Singular Artin monoids of finite Coxeter type are automatic

Ruth Corran[1], Michael Hoffmann[2], Dietrich Kuske[3], Richard M. Thomas[2] *

[1] American University of Paris, 6 Rue du Colonel Combes, 75007 Paris, France
corran@aup.fr
[2] Dept of Computer Science, University of Leicester, Leicester LE1 7RH, England
mh55@mcs.le.ac.uk, rmt@mcs.le.ac.uk
[3] Technische Universität Ilmenau, Fachgebiet Theoretische Informatik, Postfach 100565, D-98684 Ilmenau, Germany dietrich.kuske@tu-ilmenau.de

Abstract. We consider the positive singular and the singular Artin monoids of finite type. These have been the subject of a great deal of recent research and the main purpose of this paper is to prove that these monoids are automatic. In order to do this we establish a new criterion for proving monoids automatic that may be of independent interest.

1 Introduction

The concept of an automatic group was introduced in [2,10] in order to describe a large class of naturally occurring groups with an easily solvable word problem. This was then extended to automatic monoids; see [6,16,18] for example. This notion (see Definition 1) uses the concept of a *transducer*, a finite automaton with two input tapes and two one-way heads. If these two heads are required to move synchronously, we speak of a *synchronous transducer*. As a transducer has two input tapes, its language can be described as a binary relation on the set of strings. Such a relation is said to be (*synchronously*) *rational* if it is the language of a (synchronous) transducer. Whilst the definition of automatic uses synchronously rational relations, one can also consider *asynchronously automatic* monoids where general rational relations are allowed; see [13] for a comparison of asynchronously automatic, automatic and other related classes of monoids.

When constructing an automaton it can be simpler to first build an asynchronous machine which then is transformed into a synchronous one. When considering automatic monoids and groups, one technique for this transformation has mainly been used: if the positions of the two asynchronously moving heads differ uniformly by at most k, then an equivalent synchronous automaton exists; this technique requires one to show that along any successful computation, *at any given time*, the difference does not exceed k (see [14]). Using a result of Frougny

* This work was begun while the first author was the recipient of a grant from the EPSRC (UK) and continued while she was a Marie Curie Postdoctoral Researcher (EU); the support of these two funding bodies is gratefully acknowledged. The second and fourth authors would like to thank Chen-Hui Chiu and Hilary Craig for all their help and encouragement.

and Sakarovitch [11], this can be relaxed to showing that, in any successful run, the difference is at most k in the *final* configuration (see Proposition 2 below).

In this paper we apply this new approach to singular Artin monoids of finite type. The most prominent example of this class of monoids consists of the braids on n strings. The Artin groups of finite type all share the remarkable properties of the braid group B_n and B_n may be studied very fruitfully in its guise as such a group. The braid group has applications in diverse areas such as combinatorial group theory, representation theory, trace monoids and low-dimensional topology; it has even been the focus of interest as a prospect for a public-key cryptosystem based on a non-Abelian group. Shortly after B_n was introduced by Artin, a presentation by generators and relations with remarkable properties was obtained which led to the definition of the more general Artin monoids; this motivates the currently developing theory of Garside structures.

The singular braid monoid SB_n was introduced in [1,3] to study Vassiliev knot invariants; the idea is that the strings of a braid can have intersections. In the same way that the braid group may be considered as an example of an Artin group, the definition of singular braid monoid may be extended to arbitrary Artin type and a *singular Artin monoid* is obtained [8]. Roughly speaking, a singular Artin monoid is an Artin monoid with some additional "singular" generators. We combine part of the normal form from [7] for Artin monoids with the singular parts of the braids to give automatic structures for singular Artin monoids.

As indicated above, the Artin groups of finite type are fundamental objects in the representation theory of reductive algebraic groups. The right-angled Artin groups, on the other hand, are in some sense at the other end of the spectrum from being of finite type, and indeed are precisely the trace groups – groups of fractions of trace monoids (or partially commuting monoids). Another interesting connection with the theory of trace monoids is that the submonoid consisting of the purely singular braids of a singular Artin monoid defined by a graph Γ is isomorphic to the trace monoid on a graph which is the complement of Γ. Thus the singular Artin monoid is some sort of blend of an Artin group with a trace monoid, and the normal form for the automatic structure we obtain in this paper is a blend between that for the (bi)automatic structure for Artin groups of finite type and the Foata normal form for traces.

The structure of the paper is as follows. In Section 2 we discuss the connection between automaticity and rational relations and establish the new criterion for automaticity (Proposition 2 referred to above). We then turn to the positive singular Artin monoid M_Γ in Section 3 and establish some basic properties there. We establish a set of normal forms for M_Γ in Section 4 and then use this in Section 5 to show that M_Γ is automatic (see Theorem 1). Lastly we consider the singular Artin monoid M_Γ^Δ in Section 6 and show that it is automatic as well (see Theorem 2). The proofs are often quite lengthy and combinatorial in nature and we do not give the full details here; instead we provide a sequence of lemmas and previously known facts that we have used to prove these theorems and we hope that these give the reader a feeling as to the overall structure of the proofs of these results.

2 Automaticity via rational relations

Let $(M, \cdot, 1)$ be a monoid. An *M-automaton* is a structure $\mathcal{A} = (Z, \delta, \iota, F)$ where Z is a finite set of states, $\delta \subseteq Z \times M \times Z$ is a finite transition relation with $(z, 1, z') \in \delta$ if and only if $z = z'$, $\iota \in Z$ is an initial state, and $F \subseteq Z$ is a set of accepting states; thus an M-automaton is a finite graph whose edges are labeled by elements of the monoid M. A run is a finite sequence $(z_i, m_i, z_{i+1})_{1 \leqslant i \leqslant n}$ of transitions; its label is the element $m_1 \cdot m_2 \cdots m_n$ of the monoid M. A run is successful if $z_1 = \iota$ and $z_{n+1} \in F$. The set $L(\mathcal{A})$ accepted by $\mathcal{A}$ is the set of labels of successful runs. A subset X of M is said to be *rational* if there is an M-automaton $\mathcal{A}$ with $X = L(\mathcal{A})$, i.e. if it is the behaviour of some M-automaton.

Any finite set $X \subseteq M$ is rational. If $X, Y \subseteq M$ are rational, then so are the following sets (see [9] for example):

- $X \cup Y$,
- $X \cdot Y = \{x \cdot y \,:\, x \in X, y \in Y\}$,
- $\langle X \rangle = \{x_1 \cdot x_2 \cdots x_n \,:\, x_i \in X\}$.

Conversely, any rational set can be constructed from finite sets using the operations $\cup$, $\cdot$, and $\langle\,\rangle$. Some authors use X^* in place of $\langle X \rangle$.

If $M = \Gamma^*$ is a finitely generated free monoid then the rational subsets of M are also known as *regular languages*; in this case $M \setminus X$ and $X \cap Y$ are rational whenever X and Y are rational (but this does not hold for general monoids M).

If $M = \Gamma^* \times \Delta^*$ is the direct product of two finitely generated free monoids then M-automata are also known as *transducers* and rational subsets of M as *rational relations* or *transductions* (see [4] for an extensive treatment of rational relations). To emphasize that the behaviour of a transducer $\mathcal{A}$ is a relation we will write $R(\mathcal{A})$ instead of $L(\mathcal{A})$. For example, if $\Gamma = \Delta = \{a\}$, then the relation

$$\{(a^n, a^{2n}) \,:\, n \in \mathbb{N}\} = \langle \{(a, aa)\} \rangle$$

can be realized by an automaton with just one state and a loop labeled (a, aa).

Another way to consider relations accepted by a finite state device is to first transform the relation into a language and then check whether this language is regular. Let $\perp \notin \Gamma$ be a symbol and $\Gamma(2, \perp) = (\Gamma \cup \{\perp\})^2 \setminus \{(\perp, \perp)\}$. We define the *convolution* $\otimes : \Gamma^* \times \Gamma^* \to \Gamma(2, \perp)^*$ by:

$$\varepsilon \otimes \varepsilon = \varepsilon \qquad a \otimes \varepsilon = (a, \perp) \qquad \varepsilon \otimes b = (\perp, b) \qquad av \otimes bw = (a, b)(v \otimes w)$$

for $a, b \in \Gamma$ and $v, w \in \Gamma^*$. If $R \subseteq \Gamma^* \times \Gamma^*$ let $R^{\otimes} = \{v \otimes w \,:\, (v, w) \in R\}$ denote the convolution of R. Note that $R^{\otimes}$ is a language over the alphabet $\Gamma(2, \perp)$. Define a homomorphism $\eta : \Gamma(2, \perp)^* \to \Gamma^* \times \Gamma^*$ by:

$$\eta(a, b) = (a, b), \qquad \eta(a, \perp) = (a, \varepsilon), \qquad \eta(\perp, b) = (\varepsilon, b)$$

for $a, b \in \Gamma$. Since $R = \eta(R^{\otimes})$ and rational sets are closed under homomorphic images [9], we have that, if $R^{\otimes}$ is rational, then R is rational. The converse is not true however: for example, if $R = \langle (a, aa) \rangle$, then R is rational but $R^{\otimes} = \{(a, a)^n (\perp, a)^n \,:\, n \in \mathbb{N}\}$ is not. Given the following result the reason for this failure is that the length difference of u and v is unbounded for $(u, v) \in R$:

Proposition 1 (Corollary 2.5 of [11]). *If $\mathcal{A} = (Z, \delta, \iota, F)$ is a transducer and $k \in \mathbb{N}$ is such that $| |u| - |v| | \leqslant k$ for $(u, v) \in R(\mathcal{A})$ then $R(\mathcal{A})^{\otimes}$ is regular.*

Given this result, we say that a rational relation R is *difference bounded* if there is a constant k such that $| |u| - |v| | \leqslant k$ for all $(u, v) \in R$.

Let M be a monoid, Γ a finite set, $\theta : \Gamma^* \to M$ an epimorphism, and $L \subseteq \Gamma^*$. Then we define:

$$L(\varepsilon) = \{(u, v) \in L^2 : \theta(u) = \theta(v)\}; \qquad L_= = L(\varepsilon)^{\otimes};$$
$$L(a) = \{(u, v) \in L^2 : \theta(ua) = \theta(v)\}; \qquad L_a = L(a)^{\otimes}$$

for $a \in \Gamma$. We have the following definition:

Definition 1. *An* automatic structure *for a monoid M is a triple (Γ, θ, L) where:*

1. *Γ is a finite set, $\theta : \Gamma^* \to M$ is an epimorphism and $L \subseteq \Gamma^*$ is regular;*
2. *$\theta(L) = M$; and*
3. *$L_=$ and L_a are regular for every $a \in \Gamma$.*

A monoid is said to be automatic *if it has an automatic structure.*

It is not hard to see that the regularity of L follows from the remaining conditions; in the automaton for the language L_a, we replace labels of the form (a, b) by a and those of the form $(\perp, b)$ by ε and drop the remaining transitions. We can assume [6] that θ maps L injectively onto M. In this case, the regularity of $L_=$ follows immediately from the regularity of L: replace transition labels of the form a by (a, a). The resulting automaton, considered over $\Gamma(2, \perp)$, accepts $\{u \otimes u : u \in L\}$ which equals $L_=$ by the injectivity of $\theta \restriction_L$. Hence the main task in showing the automaticity of a monoid is the construction of synchronous transducers whose language is $L(a)$. Since these transducers describe the multiplication by generators, they are called *multiplier automata*.

