Solving the word problem in the singular braid monoid.

Ruth Corran*

1 Singular knots and singular braids

Knots are just (ambient isotopy classes of) embeddings $S^1 \to \mathbb{R}$, and a link is a finite disjoint union of knots. Imagine a space where each point corresponds to a smooth map: $S^1 \to \mathbb{R}$, and where homotopic knots are "near" one another. Whole regions of this space correspond to a homotopy class of knot, and neighbouring regions are separated by "walls" corresponding to maps which are not embeddings. For example, there is a path in this space from a point representing the trefoil knot to a point representing the trivial knot, which passes through the point representing the *singular knot* illustrated in Figure 1. A *singular knot*

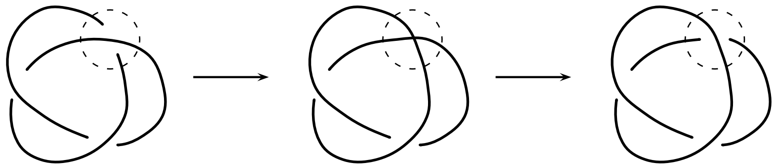

Figure 1: Some moments in a path through knot space.

is an equivalence class of smooth maps $S^1 \to \mathbb{R}$, under an equivalence known as *rigid vertex isotopy* — essentially, a neighbourhood of each double point (or intersection) must be preserved under any allowed isotopy. A *singular link* may be thought of as a finite union of singular knots.

A *singular braid on n strings* can be considered to be a collection of n intertwining strings with fixed endpoints in say the $z = 0$ and $z = 1$ planes, where the strings always run downwards — that is, each string intersects any intermediate plane at most once. Strings may intersect one another in *singular points*, but at most two strings may intersect at any one point. Singular braids are considered the same if they are *rigid vertex isotopic.* Two singular braids on n strings may be concatenated, giving a new braid on n strings. Thus concatenation acts as

*This paper is a version of a talk given by the author at the annual meeting of the Australian Mathematics Society at the University of Sydney in September 1998. The author would like to thank the Australian Mathematics Society and the organisers of the conference for the opportunity to speak. The author is supported by an Australian Postgraduate Award.

a multiplication, which is clearly associative. There is an *identity braid* where the strings neither twine nor intersect, shown in Figure 2. This braid acts as an identity with respect to concatenation. Thus the set of (isotopy classes of) singular braids on n strings forms a monoid under concatenation, denoted $\mathcal{SB}_n$.

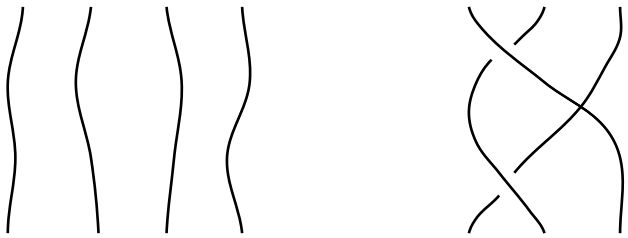

Figure 2: The identity braid on 4 strings and a singular braid on 3 strings.

Baez [2] and Birman [3] discovered a *monoid presentation* for $\mathcal{SB}_n$. The generators are $S \cup S^{-1} \cup T$ where

$$
\begin{aligned}
S &= \{\sigma_1, \sigma_2, \ldots, \sigma_{n-1}\}, \\
S^{-1} &= \{\sigma_1^{-1}, \sigma_2^{-1}, \ldots, \sigma_{n-1}^{-1}\}, \\
T &= \{\tau_1, \tau_2, \ldots, \tau_{n-1}\}.
\end{aligned}
$$

The braid corresponding to the generator σ_i is that in which the ith string crosses over the $(i+1)$th string, σ^{-1} corresponds to the ith string going under the $(i+1)$th string, and τ_i corresponds to an intersection between the ith and $(i+1)$th strings. Figure 3 shows the singular braid on four strings corresponding to the word $\sigma_1\sigma_2^{-1}\tau_3$.

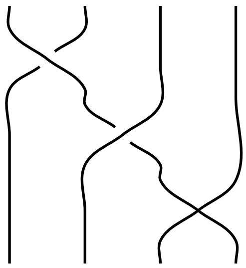

Figure 3: Singular braid on 4 strings represented by the word $\sigma_1\sigma_2^{-1}\tau_3$.

