Intersections of Principal Ideals of a Free Monoid Presentation

Scott Carson
(Supervised by Prof. Victoria Gould)

University of York

May 16, 2018

Free Monoids

- Let A be a non-empty set (called an alphabet).
- Next, let A^+ denote the set of all finite non-empty words of the form $a_1a_2\dots a_n$ where each $a_i \in A$.
- Finally, define a binary operation, $\cdot$, on A^+ as follows,

$$(a_1a_2\dots a_n)\cdot(b_1b_2\dots b_m) = a_1a_2\dots a_nb_1b_2\dots b_m.$$

Then we say $(A^+,\cdot)$ is a free semigroup. A free monoid is a free semigroup with an identity element, usually denoted ϵ, called the empty word. We write $A^* = A^+ \cup \{\epsilon\}$ so that $(A^*,\cdot)$ denotes the free monoid with alphabet A.

Presentations

Let A be an alphabet and let $\rho \subseteq A^* \times A^*$ be a set of relations, then a free monoid presentation, say M, is denoted $M = \langle A : \rho \rangle$.

Example

If $A = \{a, b\}$ and $\rho = \{(aba, baa), (bba, bab)\}$ then we obtain a free monoid presentation,

$$\begin{aligned} M &= \langle A : \rho \rangle \\ &= \langle a, b : aba = baa, bba = bab \rangle. \end{aligned}$$

A typical element in M is simply a word in A^*, but what about the equivalence classes?!

Equivalence classes

For some word $w \in M$, the equivalence class of w is written $[w]_\rho$. Given two words $w, w' \in [w]_\rho$, we will write $w \sim_\rho w'$.

Definition

In a free monoid presentation $\langle A : \rho \rangle$, we have $w \sim_\rho w'$ iff for some $n \in \mathbb{N}$ there exists a sequence of the form,

$$\begin{aligned} w &= c_1 p_1 d_1, \\ c_1 p_1' d_1 &= c_2 p_2 d_2, \\ &\vdots \\ c_{n-1} p_{n-1}' d_{n-1} &= c_n p_n d_n, \\ c_n p_n' d_n &= w'. \end{aligned}$$

where $c_i, d_i \in M$ and $(p_i, p_i') \in \rho$ for each $1 \leq i \leq n$.

The Big Questions

Let $M = \langle A : \rho \rangle$ be a free monoid presentation where $A = \{a, b, u_i, v_i : 1 \leq i \leq n\}$ and $\rho = \{(au_i, bv_i) : 1 \leq i \leq n\}$ for some $n \in \mathbb{N}$.

- Can we show that M is cancellative and that the intersection of principal right ideals of M are either empty, principal or n-generated?
- If we allow letters in M to commute, is M cancellative? Are the intersections of principal ideals finitely generated?

Cancellativity

How do we define cancellativity of a semigroup?

Definition

A semigroup S is *cancellative* iff for all $a, b, c \in S$, whenever $ab = ac \Rightarrow b = c$ and dually $ba = ca \Rightarrow b = c$.

A trivial example of a cancellative semigroup is a group!

Example

$(\mathbb{N}, +)$ is a cancellative semigroup.

Hence, we must show for all words $u, v, w \in M$, whenever $wu \sim_\rho wv \Rightarrow u \sim_\rho v$ and likewise $uw \sim_\rho vw \Rightarrow u \sim_\rho v$. How do we decide when two words are related in the first place? Can we write down the equivalence classes?

Initial observations

Some initial observations to make:

- If two words are ρ-related, they must have the same length. However, the converse is not true in general!
- Suppose for some letters $x_1, x_2, x_3 \in A$, the word $x_1x_2x_3$ appears as a factor of the word $w \in M$ (that is, $w = w_0x_1x_2x_3w_1$ for some $w_0, w_1 \in M$). If $x_1x_2 = au_i$ or bv_i for some i, then x_2x_3 cannot be equal to au_j or bv_j for some j. (Dually for $x_2x_3 = au_i$ or bv_i...)

