The Membership Problem

For the Torus, Klein Bottle and Double Torus

Max Pateman
School of Mathematics
University of East Anglia

July 2022

Contents

1 Introduction

The Submonoid Membership Problem for surface groups is an open question within Algebraic Topology and within this paper, we aim to work towards being able to say whether this problem is decidable for the Torus, Klein Bottle and the Double Torus.
To do this, we start by looking at solving the word problem, which is the least general version of the Membership Problem, where we build a finite complete rewriting system (FCRS) to solve this. Then, using our FCRS, we build the Positivity Membership Problem, and show that this is decidable for each of our examples. The next step up from this is the Monogenic Submonoid Membership Problem, which we show is decidable for each of our examples. Almost immediately from this we can build the 2-Generator Submonoid Membership Problem, which is very similar to the Monogenic Problem, except with two generators, as opposed to one. Finally, going into the most general case, the General Submonoid Membership Problem. We prove this by generalising all of the previous cases we have looked at where instead of a small amount of generators we have k generators.

It is generally believed that this problem is decidable, however, there has yet to be a proof of this, but, there also has not been a counter example. Here we aim to show that this is decidable for 3 small examples, the Torus, the Klein Bottle and the Double Torus.

2 Definitions

Within the following sections we will need some definitions. These are:

Definition 2.1 *A word is any combination of letters from the given alphabet.*

Example 2.1.1 *Given the alphabet* $\{x, x^{-1}, y, y^{-1}\}$*, we have a word* $xyxxyxy^{-1}x^{-1}yxx^{-1}yyxxy^{-1}$.

Definition 2.2 *A subword is a section of the original word.*

Example 2.2.1 *Some subwords of the word in Example 1 are:*
$1, x, xy, xxy, y, x^{-1}, y^{-1}, yy^{-1}, ...,\ xyxxyxy^{-1}x^{-1}yxx^{-1}yyxxy^{-1}$

Definition 2.3 *An overlap of rules is where two of the rules in the finite complete rewriting system have an equal substring*

Example 2.3.1 *Within any FCRS we have two rules* $(xx^{-1}, 1)$, $(x^{-1}x, 1)$ *and these would overlap to give the word* $xx^{-1}x$. *We see that within this system this would resolve trivially and so we don't check these overlaps, but they will occur in every FCRS for any generator* x.

Definition 2.4 *A word is called 'reduced' or 'irreducible' if it cannot have any rules from the groups Finite Complete Rewriting System (FCRS) applied to it.*

Example 2.4.1 *Using Example 1 we can do the following process of reducing using the rewriting system for the Torus seen later in this paper:*
$xyxxyxy^{-1}x^{-1}yxx^{-1}yyxxy^{-1} \longrightarrow yxxxyy^{-1}xx^{-1}yyyxxy^{-1} \longrightarrow yxxxyyyxy^{-1}x \longrightarrow yxxxyyyy^{-1}xx \longrightarrow yxxxyyxx \longrightarrow yxxyxyxx \longrightarrow yxyxyxxx \longrightarrow yyxyxxxx \longrightarrow yyyxxxxx$
So the reduced form of the original word is y^3x^5.

Definition 2.5 $Mon\langle w_i\rangle = \{w_i^{n_i} \mid n_i \in \mathbb{N}\}$.

Definition 2.6 $u \in Mon\langle w_i\rangle$ *if* $\exists n_i \in \mathbb{N}$ *such that* $u = \prod_{i=1}^{k} w_i^{n_i}$ *for* $i = 1, ..., k$.

3 Torus

Definition 3.1 *Write $T = \langle x, y \mid xy = yx \rangle$ as the group presentation of the Torus.*

3.1 The Word Problem

To solve the Word Problem, we must be able to find a FCRS for the group, in this case T.
Now we denote the alphabet here as $A = \{y, y^{-1}, x, x^{-1}\}$ and A^* as the free monoid of strings over A.
We look at the presentation of the Torus and we can conclude the following:

$$xy = yx \implies y^{-1}xyy^{-1} = y^{-1}yxy^{-1} \implies y^{-1}x = xy^{-1}$$

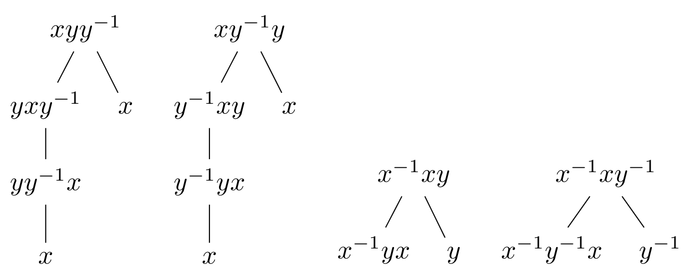
Using this, we can now write a set of rules S as follows :

$$S := \{(xx^1, 1),\ (x^{-1}x, 1),\ (yy^{-1}, 1),\ (y^{-1}y, 1),\ (xy, yx),\ (xy^{-1}, y^{-1}x)\}$$

where the last 2 rules come from the presentation itself, and the calculation above.
We define these rules in this way to preserve an order, namely the order

$$y < y^{-1} < x < x^{-1}.$$

This set of rules is not complete, however, and we must check where the rules overlap, as follows:



We see that the first two overlaps resolve (i.e. end up at the same word) but the second two overlaps that occur here do not resolve and so we must introduce 2 new rules.
From the first of these overlaps we look at the subword $x^{-1}y$ and see that if we sent this to yx^{-1}, we then have

