Positive singular Artin monoids inject into their singular Artin monoids

Noelle Antony

Abstract

We define a map φ from a given singular Artin monoid to its corresponding group algebra and show that φ is faithful precisely when Birman's conjecture – that the desingularisation map is injective – is true. We discover combinatorial properties of φ which apply to positive singular Artin monoids of any, not necessarily finite, type and infer that φ is injective on pairs of words for which a common multiple exists. Furthermore φ preserves the Intermediate Property, derived by Corran, in the sense that if $\varphi(\tau_i U) = \varphi(\tau_j V)$ then $m_{ij} = 2$ or i = j. From this it follows that φ is injective for some classes of monoids which include singular Artin monoids of type $I_2(p)$, generalising a result of East. Finally, we invoke Paris' discovery, that all Artin monoids inject into their groups, as well as our combinatorial discoveries, to deduce that all positive singular Artin monoids embed into their corresponding singular Artin monoids, extending a result of Corran.

AMS Subject Classification: 20F36, 20M05, 20M30.

1 Preliminaries

We begin with a finite indexing set I, and we let Γ^M be a complete labelled graph with n vertices in one-to-one correspondence with a finite indexing set I and with edge labels from the set $\{3, 4, 5, \ldots, \infty\}$. For $i \neq j$ let m_{ij} denote the label of the edge between nodes i and j, or set $m_{ij} = 2$ if there is no such edge. Let $\langle xy \rangle^m$ denote the alternating product xyx... of length m. Put $S = \{\sigma_i | i \in I\}, T = \{\tau_i | i \in I\}$, and let $S^{-1} = \{\sigma_i^{-1} | i \in I\}$, the set of formal inverses of S. If X is a set then X^* refers to the free monoid generated by X. The Artin group of type M, denoted G_M , is the group generated by S subject to the relations

$$\langle \sigma_i \sigma_j \rangle^{m_{ij}} = \langle \sigma_j \sigma_i \rangle^{m_{ij}}$$
 for $i, j \in I$, and $m_{ij} \neq \infty$

denoted \mathscr{R}_1 and called the *braid relations*. The *positive Artin monoid of type M*, G_M^+ , is the monoid generated by S subject to the braid relations \mathscr{R}_1 . The *Coxeter group of type M* is the group generated by S subject to the preceding relations and the relations $\sigma_i^2 = 1$ for every *i* in *I*. In this way we see that Coxeter groups arise as quotient groups of Artin groups. If the Coxeter group of type *M* is finite, then *M* is said to be of *finite type*.

Except when explicitly stated, we assume througout this paper that M is of any type. The singular Artin monoid of type M, denoted SG_M , is the monoid generated by $S \cup S^{-1} \cup T$ and has as its defining relations \mathscr{R}_1 , the free group relations $\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = 1$ and the relations \mathscr{R}_2 listed below,

$$\begin{aligned} \tau_i \sigma_i &= \sigma_i \tau_i \quad \text{for all } i \text{ in } I, \\ \tau_i \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} &= \begin{cases} \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \tau_j & \text{ if } m_{ij} < \infty \text{ and is odd, or} \\ \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \tau_i & \text{ if } m_{ij} < \infty \text{ and is even,} \end{cases} \\ \tau_i \tau_j &= \tau_j \tau_i \quad \text{if } m_{ij} = 2. \end{aligned}$$

In arguments below we may regard a relation formally as an ordered pair of words. If X is a set of ordered pairs of words then $X^{\Sigma} = \{(U, V) \mid (U, V) \text{ or } (V, U) \in X\}.$

The special case when $I = \{1, ..., n\}$, $m_{ij} = 3$ when |i - j| = 1 and $m_{ij} = 2$ when $|i - j| \ge 2$ is the singular Artin monoid of type A_n and may be familiar to some readers as the *singular braid monoid on* n + 1 *strings*, denoted SB_{n+1} , which was introduced by Baez and Birman in [2] and [4] respectively. We say M is *right-angled* if $m_{ij} = \{2, \infty\}$ for $i, j \in I$; and $M = I_2(p)$ whenever $I = \{1, 2\}$ and $m_{12} = p$ for some $p \ge 3$.

If A and B are words in the above generators, we write $A \approx B$ if A can be transformed into B by the use of the set of defining relations of SG_M , and A = B if the two words are equal letter by letter.

We define the *positive singular Artin monoid*, denoted by SG_M^+ , to be the monoid generated by $S \cup T$ and the set \mathscr{R} of defining relations comprised of both \mathscr{R}_1 and \mathscr{R}_2 listed above. Where it does not cause confusion, elements of G_M , G_M^+ , SG_M and SG_M^+ may be referred to by words which represent them. If A and B are words in the generators S and T, we write $A \sim B$ if A can be transformed into B by the use of the set \mathscr{R} of defining relations. Theorems 1.1 (1) and (2) below are proved in [13] and [6] respectively:

Theorem 1.1. (1) Let A, B be words over S such that $A \approx B$. Then $A \sim B$.

(2) Assume M is of finite type and let A, B be words over $S \cup T$ such that $A \approx B$. Then $A \sim B$.

We denote by $\ell(A)$ the length of any word A over $S \cup T$. It is easy to see, by inspection of the defining relations, that SG_M^+ is homogeneous. We define the *reduction property* as in page 258 of [6]. By Lemma 15 of [6], cancellation and the reduction property hold in SG_M^+ . By *reduction* we mean an application of the reduction property.

Let A and B be words in $(S \cup T)^*$. We say A divides B or B is a multiple of A if there exists a word X in SG_M^+ such that $B \sim AX$ in which case we write $A \prec B$. We say A right divides B, or B is a right multiple of A, if there is a word X in SG_M^+ such that $B \sim XA$ in which case we write $B \succ A$.

Let $\Omega = \{A_1, A_2, \ldots, A_k\}$ be a set of words in $(S \cup T)^*$. If Ω has a common multiple then by Corollary 13 of [6], Ω has a least common multiple (unique up to equivalence) which we denote by $lcm(A_1, A_2, \ldots, A_k)$ or $lcm(\Omega)$. By homogeneity,

 $lcm(\Omega)$ when it exists has minimal length. If Ω has no common multiple then we write $lcm(A_1, A_2, \ldots, A_k) = \infty$.