Given Proposition 1 one can derive an alternative characterization of automatic monoids as follows:

Proposition 2. *Let M be a monoid.*

1. *If there exists a finite set Γ, an epimorphism $\theta : \Gamma^* \to M$ and a regular language $L \subseteq \Gamma^*$ such that $L(a)$ is a rational relation and difference bounded for any $a \in \Gamma$, then (Γ, θ, L) is an automatic structure for M.*
2. *If M has an automatic structure (Γ, θ, L) with $\theta \restriction_L$ injective and if the set $\{x \in M : x\theta(a) = y\}$ is finite for any $y \in M$ and $a \in \Gamma$ then $L(a)$ is difference bounded for any $a \in \Gamma$.*

Note that the finiteness assumption is necessary in the second part. For example, if the automatic monoid M contains a zero element, then the relations L_a cannot be difference bounded. If the monoid M has a length function, then the finiteness assumption is always satisfied; this will be the case in our considerations.

We finish this section by introducing some notational conventions. The set of natural numbers $\{1, 2, \ldots, n\}$ is denoted by $[n]$. For a monoid $(M, \cdot, 1)$, we write $x \preceq y$ if and only if x is a left divisor of y, i.e. if there exists $z \in M$ with $x \cdot z = y$. Since the monoids under consideration will be cancellative and will have no nontrivial decomposition of the unit element, $\preceq$ will be a partial order.

3 The positive singular Artin monoid M_Γ

A *Coxeter graph* is a partially edge-labelled (undirected) graph with vertex set $[n]$ with labels coming from $\{3, 4, \ldots\} \cup \{\infty\}$. For a fixed Coxeter graph Γ, we define m_{ij} to be the label of the edge between vertices i and j if it exists, and 2 otherwise; in particular, $m_{ij} = m_{ji}$ holds. For a nonempty word w and a natural number n, let $\langle w \rangle^n$ be the prefix of length n of the word w^n.

The *positive singular Artin monoid of type* Γ, denoted by M_Γ, will be defined via a presentation. The generators are $\Sigma \cup T$ where

$$\Sigma = \{\sigma_1, \ldots, \sigma_n\} \text{ and } T = \{\tau_1, \ldots, \tau_n\},$$

that is, one σ- and one τ-type generator for each vertex of Γ. The relations are constructed via the edge information. For $m_{ij} \neq \infty$, we have the relations:

$$\langle \sigma_i \sigma_j \rangle^{m_{ij}} = \langle \sigma_j \sigma_i \rangle^{m_{ij}} \qquad (R_1)$$
$$\tau_i \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} = \langle \sigma_j \sigma_i \rangle^{m_{ij}-1} \tau_k \qquad (R_2)$$

where $k = i$ if m_{ij} is even, and j otherwise. For $m_{ij} = 2$ we have the relations:

$$\tau_i \tau_j = \tau_j \tau_i \qquad (R_3)$$

Finally, for all $i \in [n]$, we have the relations:

$$\tau_i \sigma_i = \sigma_i \tau_i \qquad (R_4)$$

The *positive singular Artin monoid* M_Γ *of type* Γ is given by the presentation

$$M_\Gamma = \mathrm{Mon} \langle \Sigma \cup T \,:\, R_1 \cup R_2 \cup R_3 \cup R_4 \rangle .$$

Our aim is to show that M_Γ is automatic.

Birman [3] and Baez [1] introduced such a monoid in the special case where Γ is linear and all labels are 3 (type A in Figure 1); the general case was introduced in [8]. Recently, Birman's conjecture (the "desingularisation map" is an embedding of M_Γ into the group algebra of the braid group) was proved for the monoid of singular braids [19], and for the singular Artin monoids of *right angled type* [12]. The case of Artin monoids of finite type not of type A (positive singular braid monoids) remains unresolved.

We now collect together some results about the monoid $M = M_\Gamma$ which we will need in this paper. The following three results are proved in [8].

(0.1) The monoid M is left and right cancellative.

(0.2) Any subset $X \subseteq M$ has a least common right (respectively left) multiple precisely when it has a common right (respectively left) multiple. When this is the case, the lcm is unique. Let X be the set of common left divisors of elements x and y. Then X has a common right multiple and therefore a least common multiple that we denote by $\gcd(x, y)$ since it equals the greatest common left divisor of x and y. In particular, any two elements of M have a greatest common left divisor.

(0.3) For $i \neq j$, τ_i and τ_j have a common multiple if and only if $\tau_i \tau_j = \tau_j \tau_i$, in which case this is the least common multiple.

Let Rev be the map on words over $\Sigma \cup T$ which reverses the word. Since $u = v$ is a defining relation precisely when $\mathrm{Rev}(u) = \mathrm{Rev}(v)$ is a defining relation, Rev extends to an anti-endomorphism of M_Γ (i.e. $\mathrm{Rev}(xy) = \mathrm{Rev}(y)\,\mathrm{Rev}(x)$ for any $x, y \in M$) and it is easy to see that:

(0.4) The map Rev is an anti-automorphism of M_Γ of order two.

Observe that all the relations involving a single element of T on each side of the equation are all of the form $\tau_i w = w\tau_j$ where w is a word over Σ and j may or may not be the same as i. Furthermore, the relations involving more than one element of T on each side involve *only* letters from T; thus we have a homomorphism $\nu : M_\Gamma \to M_\Gamma$ defined on generators by mapping $\sigma_i \mapsto \sigma_i$ and $\tau_i \mapsto 1$. The image under ν is the submonoid $S = S_\Gamma$ generated by Σ called the *positive Artin monoid*; it has presentation given by generators Σ and relations R_1. If $x\tau_i y = z\tau_j w$, where x, y, z, w are elements of S, then, by considering the image under ν, we have that $xy = zw$.

(0.5) If $x\tau_i y = z\tau_j w$ where $x, y, z, w \in S$, then $xy = zw$.

The reflection group of type Γ is the quotient of the Artin monoid S obtained by imposing order 2 on the generators. The positive singular Artin monoid M_Γ is said to be *of finite type* if the reflection group of type Γ is finite. This is equivalent to the set Σ having a common multiple in S (see [5]), or, equivalently (given that S embeds in M), having a common multiple in M.

(0.6) [5] Let Γ be of finite type. For every finite $X \subseteq S$, the lcm of X always exists. Thus, since S is a submonoid of M, any finite subset X of M where each $x \in X$ is representable by a word over Σ has a least common multiple that is itself representable as a word over Σ.

(0.7) [8] Let Γ be of finite type. For $x \in S$ and $\tau \in T$, $\mathrm{lcm}(\tau, x)$ always exists, and is of the form $\tau x a = x a \tau'$ for some $a \in S$ and $\tau' \in T$.

A Coxeter graph is of finite type if and only if it is a disjoint union of the graphs illustrated in Figure 1. *From now on we will restrict ourselves to the case where Γ is of finite type.*

Since M_Γ has unique least common multiples whenever common multiples exist, we have a unique least common multiple Δ of Σ. Let

$$Q := \{q \in M \setminus \{1\} \,:\, qp = \Delta \text{ for some } p\}.$$

By preservation of the number of τ's (all relations have same number of τ's on both sides, so all words representing any given element of M have the same number of τ's), all elements of Q are elements of S; in fact (see [5]) they are precisely the non-trivial elements of S which are not expressible in the form $uaav$ for any generator $a \in \Sigma \cup T$; given this, they are said to be *square-free elements*.

(0.8) [5] If $qxy = \Delta$ then each of q, x and y is in Q.

(0.9) [8] There is an automorphism $\bar{\cdot}$ of M_Γ defined by $w\Delta = \Delta\overline{w}$, which, in particular, defines a permutation on T, and a permutation on Σ. This automorphism is either trivial or of order 2, depending on the type of Γ.

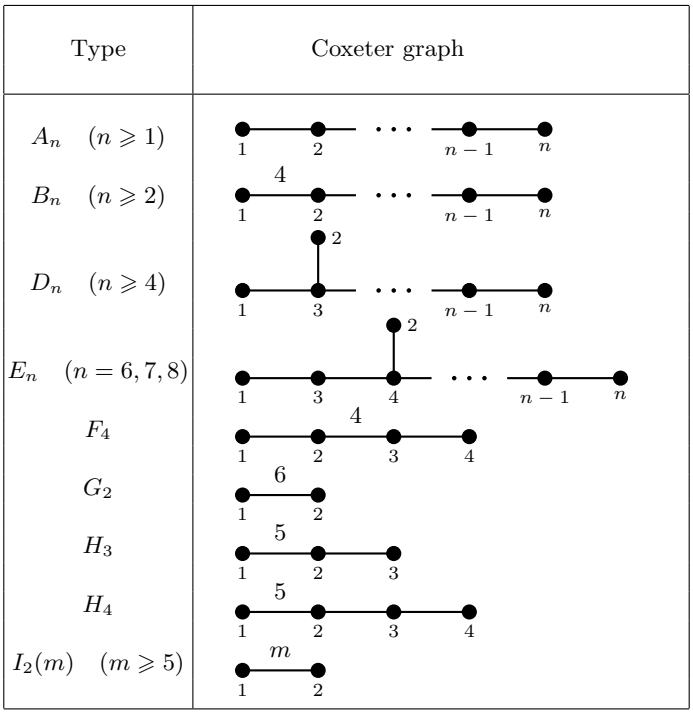

Fig. 1. Connected Coxeter graphs of finite type. Unlabelled edges have value 3.

By (0.7), $\mathrm{lcm}(\tau, q)$ exists for any $\tau \in T$ and $q \in S$ and is of the form $\tau q a$. The following two results give some more information on the element $a \in S$ provided that q is square-free. We can use (0.1), (0.5) and (0.8) to prove:

Lemma 1. *If $q \in Q$ and $\tau \in T$, then the least common multiple of q and τ exists and is of the form $qx\tau_j = \tau qx$ for some $x \in S$ and $\tau_j \in T$, and qx is square free.*

We can then use Lemma 1 to deduce:

Corollary 1. *Let $\tau \in T$ and $z \in M$ with $\tau \preceq z$ and let $q = \gcd(z, \Delta)$. Then $\tau q = q\tau'$ for some $\tau' \in T$ and $\tau q = \mathrm{lcm}(q, \tau)$.*

The restriction of the following result to elements $u, v \in S$ follows from Proposition 2.1 of [17]. As we are only interested in singular Artin monoids of finite type, one could produce an alternative proof which is a little simpler.