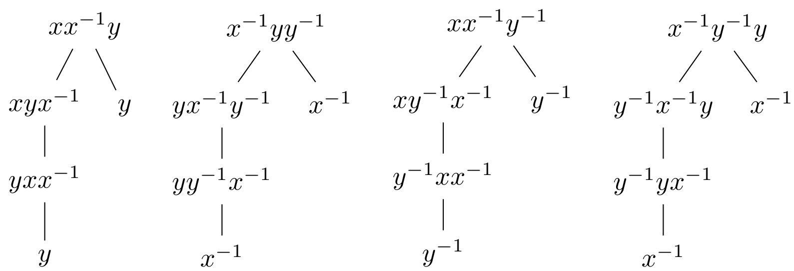
$$x^{-1}yx \to yx^{-1}x \to y,$$

as required, so we add the rule $(x^{-1}y, yx^{-1})$ to S. Similarly, with the second of these overlaps, if we look at the subword $x^{-1}y^{-1}$ and send this to $y^{-1}x^{-1}$ then we have

$$x^{-1}y^{-1}x \to y^{-1}x^{-1}x \to y^{-1},$$

as required, so we add the rule $(x^{-1}y^{-1}, y^{-1}x^{-1})$ to S.
This now gives
$S := \{(xx^1, 1),\ (x^{-1}x, 1),\ (yy^{-1}, 1),\ (y^{-1}y, 1),\ (xy, yx),\ (xy^{-1}, y^{-1}x),\ (x^{-1}y, yx^{-1}),$ $(x^{-1}y^{-1}, y^{-1}x^{-1})\}$.

So, we check the overlaps of the new rules:



And so all of the overlaps that we have resolve and so these two extra additions in S make S complete.

We now aim to prove that T is infinite using the finite complete rewriting system (FCRS).
It is clear that we get a word of the form $\bar{w} = y^n x^m$ for $n, m \in \mathbb{Z}$ when we reduce $w \in A^*$.
Suppose $m = 0$. Then $\bar{w} = y^n$. Then it is clear that none of the rules from the FCRS can be applied to $\bar{w}$ and so $\bar{w}$ is reduced for any $n \in \mathbb{Z}$.
Now suppose we have $w = y^n$ and $u = y^i$. Then it is clear from the above that $\bar{w} = w$ and $\bar{u} = u$. From the definition of being reduced we can get the following: A word w is reduced if we do not have a rule such that $w \to v$ for some word $v \in A^*$.
Then it follows that we only have a rule where $y^n \to y^i$ iff $n = i$, as both words are fully reduced. So we see that $[y^n] = [y^i]$ iff $n = i$. Then it follows that all y^n are unique for $n \in \mathbb{Z}$ and since n has infinite order, y^n must also have infinite order and so it is clear that T is infinite.

3.2 The Positivity Membership Problem

To solve this problem, we prove the following Theorem:

Theorem 3.1 *Suppose $w \in A^*$. Then using the FCRS we reduce w to get $\bar{w} = y^i x^j$. Then we have the following:*
i) $i \geq 0$ and $j \geq 0$ then $\exists\, u \in \{x, y\}^*$ such that $w =_T u$
ii) $i < 0$ or $j < 0$ then $\nexists\, u \in \{x, y\}^*$ such that $w =_T u$

Proof: Write $\bar{w} = y^i x^j$ where $i, j \in \mathbb{Z}$ and note $\bar{w} =_T w$.
i) Let $i \geq 0$ and $i \geq 0$. Then we have $\bar{w} \in \{x, y\}^*$, so setting $u = \bar{w}$ we have $u \in \{x, y\}^*$ such that $w =_T u$, as required.
ii) Here we have 2 cases:

Case 1: Suppose $i < 0$ and $j \in \mathbb{Z}$. Then, writing $-a = i$, we have $\bar{w} = y^{-a}x^j$. Note that applying any of the rules in the FCRSn in any order to $\bar{w}$, the y-exponent sum is maintained. So if $i < 0$ and $-a = i$ then any rewrite of $\bar{w}$ will always have an y-exponent sum of $-a$, meaning that no matter how you rewrite $\bar{w}$, you will always have at least one y^{-1} present, and so this cannot be written positively, as required.

Case 2: Suppose $j < 0$ and $i \in \mathbb{Z}$. Then, writing $-b = j$, we have $\bar{w} = y^i x^{-b}$. Note that applying any of the rules in the FCRS in any order to $\bar{w}$, the x-exponent sum is maintained. So if $j < 0$ and $-b = j$ then any rewrite of $\bar{w}$ will always have an x-exponent sum of $-b$, meaning that no matter how you rewrite $\bar{w}$, you will always have at least one x^{-1} present, and so this cannot be written positively, as required. □

Example 3.1.1 *Suppose $w = xyxxyxy^{-1}x^{-1}yxx^{-1}yyxxy^{-1}$. Then we have seen in the introduction that in this group $\bar{w} = y^3x^5$. Then we can see that this word can be written positively as both $i \geq 0, j \geq 0$.*

Example 3.1.2 *Suppose we have w as above, but with each individual letters power switched to its negative. Then $\bar{w} = y^{-3}x^{-5}$. So we see that we cannot write this positively as $i < 0$ and $j < 0$.*

3.3 Monogenic Submonoid Membership Problem

We see that for the following two sections, we can write $w_i^{n_i}$ in the way that we do as the rules in the FCRS only rearrange the words, but do not change the power of any element (other than the identity rules, but we do not use these here) and so, the words can be written of the form in the following theorems. This is not always true, and does not work, for example, in the 2-generator Klein Bottle case.

Theorem 3.2 *Suppose $w \in A^*$ and $u \in A^*$ are reduced words where $w = y^i x^j$ and $u = y^k x^l$. Then $u \in Mon\langle w\rangle$ iff $ni = k$ and $nj = l$ for some $n \in \mathbb{N}$.*

Proof: ($\Rightarrow$) Suppose $u \in \text{Mon}\langle w\rangle$ then $\exists\, n \in \mathbb{N}$ such that $u =_T w^n$. We see that $w^n = y^i x^j y^i x^j ... y^i x^j$ (n times), and so it is clear from the FCRS (namely the fact that there is the preservation of exponent sums) that $w^n = y^{ni}x^{nj}$. Then $y^k x^l = y^{ni}x^{nj}$ and so it is clear that we must have $k = ni$ and $l = nj$, as required.