Example

We have $abv_iu_i \sim_\rho a^2u_i^2$.

Finding $[w]_\rho$

For notation, let us define some new sets $R_i = \{au_i, bv_i\}$ for all $1 \leq i \leq n$. Also, let us write for $n \in \mathbb{N}$,

$$w_{(0,n)} = w_0 p_1 w_1 \dots w_{n-1} p_n w_n,$$
$$w'_{(0,n)} = w_0 p'_1 w_1 \dots w_{n-1} p'_n w_n,$$

where $w_i \in M$ and each $(p_i, p'_i) \in R_j \times R_j$ for some i. We will use the notation $w_{(r,s)}$ and $w'_{(r,s)}$ in a similar fashion.

Result 1

Let $w, w' \in M$, then $w \sim_\rho w'$ iff $w = w'$ or there exists an $n \in \mathbb{N}$ where $w = w_{(0,n)}$ and $w' = w'_{(0,n)}$ such that each $(p_i, p'_i) \in R_j \times R_j$ for some $1 \leq j \leq n$.

Examples...

Example

Trivially, for any $w = w_{(0,n)}$ we always have $w_{(0,n)} \sim_\rho w_{(0,n)}$.

Example

More generally, if $w = w_{(0,n)}$ and $w' = w'_{(0,n)}$ (with $w \neq w'$), then we have a sequence,

$$\begin{aligned} w_{(0,n)} &= w_0 p_1 w_{(1,n)}, \\ w_0 p'_1 w_{(1,n)} &= w'_{(0,1)} p_2 w_{(2,n)}, \\ &\vdots \\ w'_{(0,n-2)} p'_{n-1} w_{(n-1,n)} &= w'_{(0,n-1)} p_n w_n, \\ w'_{(0,n-1)} p'_n w_n &= w'_{(0,n)}. \end{aligned}$$

By definition, $w_{(0,n)} \sim_\rho w'_{(0,n)}$.

Cancellativity

Using this result, we were able to show that M is cancellative!

Sketch Proof.

Consider $uw \sim_\rho vw$ (as before). If $uw = vw$ then clearly we can cancel. If not, then for some $n \in \mathbb{N}$ we have $uw = w_{(0,n)}$ and $vw = w'_{(0,n)}$. We now have 4 possibilities where the cancellation can take place (see expertly drawn diagram). In all cases, when we cancel w, we can rewrite $u = w_{(0,m)}$ and $v = w'_{(0,m)}$ for $n \leq m$ and so they are related. Dually for left cancellativity. □

Example

From $abv_1u_2aau_2 \sim_\rho aau_1u_2abv_2$, we have $abv_1 \sim_\rho aau_1$ and $u_2aau_2 \sim_\rho u_2abv_2$.

Intersections of principal right ideals

For a word $w \in M$, we write $wM = \{ws : s \in M\}$ and let us define $r_\rho(w, w') = \{(s, t) : ws \sim_\rho w't\}$.

Result 2

Let $w, w' \in M$, then $wM \cap w'M$ can be described as follows,

- empty if $r_\rho(w, w') = \emptyset$,
- principal if (s, ϵ) or $(\epsilon, t) \in r_\rho(w, w')$ for some $s, t \in M$,
- n-generated otherwise

Example

For some i we have $u_iM \cap v_iM = \emptyset$, $abM \cap aM = abM$ and $aM \cap bM = \bigcup_i au_iM$.

Commutativity

Some questions we may need to consider when M is commutative:

- Can we describe the equivalence class $[w]_\rho$ in the same way as the non-commutative case?
- If so, how are we able to?
- Is it possible to use an algorithm to decide when $w \sim_\rho w'$?
- How can we use this understanding to show that the intersections of principal ideals of M are finitely generated?

As we will see, being able to decide if $w \sim_\rho w'$ for two words in the commutative setting is not easy in general.