Lemma 2. *If $u, v \in M$ then $\gcd(uv, \Delta) = \gcd(u \gcd(v, \Delta), \Delta)$.*

Let $\mathcal{T} \subseteq M$ be the set of elements $\mathrm{lcm}(X)$ for all nonempty subsets $X \subseteq T$ having a common multiple in M. For $x \in M$, let

$$T(x) = \mathrm{lcm}\{t \in T \,:\, t \preceq x\}.$$

For $x \in M \setminus \{1\}$, let

$$\alpha(x) = \begin{cases} \gcd(x, \Delta) & \text{if } \gcd(x, \Delta) \neq 1 \\ T(x) & \text{otherwise.} \end{cases}$$

Observe that $\alpha(x) \in \mathcal{T}$ is equivalent to saying that $\Sigma \not\preceq x$ (which is shorthand for "no element of Σ left divides x"). We can then use Lemma 2 to prove:

Lemma 3. *If $x \in M$ and $p \in Q \cup \mathcal{T}$ then the pair $(\alpha(x), T(x))$ and the element p determine $\alpha(px)$.*

From Corollary 1 one can show:

Lemma 4. *If $p \in Q \cup \mathcal{T}$ and $x \in M$ with $\alpha(px) = p$ then $T(px) = T(p\,T(x))$.*

Suppose $\tau_i u \tau_j w = w_1 \tau_\ell \tau_k w_2 = w_1 \tau_k \tau_\ell w_2$ for some elements u, w, w_1, w_2 of S. Then, intuitively, the τ's in $\tau_i u \tau_j$ can commute after extension with $w \in S$. Using (0.6) and (0,7) one can prove the following result which shows that they can commute regardless of w:

Lemma 5. *Let $u' = tu\tau_j$ where $u \in S$, $t \in \mathcal{T}$, $j \in [n]$ and such that u' is neither left nor right divisible by Σ. In addition, let $w, w_1, w_2 \in S$, $s \in \mathcal{T}$ and $l \in [n]$ be such that $tu\tau_j w = w_1 s \tau_l w_2 = w_1 \tau_l s w_2$. Then $u = 1$.*

4 The language of normal forms

Recall that $\mathcal{T} \subseteq M$ comprises all the elements $\mathrm{lcm}(X)$ for all nonempty subsets $X \subseteq T$ having a common multiple in M. Since $T \subseteq \mathcal{T}$ and $\Sigma \subseteq Q$, the singular Artin monoid M is generated by $Q \cup \mathcal{T}$. From now on, we will consider words over the generators $Q \cup \mathcal{T}$ as well as products in M of elements of $Q \cup \mathcal{T}$. To avoid confusion, we will use the following conventions.

Let $\varphi : (Q \cup \mathcal{T})^* \to M_\Gamma$ be the natural epimorphism. For words u and v in $(Q \cup \mathcal{T})^*$, we write $u \sim v$ if $\varphi(u) = \varphi(v)$, i.e. if u and v represent the same element of M_Γ. If we want to stress that u and v coincide letter by letter, we will write $u \equiv v$. This eliminates any use of $u = v$ for words u and v. On the other hand, for elements $x, y \in M$, we will write $x = y$ to denote that they are equal. Since words over $S \cup \mathcal{T}$ of length 1 are actually elements of M as well, we can then write $a = b$ for $a, b \in S \cup \mathcal{T}$. Clearly, in this case, $a = b$, $a \equiv b$, and $a \sim b$ are equivalent. To reiterate, a string $q_1 q_2 \dots q_n$ of elements of $Q \cup \mathcal{T}$ is to be understood as word over $Q \cup \mathcal{T}$ and not as the monoid element represented by this sequence. This monoid element is denoted by $\varphi(q_1 q_2 \dots q_n)$ or, if $n = 2$, simply by $q_1 \cdot q_2$.

Michel (in Section 4 of [17]) defines normal forms from Q^* for the elements of S (again without the assumption of finite type). We extend his idea to the singular Artin monoid of finite type M: for any $x \in M$, we define a unique word $\mathrm{NF}(x)$ over $Q \cup \mathcal{T}$ and later (see Lemma 10) show that the set of all words obtained this way is a regular language in $(Q \cup \mathcal{T})^*$.

Let $\omega(x)$ be the unique element of M with $\alpha(x) \cdot \omega(x) = x$; then the normal form is defined inductively by

$$\mathrm{NF}(1) \equiv \varepsilon \quad \text{and} \quad \mathrm{NF}(x) \equiv \alpha(x)\,\mathrm{NF}(\omega(x)) \text{ for } x \in M \setminus \{1\}.$$

Note that this is well-defined since, as long as $x \neq 1$, we have that $\alpha(x) \not\equiv \varepsilon$, i.e. $\omega(x)$ is properly shorter than x. Let $L \subseteq (Q \cup \mathcal{T})^*$ denote the set of all words $\mathrm{NF}(x)$ for $x \in M$.

The following results relate the normal forms of $x \in M$ and $x \cdot \tau_k$ for some $k \in [n]$. They will become useful later when we construct an automatic structure for M. We first use Corollary 1 to deduce:

Lemma 6. *Let $q_1 q_2 \dots q_p$ be in L, and suppose that the least common multiple of $\varphi(q_1 q_2 \dots q_p)$ and $\tau_i \in \mathcal{T}$ is $\varphi(q_1 q_2 \cdots q_p \tau_k)$ for some $k \in [n]$. Then there is a sequence of integers $i = i_0, i_1, \dots, i_p = k$ such that $\tau_{i_{\ell-1}} q_\ell \sim q_\ell \tau_{i_\ell}$ for each $\ell \in [p]$.*

We then use Lemmas 4 and 6 to prove:

Lemma 7. *Let $p_i \in Q \cup \mathcal{T}$ with $p_1 p_2 \dots p_m \in L$, $x = \varphi(p_1 p_2 \dots p_m)$ and let $k \in [n]$. Then either $\mathrm{NF}(x \cdot \tau_k) \equiv p_1 p_2 \dots p_m \tau_k$ or else there are $\ell \in [m]$ and $j \in [n]$ with $\mathrm{NF}(x \cdot \tau_k) \equiv p_1 p_2 \dots p_{\ell-1} (p_\ell \cdot \tau_j) p_{\ell+1} \dots p_m$. Furthermore, in this latter case, we have that $\mathrm{lcm}(\tau_j, \varphi(p_\ell \dots p_m)) = \varphi(p_\ell \dots p_m \tau_k)$.*

Having described the relation between the normal forms of $x \in M$ and $x \cdot \tau_k$, we now obtain similar results for the normal forms of x and $x \cdot \sigma_k$. Somewhat surprisingly, this turns out to be more involved. Using Corollary 1, we can prove:

Lemma 8. *Let $tw \in L$ with $t \in \mathcal{T}$ and $w \in Q^*$. In addition, let $q \in Q$. Then $\mathrm{NF}(\varphi(twq)) \equiv psu$ for some $p \in Q$, $s \in \mathcal{T}$ and $u \in Q^*$ such that $tp \sim ps$.*

We then use (0.5), Lemma 2, Lemma 5 and Lemma 7 to prove:

Lemma 9. *Let $w \equiv w_1 t_1 w_2 \dots w_k t_k w_{k+1} \in L$ with $t_i \in \mathcal{T}$ and $w_i \in Q^*$. Let $q \in Q \cup \{1\}$ and define $q_i \in Q \cup \{1\}$ for $1 \leqslant i \leqslant k+1$ by $q_{k+1} = q$ and $q_i = \gcd(\varphi(t_i w_{i+1} q_{i+1}), \Delta)$. Then there are $u_i \in Q^*$ and $s_i \in \mathcal{T}$ such that*

- $\mathrm{NF}(\varphi(t_i w_{i+1} q_{i+1})) \equiv q_i s_i u_{i+1}$,
- $\mathrm{NF}(\varphi(w_1 q_1)) \equiv u_1$, *and*
- $\mathrm{NF}(\varphi(wq)) \equiv u_1 s_1 u_2 \cdots u_k s_k u_{k+1}$.

5 Automaticity of M_Γ

If $p \in Q \cup \mathcal{T}$ let $W_p \in (\Sigma \cup T)^*$ be some representative of p. Define a homomorphism $\eta : (Q \cup \mathcal{T})^* \to (\Sigma \cup T)^*$ by $\eta(p) = W_p$ and let $K = \eta(L)$. We will show that $(\Sigma \cup T, K)$ is an automatic structure for the positive singular Artin monoid of finite type M_Γ. We first use Lemmas 3 and 4 to prove:

Lemma 10. *The set $L \subseteq (Q \cup \mathcal{T})^\star$ is regular.*

Given that homomorphic images of regular sets are regular and $K = \eta(L)$, we immediately deduce:

Lemma 11. *The set $K \subseteq (\Sigma \cup T)^*$ is regular.*

We then use Lemmas 6 and 7 to prove:

Lemma 12. *If $k \in [n]$ then the relation $L(\tau_k) = \{(u, v) \in L \times L : u\tau_k \sim v\}$ is rational.*

Our next aim is to prove that the relation $L(q) = \{(u, v) \in L \times L : uq \sim v\}$ is rational for $q \in Q$. To this aim, we consider the relations

$$H_p = \{(w, u) \in L^2 : w, u \in Q^*, wp \sim u\}$$
$$R_{p,r} = \{(w, u) \in L^2 : w, u \in Q^*, wp \sim ru\}$$

for $p, r \in Q$ and prove (using [7]):

Lemma 13. *For $p, r \in Q$, the relations H_p and $R_{p,r}$ are rational.*

We then use Lemma 9 to prove:

Lemma 14. *If $q \in Q$ then the relation $L(q)$ is rational.*

Finally we have our result:

Theorem 1. *Any positive singular Artin monoid of finite type is automatic.*

Proof. Let $\alpha \in \Sigma \cup \mathcal{T}$. Since $\Sigma \subseteq Q$ and $T \subseteq \mathcal{T}$, we can speak of the relation $L(\alpha)$ which is rational by Lemmas 12 and 14. Since rational relations are closed under the application of homomorphisms, the relation

$$K(\alpha) = \{(\eta(u), \eta(v)) : (u, v) \in L(\alpha)\}$$

is rational as well. Since the relation $K(\alpha)$ is difference bounded, the result follows from Proposition 2 and Lemma 11 .

6 Automaticity of the singular Artin monoid M_Γ^Δ

We have considered the positive singular Artin monoids of finite type. We next consider a monoid into which they embed, namely the singular Artin monoid.