Define a map φ from SG_M to the group algebra $\mathbb{Z}[G_M]$ induced by

$$\sigma_i^{\pm 1} \mapsto \sigma_i^{\pm 1}, \ \tau_i \mapsto \sigma_i^2 + 1 \quad \text{for } i \in I.$$

Then φ is easily verified to be a monoid homomorphism.

In Section 2, the Vassiliev homomorphism η is defined, we state Birman's conjecture and show that η may be replaced (up to composition) with the simpler homomorphism φ . Moreover, for finite type M, we show that if φ is injective on SG_M^+ then Birman's conjecture is true for SG_M ; this is followed by some observations regarding φ . In Section 3, we study the relationship between divisibility in SG_M^+ and the support of φ . In particular, we deduce that if $U, V \in SG_M^+, C \in G_M^+$ and $\varphi(U) = \varphi(V)$ then C divides U if and only if C divides V. Furthermore, we obtain that in SG_M^+ , φ is injective on pairs of words for which a common multiple exists. In Section 4, we prove that φ preserves the Intermediate Property which holds in SG_M^+ ; namely, if $\varphi(\tau_i U) = \varphi(\tau_i V)$ then $m_{ij} = 2$ or i = j. From this it follows that φ is injective for some classes of monoids one of which includes singular Artin monoids of type $I_2(p)$ generalising a result of East [7]. Finally, in Section 5, we discover that when M is of any (not necessarily finite) type, SG_M^+ injects into SG_M extending Theorem 1.1(2).

2 Birman's conjecture

The map η from SB_{n+1} to the group algebra $\mathbb{Z}[B_{n+1}]$ induced by

$$\sigma_i^{\pm 1} \mapsto \sigma_i^{\pm 1}, \ \tau_i \mapsto \sigma_i - \sigma_i^{-1}$$

is easily verified to be a monoid homomorphism; η is sometimes referred to as the Vassiliev homomorphism [15] or desingularisation map [14]. In Remark 1 of [4], Birman conjectured that η is faithful, so that the singular braid monoid embeds into the group algebra of the braid group. In [14], Paris proved the truth of the conjecture. In Remark 25 of [6], Corran observed that Birman's conjecture generalises to arbitrary Artin types since the Vassiliev homomorphism, η , from any singular Artin monoid to the group algebra of the corresponding Artin group is well defined by the above rule. In effect, Birman's conjecture was shown to hold when $M = I_2(p)$ and M is right-angled in [7] and [10] respectively. Thus we may conjecture the following:

Conjecture 1. The Vassiliev homomorphism $\eta : SG_M \longrightarrow \mathbb{Z}[G_M]$ is faithful, so that the singular Artin monoid embeds into the group algebra of the Artin group.

We write X = Y if X and Y are equal elements of $Im(\eta)$ which should not cause confusion with our use of equality for words.

For every $i \in I$ let $\delta_i = \sigma_i \tau_i$, and put $T' = \{\delta_i \mid i \in I\}$. In [14], Paris observed that SG_M is generated as a monoid by $S \cup S^{-1} \cup T'$ and admits a monoid presentation with

$$\begin{split} \delta_i \sigma_i &= \sigma_i \delta_i \quad \text{for all } i \in I, \\ \delta_i \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} &= \begin{cases} \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \delta_j & \text{if } m_{ij} < \infty \text{ and is odd, or} \\ \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \delta_i & \text{if } m_{ij} < \infty \text{ and is even,} \end{cases} \\ \delta_i \delta_j &= \delta_j \delta_i \quad \text{if } m_{ij} = 2. \end{split}$$

Thus the mapping $\sigma_i^{\pm 1} \mapsto \sigma_i^{\pm 1}$, $\tau_i \mapsto \delta_i$ for $i \in I$ induces an isomorphism $\mu : SG_M \to SG_M$, $\sigma_i^{\pm 1} \mapsto \sigma_i^{\pm 1}$, $\tau_i \mapsto \delta_i$. Furthermore, the Vassiliev homomorphism $\eta : SG_M \to \mathbb{Z}[G_M]$ is determined by

$$\eta(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}, \ \eta(\delta_i) = \sigma_i^2 - 1 \quad \text{for } i \in I.$$

The following Lemma 2.1 tells us that (up to composition) η may be replaced with the simpler homomorphism φ . The proof of the lemma employs Lemma 1(1) of [11]; there it is proved only for type A_n , but the argument is the same for any M.

Lemma 2.1. η is injective precisely when φ is injective, and for any elements A, B of SG_M ,

$$\varphi(A) = \varphi(B)$$
 if and only if $\eta(\mu(A)) = \eta(\mu(B))$.

Proof: Define the homomorphism, introduced in [11], $\psi : SG_M \to \mathbb{Z}[G_M]$ by $\psi(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}$ and $\psi(\tau_i) = \sigma_i + \sigma_i^{-1}$. Notice that for every $i \in I$,

$$\varphi(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}$$
 and $\varphi(\tau_i) = \psi(\delta_i),$

so that $\varphi = \psi \mu$. Moreover, by Lemma 1(1) of [11],

$$\eta(A) = \eta(B) \Leftrightarrow \psi(A) = \psi(B),$$

and the result now follows readily.

Define the homomorphism $\overline{\varphi}$ from $\mathcal{S}G_M^+$ to $\mathbb{Z}[G_M^+]$ by

$$\overline{\varphi}: \sigma_i \mapsto \sigma_i, \ \tau_i \mapsto \sigma_i^2 + 1 \ i \in I.$$

Thus we may conjecture the following:

Conjecture 2. $\overline{\varphi} : SG_M^+ \to \mathbb{Z}[G_M^+]$ is injective.

Observation 1 below tells us that Conjecture 2 implies Conjecture 1 whenever M is of finite type.