The notion of a monoid presentation is similar to that of a group presentation, except that if you would like to have inverses in your generating set you must explicitly include them and the relations of the form $xx^{-1} = 1 = x^{-1}x$. Hence the inclusion of the set S^{-1} above. Notice that there are no inverses of the singular points represented by the set T. This expresses the fact that there is nothing you can concatenate with an intersection which will undo it. The relations found by Baez and Birman are the following.

$$\left.\begin{array}{rcl} \sigma_i\sigma_j &=& \sigma_j\sigma_i \\ \tau_i\sigma_j &=& \sigma_j\tau_i \\ \tau_i\tau_j &=& \tau_j\tau_i \end{array}\right\} \quad \text{if } |i-j|>1,$$

$$\left.\begin{array}{rcl} \sigma_i\sigma_j\sigma_i &=& \sigma_j\sigma_i\sigma_j \\ \tau_i\sigma_j\sigma_i &=& \sigma_j\sigma_i\tau_j \end{array}\right\} \quad \text{if } |i-j|=1,$$

$$\left.\begin{array}{rcl} \tau_i\sigma_i &=& \sigma_i\tau_i \\ \sigma_i\sigma_i^{-1} &=& 1 \\ \sigma_i^{-1}\sigma_i &=& 1 \end{array}\right\} \quad \text{for all } i.$$

The first group of relations express the fact that if pairs of strings are far enough apart, crossings can be done in either order. Figure 4 shows the singular braids $\tau_1\sigma_4$ and $\sigma_4\tau_1$ on 5 strings, and it is clear from the picture that these are representatives of the same braid. The second group of relations is a generalisation of the braid relations and expresses how crossings and singular points on adjacent strings interact. Figure 5 shows such an interaction. The final set of relations expresses how crossings and intersections on the same pair of strings interact: inverses kill one another, and an intersection and a crossing commute.

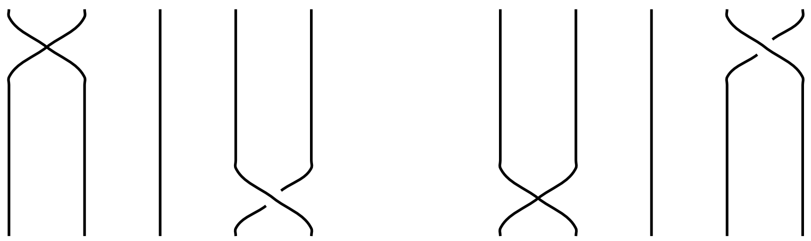

Figure 4: The singular braids on 5 strings represented by $\tau_1\sigma_4$ and $\sigma_4\tau_1$.

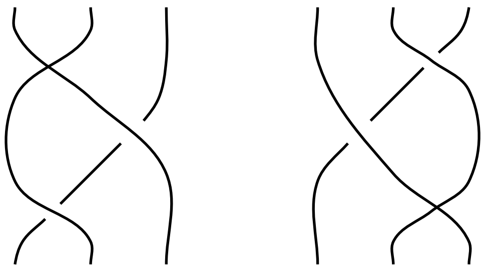

Figure 5: Singular braids on 3 strings represented by $\tau_1\sigma_2\sigma_1$ and $\sigma_2\sigma_1\tau_2$.

It turns out that in many ways the relationship between singular links and singular braids mirrors that between (non-singular) links and braids. Let $\bar{\beta}$ denote the singular link that you get if you join up corresponding endpoints of

β. We call $\bar{\beta}$ the *closure of* β. Birman [3] has shown, in analogy to Alexander's Theorem, that every singular link can be obtained from a singular braid in this way. See Figure 6 for an illustration. This suggests that if you can determine

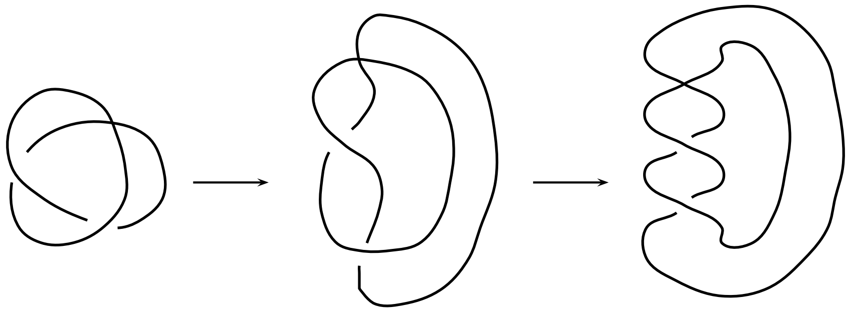

Figure 6: Transforming a singular trefoil knot to a closed singular braid.

when two singular braids are the same, you might be able to determine when two singular links are the same. However there are many occasions of inequivalent singular braids closing to give equivalent singular links.