Let Γ be any Coxeter graph with associated positive singular Artin monoid M_Γ. Define the singular Artin monoid of type Γ, denoted by M_Γ^Δ, to be the monoid defined by the presentation with generators $\Sigma \cup T \cup \Sigma^{-1}$ (the last being the set of formal inverses of Σ), and relations R_1, R_2, R_3 and R_4 (as given in Section 3) together with the additional relations

$$\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = 1 \qquad \text{for each } i \ .$$

Recall our ongoing assumption that Γ is of finite type; in this case, it is known [8] that M_Γ is a submonoid of M_Γ^Δ. Thus Δ, the lcm of Σ in M_Γ, may be considered as an element of M_Γ^Δ, and extending the automorphism $\overline{\cdot}$ to M_Γ^Δ in the natural way ($\overline{\sigma^{-1}} := \overline{\sigma_i}^{-1}$) preserves the property that $w\Delta = \Delta\overline{w}$, where w is now in M_Γ^Δ. Furthermore, since Δ is a common multiple of Σ in M_Γ, for each $\sigma \in \Sigma$, there is a unique $\Delta_\sigma \in M_\Gamma$ defined by the property $\Delta = \Delta_\sigma\sigma$. Thus, for each σ, $\Delta\sigma^{-1} = \Delta_\sigma$ lies in the submonoid M_Γ.

Define a language L^Δ over $Q \cup Q^{-1} \cup \mathcal{T}$ as follows:

$$L^\Delta := \{u^{-1}v \,:\, u \in L \cap Q^*, v \in L \text{ and } \gcd(\varphi(u), \varphi(v)) = 1\}.$$

Let $\pi : (Q \cup Q^{-1} \cup \mathcal{T})^* \to M_\Gamma^\Delta$ be the natural extension of $\varphi : (Q \cup \mathcal{T})^* \to M_\Gamma$; clearly π restricts to a map from L^Δ to M_Γ^Δ. We will write $u \approx v$ whenever $\pi(u) = \pi(v)$ holds. We then have:

Lemma 15. *The language L^Δ is a set of unique normal forms for M_Γ^Δ.*

We can also establish:

Lemma 16. *Let $u_x, u_y \in L \cap Q^*$ and $v_x, v_y \in L$ be such that $x \equiv u_x^{-1}v_x$ and $y \equiv u_y^{-1}v_y$ belong to L^Δ. Furthermore, let $\tau \in T$ and $\sigma \in \Sigma$. Then we have:*

(1) $x\tau \approx y$ if and only if $u_y \equiv u_x$ and $v_y \approx v_x\tau$;
(2) $x\sigma \approx y$ if and only if there exists $q \in Q$ such that $qu_y \approx u_x$ and $qv_y \approx v_x\sigma$;
(3) $x\sigma^{-1} \approx y$ if and only if there exists $q \in Q$ such that $qu_y \approx \Delta u_x$ and $qv_y \approx \overline{v_x}\Delta_\sigma$.

By [7], $(Q, L \cap Q^*)$ is a biautomatic structure for the positive Artin monoid S which is the submonoid of M_Γ generated by Q. Hence the language

$${}_qL = \{u \otimes v \,:\, u, v \in L, \varphi(qu) = \varphi(v)\}$$

is regular for $q \in Q$. This implies that the relation

$$R'(q) = \{(u, v) \,:\, u, v \in L \cap Q^*, \varphi(qu) = \varphi(v)\}$$

is also rational for any $q \in Q$. We can extend $R'(q)$ to all of L:

Lemma 17. *If $q \in Q$ then the relation $R(q) = \{(x, y) \in L \times L \,:\, qx \approx y\}$ is rational.*

We can then use Lemma 16 to deduce:

Lemma 18. *If $t \in \Sigma \cup \Sigma^{-1} \cup T$ then the relation*

$$L^\Delta(t) = \{(x, y) \in L^\Delta \times L^\Delta \,:\, xt \approx y\}$$

is rational.

Given all this then, exactly as in the proof of Theorem 1, we can deduce:

Theorem 2. *Any singular Artin monoid of finite type is automatic.*

References

1. J. C. Baez, Link invariants of finite type and perturbation theory, *Lett. Math. Phys.* **26** (1992), 43–51.
2. G. Baumslag, S. M. Gersten, M. Shapiro and H. Short, Automatic groups and amalgams, *J. Pure Appl. Algebra* **76** (1991), 229–316.
3. J. S Birman, New points of view in knot theory, *Bull. Amer. Math. Soc.* **28** (1993), 253–287.
4. J. Berstel, *Transductions and Context-free Languages* (Teubner Studienbücher, Stuttgart, 1979).
5. E. Brieskornand and K. Saito, Artin-Gruppen und Coxeter-Gruppen, *Invent. Math.* **17** (1972), 245–271.
6. C. M. Campbell, E. F. Robertson, N. Ruškuc and R. M. Thomas, Automatic semigroups, *Theoret. Comput. Sci.* **250** (2001), 365–391.
7. R. Charney, Artin groups of finite type are biautomatic, *Math. Ann.* **292** (1992), 671–683.
8. R. Corran, A normal form for a class of monoids including the singular braid monoids, *J. Algebra* **223** (2000), 256–282.
9. S. Eilenberg, *Automata, Languages and Machines, Volume A* (Academic Press, New York, 1974).
10. D. B. A. Epstein, J. W. Cannon, D. F. Holt, S. V. F. Levy, M. S. Paterson and W. P. Thurston, *Word Processing In Groups* (Jones and Bartlett, Boston, 1992).
11. Ch. Frougny and J. Sakarovitch, Synchronized rational relations of finite and infinite words, *Theoret. Comput. Sci.* **108** (1993), 45–82.
12. E. Godelle and L. Paris, On singular Artin monoids, *Geometric Methods in Group Theory* (Contemp. Math. **372**, Amer. Math. Soc., Providence, RI, 2005), 43–57.
13. M. Hoffmann, D. Kuske, F. Otto and R. M. Thomas, Some relatives of automatic and hyperbolic groups, *Semigroups, Algorithms, Automata and Languages, Coimbra, 2001* (World Sci. Publishing, River Edge, NJ, 2002), 379–406.
14. M. Hoffmann and R. M. Thomas, Notions of automaticity in semigroups, *Semigroup Forum* **66** (2003), 337–367.
15. J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation* (Addison Wesley, 1979).
16. J. F. P. Hudson, Regular rewrite systems and automatic structures, *Semigroups, Automata and Languages, Porto, 1994* (World Sci. Publishing, River Edge, NJ, 1996), 145–152.
17. J. Michel, A note on words in braid monoids, *J. Algebra* **215** (1999), 366–377.
18. F. Otto, A. Sattler-Klein and K. Madlener, Automatic monoids versus monoids with finite convergent presentations, *Rewriting Techniques and Applications, Tsukuba, 1998* (LNCS **1379**, Springer, Berlin, 1998), 32–46.
19. L. Paris, The proof of Birman's conjecture on singular braid monoids, *Geom. Topol.* **8** (2004), 1281–1300.

Appendix

Proof of Proposition 2

Proof. The first statement is immediate by Proposition 1. To prove the second one, let (Γ, θ, L) be an automatic structure for M such that $\theta \restriction_L$ is injective. Suppose there is $a \in \Gamma$ such that $L(a)$ is not difference bounded. Let k be the number of states of some automaton accepting L_a. Then there are $u, v \in \Gamma^*$ with $(u, v) \in L(a)$ and $||u| - |v|| > k$. First suppose $|u| + k < |v|$. Then

$$u \otimes v = (u \otimes w)(\bot, b_1)(\bot, b_2) \dots (\bot, b_{k+1})$$

for some $w \in \Gamma^*$ and $b_i \in \Gamma$ with $v = wb_1b_2 \dots b_{k+1}$; hence, a successful run on $u \otimes v$ visits some state at least twice when executing the suffix. This allows us to iterate the corresponding factor which yields

$$(u \otimes w)\,(\bot, b_1) \dots [(\bot, b_i) \dots (\bot, b_j)]^n \dots (\bot, b_{k+1}) \in L_a$$

for $n \in \mathbb{N}$. Thus we have

$$\theta(wb_1b_2 \dots b_{k+1}) = \theta(v) = \theta(ua) = \theta(wb_1 \dots (b_i \dots b_j)^2 \dots b_{k+1})$$

and $wb_1 \dots (b_i \dots b_j)^2 \dots b_{k+1} \in L$; but this contradicts our assumption that $\theta \restriction_L$ be injective. Thus we can only have $|v| + k < |u|$. Then a similar pumping argument shows that there are infinitely many words $u_i \in L$ with $(u_i, v) \in L(a)$, i.e. with $\theta(u_i a) = \theta(v)$. Since $\theta \restriction_L$ was assumed injective, this contradicts our finiteness assumption on M.

Proof of Lemma 1

Proof. Since $\tau_i \Delta = \Delta \overline{\tau}_i = qp\overline{\tau}_i$ for some $p \in Q$, $\tau_i \Delta$ is a common multiple of τ_i and q. Thus the least common multiple exists, and has exactly one occurrence of an element of T. This lcm may be written in the form $\tau_i z = qx\tau_j y$ for some j, and for some $z, x, y \in S$. Since $\tau_i z$ divides $\tau_i \Delta$, cancellation implies that z divides Δ; that is, $z \in Q$. By (0.5), we can delete the τ's to get $z = qxy$. Then, by (0.8), we have that q, x and y are all square-free, and cancelling (0.1) gives $\tau_i qx = qx\tau_j$. Since $\tau_i qxy$ was assumed to be a lcm, "leastness" implies y must be empty, and so $\tau_i qx = qx\tau_j$ is the lcm.

Proof of Corollary 1

Proof. Since q divides Δ, we have that q is square free. By Lemma 1, there is a square free $x \in Q$ with $\operatorname{lcm}(q, \tau) = qx\tau'$ for some $\tau' \in T$ such that qx is square free. Since q and τ divide z, so does their least common multiple $qx\tau'$. Hence the square free qx divides $\gcd(z, \Delta) = q$, and hence $x = 1$. In other words, $\tau q = q\tau'$ holds. Furthermore, since q contains no occurrence of an element of T, it is not a multiple of τ itself. Hence $q\tau' = \tau q$ has to be the *least* common multiple of q and τ.

Proof of Lemma 2

Proof. As we mentioned, this folows from Proposition 2.1 of [17]. We give an alternative proof here for the case which we are considering.

If $x \preceq z$, there is a unique element $y \in M$ with $xy = z$. In this proof, we denote this element by $(x^{-1}z)$.