($\Leftarrow$) Suppose $ni = k$ and $nj = l$ for some $n \in \mathbb{N}$.
Then $w^n = y^{ni}x^{nj} = y^k x^l = u$ and so it is clear that $w^n = u$ and so, by definition, $u \in \text{Mon}\langle w\rangle$, as required. □

Example 3.1.3 *Suppose $w = y^3x^5$. Then $w^n = y^{3n}x^{5n}$. We can check this for small n but it works for all $n \in \mathbb{N}$.*
Then suppose we have a word $u = y^k x^l \in A^*$. Then $u \in Mon\langle w\rangle$ iff $k = 3n, l = 5n$. So we could have:
i) $n = 1$: $k = 3, l = 5$
ii) $n = 2$: $k = 6, l = 10$
iii) $n = 3$: $k = 9, l = 15$, etc.

3.4 2-Generator Submonoid Membership Problem

Suppose $w_1, w_2 \in A^*$ and $u \in A^*$ are reduced words.
Here we have $u \in \text{Mon}\langle w_1, w_2\rangle$ if $\exists\, n, m \in \mathbb{N}$ such that $u =_T w_1^n w_2^m$.
We have seen that any reduced word in A^* has the form $y^i x^j$ so we write

$$w_1 = y^{i_1} x^{j_1}, \qquad w_2 = y^{i_2} x^{j_2}.$$

Then it is clear that we have

$$w_1^n = y^{ni_1} x^{nj_1}, \qquad w_2^m = y^{mi_2} x^{mj_2}.$$

Then,

$$w_1^n w_2^m = y^{ni_1} x^{nj_1} y^{mi_2} x^{mj_2} = y^{ni_1} y^{mi_2} x^{nj_1} x^{mj_2} = y^{ni_1+mi_2} x^{nj_1+mj_2}$$

We can see that this reduction is true as the rules in the FCRS only change the position of the terms while keeping the powers the same.

Theorem 3.3 *Suppose we have $u = y^k x^l$ and w_1, w_2 as defined above. Then*

$$u \in \mathit{Mon}\langle w_1, w_2\rangle \text{ iff } k = ni_1 + mi_2 \text{ and } l = nj_1 + mj_2 \text{ for some } n, m \in \mathbb{N}.$$

Proof: ($\Rightarrow$) Suppose $u \in \text{Mon}\langle w_1, w_2\rangle$ then $\exists\, n, m \in \mathbb{N}$ such that $u =_T w_1^n w_2^m$. We see that $w_1^n = y^{i_1} x^{j_1} y^{i_1} x^{j_1} ... y^{i_1} x^{j_1}$ (n times), and $w_2^m = y^{i_2} x^{j_2} y^{i_2} x^{j_2} ... y^{i_2} x^{j_2}$ (m times) and so it is clear from the FCRS (namely the fact that there is the preservation of exponent sums) that $w_1^n = y^{ni_1} x^{nj_1}$ and $w_2^m = y^{mi_2} x^{mj_2}$. Then we see, as above that $w_1^n w_2^m = y^{ni_1+mi_2} x^{nj_1+mj_2}$ Then $y^k x^l = y^{ni_1+mi_2} x^{nj_1+mj_2}$ and so it is clear that we must have $k = ni_1 + mi_2$ and $l = nj_1 + mj_2$, as required.

($\Leftarrow$) Suppose $ni_1 + mi_2 = k$ and $nj_1 + mj_2 = l$ for some $n, m \in \mathbb{N}$.
Then $w_1^n w_2^m = y^{ni_1+mi_2} x^{nj_1+mj_2} = y^k x^l = u$ and so it is clear that $w_1^n w_2^m = u$ and so, by definition, $u \in \text{Mon}\langle w_1 w_2\rangle$, as required. □

3.5 General Submonoid Membership Problem

This is a generalisation of the above 2 questions for when we have k generators.

Theorem 3.4 *Suppose we have $w_i \in A^*$ for $i = 1, ...k$ and $u = y^a x^b$. Then, write $w_i = y^{p_i} x^{q_i}$. Now take $n_i \in \mathbb{N}$ for $i = 1, ..., k$. Then*

$$w_i^{n_i} = y^{n_i p_i} x^{n_i q_i}$$

Then $u \in \mathit{Mon}\langle w_i\rangle$ iff

$$a = \sum_{i=1}^{k} n_i p_i \text{ and } b = \sum_{i=1}^{k} n_i q_i$$

for some $n_i \in \mathbb{N}$.

Proof: ($\Rightarrow$) Suppose $u \in \text{Mon}\langle w_i \rangle$. Then $\exists\, n_i \in \mathbb{N}$ such that

$$y^a x^b = u = \prod_{i=1}^{k} w_i^{n_i} = \prod_{i=1}^{k} y^{n_i p_i} x^{n_i q_i} = y^{\sum_{i=1}^{k} n_i p_i} x^{\sum_{i=1}^{k} n_i q_i}$$
$$\implies a = \sum_{i=1}^{k} n_i p_i \;\; and \;\; b = \sum_{i=1}^{k} n_i q_i,$$

as required.

($\Leftarrow$) Suppose

$$a = \sum_{i=1}^{k} n_i p_i \;\; and \;\; b = \sum_{i=1}^{k} n_i q_i$$

for some $n_i \in \mathbb{N}$.
Then

$$\prod_{i=1}^{k} w_i^{n_i} = \prod_{i=1}^{k} y^{n_i p_i} x^{n_i q_i} = y^{\sum_{i=1}^{k} n_i p_i} x^{\sum_{i=1}^{k} n_i q_i} = y^a x^b = u$$

So, we have $u =_T \prod_{i=1}^{k} w_i^{n_i}$ for some $n_i \in \mathbb{N}$ so $u \in \text{Mon}\langle w_i \rangle$, as required.
□

Corollary 3.4.1 *The Submonoid Membership Problem is decidable for the Torus iff there is an algorithm to solve the set of linear equations given in Theorem 3.4.*

Proof: We see that here we would be aiming to solve a set of Linear Diophantine equations and we see that this can be solved using the Smith Normal Form and we can then check for solutions in the natural numbers with the use of a computer, and so this problem is decidable, as required. The other direction of the proof is trivial. If the problem is decidable, then we must be able to solve the equations and check the solutions as we would then be able to answer YES or NO.