Let U be any word over $S \cup S^{-1} \cup T$ also regarded as an element of SG_M . A summand of $\varphi(U)$ is any word over $S \cup S^{-1}$ obtained by replacing any given instance of τ by σ^2 or 1. The support of $\varphi(U)$ is the set of summands of $\varphi(U)$. For example, in type A_2 , $\varphi(\tau_1 \sigma_2 \tau_1)$ has summands $\sigma_1^2 \sigma_2 \sigma_1^2$, $\sigma_2 \sigma_1^2$, $\sigma_1^2 \sigma_2$ and σ_2 .

The ensuing result is a consequence of Theorem 1.1(1):

Corollary 2.2. Let U, V be words over $S \cup T$, regarded alternatively as elements of SG_M and SG_M^+ , such that $\varphi(U) = \varphi(V)$. Then $\overline{\varphi}(U) = \overline{\varphi}(V)$.

Proof: Let F be any summand of $\varphi(U)$. Then F is a word over S, and there exists an element F' in the support of $\varphi(V)$ such that $F \approx F'$. Since F' is also over S, Theorem 1.1(1) gives $F \sim F'$. Hence, for every element F in the support of $\varphi(U)$ there is a corresponding summand F' of $\varphi(V)$ such that $F \sim F'$. By regarding U and V also as elements of SG_M^+ , we infer that $\overline{\varphi}(U) = \overline{\varphi}(V)$ as required. \Box

Define a map $^+$ from $(S \cup T)^*$ to S^* by $^+ : \sigma_i \mapsto \sigma_i, \tau_i \mapsto \sigma_i^2$, for every $i \in I$. Then it is easily verified that $^+$ induces a homomorphism : $SG_M^+ \to G_M^+$.

Remark 1. Whenever U, V are elements of $(S \cup T)^*$ with the same image under $\overline{\varphi}$, $U^+ \sim V^+$ as they both represent the unique monomial of maximal exponent sum of $\overline{\varphi}(U) = \overline{\varphi}(V)$.

Let $\Delta = \text{lcm}(\sigma_1, \dots, \sigma_n)$. Theorem 5.6 of [5] tells us that Δ exists precisely when M is of finite type, whilst by Section 5 of [6] the following holds:

Theorem 2.3. Let M be of finite type. For any word W over $S \cup S^{-1} \cup T_1$, where $T_1 \subseteq T$, there exists a word \overline{W} over $S \cup T_1$ and integer p such that $W \approx \Delta^p \overline{W}$.

Observation 1. Whenever M is of finite type, Conjecture 2 implies Conjecture 1.

Proof: Suppose M is of finite type, Conjecture 2 holds and that $\eta(U) = \eta(V)$ for some words U and V in $(S \cup S^{-1} \cup T')^*$, where without causing confusion, we denote the equivalence class of a word by the word itself. By noting that μ is an isomorphism, we deduce the existence of words U', V' such that $U = \mu(U')$ and $V = \mu(V')$; thus,

$$\eta(\mu(U')) = \eta(U) = \eta(V) = \eta(\mu(V')),$$

so by Lemma 2.1, $\varphi(U') = \varphi(V')$. By Theorem 2.3, there exist integers p and q, and words P, Q over $S \cup T$ such that $U' \approx \Delta^p P$ and $V' \approx \Delta^q Q$. Hence there exist positive integers k_1 , k_2 and k such that

$$\Delta^k U' \approx \Delta^{k_1} P$$
 and $\Delta^k V' \approx \Delta^{k_2} Q.$ (2.1)

Thus (by recalling Δ is over S),

$$\varphi(\Delta^{k_1} P) = \varphi(\Delta^k U') = \varphi(\Delta^k V') = \varphi(\Delta^{k_2} Q).$$

But k_1, k_2 are positive integers and P, Q are over $S \cup T$, so by Corollary 2.2, $\overline{\varphi}(\Delta^{k_1} P) = \overline{\varphi}(\Delta^{k_2} Q)$, whence $\Delta^{k_1} P \sim \Delta^{k_2} Q$ (since Conjecture 2 is assumed to be true). By (2.1), it follows that $\Delta^k U' \approx \Delta^k V'$. By cancellation, $U' \approx V'$, and hence

$$U = \mu(U') \approx \mu(V') = V$$

as required.

3 Common divisors and the support of φ

The following Lemma 3.1 tells us common "factors" of elements of SG_M with the same image under φ may be "cancelled out". The proof of the lemma employs Lemmas 1(1) and 2 of [11]; there they are proved only for type A_n , but the proofs proceed unmodified for any M.

Lemma 3.1. Let C, A and B be elements of SG_M such that $\varphi(CA) = \varphi(CB)$. Then $\varphi(A) = \varphi(B)$.

Proof: By Lemma 2.1,

$$\eta\left(\mu(C)\mu(A)\right) = \eta\left(\mu(CA)\right) = \eta\left(\mu(CB)\right) = \eta\left(\mu(C)\mu(B)\right),$$

whence $\eta(\mu(A)) = \eta(\mu(B))$ by Lemmas 1(1) and 2 of [11]. This implies that $\varphi(A) = \varphi(B)$, again by Lemma 2.1, as required.

Let U be any word over $S \cup T$, also regarded as an element of SG_M^+ . We call U prime if there exists an $s \in I$ such that $\sigma_s \not\prec U$. Let \mathcal{M}_U denote the summands of $\overline{\varphi}(U)$ that are prime. For example, in type A_2 , $\overline{\varphi}(\tau_1 \sigma_2 \tau_1)$ has summands $\sigma_1^2 \sigma_2 \sigma_1^2$, $\sigma_1^2 \sigma_2$, $\sigma_2 \sigma_1^2$, σ_2 and a routine calculation shows

$$\mathcal{M}_{\tau_1 \sigma_2 \tau_1} = \left\{ \sigma_1^2 \sigma_2, \ \sigma_2 \sigma_1^2, \ \sigma_2 \right\}.$$

Lemma 3.2. Let U, V be words in $(S \cup T)^*$, also regarded as elements of SG_M^+ , such that $\overline{\varphi}(U) = \overline{\varphi}(V)$. For every summand F of $\overline{\varphi}(U)$ there is a corresponding summand G of $\overline{\varphi}(V)$ such that $F \sim G$, and $F \in \mathcal{M}_U$ if and only if $G \in \mathcal{M}_V$.