Since $\gcd(v, \Delta) \preceq v$, then

$$\gcd(u \gcd(v, \Delta), \Delta) \preceq \gcd(uv, \Delta) =: q.$$

Let $p = \gcd(u, \Delta)$, so that $p \preceq q$. Since q is square free, there exists $p' \in Q$ with $q = pp'$. Then $pp' \preceq uv = p(p^{-1}u)v$ and therefore $p' \preceq (p^{-1}u)v$. Hence there exists $r \in Q$ with

$$(p^{-1}u)r = \operatorname{lcm}(p', (p^{-1}u)) \preceq (p^{-1}u)v.$$

Hence $r \preceq v$. Since r is square free, this implies $r \preceq \gcd(v, \Delta)$. Thus, we obtain

$$q = pp' \preceq p(p^{-1}u)r \preceq u \gcd(v, \Delta).$$

Since q is square free, it follows that $q \preceq \gcd(u \gcd(v, \Delta), \Delta)$. Hence

$$\gcd(uv, \Delta) = \gcd(u \gcd(v, \Delta), \Delta)$$

as required.

Proof of Lemma 3

Proof. By Lemma 2 we have

$$\gcd(px, \Delta) = \gcd(p \gcd(x, \Delta), \Delta) = \begin{cases} \gcd(p\alpha(x), \Delta) & \text{if } \alpha(x) \in Q \\ \gcd(p, \Delta) & \text{if } \alpha(x) \in \mathcal{T}. \end{cases}$$

Furthermore, if $\alpha(x) \in \mathcal{T}$, then $\gcd(p\alpha(x), \Delta) = \gcd(p, \Delta)$, so we always have

$$\gcd(px, \Delta) = \gcd(p\alpha(x), \Delta).$$

So, if $\gcd(p\alpha(x), \Delta) \neq 1$, then $\alpha(px) = \gcd(p\alpha(x), \Delta)$.

On the other hand, if $\gcd(p\alpha(x), \Delta) = 1$, then $p \in \mathcal{T}$, and $\alpha(px) = T(px)$. Suppose $\tau \preceq px$ but $\tau \not\preceq p$; then $\operatorname{lcm}(\tau, p) \preceq px$, and, by extension of (0.3), $\operatorname{lcm}(\tau, p) = \tau p = p\tau$. Thus $\tau \preceq x$; so $\tau \in T(x)$, and $\operatorname{lcm}(\tau, p) = p\tau \preceq pT(x)$. Thus $T(px) \preceq T(pT(x)) \preceq T(px)$, and hence they are equal.

In summary,

$$\alpha(px) = \begin{cases} \gcd(p\alpha(x), \Delta) & \text{if } \gcd(p\alpha(x), \Delta) \neq 1 \\ T(pT(x)) & \text{otherwise,} \end{cases}$$

so $\alpha(px)$ is completely determined by p and $(\alpha(x), T(x))$.

Proof of Lemma 4

Proof. Suppose firstly that $p \in \mathcal{T}$. Then $\alpha(p \cdot x) = p$ implies

$$\alpha(p \cdot x) = T(p \cdot x) = p.$$

So $p \preceq T(p \cdot T(x)) \preceq T(p \cdot x) = p$ implies $T(p \cdot x) = T(p \cdot T(x))$.

Suppose now that $p \in Q$; thus $\gcd(p \cdot x, \Delta) = \alpha(p \cdot x) = p$. By Corollary 1, $\tau \preceq p \cdot x$ implies

$$\tau \cdot p = p \cdot \tau' = \mathrm{lcm}(p, \tau) \preceq p \cdot x$$

for some $\tau' \in \mathcal{T}$. Hence, by cancellation, $\tau' \preceq T(x)$ and therefore

$$\tau \cdot p = p \cdot \tau' \preceq p \cdot T(x).$$

Now $\tau \preceq T(p \cdot T(x))$ and therefore $T(p \cdot x) \preceq T(p \cdot T(x))$ follows immediately. Since $T(x) \preceq x$, the other comparision $T(p \cdot T(x)) \preceq T(p \cdot x)$ is immediate. Thus $T(p \cdot T(x)) \preceq T(p \cdot x)$ as required.

Proof of Lemma 5

Proof. Using the fact that $w_1 = w_2$ if and only if $\mathrm{Rev}(w_1) = \mathrm{Rev}(w_2)$, we may approach the problem "backwards". Suppose that

(1) $\tau_j u t$ has no left divisor in S,
(2) $\tau_j u t$ has no right divisor in S, and
(3) there exist $w, w_1, w_2 \in S$ and $s \in \mathcal{T}$ such that

$$w \tau_j u t = w_2 \tau_\ell s w_1 = w_2 s \tau_\ell w_1. \tag{A}$$

We will show that the only way for these three assumptions to hold simultaneously is if we have that $u = 1$. Observe that, by (0.5), $wu = w_2 w_1$.

By (0.6), $\mathrm{lcm}(w, w_2)$ exists, and is itself in S, so $\mathrm{lcm}(w, w_2) = wx = w_2 y$ for some x and y from S. This lcm left divides (A), so x left divides $\tau_j u t$, which by (1) implies that $x = 1$. Thus $w = w_2 y$, and then since $w_2 y u = wu = w_2 w_1$, left cancellation gives $yu = w_1$. Hence (A) becomes

$$y \tau_j u t = \tau_\ell s y u = s \tau_\ell y u. \tag{B}$$

By (0.7), there exist $\tau_p \in T$ and $a \in S$ such that $\mathrm{lcm}(y, \tau_\ell) = ya\tau_p = \tau_\ell y a$. Since this lcm divides (B) then $a\tau_p$, and hence a, divides $\tau_j u \tau_i$; assumption (1) then forces $a = 1$. Using a similar argument for $\mathrm{lcm}(y, \tau)$, for each of the $\tau \preceq s$, we have the existence of a $\tau' \preceq s$ such that $\mathrm{lcm}(y, \tau) = y\tau' = \tau y$. Putting these all together gives

$$\mathrm{lcm}(y, \tau_\ell) = y\tau_p = \tau_\ell y, \text{ and } \mathrm{lcm}(y, s) = ys' = sy. \tag{C}$$

Putting (B) and (C) together, we have $y\tau_j u t = \tau_\ell s y u = y s' \tau_p u$ so after left cancellation, we have $\tau_j u t = s' \tau_p u$. By assumption (2), $u = 1$.

Proof of Lemma 6

Proof. Suppose $q_1 \in Q$. Then $q_1 = \gcd(\varphi(q_1 q_2 \dots q_p), \Delta)$ since $q_1 q_2 \dots q_p \in L$. Thus, by Corollary 1, there is $i_1 \in [n]$ with $\tau_i q_1 \sim q_1 \tau_{i_1}$.

Now suppose $q_1 \in \mathcal{T}$. Since $\varphi(q_1 q_2 \dots q_p)$ is not a multiple of τ_i, we get $\tau_i \not\preceq q_1$. Since τ_i and q_1 divide $\varphi(\tau_i q_1 q_2 \dots q_p)$, they have a least common multiple which is $\varphi(\tau_i q_1) = \varphi(q_1 \tau_i)$. Thus setting $i_1 = i$ gives $\tau_i q_1 \sim q_1 \tau_{i_1}$ as desired.

In both cases, the least common multiple of $\varphi(q_1 q_2 \cdots q_p)$ and $\varphi(q_1 \tau_{i_1}) \succeq \tau_i$ is $\varphi(q_1 q_2 \cdots q_p \tau_k)$. By cancellation, the least common multiple of $\varphi(q_2 \cdots q_p)$ and τ_{i_1} is $\varphi(q_2 \cdots q_p \tau_k)$. The result now holds by a repeated application of the same argument.

Proof of Lemma 7

Proof. The lemma is shown by induction on m. For $m = 0$, we get immediately $\mathrm{NF}(x \cdot \tau_k) \equiv \tau_k \equiv p_1 p_2 \dots p_m \tau_k$. For the induction step, we have to distinguish several cases.

First suppose $\alpha(x \cdot \tau_k) = \alpha(x)$. Then $\alpha(x) \neq 1$ implies $m \geqslant 1$ and $\alpha(x) = p_1$. Then $\omega(x \cdot \tau_k) = \varphi(p_2 p_3 \dots p_m \tau_k)$. Thus, $\mathrm{NF}(x \cdot \tau_k) \equiv p_1 \mathrm{NF}(\varphi(p_2 \dots p_m \tau_k))$ which allows us to apply the induction hypothesis.

So let $\alpha(x \cdot \tau_k) \neq \alpha(x)$. Because of

$$\gcd(x, \Delta) = \gcd(x \cdot \tau_k, \Delta),$$

this implies that $\gcd(x, \Delta) = 1$. Hence p_1 and $\alpha(x \cdot \tau_k)$ are distinct elements of $\mathcal{T}$. Since $p_1 \preceq \alpha(x \cdot \tau_k)$, there exists $i \in [n]$ with $\tau_i \preceq \alpha(x \cdot \tau_k)$ and $\tau_i \not\preceq x$. Hence $x \cdot \tau_k = \mathrm{lcm}(\tau_j, x)$ implying, by Lemma 6, that $x \cdot \tau_k = \tau_i \cdot x$. Hence we have

$$T(x \cdot \tau_k) = T(\tau_i \cdot x) = T(\tau_i \cdot T(x)) = T(\tau_i \cdot p_1)$$

by Lemma 4. Hence p_1 is a proper prefix of $T(\tau_i \cdot p_1)$, implying

$$\tau_i \cdot p_1 = T(x \cdot \tau_k) = \alpha(x \cdot \tau_k).$$

Hence $\mathrm{NF}(x \cdot \tau_k) \equiv (\tau_i \cdot p_1)\, \mathrm{NF}(\varphi(p_2 p_3 \dots p_m)) \equiv (\tau_i \cdot p_1)\, p_2 p_3 \dots p_m$ as required.

Proof of Lemma 8

Proof. Let $p = \gcd(\varphi(twq), \Delta)$. If $p = 1$, we obtain $\alpha(\varphi(twq)) = t$ and therefore $\mathrm{NF}(\varphi(twq)) \equiv t\, \mathrm{NF}(\varphi(wq))$ which is of the form desired.

So assume $p \neq 1$. Then, from Corollary 1, we obtain $twq \sim psv$ for some $s \in \mathcal{T}$ and $v \in Q^*$. Let $r = \gcd(\varphi(sv), \Delta)$. So

$$\varphi(pr) \preceq \varphi(twq) \preceq \varphi(tw) \cdot \Delta = \Delta \cdot \overline{\varphi(tw)}.$$

Recall the automorphism $\overline{\cdot}$ defined in (0.9). Since $tw \in L$, $\Sigma \not\preceq \varphi(tw)$; so by application of $\overline{\cdot}$, $\Sigma \not\preceq \overline{\varphi(tw)}$. Thus $\varphi(pr) \preceq \Delta$. But $p = \gcd(\varphi(twq), \Delta)$, so $r = 1$. Thus $\alpha(\varphi(sv)) = s$ and

$$\mathrm{NF}(\varphi(twq)) \equiv ps\mathrm{NF}(\varphi(v)).$$

Writing $u \equiv \mathrm{NF}(\varphi(v))$ gives the desired form.