Corollary 3.4.2 *By having that the Submonoid Membership Problem as decidable for the Torus, it is automatic that he previous problems, namely the Positivity Problem, the Monogenic Submonoid Membership Problem and the 2-generator Submonoid Membership Problem, are also decidable for the Torus.*

4 Klein Bottle

Definition 4.1 *Write $K = \langle x, y \mid xy = yx^{-1} \rangle$ as the group presentation of the Klein Bottle.*

4.1 The Word Problem

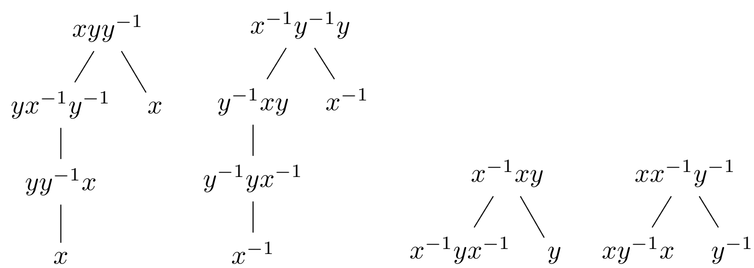
We say $A = \{y, y^{-1}, x, x^{-1}\}$ and A^* is the free monoid of strings over A.
We see the following:

$$xy = yx^{-1} \implies y^{-1}xyy^{-1} = y^{-1}yx^{-1}y^{-1} \implies y^{-1}x = x^{-1}y^{-1}.$$

So we start with

$$S := \{(xx^1, 1),\ (x^{-1}x, 1),\ (yy^{-1}, 1),\ (y^{-1}y, 1),\ (xy, yx^{-1}),\ (x^{-1}y^{-1}, y^{-1}x)\}.$$

As before we must check overlaps.



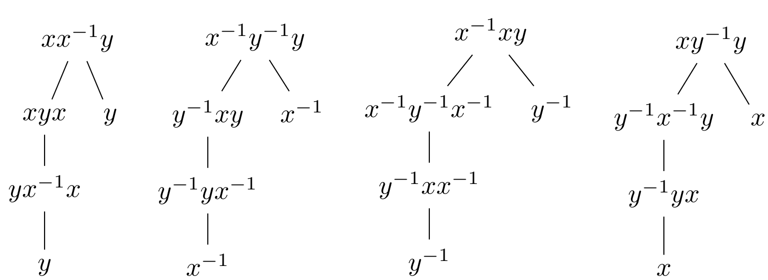
We see that the first two overlaps resolve and so we need not add any new rules for these. However, the second two do not resolve and so if we add the rules $(x^{-1}y, yx)$ and $(xy^{-1}, y^{-1}x^{-1})$ we see

$$x^{-1}yx^{-1} \to yxx^{-1} \to y$$

and

$$xy^{-1}x \to y^{-1}x^{-1}x \to y^{-1}$$

and so now these overlaps resolve. Now we have
$S := \{(xx^1, 1),\ (x^{-1}x, 1),\ (yy^{-1}, 1),\ (y^{-1}y, 1),$
$(xy, yx^{-1}),\ (x^{-1}y^{-1}, y^{-1}x),\ (x^{-1}y, yx),\ (xy^{-1}, y^{-1}x^{-1})\}$. We must again check the overlaps of the new rules:



All of these overlaps resolve and so the new rules make S a FCRS for K.
Similarly to the Torus, all reduced words result in a word of the form $y^i x^j$ for some $i, j \in \mathbb{Z}$. Now suppose we have $y^n, y^m \in A^*$ for some $n, m \in \mathbb{Z}$. Then it is clear that y^n and y^m are reduced here. Then, since both words are fully reduced, we can only have $y^n \to y^m$ if $n = m$ and so it follows that $[y^n] = [y^m]$ iff $n = m$.
It follows then that y^n are unique for all n and so, since n has infinite order, y^n has infinite order and so it follows that K is also infinite.

4.2 The Positivity Membership Problem

To solve this problem, we prove the following theorem:

Theorem 4.1 *Suppose $w \in A^*$. Then using the FCRS we reduce w to get $\bar{w} = y^i x^j$. Then we have one of the following:*
i) $i < 0$, then $\nexists u \in \{x, y\}^*$ such that $w =_K u$
ii) $i \geq 1$ then $\exists u \in \{x, y\}^*$ such that $w =_K u$ where either:
a) $j < 0$ and $u = x^a y^i$ with $a = -j$ or
b) $j \geq 0$ and $u = y^i x^j$
iii) $i = 0$ then either
a) $j < 0$ and $\nexists u \in \{x, y\}^*$ such that $w =_K u$ or
b) $j \geq 0$ and $\exists u \in \{x, y\}^*$ such that $w =_K u$ with $u = x^j$

Proof: Write $\bar{w} = y^i x^j$ where $i, j \in \mathbb{Z}$ and note that $w =_K \bar{w}$. Then
i) Suppose $i < 0$. Then $\bar{w} = y^{-a} x^j$ where $-a = i$. Then we see that applying any of the FCRS rules in either direction maintain the y-exponent sum, and so there will always be at least one case of y^{-1} present in any rewrite of our word so we can never have $u \in \{x, y\}^*$ such that $w =_K u$, as required.
ii) $i \geq 1 \implies \bar{w} = y^i x^j$
a) If $j < 0$ then $\bar{w} = y^i x^{-b}$ where $-b = j$. Then we can use $yx^{-1} \to xy$ repeatedly to get $u = x^b y^i$ and so $\exists u \in \{x, y\}^*$ such that $w =_K u$, as required.
b) If $j \geq 0$ then $\bar{w} = y^i x^j \in \{x, y\}^*$ so $u = \bar{w}$ and so by definition we have $u \in \{x, y\}^*$ such that $w =_K u$, as required.
iii) $i = 0 \implies \bar{w} = x^j$. Then either
a) $j < 0 \implies \bar{w} = x^{-a}$ where $-a = j$ so $\nexists u \in \{x, y\}^*$ such that $w =_K u$ or
b) $j \geq 0 \implies u = x^j = \bar{w}$ so $\exists u \in \{x, y\}^*$ such that $w =_K u$, as required. □