Proof: Let F be any element in the support of $\overline{\varphi}(U)$. Then there exists an element G in the support of $\overline{\varphi}(V)$ such that $F \sim G$. Furthermore, if $F \in \mathcal{M}_U$, $\sigma_i \not\prec F \sim G$ for some $i \in I$; this implies that G is prime and so must be an element of \mathcal{M}_V . \Box

Lemma 3.3 below is a preliminary result to Proposition 3.4.

Lemma 3.3. Let W be a word over $S \cup T$, $a \in I$, and suppose $\sigma_a \not\prec W$. Then there exists a word $Z \in \mathcal{M}_W$ that is not divisible by σ_a .

Proof: We prove the result by induction on $\ell(W)$ which holds trivially if W is the empty word. So assume $W \neq 1$, and as an inductive hypothesis, that the result holds for words of length $< \ell(W)$. Then $W = \alpha_r W_1$ for some word $W_1, r \in I$ and $\alpha = \sigma$ or τ .

Suppose first that r = a. Then $\sigma_a \not\prec W = \alpha_a W_1$ gives $\alpha = \tau$, and since σ_a and τ_a commute, $\sigma_a \not\prec W_1$. By the inductive hypothesis, we infer the existence of a word $Y \in \mathcal{M}_{W_1}$ such that $\sigma_a \not\prec Y$. Notice that since $W = \tau_a W_1$, Y is also an element of \mathcal{M}_W . Putting Z = Y thus gives the desired result.

Assume then that $m_{ra} \ge 2$. There exists a word W_2 and a largest integer q such that

$$W = \alpha_r W_1 \sim \alpha_r \langle \sigma_a \sigma_r \rangle^q W_2 \text{ and } \sigma_c \not\prec W_2, \tag{3.1}$$

where c = a if q is even and c = r if q is odd. By the inductive hypothesis, we deduce the existence of a word Y in \mathcal{M}_{W_2} such that $\sigma_c \not\prec Y$. Observe that $\sigma_a \prec \alpha_r \langle \sigma_a \sigma_r \rangle^{m_{ra}-1}$ whenever $m_{ra} < \infty$ and that $\sigma_a \not\prec \alpha_r W_1 = W$; this tells us that $0 \le q \le m_{ra} - 2$. Put $Y' = \lambda_r \langle \sigma_a \sigma_r \rangle^q Y$ where $\lambda_r = \sigma_r^2$ if $\alpha = \tau$ and $\lambda_r = \sigma_r$ if $\alpha = \sigma$. Then Y' is clearly a summand of $\overline{\varphi} (\alpha_r \langle \sigma_a \sigma_r \rangle^q W_2)$. Furthermore, if σ_a were to divide Y', reduction would show that σ_c divides Y which would contradict that $\sigma_c \not\prec Y$. This implies $\sigma_a \not\prec Y'$, so $Y' \in \mathcal{M}_{\alpha_r \langle \sigma_a \sigma_r \rangle^q W_2}$. Certainly $\overline{\varphi}(W) = \overline{\varphi}(\alpha_r \langle \sigma_a \sigma_r \rangle^q W_2)$, where by (3.1), W and $\alpha_r \langle \sigma_a \sigma_r \rangle^q W_2$ are regarded as (the same) elements of SG_M^+ . By Lemma 3.2, we deduce that $\sigma_a \not\prec Y' \sim Z$ for some word $Z \in \mathcal{M}_W$ as required, and the result follows by induction.

Proposition 3.4. Let U, V be words in $(S \cup T)^*$, also regarded as elements of SG_M , such that $\varphi(U) = \varphi(V)$, and let C be any word over S. Then C divides U if and only if C divides V.

Proof: We first prove the "only if " part of the result. By Corollary 2.2, $\overline{\varphi}(U) = \overline{\varphi}(V)$. Let $s \in I$ and suppose that $\sigma_s \prec U$ yet $\sigma_s \not\prec V$. Then $U \sim \sigma_s U_1$ for some word U_1 , and by Lemma 3.3, there exists a word $X \in \mathcal{M}_V$ such that $\sigma_s \not\prec X$. By Lemma 3.2, we infer the existence of a word $Y \in \mathcal{M}_{\sigma_s U_1}$ such that $X \sim Y$. But Y is a summand of $\overline{\varphi}(\sigma_s U_1)$, whence $Y = \sigma_s Y'$ for some word Y' in the support of $\overline{\varphi}(U_1)$. Thus $\sigma_s \not\prec X \sim Y = \sigma_s Y'$, a contradiction; so $\sigma_s \prec U$ only if $\sigma_s \prec V$. This proves the result for $\ell(C) = 1$, and by noting that it holds trivially for $\ell(C) = 0$, starts an induction. So assume that C divides U and $\ell(C) \ge 2$. Then there exists a letter a in S and non-empty word C_1 over S such that $C = C_1 a$ and $U \sim C_1 a U_1$ for some word U_1 over $S \cup T$. By the inductive hypothesis, we derive the existence of a word V_1 over $S \cup T$, such that $V \sim C_1 V_1$. Thus, $\varphi(C_1 a U_1) = \varphi(U) = \varphi(V) = \varphi(C_1 V_1)$, whence $\varphi(a U_1) = \varphi(V_1)$ by Lemma 3.1, so that a divides V_1 . Hence $C = C_1 a$ also divides $V \sim C_1 V_1$ as required, and the result for any $\ell(C)$ follows by induction. Swapping the roles of U and V in the preceding argument gives the "if" part of the claim. \Box

The proof of the following result proceeds identically to that of Proposition 2.1 of [1]:

Lemma 3.5. Let $j \in I$ and W any word in $(S \cup T)^*$ such that $lcm(\tau_j, W)$ exists. Then σ_j divides W^+ precisely when either σ_j or τ_j divides W.

Lemma 3.6. Let U, V be words in $(S \cup T)^*$ also regarded as elements of SG_M^+ such that $\overline{\varphi}(U) = \overline{\varphi}(V)$. Suppose τ_j divides U and $\operatorname{lcm}(\tau_j, V)$ exists. Then either σ_j or τ_j is a common divisor of U and V.