Proof of Lemma 9

Proof. Since $q_i \in Q \cup \{1\}$, by Lemma 8 there are $s_i \in \mathcal{T}$ and $u_i \in Q^*$ with

$$\mathrm{NF}(\varphi(t_i w_{i+1} q_{i+1})) \equiv q_i s_i u_{i+1} \tag{D}$$

where

$$t_i q_i \sim q_i s_i \tag{E}$$

and consequently, by (0.5),

$$w_{i+1} q_{i+1} \sim q_i u_{i+1}. \tag{F}$$

By the construction at (D), $s_i u_{i+1} \in L$. In particular, $s_k u_{k+1} \in L$.

Suppose that $z_i :\equiv s_i u_{i+1} \cdots s_k u_{k+1} \in L$. We show that $u_i z_i \in L$. If $u_i = \varepsilon$ then the statement is trivial. Otherwise write $u_i \equiv p_1 \cdots p_r$ where $p_j \in Q$. Then, for each j,

$$\begin{aligned}
&\gcd(p_j \cdots p_r z_i, \Delta) \\
&= \gcd(\varphi(p_j \gcd(p_{j+1} \cdots p_r z_i, \Delta)), \Delta) && \text{by Lemma 2} \\
&= \gcd(p_j \cdot \gcd(\varphi(p_{j+1} \cdots p_r) \cdot \gcd(\varphi(z_i), \Delta), \Delta), \Delta) && \text{Lemma 2 again} \\
&= \gcd(p_j \cdot \gcd(\varphi(p_{j+1} \cdots p_r), \Delta), \Delta) && \text{since } \gcd(\varphi(z_i), \Delta) = 1 \\
&= \gcd(\varphi(p_j p_{j+1} \cdots p_r), \Delta) && \text{Lemma 2 again} \\
&= p_j && \text{since } p_j p_{j+1} \cdots p_r \in L
\end{aligned}$$

Thus $p_j \cdots p_r z_i \in L$ for each j; so in particular, $u_i z_i \in L$ whenever $z_i \in L$.

Now suppose that $u_i z_i \in L$. We want to show that $s_{i-1} u_i z_i \in L$. By the same repeated application of Lemma 2, we have that

$$\gcd(\varphi(s_{i-1} u_i z_i), \Delta) = \gcd(\varphi(s_{i-1} u_i), \Delta),$$

which, by $s_{i-1} u_i \in L$, equals 1. Hence $\gcd(\varphi(s_{i-1} u_i z_i), \Delta) = 1$; so it remains to show that $T(\varphi(s_{i-1} u_i z_i)) = s_{i-1}$.

Let $t = T(\varphi(s_{i-1} u_i z_i))$, so that $s_{i-1} \preceq t$. Suppose that $t \not\preceq s_{i-1}$. Then there exists $j \in [n]$ with $\tau_j \preceq t$ but such that $\tau_j \not\preceq s_{i-1}$. We will obtain a contradiction. Observe that (0.3) implies that $s_{i-1} \tau_j \sim \tau_j s_{i-1}$.

Now $\tau_j \preceq \varphi(u_i z_i)$. By (0.7), $\mathrm{lcm}(\tau_j, \varphi(u_i)) = \varphi(\tau_j u_i) \cdot a$ for some $a \in S$; but since $\Sigma \not\preceq z_i$, a is forced to be trivial. Thus $\tau_j u_i \sim u_i \tau_\ell$ for some $\ell \in [n]$. Furthermore, $\tau_\ell \preceq \varphi(z_i)$; so, in fact, $\tau_\ell \preceq s_i$. Equation (E), together with $\tau_\ell \preceq s_i$, implies the existence of $p \in [n]$ such that $\tau_p q_i \sim q_i \tau_\ell$ with $\tau_p \preceq t_i$. Thus

$$q_{i-1} s_{i-1} \tau_j u_i \sim q_{i-1} s_{i-1} u_i \tau_\ell \overset{(D)}{\sim} t_{i-1} w_i q_i \tau_\ell \sim t_{i-1} w_i \tau_p q_i.$$

Hence

$$t_{i-1} w_i \tau_p q_i \sim q_{i-1} \tau_j s_{i-1} u_i \sim q_{i-1} s_{i-1} \tau_j u_i \tag{G}$$

There exist $x, y \in Q^*$ and $q \in [n]$ such that $t_{i-1} w_i \tau_p \sim t_{i-1} x \tau_q y$ and such that $\varphi(t_{i-1} x \tau_q)$ is not divisible by Σ on the left nor on the right. Now we have a word $y' \equiv y q_i \in Q^*$ such that $t_{i-1} x \tau_q y' \sim q_{i-1} s_{i-1} \tau_j u_i \sim q_{i-1} \tau_j s_{i-1} u_i$ (see (G)). That is, such that τ_j and s_{i-1} commute inside. This is precisely the situation of Lemma 5; so we have that $x = \varepsilon$, and so $y \sim w_i$.

Thus $t_{i-1}\tau_q y \sim t_{i-1}\tau_q w_i \sim t_{i-1}w_i\tau_p$, where $\tau_p \preceq t_i$, so $t_{i-1}\cdot\tau_q \preceq \varphi(t_{i-1}w_it_i)$. This last word $t_{i-1}w_it_i$ is in L, so $T(\varphi(t_{i-1}w_it_i)) = t_{i-1}$, hence either $\tau_q \preceq t_{i-1}$ or $\tau_q \not\preceq t_i\cdot\tau_q$.

We now have to collect together our sums:

$$q_{i-1}\tau_j u_i \sim q_{i-1}u_i\tau_l \overset{(F)}{\sim} w_iq_i\tau_l \sim w_i\tau_pq_i \sim \tau_q w_iq_i \sim \tau_q q_{i-1}u_i;$$

so by right cancellation, $q_{i-1}\tau_j \sim \tau_q q_{i-1}$. We find that

$$t_{i-1}w_i\tau_pq_i \overset{(G)}{\sim} q_{i-1}\tau_j s_{i-1}u_i \sim \tau_q q_{i-1}s_{i-1}u_i \sim \tau_q t_{i-1}q_{i-1}u_i \sim \tau_q t_{i-1}w_iq_i.$$

Right cancelling gives $t_{i-1}w_i\tau_p \sim \tau_q t_{i-1}w_i$. Then, since $\tau_p \preceq t_i$,

$$t_{i-1} \preceq T(\varphi(t_{i-1}w_i\tau_p)) = T(\varphi(\tau_q t_{i-1}w_i)),$$

which ensures that $\tau_q \preceq t_{i-1}$. Now $t_{i-1}q_{i-1} \sim q_{i-1}s_{i-1}$ (equation type (E)) tells us that there exists $\tau_r \preceq s_{i-1}$ such that $\tau_q q_{i-1} \sim q_{i-1}\tau_r$. But equation (H) forces $r = j$; that is, $\tau_j \preceq s_{i-1}$, contradicting the initial assumption on τ_j.

Proof of Lemma 10

Proof. We show that $\mathrm{Rev}(L) = \{\mathrm{Rev}(u) : u \in L\}$ is regular which implies the result since regular languages are closed under reversal (see [9,15] for example). Let

$$H = \{(\alpha(x), T(x)) : x \in M\} \cup \{\bot\}$$

and $\theta : (Q \cup \mathcal{T})^* \to H$ be given by

$$\theta(w) = \begin{cases} (\alpha(\varphi(w)), T(\varphi(w))) & \text{if } w \in L \\ \bot & \text{otherwise.} \end{cases}$$

We show that $\theta(u) = \theta(v)$ implies $\theta(pu) = \theta(pv)$ for $p \in Q \cup \mathcal{T}$ and $u, v \in (Q \cup \mathcal{T})^*$. If $u \notin L$, then $\bot = \theta(u) = \theta(v)$ implies $v \notin L$ and therefore $pu, pv \notin L$. Hence $\theta(pu) = \bot = \theta(pv)$. Next suppose $u \in L$. Then $\bot \neq \theta(u) = \theta(v)$ implies

$$\alpha(\varphi(u)) = \alpha(\varphi(v)) \quad \text{and} \quad T(\varphi(u)) = T(\varphi(v)).$$

Hence, by Lemma 3, $\alpha(\varphi(pu)) = \alpha(\varphi(pv))$. If $pu \notin L$, then $p \neq \alpha(\varphi(pu))$ since $u \in L$. Hence $p \neq \alpha(\varphi(pv))$ implying $pv \notin L$ and therefore $\theta(pu) = \bot = \theta(pv)$. Finally, let $pu \in L$. Then $p = \alpha(\varphi(pu)) = \alpha(\varphi(pv))$. Hence, by Lemma 4,

$$T(\varphi(pv)) = T(p\,T(\varphi(v))) = T(p\,T(\varphi(u))) = T(\varphi(pu)),$$

and therefore $\theta(pu) = \theta(pv)$.

Thus, a left action of the free monoid $(Q \cup \mathcal{T})^*$ on H is given by ${}^w\bot = \bot$ and

$${}^w(\alpha(x), T(x)) = \begin{cases} (\alpha(\varphi(w)\cdot x), T(\varphi(w)\cdot x)) & \text{if } w\,\mathrm{NF}(x) \in L \\ \bot & \text{otherwise} \end{cases}$$

for $x \in M$ and $w \in (Q \cup \mathcal{T})^*$. Since ${}^w(1,1) = \theta(w)$, we get ${}^w(1,1) \neq \bot$ if and only if $w \in L$, proving that $\mathrm{Rev}(L)$ is regular.

Proof of Lemma 12

Proof. We consider the following transducer $\mathcal{A} = (Z, \delta, \iota, F)$:

- $Z = \{\iota, f\} \cup T$;
- $\delta = \{(\iota, (p,p), \iota) : p \in Q \cup \mathcal{T}\}$;
  $\cup \{(\iota, (p, \tau_j \cdot p), \tau_j) : p, \tau_j \cdot p \in \mathcal{T}, j \in [n]\}$
  $\cup \{(\tau_i, (p,p), \tau_j) : i, j \in [n], p \in Q \cup \mathcal{T}, \tau_i p \sim p\tau_j\}$
  $\cup \{(\iota, (\varepsilon, \tau_k), f)\}$
- $F = \{\tau_k, f\}$.