A singular analogy to Markov's theorem, due to Armand-Ugon *et al.* [1] describes precisely when this happens. Suppose that β and γ are two singular braids such that $\bar{\beta}$ and $\bar{\gamma}$ are the same singular link. Then there is a sequence of singular braids $\beta = \beta_0, \beta_1 \ldots, \beta_{k-1}, \beta_k = \gamma$ such that for each i, β_{i+1} is obtained from β_i by a *(singular) Markov move.* There are two types of Markov move; examples are shown in Figure 7. The first type is like conjugation. The second type consists of adding a string (considering a singular braid in $\mathcal{SB}_n$ as one in $\mathcal{SB}_{n+1}$) and concatenating with a crossing σ_n. Hence if we can determine when two singular braids are conjugate and when one singular braid is a factor of another, then we can determine if two singular braids are related by a singular Markov move.

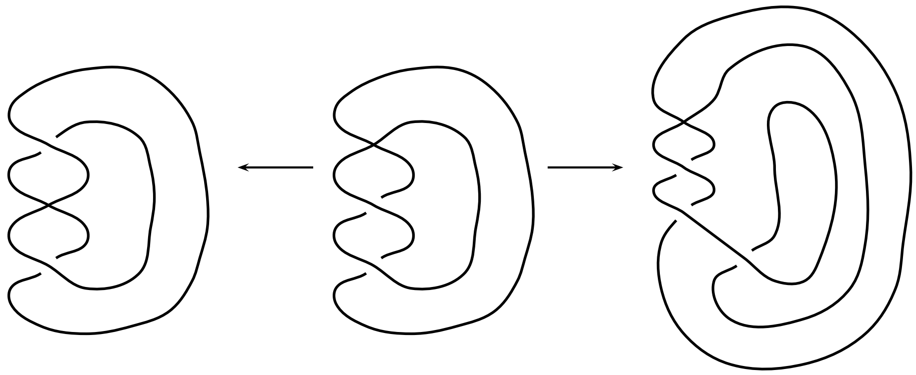

Figure 7: Markov moves.

Given two words W and V over the generators, we will write $W \equiv V$ to indicate when the two words are the same letter for letter, and $[W] = [V]$ to indicate that they represent the same element in the monoid. Given a presentation of a monoid M, and words W and V over the generators, the problems of determining when $[W] = [V]$, when $[W] = [VX]$ for some word X and when $[XW] = [VX]$ for some word X are called the *word, division* and *conjugacy problems* respectively. This paper deals with a solution in $\mathcal{SB}_n$ to the first two problems. The author also has a solution to the conjugacy problem. The problem is first considered in the submonoid of $\mathcal{SB}_n$ consisting of *positive singular braids*. It turns out that for any word W over $S \cup S^{-1} \cup T$, there exist words W^- over S^{-1} and W^+ over $S \cup T$ such that $[W] = [W^- W^+]$. If a singular braid can be represented by a word over $S \cup T$ it is called a *positive singular braid.*

2 The positive singular braid monoid.

We define the positive singular braid monoid on n strings, denoted $\mathcal{SB}_n^+$, to be the monoid generated by S and T, subject to the relations:

$$\begin{array}{rll} \sigma_i\sigma_j = \sigma_j\sigma_i, \quad \tau_i\sigma_j = \sigma_j\tau_i \text{ and } \tau_i\tau_j = \tau_j\tau_i & & \text{if } |i-j| > 1, \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ and } \tau_i\sigma_j\sigma_i = \sigma_j\sigma_i\tau_j & & \text{if } |i-j| = 1, \\ \tau_i\sigma_i = \sigma_i\tau_i & & \text{for all } i. \end{array}$$

This is obtained from the presentation of $\mathcal{SB}_n$ by just excluding all inverse generators and all relations involving the inverse generators. It can be shown [5, Theorem 19] that the monoid of positive singular braids on n strings embeds in $\mathcal{SB}_n$. This is analogous to the result of Garside [6, Theorem 4] that the monoid of positive braids embeds in the braid group.