Proof: We have $\sigma_j \prec U^+ \sim V^+$, so by Lemma 3.5, we infer that $V \sim \alpha_j V'$ for some word V' over $S \cup T$, $\alpha = \sigma$ or τ . If $\alpha = \tau$, it is evident that τ_j is a common divisor of U and V; whilst if $\alpha = \sigma$ then by Proposition 3.4 we see that σ_j also divides U and hence is a common divisor of U and V.

Define monoid homomorphisms ϵ and \mathcal{N} from $\mathcal{S}G_M$ to $(\mathbb{Z}, +)$ by

$$\epsilon : \sigma_i^{\pm 1} \mapsto \pm 1, \ \tau_i \mapsto 0, \ \mathcal{N} : \sigma_i^{\pm 1} \mapsto 0, \ \tau_i \mapsto 1 \quad \text{for } i \in I.$$

So $\epsilon(A)$ is the exponent sum of sigmas and $\mathcal{N}(A)$ counts the number of singularities (taus) of any word A in $\mathcal{S}G_M$.

Lemma 3.7. Let U and V be words over $S \cup T$ regarded as elements of SG_M , and suppose $\varphi(U) = \varphi(V)$. Then $\ell(U) = \ell(V)$ and $\mathcal{N}(U) = \mathcal{N}(V)$.

Proof: By Corollary 2.2, $\overline{\varphi}(U) = \overline{\varphi}(V)$, whence $U^+ \sim V^+$. Thus

$$\epsilon(U) + 2\mathcal{N}(U) = \ell(U^+) = \ell(V^+) = \epsilon(V) + 2\mathcal{N}(V).$$
(3.2)

Notice that for every word A over $S \cup T$ there is a unique monomial, represented by A^- , obtained by replacing each τ_i by 1, in the support of $\varphi(A)$ with minimal exponent sum $\epsilon(A)$. Then since $\overline{\varphi}(U) = \overline{\varphi}(V)$, it follows that $U^- \sim V^-$ which gives

$$\epsilon(U) = \ell(U^{-}) = \ell(V^{-}) = \epsilon(V). \tag{3.3}$$

By (3.2) and (3.3), we infer that $\mathcal{N}(U) = \mathcal{N}(V)$, whence

$$\ell(U) = \epsilon(U) + \mathcal{N}(U) = \epsilon(V) + \mathcal{N}(V) = \ell(V)$$

as required.

Theorem 3.8. Over $S \cup T$, φ is injective on pairs of words for which a common multiple *exists.*

Proof: Let U, V be words in $(S \cup T)^*$ such that $\varphi(U) = \varphi(V)$ and $\operatorname{lcm}(U, V)$ exists. We show $U \sim V$ by induction on $\ell(U)$. By Corollary 2.2, $\overline{\varphi}(U) = \overline{\varphi}(V)$. If U is the empty word, there is nothing to show, so suppose $\ell(U) \geq 1$. If $\tau_j \prec U$ then either σ_j or τ_j is a common divisor of U and V by Lemma 3.6; whilst if $\sigma_j \prec U$ then σ_j also divides V by Proposition 3.4. In either case we see that $U \sim \alpha_j U'$ and $V \sim \alpha_j V'$ for some words U', V' and $\alpha = \sigma$ or τ . By Lemma 3.1, this implies that $\varphi(U') = \varphi(V')$, and since $\operatorname{lcm}(\alpha_j U', \alpha_j V') \sim \operatorname{lcm}(U, V) \neq \infty$, we obtain that $\operatorname{lcm}(U', V')$ also exists. By the inductive hypothesis, we deduce that $U' \sim V'$, whence $U \sim \alpha_j U' \sim \alpha_j V' \sim V$ as required, and the result now follows by induction.

4 The Intermediate Lemma

In this section we prove that the Intermediate Property – discovered in Intermediate Lemma of [6] and expressed in Lemma 4.1 below – is preserved under φ . As a corollary we deduce that φ is injective for a class of monoids which include singular Artin monoids of type $I_2(p)$.

Lemma 4.1. Let U, V be words in $(S \cup T)^*$ such that $\tau_i U \sim \tau_j V$. Then i = j or $m_{ij} = 2$.

The ensuing Lemma 4.2 is a preliminary result to Theorem 4.3 below.

Lemma 4.2. Let $F, G \in (S \cup T)^*$, $i, j \in I$, and suppose $\sigma_j \not\prec \sigma_i^2 F \sim G$. Then either $\sigma_i \not\prec \sigma_j^2 G$ or $m_{ij} = 2$.

Proof: Cleary $m_{ij} \geq 2$ since $\sigma_j \not\prec \sigma_i^2 F$. So suppose $m_{ij} \geq 3$ yet $\sigma_j^2 G \sim \sigma_i H$ for some word H. By reduction, $\sigma_i \prec \sigma_j G$, which gives by another reduction, $G \sim \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} G'$ for some word G'. Thus,

$$\sigma_i^2 F \sim G \sim \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} G' = \sigma_i \langle \sigma_j \sigma_i \rangle^{m_{ij}-2} G'.$$

By noting that $m_{ij} \ge 3$, cancellation applied to the preceding equivalence shows that $\sigma_j \prec \sigma_i F$, so by reduction,

$$F \sim \langle \sigma_j \sigma_i \rangle^{m_{ij} - 1} F_1 \tag{4.1}$$

for some word F_1 . Put c = j if m_{ij} is odd and c = i if m_{ij} is even. Then

$$\sigma_j \prec \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \sigma_c^2 F_1 \sim \sigma_i^2 \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} F_1 \sim \sigma_i^2 F_1$$

by (4.1), and this contradicts the hypothesis.

Theorem 4.3. Let $U = \tau_i U_1$, $V = \tau_j V_1$ be words in $(S \cup T)^*$, also regarded as elements of SG_M , such that $\varphi(U) = \varphi(V)$. Then i = j or $m_{ij} = 2$.