Now let $p_i \in Q \cup \mathcal{T}$ with $u \equiv p_1 p_2 \dots p_m \in L$. If $\mathrm{NF}(\varphi(u\tau_k)) \equiv u\tau_k$, then the pair $(u, u\tau_k)$ is accepted by a run using transitions from the first and the last set. So suppose $\mathrm{NF}(\varphi(u\tau_k)) \not\equiv u\tau_k$. By Lemmas 6 and 7, there are $\ell \in [m]$ and $j_i \in [n]$ for $\ell \leqslant i \leqslant m+1$ such that

$$\mathrm{NF}(\varphi(u\tau_k)) \equiv p_1 p_2 \dots p_{\ell-1} (\tau_{j_\ell} \cdot p_\ell) p_{\ell+1} \dots p_m,$$

$\tau_{j_i} \cdot p_i \sim p_i \cdot p_{j_{i+1}}$ and $j_{m+1} = k$. Then the pair $(u, \mathrm{NF}(\varphi(u\tau_k)))$ is accepted by $\mathcal{A}$ by the following run

$$\iota \xrightarrow{(p_1,p_1)} \iota \cdots \iota \xrightarrow{(p_{\ell-1},p_{\ell-1})} \iota \xrightarrow{(p_\ell,(\tau_{j_\ell}\cdot p_\ell))} \tau_{j_\ell} \xrightarrow{(p_{\ell+1},p_{\ell+1})} \tau_{j_{\ell+1}} \cdots \tau_{j_m} \xrightarrow{(p_m,p_m)} \tau_{j_{m+1}} = \tau_k \in F$$

Thus, $L_{\tau_k} \subseteq R(\mathcal{A}) \cap (L \times L)$. Next let $u, v \in L$ and suppose there exists a successful run of $\mathcal{A}$ labeled (u, v). If the last state of this run is f, then $u\tau_k \equiv v$. Otherwise, the successful run is of the form described above. Hence we have

$$\begin{aligned} u \equiv p_1 p_2 \dots p_m \tau_k &\sim p_1 p_2 \cdots p_{m-1} \tau_{j_m} p_m \\ &\sim p_1 p_2 \cdots p_{m-2} \tau_{j_{m-1}} p_{m-1} p_m \\ &\;\;\vdots \\ &\sim p_1 p_2 \cdots p_{\ell-1} \tau_{j_\ell} p_\ell \cdots p_{m-1} p_m \\ &\sim p_1 p_2 \cdots p_{\ell-1} (\tau_{j_\ell} \cdot p_\ell) p_{\ell+1} \dots p_m \equiv v. \end{aligned}$$

Since $v \in L$, Lemma 7 implies $\mathrm{NF}(\varphi(u\tau_k)) \equiv v$. From $u, v \in L$, we therefore obtain $(u, v) \in L_{\tau_k}$, i.e. $R(\mathcal{A}) \cap (L \times L) = L_{\tau_k}$. Since the rationality of a relation is preserved when intersected with a direct product of regular languages [4], L_{τ_k} is indeed rational.

Proof of Lemma 13

Proof. By [7], $(Q, L \cap Q^*)$ is a biautomatic structure for the positive Artin monoid S which is the submonoid of M generated by Q. Hence $H_p^{\otimes}$ is a regular language implying that H_p is rational. Since $(Q, L \cap Q^*)$ is a biautomatic structure, also the language

$$\{v \otimes u : v, u \in L \cap Q^*, ru \sim v\}$$

is regular. Hence the corresponding relation

$$\overline{H}_r = \{(v, u) \in L^2 : v, u \in Q^*, ru \sim v\}$$

is rational. Now $R_{p,r} = H_p \circ \overline{H}_r$ implies that $R_{p,r}$ is rational [4].

Proof of Lemma 14

Proof. For $p, r \in Q \cup \{1\}$, let $\boldsymbol{R}_{p,r}$ be a transducer with behaviour $R_{p,r}$, and let $\boldsymbol{H}_p$ be a transducer with behaviour H_p.

We construct a transducer $\mathcal{A}$ with behaviour $L(q)$ as follows: its skeleton is provided by the disjoint union of all the transducers $\boldsymbol{R}_{p,r}$ and $\boldsymbol{H}_p$ where we identify the initial states of the transducers $\boldsymbol{H}_p$ into one state ι. This state ι will be the initial state of the new transducer $\mathcal{A}$. A state of $\mathcal{A}$ is accepting if and only if it is an accepting state of $\boldsymbol{H}_q$ or of some $\boldsymbol{R}_{p,q}$ for some $p \in Q \cup \{1\}$. Finally, we add the transition $(z', (t, s), z)$ with $s, t \in \mathcal{T}$ if and only if there are $p, r \in Q \cup \{1\}$ such that z is accepting in $\boldsymbol{H}_p$ or in $\boldsymbol{R}_{p',p}$, z' is the initial state of $\boldsymbol{R}_{p,p''}$, and $tp \sim pt$.

First let $(w, u) \in L(q)$, i.e., $w, u \in L$ and $\mathrm{NF}(\varphi(wq)) \equiv u$. Then, by Lemma 9, there exist $q_i \in Q \cup \{1\}$, $w_i, u_i \in Q^*$, and $t_i, s_i \in \mathcal{T}$ such that

1. $w \equiv w_1 t_1 w_2 t_2 \dots w_k t_k w_{k+1}$ and $u \equiv u_1 s_1 u_2 s_2 \dots u_k s_k u_{k+1}$,
2. $\mathrm{NF}(\varphi(t_i w_{i+1} q_{i+1})) \equiv q_i s_i u_{i+1}$,
3. $\mathrm{NF}(\varphi(w_1 q_1)) \equiv u_1$, and $q_{k+1} = q$.

Since the words w_i and u_i are factors of some elements of L, they belong themselves to L. From $\mathrm{NF}(\varphi(w_1 q_1)) \equiv u_1$, we therefore infer $(w_1, u_1) \in \boldsymbol{H}_{q_1}$. Hence there exists a successful (w_1, u_1)-labeled run of $\boldsymbol{H}_{q_1}$ with first state $z_1 = \iota$ and final state z_1'. From $\mathrm{NF}(\varphi(t_i w_{i+1} q_{i+1})) \equiv q_i s_i u_{i+1}$, we get $t_i q_i \sim q_i s_i$ and therefore $w_{i+1} q_{i+1} \sim q_i u_{i+1}$. Hence $(w_{i+1}, u_{i+1}) \in R_{q_i, q_{i+1}}$ which ensures the existence of some (w_{i+1}, u_{i+1})-labeled successful run of $\boldsymbol{R}_{q_i,q_{i+1}}$ from, say, z_i to z_i'. In particular, z_i is the initial state and z_i' is some accepting state of the transducer $\boldsymbol{R}_{q_i,q_{i+1}}$. Finally, $t_i q_i \sim q_i s_i$ implies the existence of transitions $(z_i', (t_i, s_i), z_{i+1})$ in $\mathcal{A}$. Hence, altogether, there exists a run in $\mathcal{A}$ labeled (w, u) from $z_1 = \iota$ to z_{k+1}'. Since $q_{k+1} = q$, the last state of this run is accepting in $\boldsymbol{R}_{q_k,q}$. Hence the run as a whole is successful in $\mathcal{A}$. Thus we have shown that $L(q) \subseteq R(\mathcal{A})$.

Conversely let $(w, u) \in R(\mathcal{A}) \cap L^2$. Since the transducers $\boldsymbol{H}_p$ and $\boldsymbol{R}_{p,r}$ do not allow letters from $\mathcal{T}$, these letters can only appear in the additional transitions. Thus the successful (w, u)-labeled run of $\mathcal{A}$ has the form

$$z_1 \xrightarrow{(w_1,u_1)} z_1' \xrightarrow{(t_1,s_1)} z_2 \xrightarrow{(w_2,u_2)} z_2' \xrightarrow{(t_2,s_2)} z_3 \cdots \xrightarrow{(w_{k+1},u_{k+1})} z_{k+1}'$$

with $w_i, u_i \in L \cap Q^*$, $s_i, t_i \in \mathcal{T}$ where

$$w \equiv w_1 t_1 w_2 t_2 \dots w_k t_k w_{k+1} \quad \text{and} \quad u \equiv u_1 s_1 u_2 s_2 \dots u_k s_k u_{k+1}.$$

Using the definition of the transducer $\mathcal{A}$, we find $q_i \in Q \cup \{1\}$ such that

(1) $z_1 \xrightarrow{(w_1,u_1)} z_1'$ is a run in the transducer $\boldsymbol{H}_{q_1}$ leading from the initial state $z_1 = \iota$ to some state z_1'.

(2) $z_1' \xrightarrow{(t_1,s_1)} z_2$ connects a final state of $\boldsymbol{H}_{q_1}$ with the initial state of $\boldsymbol{R}_{q_1,q_2}$. In particular, z_1' is accepting in $\boldsymbol{H}_{q_1}$ and z_2 is initial in $\boldsymbol{R}_{q_1,q_2}$.

(3) $z_i \xrightarrow{(w_i,u_i)} z_i'$ is a run in $\boldsymbol{R}_{q_{i-1},q_i}$. By induction, we know that z_i is initial in R_{q_{i-1},q_i}.

(4) $z_i' \xrightarrow{(t_i,s_i)} z_{i+1}$ connects a final state of $\boldsymbol{R}_{q_{i-1},q_i}$ with the initial state of $\boldsymbol{R}_{q_i,q_{i+1}}$. In particular, z_i' is accepting in $\boldsymbol{R}_{q_{i-1},q_i}$ and z_{i+1} is initial in $\boldsymbol{R}_{q_i,q_{i+1}}$. Furthermore, $t_i q_i \sim q_i s_i$.

From (1), we obtain $w_1 q \sim u_1$. Since z_i is initial and z_i' is final in $\boldsymbol{R}_{q_{i-1},q_i}$, (3) implies $w_i q_i \sim q_{i-1} u_i$. From (2) and (4), we obtain $t_i q_i \sim q_i s_i$. Putting these equations together, we obtain

$$\begin{aligned} wq &\equiv w_1 t_1 w_2 t_2 \dots t_k w_{k+1} q_{k+1} \\ &\sim w_1 t_1 w_2 t_2 \dots t_k q_k u_{k+1} \\ &\sim w_1 t_1 w_2 t_2 \dots q_k s_k u_{k+1} \\ &\vdots \\ &\sim w_1 q_1 s_1 u_2 s_2 \dots s_k u_{k+1} \\ &\sim u_1 s_1 u_2 s_2 \dots s_k u_{k+1} \equiv u. \end{aligned}$$

Now $w, u \in L$ imply $(w, u) \in L(q)$, i.e. we have shown that $L(q) = R(\mathcal{A}) \cap L^2$. Since the rationality of a relation is preserved when intersected with a direct product of regular languages (see [4] for example, although, in general, the intersection of rational relations need not be rational), $L(q)$ is indeed rational.