Corollary 4.1.1 *The Positivity Membership Problem for the Klein Bottle is decidable iff we can check the conditions given in Theorem 4.1.*

Proof: If the problem is decidable, then it is clear that we must be able to check the conditions given in Theorem 4.1, as that is the way we can get an answer for if $u \in$Mon$\langle a, b\rangle$. If we can check the conditions given in the statement of the theorem, then it is clear that we can say if $u \in \text{Mon}\langle a, b\rangle$, and so the problem is decidable. □

4.3 Monogenic Submonoid Membership Problem

Theorem 4.2 *Suppose $w \in A^*$ and $u \in A^*$ are reduced words where $w = y^i x^j$ and $u = y^k x^l$. Then $u \in Mon\langle w \rangle$ iff only one of the following is satisfied:*
i) For i even, $ni = k$ and $nj = l$ for some $n \in \mathbb{N}$.
ii) For i odd, $ni = k$ and either $l = 0$ or $l = j$

Proof: ($\Rightarrow$) Suppose $u \in \text{Mon}\langle w \rangle$ then $\exists n \in \mathbb{N}$ such that $u =_K w^n$.
If i is odd then we see $w^n = \begin{cases} y^{ni} & \text{if } n \in \mathbb{N} \text{ even} \\ y^{ni}x^j & \text{if } n \in \mathbb{N} \text{ odd} \end{cases}$

or if i is even then $w^n = y^{ni}x^{nj}$for all $n \in \mathbb{N}$.
So now, if we have $u = w^n \implies$ i) for i even, $u = w^n \implies u = y^{ni}x^{nj} \implies y^k x^l = y^{ni}x^{nj} \implies k = ni$ and $l = nj$, as required, or

ii) for i odd $u = \begin{cases} y^{ni} & \text{if } n \in \mathbb{N} \text{ even} \\ y^{ni}x^j & \text{if } n \in \mathbb{N} \text{ odd} \end{cases}$

$\implies y^k x^l = \begin{cases} y^{ni} & \text{if } n \in \mathbb{N} \text{ even} \\ y^{ni}x^j & \text{if } n \in \mathbb{N} \text{ odd} \end{cases}$

$\implies k = ni$ and either $l = 0$ or $l = j$, as required.

($\Leftarrow$) i) Suppose i is even and $k = ni$, $l = nj$. Then $w^n = y^{ni}x^{nj} = y^k x^l = u$ and so for i even $\exists n \in \mathbb{N}$ such that $u =_K w^n \implies u \in \text{Mon}\langle w \rangle$, as required.
ii) Suppose i is odd and
a) $k = ni$ and $l = 0$ then $w^n = y^{ni}x^0 = y^k = u$ for $n \in \mathbb{N}$ even, or
b) $k = ni$ and $l = j$ then $w^n = y^{ni}x^j = y^k x^l = u$ for $n \in \mathbb{N}$ odd.
So for i odd, $\exists n \in \mathbb{N}$ such that $u =_K w^n \implies u \in \text{Mon}\langle w \rangle$, as required. □

Corollary 4.2.1 *The Monogenic Submonoid Membership Problem is decidable iff there exists an algorithm to solve the statement in Theorem 4.2.*

Proof: ($\Leftarrow$) For i) we must be able to find $ni = k$ and $nj = l$. Here, we are given i, j, k and l, so all we must do is find such an $n \in \mathbb{N}$ where $ni = k$, and then check if $nj = l$, given that i is even. If both of these are true, then we would output yes, otherwise we would output no, and so the problem is decidable here. For ii) We would first check that $l = 0$ or $l = j$, which we would be given. If this is the case, then we would try and find some $n \in \mathbb{N}$ such that $ni = k$. If this is true, then we would say yes, otherwise, we would say no. If we do not have $l = 0$ or $l = j$, then we would output no, and so the problem is decidable here also, as required.
($\Rightarrow$) This direction of the proof is trivial.

4.4 2-Generator Submonoid Membership Problem

Suppose we have $u = y^k x^l$ and suppose we have two words, $w_1 = y^{i_1} x^{j_1}$ and $w_2 = y^{i_2} x^{j_2}$. We see that the rules in the FCRS preserve the y-exponent sum, and so the first step to solving this problem is finding all of the solutions of the equation $k = ai_1 + bi_2$. From this we will get a solution space (a, b) that we will use for the next step. We see that a and b here correspond to what the total sums of the powers of each word will need to be, i.e. w_1 will always have to have powers that add up to a for the different values of a, and the same for w_2 and b.

Now we can see that we will have at most

$$\sum_{(a,b)} \binom{a+b}{b}$$

combinations of words. This is clear as we will have $a + b$ total spaces for the powers of the words to go, and we are finding how many ways we can put b in there.

Then, to determine if $u \in \mathrm{Mon}\langle w_1, w_2\rangle$, we must check all of these possible combinations until we find one where we get exactly $u = y^k x^l$.

Corollary 4.2.2 *The 2-generator Submonoid Membership Problem is decidable iff there is an algorithm that checks all combinations of words as described above.*

Proof: ($\Rightarrow$) If the 2-generator problem is decidable, then it is clear that we can decide whether $u \in \mathrm{Mon}\langle w_1, w_2\rangle$, and so we must have being able to check the combinations to make sure that they match or do not match.

($\Leftarrow$) Firstly, we must solve the Diophantine equation $ai_i + bi_2$, which we have seen can be done [7]. Then, we see that there is an algorithm that is able to output all combinations as we want them [8], and then we can add another algorithm that computes the reduced forms of these words using the FCRS, and then we can check if any of the words are exactly u.