The presentation for $\mathcal{SB}_n^+$ has a number of special properties. Let

$$\mathcal{R}^\Sigma = \{(U, V), (V, U) \mid U = V \text{ is a relation } \}.$$

We say a presentation has

- the property **U** (for *uniqueness*) if for each pair of generators (a, b) there is at most one (aU_1, bU_2) in $\mathcal{R}^\Sigma$;
- the property **C** (for *cancellativity*) if there are no pairs (aU_1, aU_2) in $\mathcal{R}^\Sigma$;
- the property **H** (for *homogeneity*) if $(U, V) \in \mathcal{R}^\Sigma$ implies the lengths of U and V must be the same; and
- the property **R** (for *reduction*) if whenever $[aV] = [bW]$, there are words U_1, U_2 and X such that $(aU_1, bU_2) \in \mathcal{R}^\Sigma \cup \{(x, x) \mid x \text{ is a generator } \}$, and $[V] = [U_1X]$ and $[W] = [U_2X]$.

The reader can see, by inspection of the relations, that the presentation for $\mathcal{SB}_n^+$ has the properties **U**, **C** and **H**. It also has the property **R**, although this is much harder to check (see [5, Lemma 14]). Brieskorn and Saito [4, Lemma 2.1, *Reduction Lemma*] were the first to recognise property **R** as being significant, in that case in the context of positive Artin monoids. However Garside [6, Theorem 1.2] had earlier shown that the monoid of positive braids has this property.

These four properties are the essence of the solution to the word problem described here, and any presentation with these four properties has solvable word and division problem. Monoids with such a presentation have a number of special properties, making them somewhat rare. The following two results indicate some of the algebraic properties these combinatorial properties imply.

Proposition 1 *If a monoid M has a presentation with the properties* **C** *and* **R** *then M is left cancellative.*

Proof. Suppose $[aW] = [aV]$. Then by **R**, there are (possibly empty) words V_1, V_2 and X such that $(aV_1, aV_2) \in \mathcal{R}^\Sigma \cup \{(a,a) \mid a \in \mathcal{A}\}$, and

$$[V] = [V_1X] \quad \text{and} \quad [W] = [V_2X].$$

By **C**, $V_1$and V_2 must be empty, so $[V] = [X] = [W]$. □

A word V *divides* W if there is a word X such that

$$[W] = [VX].$$

Then we also say that W *is a multiple of* V. If W is a multiple of every word in a set $\Omega = \{V_1, \ldots, V_k\}$ then W *is a common multiple of* Ω. A word Z is a *least common multiple* of Ω if it divides every common multiple of Ω.

If M is a monoid with the property **H** then all words representing the same element must have the same length. It is an easy exercise to show that M must then have unique least common multiples, when a least common multiple exists.

Theorem 2 ([5], Corollary 12) *Suppose that M has a presentation $\langle \mathcal{A} \mid \mathcal{R} \rangle$ with the properties* **U**, **C**, **H** *and* **R**. *Then whenever a set of words $\Omega = \{V_1, \ldots, V_k\}$ has a common multiple, it has a least common multiple which is unique.*

If $\Omega = \{a, b\}$, a pair of generators, the proof goes quite easily, as follows. We first show that if $(aU, bV) \in \mathcal{R}^\Sigma$ then $[aU] = [bV]$ is a least common multiple of a and b. It is clearly a common multiple. If $[aX] = [bY]$ is any common multiple of a and b then by **R** there is a relation in $\mathcal{R}^\Sigma$ left dividing it. By the property **U**, that relation must be (aU, bV). Hence $[aU] = [bV]$ divides every common multiple of $a$and b, making it a least common multiple.

Now suppose that $\Omega = \{a, b\}$ has a common multiple Z. The property **R** ensures that there are words U, V and W such that $(aU, bV) \in \mathcal{R}^\Sigma$ and $[aUW] = [Z] = [bVW]$. Thus by the previous paragraph, $[aU] = [bV]$ is the least common multiple of Ω, and as remarked earlier, the **H** property gives uniqueness.

We do not provide here a proof of when Ω is an arbitrary set of words. For more details on the proof and the constructions defined below, see [5]. Given that $\mathcal{SB}_n^+$ has the properties **U**, **C**, **H** and **R**, we can get on with finding a solution to the word problem.

For each generator a we define K_a, a partial operator on words, with the property that whenever a word W is divisible by a, the word $K_a(W)$ is defined and begins with the letter a. This operator is defined recursively on word length, and so is calculable. The job of K_a is to determine if the letter a divides a word, and if so to factorize the word into a and its quotient.

