $S$ with respect to the set $A$.

- We want a computer to be able to tell whether a pair of strings is in $WP(S, A)$. 

The Word Problem

Definition
Let $S$ be a semigroup such that for some finite set $A$ and a choice for $f$, the homomorphism $\varphi : A^+ \to S$ is surjective. We call the set

$$WP(S, A) := \{(v, w) | \varphi(v) = \varphi(w)\} \subseteq A^+ \times A^+$$

the word problem of $S$ with respect to the set $A$.

- We want a computer to be able to tell whether a pair of strings is in $WP(S, A)$.
- But you can’t always get what you want:
The Word Problem

Definition
Let $S$ be a semigroup such that for some finite set $A$ and a choice for $f$, the homomorphism $\varphi : A^+ \rightarrow S$ is surjective. We call the set

$$WP(S, A) := \{(v, w) \mid \varphi(v) = \varphi(w)\} \subseteq A^+ \times A^+$$

the word problem of $S$ with respect to the set $A$.

- We want a computer to be able to tell whether a pair of strings is in $WP(S, A)$.
- But you can’t always get what you want:
- This is fundamentally undecidable, even for groups.
Word Problems decided by \textit{afsa}

Defined $\text{WP}(S, A) \subseteq A^+ \times A^+$. Try using \textit{afsa}.

- Are there semigroups $S$ with $\text{WP}(S, A)$ accepted by an \textit{afsa}?
Word Problems decided by **afsa**

Defined $\text{WP} \left( S, A \right) \subseteq A^+ \times A^+$. Try using **afsa**.

- Are there semigroups $S$ with $\text{WP}(S, A)$ accepted by an **afsa**?
- Short answer: Yes.
Examples and Counterexamples

Examples

- All finite semigroups (in particular all finite groups).

Counterexamples
Examples and Counterexamples

Examples

- All finite semigroups (in particular all finite groups).
- $(\mathbb{N}, +)$

Counterexamples

$T := (\mathbb{N} \times \mathbb{N}, +)$

All infinite groups. All semigroups $S$ with $T \leq S$ finitely generated and nonrational word problem.
Examples and Counterexamples

Examples

- All finite semigroups (in particular all finite groups).
- \((\mathbb{N}, +)\)
- (other examples)

Counterexamples
Examples and Counterexamples

Examples
- All finite semigroups (in particular all finite groups).
- $(\mathbb{N}, +)$
- (other examples)

Counterexamples
- $T := (\mathbb{N} \times \mathbb{N}, +)$
Examples and Counterexamples

Examples

- All finite semigroups (in particular all finite groups).
- $\langle \mathbb{N}, + \rangle$
- (other examples)

Counterexamples

- $T := (\mathbb{N} \times \mathbb{N}, +)$
- All infinite groups.
Examples and Counterexamples

Examples

- All finite semigroups (in particular all finite groups).
- \((\mathbb{N}, +)\)
- (other examples)

Counterexamples

- \(T := (\mathbb{N} \times \mathbb{N}, +)\)
- All infinite groups.
- All semigroups \(S\) with \(T \leq S\) finitely generated and non rational word problem.
Generating Set

Theorem

Let $S = Sg\langle A \rangle$, finite set $A$ and $WP(S, A)$ rational. Then

- $B := A \cup \{b\}$ then $WP(S, B)$ is rational.
- $C := A \setminus \{a\}$ then $WP(T, C)$ is rational.

In particular, rational word problem is independent of choice of $A$ and $f$ and thus a property of the semigroup itself.
The direct product (and why semigroups can be nasty)

Theorem

If $S \times T$ is finitely generated and has rational word problem, then $S$ and $T$ are finitely generated and have rational word problem.

Converse?
The direct product (and why semigroups can be nasty)

Theorem
If $S \times T$ is finitely generated and has rational word problem, then $S$ and $T$ are finitely generated and have rational word problem.

Converse?

Example
Let $S$, $T$ be infinite monogenic semigroups.
The direct product (and why semigroups can be nasty)

Theorem

If $S \times T$ is finitely generated and has rational word problem, then $S$ and $T$ are finitely generated and have rational word problem.

Converse?

Example

Let $S, T$ be infinite monogenic semigroups.

- $S \times T$ is not even finitely generated.
The direct product (and why semigroups can be nasty)

Theorem
If $S \times T$ is finitely generated and has rational word problem, then $S$ and $T$ are finitely generated and have rational word problem.

Converse?

Example
Let $S, T$ be infinite monogenic semigroups.
- $S \times T$ is not even finitely generated.
- $S^1 \times T^1$ is finitely generated, isomorphic to $\text{Mon} \langle a, b | ab = ba \rangle$ no rational word problem.
The direct product (and why semigroups can be nasty)

**Theorem**

*If* $S \times T$ *is finitely generated and has rational word problem, then* $S$ *and* $T$ *are finitely generated and have rational word problem.*

Converse?

**Example**

Let $S, T$ be infinite monogenic semigroups.

- $S \times T$ is not even finitely generated.
- $S^1 \times T^1$ is finitely generated, isomorphic to $\text{Mon} \langle a, b \mid ab = ba \rangle$ no rational word problem.

Furthermore
The direct product (and why semigroups can be nasty)

Theorem
If \( S \times T \) is finitely generated and has rational word problem, then \( S \) and \( T \) are finitely generated and have rational word problem.

Converse?

Example
Let \( S, T \) be infinite monogenic semigroups.

- \( S \times T \) is not even finitely generated.
- \( S^1 \times T^1 \) is finitely generated, isomorphic to \( \text{Mon} \langle a, b \mid ab = ba \rangle \) no rational word problem.

Furthermore

- \( T := \text{Sg} \langle a, b \mid a^2 = a, ba = b \rangle \), then \( T \times T \) rational word problem.
The direct product (and why semigroups can be nasty)

**Theorem**

*If* $S \times T$ *is finitely generated and has rational word problem, then* $S$ *and* $T$ *are finitely generated and have rational word problem.*

Converse?

**Example**

Let $S$, $T$ be infinite monogenic semigroups.

- $S \times T$ is not even finitely generated.
- $S^1 \times T^1$ is finitely generated, isomorphic to $\text{Mon} \langle a, b \mid ab = ba \rangle$ no rational word problem.

Furthermore

- $T := \text{Sg} \langle a, b \mid a^2 = a, ba = b \rangle$, then $T \times T$ rational word problem.
- If $S$ is infinite, has rational word problem, $T$ finite and $S \times T$ is finitely generated then $S \times T$ has rational word problem.
My research wants “Easily Solvable Word Problem”

- Rational word problem is easy
- But for $T := Sg \langle a, b | ab = ba \rangle$ word problem is “easy” too:

\[(v, w) \in WP(T, \{a, b\}) \iff |v|_a = |w|_a \text{ and } |v|_b = |w|_b\]

($v$ and $w$ contain the same number of $a$ and the same number of $b$ each.)

- Problem: Finite state devices cannot count (in $\mathbb{N}$)
- Solution: We dont need to count! Use two fsa that work independently on the same input. Accept when both accept.
Thanks for listening!