Some motivating examples

Describing the equivalence classes of words is a combinatorial problem.

Example

Let $w = au_iu_j$, in the non-commutative case $[w]_\rho = \{au_iu_j, bv_iu_j\}$ whereas in the commutative case $[w]_\rho = \{au_iu_j, bv_iu_j, bu_iv_j\}$.

The problem of deciding if $w \sim_\rho w'$ arises because, if in fact $w \nsim_\rho w'$, we would have to show that there does not exist a finite sequence of ρ-transitions between them.

Example

Is $a^2b^3u_1^2v_1u_2v_2^4u_3^3v_3u_4^3v_4^5 \sim_\rho ab^4u_1v_1^2u_2^4v_2u_3^4u_4v_4^7$?

Finding an algorithm that can decide this for us might make this easier!

Algorithm

Consider the following algorithm:

Definition

Let $\mathcal{B} : M \to M$ be an algorithm acting on words in M in the following way,

1. Make as many au_i to bv_i as possible for $i = n$, then $i = n - 1$ until you reach $i = 1$.
2. Now, make as many bv_i to au_i as possible for $i = 1$, then $i = 2$ until you reach $i = n$.

We will write $\mathcal{B}(\mathcal{B}(w)) = \mathcal{B}^2(w)$ and if $w = w_0$ then we define $\mathcal{B}^i(w) = w_i$ iteratively. For an n such that $\mathcal{B}(w_n) = w_n$, we say $w_n = w^*$ is the *normal form* of w.

An example

Example

Let $w = w_0 = av_1^n u_2^n$,

$$\begin{aligned} \mathcal{B}(w_0) &= au_1 v_1^{n-1} u_2^{n-1} v_2 = w_1, \\ \mathcal{B}(w_1) &= au_1^2 v_1^{n-2} u_2^{n-2} v_2^2 = w_2, \\ &\vdots \\ \mathcal{B}(w_{n-1}) &= au_1^n v_2^n = w_n, \\ \mathcal{B}(w_n) &= au_1^n v_2^n = w_n. \end{aligned}$$

Hence the normal form is $w_n = w^*$.

Hold up...wait a minute! How do we know that w^* is even a normal form?

Reduction systems

We can view $\mathcal{B}$ as a reduction system!

Definition

For a set A and binary operation $\rightarrow$ on A, we say $(A, \rightarrow)$ is a *reduction system* and we write $\xrightarrow{*}$ to denote the reflexive transitive closure of $\rightarrow$.

Definition

A reduction system is *noetherian* if there is no infinite sequence of $a_i \in A$ such that $a_i \rightarrow a_{i+1}$ for all $i \geq 0$.

Confluence

Definition

A reduction system $(A, \to)$ is *locally confluent* if $\forall a, b, c \in A$ such that $a \to b$ and $a \to c$, there exists an element $d \in A$ such that $b \xrightarrow{*} d$ and $c \xrightarrow{*} d$.

Definition

A reduction system $(A, \to)$ is *confluent* if $\forall a, b, c \in A$ such that $a \xrightarrow{*} b$ and $a \xrightarrow{*} c$, then there exists an element $d \in A$ such that $b \xrightarrow{*} d$ and $c \xrightarrow{*} d$.

Important results

Theorem

If $(A, \to)$ is a noetherian reduction system then it is locally confluent iff *it is confluent.*

Theorem

If $(A, \to)$ is noetherian and confluent then for each $x \in A$, $[x]$ contains a unique normal form.

It turns out that $\mathcal{B}$ is noetherian and locally confluent:

- Use partial ordering (lexicographical, $a, u_1, u_2, \ldots$)
- Let $\to$ be $bv_i \to au_i$ and $au_iv_j \to au_jv_i$ for $j < i$

Back to the example!

Result 3

For $w, w' \in M$ we have $w \sim_\rho w'$ iff $w^* = (w')^*$.