Proof of Lemma 15

Proof. Let

$$\pi : (Q \cup Q^{-1} \cup \mathcal{T})^* \to M_\Gamma^\Delta$$

be the natural extension of $\varphi : (Q \cup \mathcal{T})^* \to M_\Gamma$. We first show that π maps the language L^Δ surjectively onto M_Γ^Δ. To this aim, note that, for $v \in (Q \cup \mathcal{T})^*$, $\Delta v \approx \overline{v}\Delta$ implies $v\Delta^{-1} \approx \Delta^{-1}\overline{v}$. Now let $u^{-1}vq^{-1}w$ be a word with $u, v \in (Q \cup \mathcal{T})^*$, $w \in (Q \cup Q^{-1} \cup \mathcal{T})^*$, and $q \in Q$. Then there are $\sigma \in \Sigma$ and $p \in Q$ with $q \approx p\sigma$. This allows us to derive

$$u^{-1}vq^{-1}w \approx u^{-1}v\sigma^{-1}p^{-1}w \approx u^{-1}v\Delta^{-1}\Delta\sigma^{-1}p^{-1}w \approx u^{-1}\Delta^{-1}\overline{v}\Delta_\sigma p^{-1}w.$$

Applying this procedure iteratively, we obtain an equivalent word of the form $u^{-1}v$ with $u \in Q^*$ and $v \in (Q \cup \mathcal{T})^*$. Replacing u and v by their respective normal forms in L yields a word in L^Δ. Hence the language L^Δ is mapped surjectively onto M_Γ^Δ. To show injectivety, suppose that $u_1^{-1}v_1$ and $u_2^{-1}v_2$ both lie in L^Δ, and have the same image under π. Let u be the right lcm of u_1 and u_2; so there exist p_1, p_2 such that $u \sim p_1 u_1 \sim p_2 u_2$. Hence multiplying on the left by u, we have

$$v :\equiv p_1 v_1 \approx u u_1^{-1} v_1 \approx u u_2^{-1} v_2 \approx p_2 v_2.$$

Thus both p_1 and p_2 divide u and v, so $\operatorname{lcm}(p_1, p_2)$ divides the gcd of u and v, which is $p_i \gcd(u_i, v_i) \sim p_i$ for either i. Thus $\operatorname{lcm}(p_1, p_2) \sim p_i$ for either i, forcing $p_1 \sim p_2$, and hence by cancellation, $u_1 \sim u_2$ and $v_1 \sim v_2$. By the uniqueness of the normal form in M_Γ we get $u_1^{-1}v_1 \equiv u_2^{-1}v_2$.

Proof of Lemma 16

Proof. (1) If $u_y \equiv u_x$ and $v_y \approx v_x\tau$, then we get immediately

$$x\tau \equiv u_x^{-1}v_x\tau \approx u_y^{-1}v_y \equiv y$$

which proves one direction of the equivalence. For the converse implication, suppose that $x\tau \approx y$. Since $u_x \in Q^*$, we get

$$\gcd(\varphi(u_x), \varphi(v_x\tau)) = \gcd(\varphi(u_x), \varphi(v_x)) = 1.$$

Hence the unique normal form of $\varphi(x\tau)$ is $u_x^{-1}\mathrm{NF}(\varphi(v_x\tau))$. Since $y \in L^\Delta$ represents $\varphi(x\tau)$, we obtain $u_y = u_x$ and $v_y \approx v_x\tau$.

(2) If $q \in Q$ with $qu_y \approx u_x$ and $qv_y \approx v_x\sigma$, the equalities

$$x\sigma \equiv u_x^{-1}v_x\sigma \approx u_y^{-1}q^{-1}qv_y \approx u_y^{-1}v_y \equiv y$$

are immediate. Conversely assume $x\sigma \approx y$ and let $q = \gcd(\varphi(u_x), \varphi(v_x\sigma))$. Since σ divides Δ, the monoid element q divides

$$\gcd(\varphi(u_x)\cdot\Delta, \varphi(v_x)\cdot\Delta) = \gcd(\Delta\cdot\overline{\varphi(u_x)}, \Delta\cdot\overline{\varphi(v_x)}) = \Delta\cdot\gcd(\overline{\varphi(u_x)}, \overline{\varphi(v_x)}) = \Delta.$$

Hence q is squarefree. Now let $u_z, v_z \in L^\Delta$ be the unique words from L^Δ with $qu_z \approx u_x$ and $qv_z \approx v_x\sigma$. Then $\varphi(u_z)$ divides the element $\varphi(u_x)$ of S from the right. Hence $u_z \in Q^*$. By the definition of q as greatest common left divisor, we obtain immediately $\gcd(\varphi(u_z), \varphi(v_z)) = 1$ and therefore $u_z^{-1}v_z \in L^\Delta$. Furthermore,

$$u_z^{-1}v_z \approx u_z^{-1}q^{-1}qv_z \approx u_x^{-1}v_x\sigma \equiv x\sigma \approx y.$$

Hence y and $u_z^{-1}v_z$ are two elements of L^Δ representing the same element of M_Γ^Δ, implying $u_z \equiv u_y$ and $v_z \equiv v_y$. But now the choice of u_z and v_z implies $qu_y \approx u_x$ and $qv_y \approx v_x\sigma$.

(3) If $q \in Q$ such that $qu_y \approx \Delta u_x$ and $qv_y \approx \overline{v_x}\Delta_\sigma$, then direct calculations reveal

$$\begin{aligned} y \equiv u_y^{-1}v_y &\approx u_y^{-1}q^{-1}qv_y \approx u_x^{-1}\Delta^{-1}\overline{v_x}\Delta_\sigma\sigma\sigma^{-1} \\ &\approx u_x^{-1}\Delta^{-1}\Delta v_x\sigma^{-1} \approx u_x^{-1}v_x\sigma^{-1} \equiv x\sigma^{-1}. \end{aligned}$$

Conversely, suppose $y \approx x\sigma^{-1}$ and let $q = \gcd(\varphi(\Delta u_x), \overline{\varphi(v_x)}\cdot\Delta_\sigma)$. Since Δ_σ divides Δ, the monoid element q divides

$$\gcd(\Delta\cdot\varphi(u_x), \overline{\varphi(v_x)}\cdot\Delta) = \gcd(\Delta\cdot\varphi(u_x), \Delta\cdot\varphi(v_x)) = \Delta\cdot\gcd(\varphi(u_x), \varphi(v_x)) = \Delta,$$

i.e. $q \in Q$. Now choose $u_z, v_z \in L^\Delta$ such that $qu_z \approx \Delta u_x$ and $qv_z \approx \overline{v_x}\Delta_\sigma$. Then, as in case (2), $u_z \in Q^*$ and $\gcd(\varphi(u_z), \varphi(v_z)) = 1$. Furthermore,

$$\begin{aligned} u_z^{-1}v_z &\approx u_z^{-1}q^{-1}qv_z \approx u_x^{-1}\Delta^{-1}\overline{v_x}\Delta_\sigma\sigma\sigma^{-1} \\ &\approx u_x^{-1}\Delta^{-1}\Delta v_x\sigma^{-1} \approx u_x^{-1}v_x\sigma^{-1} \equiv x\sigma^{-1} \equiv y. \end{aligned}$$

Now the claim follows as in case (2) above.

Proof of Lemma 16

Proof. Let $w \in Q^*$, $t \in \mathcal{T}$, and $z \in (Q \cup \mathcal{T})^*$ with $x \equiv wtz \in L$. There are $v \in Q^*$ and $p \in Q$ with $qw \approx vp \in L$. Then $\alpha(\varphi(ptz), \Delta) = \varphi(pr)$ for some $r \in Q^*$. Hence r divides $\varphi(tz)$ implying $r = 1$ since $tz \in L$. Thus, $u \equiv vp \in L$ satisfies $qx \approx utz \in L$.

So far, we showed $(x, y) \in R(q)$ iff $(x, y) \in (q)L$ or there are $u, w \in Q^*$, $t \in \mathcal{T}$, and $z \in (Q \cup \mathcal{T})^*$ with $x \equiv wtz \in L$, $qw \approx u \in L \cap Q^*$, and $y \equiv utz \in L$. Hence

$$R(q) = R'(q) \cup [R'(q) \cdot \{(t,t) \,:\, t \in \mathcal{T}\} \cdot \{(a,a) \,:\, a \in Q \cup \mathcal{T}\}^*] \cap (L \times L)$$

which is rational.

Proof of Lemma 18

Proof. First, let $t = \tau \in T$. Then, by Lemma 16(1), we get

$$L^{\Delta}(\tau) = (\{(a,a) \,:\, a \in \Sigma^{-1}\}^* \cdot L(\tau)) \cap (L^{\Delta} \times L^{\Delta})$$

which is rational.

Now let $t = \sigma \in \Sigma$. Then, by Lemma 16(2), we have $(u_x^{-1}v_x, u_y^{-1}v_y) \in L^{\Delta}(\sigma)$ if and only if $x = u_x^{-1}v_x$ and $y = u_y^{-1}v_y$ belong to L^{Δ}, and there exist $q \in Q$ and $v \in L$ with $qu_y \equiv u_x$, $qv_y \equiv v$, and $v_x\sigma \equiv v$. But this is equivalent to saying that (x, y) belongs to the rational relation

$$\bigcup_{q \in Q} [\{(u^{-1}, v^{-1}) \,:\, (u,v) \in R'(q)\}\,(R'(q) \circ \{(v,u) \,:\, (u,v) \in L(\Sigma)\})] \cap [L^{\Delta} \times L^{\Delta}].$$

Finally, let $t = \sigma^{-1}$ for some $\sigma \in \Sigma$. Then, by Lemma 16(3), we have that $(u_x^{-1}v_x, u_y^{-1}v_y) \in L^{\Delta}(\sigma)$ if and only if $x = u_x^{-1}v_x$ and $y = u_y^{-1}v_y$ belong to L^{Δ}, and there are $p, q \in Q$ and $v \in L$ with $pq \approx \Delta$, $u_y \approx pu_x$ and $qv_y \approx v \approx \overline{v_x}\Delta_\sigma$. Let

$$\begin{aligned}
R_1(p,q) &= \{(u_x^{-1}, u_y^{-1}) \,:\, u_x, u_y \in L \cap Q^*, u_x \approx pu_y\} \\
&= \{(u_x^{-1}, u_y^{-1}) \,:\, (u_y, u_x) \in R'(q)\} : \\
R_2(p,q) &= \{(v_x, v) \,:\, v_x, v \in L, \overline{v_x}\Delta_\sigma \approx v\} \\
&= \{(v_x, v) \,:\, v_x, v \in L, \exists w \in L : w \equiv \overline{v}, (w,u) \in L(\Delta_\sigma)\}; \\
R_3(p,q) &= \{(v, v_y) \,:\, v, v_y \in L, qv_y \approx v\} \\
&= \{(v, v_y) \,:\, (v_y, v) \in R(q)\}.
\end{aligned}$$

Then all these relations are rational. Hence

$$L(\sigma^{-1}) = [R_1 \cdot (R_2 \circ R_3)] \cup (L \times L)$$

is also rational.