Proof: Suppose $U = \tau_i U_1$ and $V = \tau_j V_1$ provide a counterexample. That is, $\varphi(\tau_i U_1) = \varphi(\tau_j V_1)$ but $m_{ij} \geq 3$. Suppose further that this counterexample is minimal with respect to $\ell(U)$ which by Lemma 3.7 is equal to $\ell(V)$. Then $\ell(U) \geq 2$, since $\ell(U) = \ell(V) = 1$ gives $\sigma_i^2 + 1 = \varphi(U) = \varphi(V) = \sigma_j^2 + 1$ and shows i = j. We first prove that $V = \tau_j V_1$ is not divisible by σ_j . Suppose, by way of contradiction, that it is. Reduction yields a word P such that $V_1 \sim \sigma_j P$, and by recalling that $\varphi(U) = \varphi(V)$, Proposition 3.4 implies that σ_j also divides $U = \tau_i U_1$, so by reduction again, $U_1 \sim \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} Q$ for some word Q. Put $C = \langle \sigma_j \sigma_i \rangle^{m_{ij}-1}$. Then

$$U = \tau_i U_1 \sim \tau_i CQ \sim C\tau_d Q \tag{4.2}$$

where d = j if m_{ij} is odd and d = i if m_{ij} is even. Since C is over S, Proposition 3.4 may be applied and this shows that

$$C = \sigma_i \langle \sigma_i \sigma_j \rangle^{m_{ij-2}} \prec V \sim \tau_j \sigma_j P \sim \sigma_j \tau_j P.$$

By recalling that $m_{ij} \ge 3$, we deduce (after cancelling) that $\sigma_i \prec \tau_j P$, so by reduction, $P \sim \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} P'$ for some word P' over $S \cup T$. Thus,

$$V \sim \sigma_j \tau_j P \sim \sigma_j \tau_j \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} P' \sim \sigma_j \langle \sigma_i \sigma_j \rangle^{m_{ij}-1} \tau_c P'$$

$$\sim \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \sigma_d \tau_c P'$$

$$= C \sigma_d \tau_c P',$$

where $m_{cd} \ge 3$ (since $\{c, d\} = \{i, j\}$). When combined with (4.2), this implies

$$\varphi(C\sigma_d\tau_c P') = \varphi(V) = \varphi(U) = \varphi(C\tau_d Q),$$

so by Lemma 3.1, $\varphi(\sigma_d \tau_c P') = \varphi(\tau_d Q)$. By invoking Proposition 3.4 again, we infer that σ_d divides $\tau_d Q$, and by reduction, this yields a word Q' such that $Q \sim \sigma_d Q'$. Hence

$$\varphi(\sigma_d \tau_c P') = \varphi(\tau_d Q) = \varphi(\tau_d \sigma_d Q') = \varphi(\sigma_d \tau_d Q')$$

so by Lemma 3.1 again, $\varphi(\tau_c P') = \varphi(\tau_d Q')$, and $m_{cd} \geq 3$. Since $\ell(V) > \ell(\tau_c P')$, this contradicts the minimality of $\ell(U) = \ell(V)$. Thus $\sigma_j \not\prec V$, and so by a final application of Proposition 3.4, we deduce that $\sigma_j \not\prec U$. Observe that $\overline{\varphi}(U) = \overline{\varphi}(V)$ by Corollary 2.2. Now let F be an element of \mathcal{M}_U such that $\sigma_j \not\prec F$, the existence of which is assured by Lemma 3.3. Assume further that $\ell(F)$ is maximal; that is,

if
$$\sigma_j \not\prec F'$$
 and $F' \in \mathcal{M}_U$ then $\ell(F') \le \ell(F)$. (4.3)

By noting that $U = \tau_i U_1$, we infer the existence of a summand F_1 of $\overline{\varphi}(U_1)$ such that either $F = \sigma_i^2 F_1$ or $F = F_1$. Suppose that $F = F_1$, and put $F' = \sigma_i^2 F_1$. Then F' is clearly an element in the support of $\overline{\varphi}(U)$ and $\ell(F') > \ell(F)$. By (4.3), we deduce that $\sigma_j \prec \sigma_i^2 F_1$. Since $m_{ij} \ge 3$, the reduction property implies that σ_j divides $F_1 = F$, which contradicts that $\sigma_j \not\prec F$. This shows that $F = \sigma_i^2 F_1$. By Lemma 3.2, there exists a word $G \in M_V$ such that $F \sim G$. By recalling $V = \tau_j V_1$, we deduce that either $G = \sigma_j^2 G_1$ or $G = G_1$, for some word G_1 in the support of $\overline{\varphi}(V_1)$. The first possibility must be excluded since $\sigma_j \not\prec F \sim G$, so $G = G_1$. Thus,

$$\sigma_j \not\prec \sigma_i^2 F_1 = F \sim G = G_1 \text{ and } G_1 \in \mathcal{M}_{V_1}.$$

$$(4.4)$$

Put $G' = \sigma_j^2 G_1$, and note that it is a summand of $\overline{\varphi}(V) = \overline{\varphi}(\tau_j V_1)$. By Lemma 4.2, $\sigma_i \not\prec G'$, so G' is an element of \mathcal{M}_V . By Lemma 3.2, $G' \sim F'$ for some word $F' \in \mathcal{M}_U$, and by (4.4), $\ell(G') = 2 + \ell(G_1) = 2 + \ell(F)$. Hence

$$\sigma_i \not\prec \sigma_j^2 G_1 = G' \sim F', \ F' \in \mathcal{M}_U \text{ and } \ell(F') = 2 + \ell(F).$$

$$(4.5)$$

Since F' is a summand of $\overline{\varphi}(U) = \overline{\varphi}(\tau_i U_1)$, we infer the existence of a word F_2 in the support of U_1 such that either $F' = \sigma_i^2 F_2$ or $F' = F_2$. As the first possibility evidently contradicts (4.5), we deduce that $F' = F_2$. Put $F'' = \sigma_i^2 F_2$, and note that it is a summand of $\overline{\varphi}(\tau_i U_1) = \overline{\varphi}(U)$. By Lemma 4.2 and (4.5), $\sigma_j \not\prec \sigma_i^2 F' = F''$, whence the latter word is an element of \mathcal{M}_U . When combined with (4.3), this implies that $\ell(F'') \leq \ell(F)$. However, $F'' = \sigma_i^2 F_2 = \sigma_i^2 F'$, so by (4.5),

$$\ell(F'') = 2 + \ell(F') = 4 + \ell(F),$$

a contradiction.