Example

Is $a^2 b^3 u_1^2 v_1 u_2 v_2^4 u_3^3 v_3 u_4^3 v_4^5 \sim_\rho ab^4 u_1 v_1^2 u_2^4 v_2 u_3^4 u_4 v_4^7$?

$$\begin{aligned}
\mathcal{B}(a^2 b^3 u_1^2 v_1 u_2 v_2^4 u_3^3 v_3 u_4^3 v_4^5) &= a^5 u_1^3 u_2^5 u_3^3 v_3 u_4 v_4^7 \\
\mathcal{B}(a^5 u_1^3 u_2^5 u_3^3 v_3 u_4 v_4^7) &= a^5 u_1^3 u_2^5 u_3^4 v_4^8 \\
\mathcal{B}(a^5 u_1^3 u_2^5 u_3^4 v_4^8) &= a^5 u_1^3 u_2^5 u_3^4 v_4^8 \\
\mathcal{B}(ab^4 u_1 v_1^2 u_2^4 v_2 u_3^4 u_4 v_4^7) &= a^5 u_1^3 u_2^5 u_3^4 u_4^2 v_4^6 \\
\mathcal{B}(a^5 u_1^3 u_2^5 u_3^4 u_4^2 v_4^6) &= a^5 u_1^3 u_2^5 u_3^4 u_4^2 v_4^6
\end{aligned}$$

No, since $(a^2 b^3 u_1^2 v_1 u_2 v_2^4 u_3^3 v_3 u_4^3 v_4^5)^* \neq (ab^4 u_1 v_1^2 u_2^4 v_2 u_3^4 u_4 v_4^7)^*$.

Cancellativity

Unfortunatively, M is not cancellative. We can prove this via a simple counterexample.

Proof.

For example, $au_iv_j \sim_\rho au_jv_i$, but $u_iv_j \nsim_\rho u_jv_i$ for $i \neq j$. □

This can be verified by applying $\mathcal{B}$ to both sides! What can be said about the intersections of principal ideals?

Intersections of principal ideals

In order to show that the intersections of principal ideals of M are finitely generated, we have a number of options:

- Explicitly define the intersections. Perhaps a different algorithm can do this for us?
- Show that for some words $w_i \in M$ and index I, we have $wM \cap w'M = \bigcup_{i \in I} w_i M$ where each $|w_i| \leq n \in \mathbb{N}$.

Current thoughts

Let $w, w' \in M$ and let h be the largest common subword in w and w'. That is, for some $r, r' \in M$ we have,

$$w = hr \text{ and } w' = hr'.$$

Note: at this point, finding h, r and r' would be easily computable since,

$$wM \cap w'M = w^*M \cap (w')^*M.$$

Result 4

We have that $wM \cap w'M = hrr'M \cup \left(\bigcup_{i \in I} w_i M\right)$ for some index I and words $w_i \in M$.

If we can show that $|hrr'| \geq w_i$ for each $i \in I$, we are done...

Other interesting questions!

For lovers of combinatorial and/or computational problems:

- What is $|[w]_\rho|$?
- Is there an algorithm that requires fewer iterations?
- Are there any relationships between words of length k and the least upper bound n for which $\mathcal{B}^n(w) = w^*$ for all such words?

What questions can we ask next?

- If we define a new set of relations $\sigma \subset A^* \times A^*$ such that $\sigma = \rho \cup \{(u_i v_j, u_j v_i) : 1 \leq i, j \leq n\}$, is $M = \langle A : \sigma \rangle$ cancellative and are the intersections of principal ideals finitely generated?

Thanks for listening! Any questions?

References

- *Rewriting Systems and Embedding of Monoids in Groups*, F.Chouraqui.
- *Free idempotent generated semigroups over bands and biordered sets with trivial products*, V.Gould and D.Yang.
- *Fundamentals of Semigroup Theory*, J.Howie.
- *Adian inverse semigroups* , M.Inam.