4.5 General Submonoid Membership Problem

We see here that we would get a solution space $(a_1, a_2, ..., a_n)$ when we have n generators, similarly to what we say for the 2 generator case.

Then there will be a finite combination of words that is computable in finite polynomial time.

Then we see that the following holds:

Corollary 4.2.3 *The General Submonoid Membership Problem is decidable iff there is an algorithm that checks all combinations of words.*

Proof: This result is a more general form of the previous result, where we see the result still holds if we extend it to a finite amount of generators.

Remark 4.2.1 *This result is computable in finite polynomial time, but the algorithm to do so becomes inefficient for large numbers of generators due to the size of the strings that would be inputted.*

5 Double Torus

Definition 5.1 *Write* $D = \langle a, b, c, d | aba^{-1}b^{-1}cdc^{-1}d^{-1} = 1\rangle$ *as the group presentation for the Double Torus. We also have* $A = \{b, b^{-1}, a, a^{-1}, d, d^{-1}, c, c^{-1}\}$ *and* A^* *is the free monoid of words over* A*.*

5.1 The Word Problem

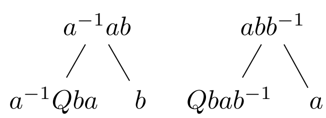
We can see that

$$\begin{aligned} aba^{-1}b^{-1}cdc^{-1}d^{-1} = 1 &\implies aba^{-1}b^{-1} = dcd^{-1}c^{-1} \\ &\implies a^{-1}b^{-1} = b^{-1}a^{-1}dcd^{-1}c^{-1}, \;\; ab = dcd^{-1}c^{-1}ba \end{aligned}$$

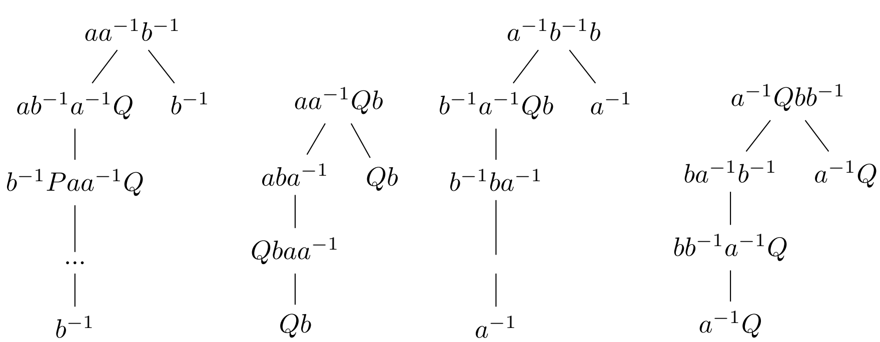
Now write $P = cdc^{-1}d^{-1}, \;\; Q = dcd^{-1}c^{-1}$.
Then, from the above calculations, we write

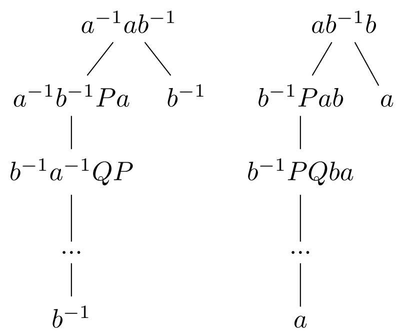
$$\begin{aligned} S := \{&(aa^{-1}, 1), (a^{-1}a, 1), (bb^{-1}, 1), (b^{-1}b, 1), \\ &(cc^{-1}, 1), (c^{-1}c, 1), (dd^{-1}, 1), (d^{-1}d, 1), \\ &(ab, Qba), (a^{-1}b^{-1}, b^{-1}a^{-1}Q)\}. \end{aligned}$$

As in the previous two examples, we check overlaps:



We see that these two overlaps do not resolve and so we add the two new rules $(a^{-1}Qb, ba^{-1})$ and $(ab^{-1}, b^{-1}Pa)$ and check the remaining overlaps as follows:





We see that all of these overlaps now resolve and so these two new rules create the FCRS when adjoined with S, and so

$$S := \{(aa^{-1}, 1), (a^{-1}a, 1), (bb^{-1}, 1), (b^{-1}b, 1),\\ (cc^{-1}, 1), (c^{-1}c, 1), (dd^{-1}, 1), (d^{-1}d, 1),\\ (ab, Qba), (a^{-1}b^{-1}, b^{-1}a^{-1}Q), (a^{-1}Qb, ba^{-1}), (ab^{-1}, b^{-1}Pa)\}.$$

For this example, we must check that the FCRS is Noetherian, as in the others this is obvious. Here we will use the following definition from Rewriting Systems for Coxeter Groups, Susan M. Hermiller:

Definition 5.2 *Let $>$ be a partial well-founded ordering on a set S. The recursive path ordering $>_{rpo}$ on S^* is defined recursively from the ordering on S as follows.*
Given $s_1, ...s_m, t_1, ...t_n \in S, s_1...s_m >_{rpo} t_1...t_n$ iff one of the following holds.
1) $s_2...s_m \geq_{rpo} t_1...t_n$
2) $s_1 > t_1$ and $s_1...s_m >_{rpo} t_2...t_n$
3) $s_1 = t_1$ and $s_2...s_m >_{rpo} t_2...t_n$
The recursion is started from the ordering $>$ on S and from $s > rpo1$ for all $s \in S$, where 1 is the empty word in S^*. Note that if $>$ is a total ordering on S, then $>_{rpo}$ is a total ordering on S^*.

Now we can see that for all rules $v \to w$ in S, $v >_{rpo} w$ and so it is clear that S is Noetherian. Note, here we use S as our FCRS, but in the above definition S refers to the set of letters, denoted A in this paper.