Fix $i, j \in I$ such that $m_{ij} \geq 3$. Let T_{ij} and T_{ij}^+ denote the sets of equivalence classes of words in $(S \cup S^{-1} \cup {\tau_i, \tau_j})^*$ and $(S \cup {\tau_i, \tau_j})^*$ under \approx and \sim respectively. Then T_{ij} and T_{ij}^+ are both submonoids of SG_M and SG_M^+ respectively.

Corollary 4.4. The restriction of $\overline{\varphi}$ from T_{ij}^+ to the group algebra $\mathbb{Z}[G_M^+]$ is injective. In particular, the desingularisation map $\eta : SG_{I_2(p)} \to \mathbb{Z}[G_{I_2(p)}]$ is injective.

Proof: Suppose that U, V in $(S \cup \{\tau_i, \tau_j\})^*$ provide a counterexample. That is, assume that $U \not\sim V$ yet $\overline{\varphi}(U) = \overline{\varphi}(V)$. Note that trivially $\varphi(U) = \varphi(V)$ where U, V are also regarded as elements of SG_M . Suppose further that this counterexample is minimal with respect to $\ell(U)$ which, by Lemma 3.7, is the same as $\ell(V)$. Certainly $\ell(U) \ge 2$. If $U \sim CU'$, $V \sim CV'$ for some non-empty word C then $\overline{\varphi}(U') = \overline{\varphi}(V')$ by Lemma 3.1 and Corollary 2.2, $U' \not\sim V', \ell(U') < \ell(U)$, and hence the minimality of $\ell(U)$ is contradicted. Thus U, V have no common divisor from which we infer, by Proposition 3.4, that U and V are not divisible by any generator from S. This tells us that $U = \tau_r U_1$ and $V = \tau_s V_1$ for some words U_1, V_1 in T_{ij}^+ and generators $\tau_r, \tau_s \in \{\tau_i, \tau_j\}$. Since $m_{ij} \ge 3$, we deduce from Theorem 4.3 that r = s, so τ_r is a common divisor. By noting $I_2(p)$ is of finite type, the last statement of the result follows by Observation 1, since $T_{12}^+ = SG_{I_2(p)}^+$.

5 Embedding SG_M^+ into SG_M

Recall that in [13], Paris discovered that all positive monoids inject into their groups (Theorem 1.1(1)), whilst in [6], Corran showed that SG_M^+ embeds into SG_M whenever M is of finite type (Theorem 1.1(2)). It would thus seem natural to ask whether the latter result can be extended to all singular Artin monoids, which is what we derive in this section (Theorem 5.3).

Let U, V be words over $S \cup S^{-1} \cup T$. We say U and V differ by an elementary transformation if there are words X and Y and a relation $(\rho_1, \rho_2) \in \mathscr{R}^{\Sigma}$ such that $V = X\rho_1 Y$ and $U = X\rho_2 Y$. We say that a word V is obtained from U by a trivial insertion if there are words X, Y and a letter $a \in S \cup S^{-1}$ such that U = XY and $V = Xaa^{-1}Y$. In this case we also say that U is obtained from V by a trivial deletion.

The reader is reminded of the monoid homomorphism \mathcal{N} from $\mathcal{S}G_M$ to $(\mathbb{Z}, +)$ defined by $\sigma_i^{\pm 1} \mapsto 0$, $\tau_i \mapsto 1$. Thus \mathcal{N} counts the number of taus in any given word. Now let Wbe a word over $S \cup S^{-1} \cup T$, and suppose $\mathcal{N}(W) = k \ge 1$. Then there are words W_i over $S \cup S^{-1}$ and generators $\tau_{a_i} \in T$ such that

$$W = W_0 \tau_{a_1} W_1 \tau_{a_2} W_2 \dots W_{k-1} \tau_{a_k} W_k.$$

For $r = 1, \ldots, k$, let

$$\theta_r(W) = W_0 \tau_{a_1} W_1 \dots W_{r-2} \tau_{a_{r-1}} W_{r-1} \sigma_{a_r} W_r \tau_{a_{r+1}} W_{r+1} \dots W_{k-1} \tau_{a_k} W_k;$$

hence θ_r reduces the number of taus of W by 1.

Lemma 5.1. Let W, V be equivalent words over $S \cup S^{-1} \cup T$, and suppose $\mathcal{N}(W) = k \ge 1$. Then for every $r \in \{1, \ldots, k\}$ there exists $s \in \{1, \ldots, k\}$ such that $\theta_r(W) \approx \theta_s(V)$.

Proof: Let r be any integer such that $1 \le r \le k$. Since $W \approx V$ there is a sequence Z_1, \ldots, Z_t of words over $S \cup S^{-1} \cup T$ such that $W = Z_1 \approx Z_2 \approx \ldots \approx Z_t = V$ and Z_{i+1} is obtained from Z_i by an elementary transformation or by a trivial insertion or deletion. If t = 1, the result is trivial and hence starts an induction. So suppose t is at least 2. If Z_1 and Z_2 differ by an elementary transformation, inspection of \mathscr{R} gives $\theta_r(Z_1) \approx \theta_r(Z_2)$ if the relation involves any σ and either $\theta_r(Z_1) \approx \theta_{r+1}(Z_2)$, $\theta_r(Z_2)$ or $\theta_{r-1}(Z_2)$ if the relation involves commuting τ 's; whilst if Z_2 is obtained from Z_1 by a trivial insertion or deletion, it is evident that $\theta_r(Z_1) \approx \theta_r(Z_2)$. By the inductive hypothesis, we deduce that $\theta_r(Z_2) \approx \theta_s(Z_t)$ for some $s \in \{1, \ldots, k\}$, whence

$$\theta_r(W) = \theta_r(Z_1) \approx \theta_r(Z_2) \approx \theta_s(Z_t) = \theta_s(V)$$

as required. The result now follows by induction.