Given two words W and V, the word (W/V) is defined precisely when V divides W, and is calculated in the following way. Suppose $V \equiv a_1 \cdots a_k$. Then since V divides W, a_1 divides W, and so $K_{a_1}(W)$ is defined and begins with a_1. Write ${}^{a_1^{-1}}K_{a_1}(W)$ for the word obtained by removing the first letter, a_1, from $K_{a_1}(W)$. This process can be continued, and we define:

$$(W/V) \equiv {}^{a_k^{-1}}K_{a_k}(\cdots {}^{a_2^{-1}}K_{a_2}({}^{a_1^{-1}}K_{a_1}(W))\cdots).$$

It is easy to see that (W/V) has the property that

$$[W] = [V(W/V)].$$

Thus the job of (W/V) is to determine when a word divides another, and when it does, to calculate the quotient.

In fact this is a solution to the division problem, as (W/V) exists precisely when V divides W. Thus we have the following solution to the word problem.

Theorem 3 ([5], Corollary 6) $[W] = [V]$ *precisely when* (W/V) *is the empty word.*

Define $\Lambda(W)$ to be the set of generators which divide the word W. This is calculable, as we can calculate $K_a(W)$ for each generator a and if $K_a(W)$ begins with a then a belongs in $\Lambda(W)$. Since W is a common multiple of $\Lambda(W)$ then a least common multiple, denoted $\Delta_{\Lambda(W)}$ exists. Define recursively on length a (total) operator N^+, by

$$N^+(W) \equiv \Delta_{\Lambda(W)} N^+(W/\Delta_{\Lambda(W)}).$$

The following result says that $N^+(W)$ is a *unique normal form* for $\mathcal{SB}_n^+$.

Theorem 4 ([5], Theorem 13) $[V] = [W]$ *precisely when* $N^+(V) \equiv N^+(W)$.

We can now return to $\mathcal{SB}_n$ to complete the story.

3 The word problem in $\mathcal{SB}_n$.

Recall that the $\mathcal{SB}_n$ has a presentation which can be obtained from that of $\mathcal{SB}_n^+$ by adding the generators S^{-1} (the inverses of the crossings S) and the free group relations $\sigma_i\sigma_i^{-1} = 1 = \sigma_i^{-1}\sigma_i$ for each i.

It can be shown that the set S has a least common multiple $\Delta \equiv \Delta_S$, known as the *fundamental element*, which indeed plays a fundamental role. It turns out that either Δ (when $n \leq 2$) or Δ^2 (when $n \geq 3$) freely generates the centre of $\mathcal{SB}_n$. This fact can be used to show that $\mathcal{SB}_n^+$ embeds in $\mathcal{SB}_n$(see [[5], Theorem 19]).

For any word W over $S \cup S^{-1} \cup T$ a least non-negative integer $q(W)$ can be calculated such that $[W] = [\Delta^{q(W)} W^+]$ for some word W^+ over $S \cup T$. Given such a decomposition of a word W, the operator N gives us a unique normal form for W:

$$N(W) \equiv \Delta^{q(W)} N^+(W^+),$$

where N^+ is the positive normal form defined previously. Then

Theorem 5 ([5], Theorem 22) *For any word W, $[N(W)] = [W]$. Moreover, $[V] = [W]$ if and only if $N(V) \equiv N(W)$.*

Since we can calculate $N(W)$ and $N(V)$, we have a solution to the word problem: to determine if $[V] = [W]$ we just have to check that $N(V)$ and $N(W)$ agree letter for letter.

References

[1] D. Armand-Ugon, R. Gambini & P. Mora, *Intersecting braids and intersecting knot theory,* J. Knot Theory Ramifications, **4** (1995),no.1, 1 - 12.

[2] J. Baez, *Link invariants and perturbation theory,* Lett. Math. Phys. 2 (1992), 43 - 51.

[3] Joan Birman, *New points of view in knot theory,* Bull. AMS (1993), 253 - 287.

[4] E. Brieskorn & K. Saito, *Artin-Gruppen und Coxeter-Gruppen,* Inventiones Math. **17**, 245 - 271, (1972).

[5] Ruth Corran, *A normal form for a class of monoids including the singular braid monoid,* Research Report 99-03, School of Mathematics and Statistics, University of Sydney.

[6] F.A. Garside, *On the braid group and other groups,* Quart. J. Math. Oxford (2), **20** (1969), 235-254.