Suppose we take $b^n \in A^*$. Now, by looking at S, we see that we cannot apply any rules to b^n and so it is clear that b^n is reduced.
Now suppose for contradiction that b^m is not reduced for some $m \in \mathbb{Z}, m \neq n$ and that we have the map $b^m \to b^n$. Then it is clear that $[b^m] = [b^n]$ by definition. However, we have seen that b^n is reduced for all $n \in \mathbb{Z}$ and so the above is only true iff $m = n$. So now we have seen that $[b^n]$ is unique for all $n \in \mathbb{Z}$ and so, since n has infinite order, b^n also has infinite order and so D has infinite order.

5.2 The Positivity Membership Problem

Theorem 5.1 *Suppose $w \in A^*$. Then w can be written positively if it reduces to $\bar{w}$ of the form*

$$\bar{w} = \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_{k+1}$$

where α_n are positive, reduced, and do not contain ab for $n = 1, ..., k+1$ and $i_n \in \mathbb{N}$.

Proof: Firstly, we prove by induction on n that $(Qb)^n a$ can be written positively as $(Qb)^n a = ab^n$ for finite $n \in \mathbb{N}$.
Base Cases: $n = 0 \implies (Qb)^0 a = 1 \times a = a = a \times 1 = ab^0$.
$n = 1 \implies (Qb)^1 a = Qba \to ab = ab^1$

Inductive Hypothesis: $(Qb)^n a = ab^n$.

Inductive Step: Take $(Qb)^{n+1} a$.
Then $(Qb)^{n+1} a = (Qb)^n Qba \to (Qb)^n ab$. Then using the inductive hypothesis

$$(Qb)^{n+1} a = (Qb)^n Qba \to (Qb)^n ab \to ab^n b = ab^{n+1}.$$

And so we can rewrite $(Qb)^n a$ positively as ab^n for any finite $n \in \mathbb{N}$.

Now we will prove by induction on $|w|$ that for any positive word w it has reduced form $\bar{w}$ of the form given in the statement of the theorem.
Base Case: $|w| = 1 \implies w = x$ where $x \in A$ and so is in the desired form.

Inductive Hypothesis: $|w| = n \implies \bar{w} = \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_{k+1}$.

Inductive Step: Suppose $|w| = n+1$. Then $\bar{w} = \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_{k+1} x$ where $x \in \{a, b, c, d\}$, i.e. we are adjoining a positive letter to the end of $\bar{w}$. We see that this would still have length $n+1$ in its unreduced form as we can reduce our original w, without the adjoined x, and get the form we have here. Suppose we have $\alpha_{k+1} = \alpha_p a$ (i.e α_{k+1} ends with an a), then, if $x = b$ we have

$$\begin{aligned} \bar{w} &= \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_p ab \\ &\to \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_p Qba \\ &= \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_p (Qb)^1 a\alpha_{p+1} \end{aligned}$$

where $\alpha_{p+1} = 1$.
If we have $\alpha_{k+1} = \alpha_p y$ where $y \in \{a, c, d\}$ then $\alpha_p yx$ is still reduced for any $x \in \{a, b, c, d\}$ and so we can write $\alpha_q = \alpha_p yx$ and so

$$\bar{w} = \alpha_1 (Qb)^{i_1} a\alpha_2 (Qb)^{i_2} a\alpha_3 ... \alpha_k (Qb)^{i_k} a\alpha_q,$$

giving the required form in each case.

Now, it is a necessary condition within the statement of the theorem that all of the α_n for $n = 1, ..., k+1$ are positive themselves and do not contain ab. Firstly, if they contained ab, then they would not be reduced and so this would contradict the statement of having $\bar{w}$ being the reduced form of w.
It is clear that α_n will be made up of some combination of a^i, b^j, c^k, d^l for some $i, j, k, l \in \mathbb{Z}$. The claim here is that if $i < 0$ or $j < 0$ or $k < 0$ or $l < 0$, α_n cannot be written positively.
Suppose there exists i, j, k or l such that $i < 0$ or $j < 0$ or $k < 0$ or $l < 0$. Now we must check each case as follows:
i) $i < 0$: If we have $i < 0$ then using our FCRS we will be able to use the rules $(b^{-1}a^{-1}Q, a^{-1}b^{-1})$ or $(ba^{-1}, a^{-1}Qb)$ to try and rewrite α_n. So, to apply any rules, we must have these occur within α_n, and so we can observe that to rewrite these positively we would need either $b^{-1}a^{-1}Qba$ or $Paba^{-1}$ in α_n.
We now observe that, in the first case, this would not be in $alpha_n$ as we have an occurrence of Qba, which should be outside of $alpha_n$ by the statement of the theorem.
For the second case here, we would have $Paba^{-1}$. However, it was a given condition in the statement of the theorem that α_n is reduced, but if this appears, we have an occurrence of ab which then means that this is not reduced, and so by definition, $Paba^{-1}$ cannot appear in α_n.
And so, it is clear that no rules from the FCRS can be applied when $i < 0$ and so if we have $i < 0$, α_n cannot be written positively.

ii) $j < 0$: Here, we can either use $(b^{-1}a^{-1}Q, a^{-1}b^{-1})$ or $(b^{-1}Pa, ab^{-1})$. We have seen that the first case cannot happen through i), and so we must only check the second.
To be able to write $b^{-1}Pa$ positively, we would need to have $b^{-1}Pab$ in α_n but we see that we must have ab, and so this would then not be reduced and so $b^{-1}Pab$ cannot appear in α_n. Then, no rules can applied from the FCRS when $j < 0$ and so if $j < 0$, α_n cannot be written positively.

iii) $k < 0$ or $l < 0$: The rules that can be applied for this case are either $(b^{-1}a^{-1}Q, a^{-1}b^{-1})$ or or $(b^{-1}Pa, ab^{-1})$, but we have seen by parts i) and ii) that neither of these are possible and so it is clear that if $k < 0$ or $l < 0$ then α_n cannot be written positively.