In [8], it was shown that the singular braid monoid on n+1 strings (that is, the singular Artin monoid of type A_n) can be embedded in a group. The group constructed by the authors relies heavily on the geometry of singular braids in space; more specifically, it has a geometric interpretation as singular braids with two types of (cancelling) singularities. By employing purely algebraic methods, Paris [14] gave another proof of the fact that singular braid monoids inject into groups. In effect, all singular Artin monoids embed into groups. This was shown (chronologically and with completely different proofs) in [3], [12] and [10]. An evident corollory of the fact that SG_M injects into a group is that left and right cancellation hold in SG_M ; namely,

Proposition 5.2. Let C, W, V be words over $S \cup S^{-1} \cup T$ such that either $CW \approx CV$ or $WC \approx VC$. Then $W \approx V$.¹

Theorem 5.3. Let W, V be words over $S \cup T$ such that $W \approx V$. Then $W \sim V$.

Proof: Put $k = \mathcal{N}(W)$. If k = 0, the result follows by Theorem 1.1(1) and starts an induction. So assume $k \ge 1$. Certainly $\varphi(W) = \varphi(V)$. Suppose $\operatorname{lcm}(W, V) = \infty$. But $W \sim CW', V \sim CV'$ for some words C, W' and V' over $S \cup T$, such that W', V' have no (non-trivial) common divisor. Thus $\operatorname{lcm}(W', V') = \infty$ and

$$CW' \sim W \approx V \sim CV',$$

so by Proposition 5.2, $W' \approx V'$; this implies $\varphi(W') = \varphi(V')$, and by Corollary 2.2, $\overline{\varphi}(W') = \overline{\varphi}(V')$. Since W' and V' have no common divisor, Proposition 3.4 yields

$$W' = \tau_i W'', \quad V' = \tau_i V''$$

for some distinct $i, j \in I$ and words W'', V'' over $S \cup T$. By Theorem 4.3, $m_{ij} = 2$ (since $i \neq j$), whilst Lemma 3.6 gives

$$\operatorname{lcm}(\tau_j, W') = \infty. \tag{5.1}$$

¹The reader is referred to Proposition 5.1 of [9] for a (geometric) demonstration of this result, when $M = A_n$, without invoking the embedding of $(SB_{n+1} =) SG_{A_n}$ into a group.

But $\tau_i W'' = W' \approx V' = \tau_j V''$, so by Lemma 5.1,

$$\sigma_i W'' = \theta_1(\tau_i W'') \approx \theta_r(\tau_j V'') \quad \text{for some } r \in \{1, \dots, k\}.$$

The inductive hypothesis now tells us that $\sigma_i W'' \sim \theta_r(\tau_j V'')$, whence

$$\sigma_i W'' \sim \begin{cases} \sigma_j V'' & \text{if } r = 1, \\ \tau_j \ \theta_{r-1}(V'') & \text{if } 2 \le r \le k \end{cases}$$

If $\sigma_i W'' \sim \sigma_j V''$, reduction implies that $\sigma_j \prec W''$, so by noting that $m_{ij} = 2$, τ_i and σ_j commute, whence $\sigma_j \prec \tau_i W'' = W'$; Proposition 3.4 can now be invoked to deduce that W' and V' have a non-trivial common divisor, a contradiction. Hence $\sigma_i W'' \sim \tau_j \theta_{r-1}(V'')$. By recalling that $m_{ij} = 2$, another application of reduction gives $\tau_j \prec W''$, so that $\tau_j \prec \tau_i W'' = W'$; this clearly contradicts (5.1). Thus lcm(W, V) exists, so $W \sim V$ by Theorem 3.8, and the result follows by induction.

References

- N. Antony, http://www.maths.usyd.edu.au:8000/u/pubs/publist/preprints/2004/antony-12.html (accessed March 9, 2004).
- [2] J. Baez, *Link invariants of finite type and perturbation theory*, Lett. Math. Phys. **26** (1992), no. 1, 43-51.
- [3] G. Basset, *Quasi-commuting extensions of groups*, Comm. Algebra 28 (2000), 5443-5454.
- [4] J. S. Birman, New points of view in knot theory, Bull. Amer. Math. Soc. (N.S.) 28 (1993), no. 2, 253 286
- [5] E. Brieskorn and K. Saito, *Artin-Gruppen und Coxeter-Gruppen*, Invent. Math. **17** (1972), 245-271.
- [6] R. Corran, A normal form for a class of monoids including the singular braid monoid, J. Algebra 223 (2000), 256-282.
- [7] J. East, http://www.maths.usyd.edu.au:8000/u/pubs/publist/preprints/2002/east-8.html (accessed April 18, 2002, updated December 22, 2003).

- [8] R. Fenn, E. Keyman and C. Rourke, *The singular braid monoid embeds in a group*, J. Knot Theory Ramifications **7** (1998), no. 7, 881-892.
- [9] R. Fenn, D. Rolfsen and J. Zhu, *Centralizers in the braid group and the singular braid monoid*, Enseign. Math. (2) **42** (1996), no. 1-2, 75-96.
- [10] E. Godelle and L. Paris, http://math.u-bourgogne.fr/topolog/IMB2-publication.html année 2003, n.356 (accessed November 20, 2003).
- [11] A. Járai Jr, On the monoid of singular braids, Topology Appl. 96 (1999), 109-119.
- [12] E. Keyman, A class of monoids embeddable in a group, Turkish J. Math. 25 (2001), 299-305.
- [13] L. Paris, Artin monoids inject in their groups, Comment. Math. Helv. 77 (2002), 609-637.
- [14] L. Paris, http://math.u-bourgogne.fr/topolog/IMB2-publication.html année 2003, n.338 ArXiv:math.GR/0306422 v1 (accessed June 30, 2003).
- [15] V. Vassiliev, Cohomology of knot spaces, in V.I. Arnold (Ed.), *Theory of Singularities and its Applications*, Vol 1 (Amer. Math. Soc. 1990).