And so we have proven that we can rewrite $(Qb)^n a$ positively, and that w can be written positively if it has reduced $\bar{w}$ as seen in the statement of the theorem where α_n are positive, reduced and do not contain ab. □

Corollary 5.1.1 *The Positivity Membership Problem for the Double Torus is decidable iff there is an algorithm to check the conditions given in Theorem 5.1.*

Proof: ($\Leftarrow$)It is obvious that such an algorithm exists, as this algorithm would check for occurrences of $(Qb)^n a$ for some $n \in \mathbb{N}$ and then separate $\bar{w}$ as in the form given in the statement of theorem 5.1. The algorithm would then only need

to check the conditions given for each α_n, namely that it is positive, reduced and does not contain ab, although the last check would be trivial, as if it did contain ab, then it would not be reduced, by definition. We still include this however, as it provides clarity when proving Theorem 5.1. And so, we have an algorithm that checks the conditions given in theorem 5.1 which will tell us YES or NO to answer whether w can be written positively, and so the problem is decidable.
($\Rightarrow$) If the problem is decidable, then we must always get a YES or NO, and so it is obvious that an algorithm must exist to check the conditions given in Theorem 5.1. $\square$

6 Further Work

In this section, we will discuss some further ideas that come from the solutions in this paper.

6.1 The Double Torus

Within Section 5, we were unable to prove the Monogenic Submonoid Membership Problem, the 2-Generator Submonoid Membership Problem and the General Submonoid Membership Problem, as the more general this example gets, the more complicated the proof will become and this is outside the scope of this project. The aim for further work would be to be able to prove that these three cases are true for the Double Torus, extending what has already been done within Section 5. We can however, give an idea of where we would start with the Monogenic Submonoid Membership Problem.

6.1.1 Monogenic Submonoid Membership Problem

For this problem, we can see that all reduced words will be of the form $w = \lambda\alpha\lambda^{-1}$. It is clear that if $w = \alpha$ then $\lambda = 1 = \lambda^{-1}$.
Now we look at the powers of w as follows:

$$w = \lambda\alpha\lambda^{-1} \implies w^2 = \lambda\alpha\lambda^{-1}\lambda\alpha\lambda^{-1} = \lambda\alpha 1\alpha\lambda^{-1} = \lambda\alpha\alpha\lambda^{-1}$$
$$\implies w^n = \lambda\alpha^n\lambda^{-1}.$$

And so to check if a word u is some power of the word w we must first check that $\lambda_u = \lambda_w$ where $u = \lambda_u\alpha_u\lambda_u^{-1}$ and $w = \lambda_w\alpha_w\lambda_w^{-1}$. If this is true, then we must look at α_u and α_w^n. If $\alpha_w^n = \alpha_u$ with no reductions necessary, then it is clear that $u = w^n$ and we see that this is easily decidable.
If $\alpha_w^n \neq \alpha_u$ then we must check the possible reductions in the overlaps between each α_w. This can be done as follows:
If α_w^n can be reduced, then the overlaps it would contain would be $ab, ab^{-1}, a^{-1}Qb, a^{-1}b^{-1}$ and so α_w can start in $b.b^{-1}$ or d and end in a, a^{-1} or c^{-1}. This comes from the fact that α_w is reduced by definition and so cannot contain $ab, ab^{-1}, a^{-1}Qb, a^{-1}b^{-1}$, unlike the overlaps.

6.2 N-holed Torus Positivity Problem

We see that for the 2 holed torus, we have a FCRS as follows

$$S := \{(aa^{-1}, 1), (a^{-1}a, 1), (bb^{-1}, 1), (b^{-1}b, 1),$$
$$(cc^{-1}, 1), (c^{-1}c, 1), (dd^{-1}, 1), (d^{-1}d, 1),$$
$$(ab, Qba), (a^{-1}b^{-1}, b^{-1}a^{-1}Q), (a^{-1}Qb, ba^{-1}), (ab^{-1}, b^{-1}Pa)\}.$$

Here we have $Q = dcd^{-1}c^{-1}$ and $P = cdc^{-1}d^{-1}$. We have seen in the Hermiller paper that we can actually defined a finite complete rewriting system exactly the same as above, only with different definitions for Q and P, and the extra identity rules.
Suppose we have an n-holed torus, then we get the group presentation

$$\langle a_1, a_2, ..., a_n, b_1, b_2, ..., b_n | a_1 b_1 a_1^{-1} b_1^{-1} ... a_n b_n a_n^{-1} b_n^{-1} \rangle.$$

Then, we will define

$$P = a_2 b_2 a_2^{-1} b_2^{-1} ... a_n b_n a_n^{-1} b_n^{-1} \quad \text{and} \quad Q = b_n a_n b_n^{-1} a_n^{-1} ... b_2 a_2 b_2^{-1} a_2^{-1}.$$

Then, we would be able to check that this FCRS is still Noetherian and Confluent, and so we have the FCRS defined the same as for the 2-holed torus.
In fact, this applies to the 1-holed torus, where we define $Q = 1$ and $P = 1$, giving the same FCRS as we found in section 2.
Now, we can look at the Positivity Membership Problem and we can say that it can be solved in a similar way as for the double torus case for the n-holed torus. We can observe that the same arguments can be observed, other than extending the final argument of the proof to the new letters a_3, b_3, etc. This will not be proved in this paper but can be proved for each case using the same method discussed in the proof for the Double Torus Positivity Membership Problem.

7 References

[1] Rosen, K. H. (2005) *'Discrete Mathematics and Its Applications'*, Presentations of groups, pp. 33-39

[2] Rosen, K. H. (2005) *'Discrete Mathematics and Its Applications'*, Rewriting Systems and the Knuth-Bendix Completion Process, pp. 411-432

[3] Hermiller, S. M. (1993) *'Rewriting Systems for Coxeter Groups'*

[4] Lohrey, M. (2013) *'The Rational Subset Membership Problem for Groups: A Survey'*

[5] Putman, A. (2016) *'One-relator groups'*

[6] Putman, A. *'The word problem for surface groups and hyperbolic geometry'*

[7] Wikipedia, *Linear Diophantine Equations*

[8] rtybase, *Generating Subsets*