An asymmetric generalisation of Artin monoids

Daan Krammer

November 23, 2012

Abstract

We propose a slight weakening of the definitions of Artin monoids and Coxeter monoids. We study one ‘infinite series’ in detail.

1 Introduction

This paper begins with a classification of monoids generated by two idempotents such that the ordering of left-division is a lattice ordering.

The result suggests a definition (definition 4) of a class of monoids which we call AI monoids (A for Artin, I for idempotent). It contains the well-known Artin monoids.

Every AI monoid comes hand-in-hand with what we call a CI monoid (C for Coxeter, I for idempotent). The twin of an Artin monoid may be called a Coxeter monoid.

An example of an AI monoid is A_n presented by generators $\{p_a \mid 1 \leq a \leq n\}$ and relations

$$\begin{aligned} p_a\, p_b &= p_b\, p_a && \text{if } |a-b| > 1 \\ p_{a-1}\, p_a\, p_{a-1} &= p_a\, p_{a-1}\, p_a\, p_{a-1} && \text{if } 2 \leq a \leq n. \end{aligned}$$

The CI monoid M_n of the same type is presented by generators $\{m_a \mid 1 \leq a \leq n\}$ and relations

$$\begin{aligned} m_a\, m_b &= m_b\, m_a && \text{if } |a-b| > 1 \\ m_{a-1}\, m_a\, m_{a-1} &= m_a\, m_{a-1}\, m_a\, m_{a-1} && \text{if } 2 \leq a \leq n \\ m_{a-1}\, m_a\, m_{a-1} &= m_{a-1}\, m_a\, m_{a-1}\, m_a && \text{if } 2 \leq a \leq n \\ m_a\, m_a &= m_a && \text{if } 1 \leq a \leq n. \end{aligned}$$

The monoid M_n appeared earlier in [He], [O] and [D2] as an overarching object in Garside theory; also see section 7. In [He] and [O] Q_n is the notation for M_n.

If a Coxeter group is finite then the corresponding Artin group A is commonly called spherical. Equivalent to this is that any two elements of A have a common right-multiple. Again equivalent is that the corresponding Coxeter monoid M has an element w_0, called a sink, such that $x\, w_0\, y = w_0$ for all $x, y \in M$. Again equivalent to this is that the Coxeter *monoid* is finite.

We shall show that M_n has a sink. This is proposition 67 and was previously proved in [D2] and [He]. On the other hand M_n is infinite if $n \geq 3$ (proposition 69).

Thus M_n has some properties in common with the spherical Coxeter monoids, some with the nonspherical ones. We feel however that the similarity with the spherical Coxeter monoids is stronger.

As the full class of AI monoids seems beyond reach (even assuming that the corresponding CI monoid has a sink) we decide to focus on the monoids A_n and M_n. Two of our main results, corollaries 37 and 66, are fast solutions to the word problems in A_n and M_n. For both monoids we use the shortlex language.

Spherical Artin groups are examples of Garside groups. See [D1] or [D2] for Garside theory. Being a Garside group is an elegant and powerful property implying, among others, a fast solution to the word problem.

Our solution to the word problem for A_n is very different and seems unrelated to Garside properties. Instead we conjecture that A_n is a weak kind of left-Garside monoid, see conjecture 57. As partial results towards this conjecture we prove that A_n is left-cancellative (proposition 39) and that it has a Garside element (proposition 56).

It is known that every Artin monoid A satisfies the so-called cube condition. A closely related property is that if two elements of A have a common right-multiple then they have a least such. AI monoids are not this well-behaved. In section 5 we present an AI monoid which doesn't satisfy the cube condition.

Every Coxeter group comes with a well-known faithful linear representation defined over $\mathbb{R}$ [Hu]. In proposition 12 we present a similarly looking linear representation of any CI monoid, with the difference that we make the base ring depend on the Coxeter monoid in question. We don't know if these representations are faithful.

Acknowledgement. Many thanks to V. Ozornova for pointing out the relevance of the thesis of A. Hess [He].

2 Monoids generated by two idempotents

An element x of a monoid is said to be *idempotent* if $x^2 = x$.

If a, b are elements of a monoid and $n \geq 0$ we write

$$[a, b; 2n] = (ab)^n, \quad [a, b; 2n+1] = (ab)^n a.$$

A *lattice* is an ordered set in which any two elements x, y have a least common upper bound or *join* and a greatest common lower bound or *meet.*

Proposition 1. *Let M be a monoid generated by two idempotents a, b. Let $\leq$ be the relation on M defined by $x \leq y$ if and only if $y \in xM$, in words, x is a left-divisor of y. Suppose $1, a, b$ are distinct and neither $a \leq b$ nor $b \leq a$. Then the following are equivalent:*

(a) *The relation $\leq$ is an ordering, and a lattice ordering.*

(b) *There are $k, \ell \geq 2$ with $|k - \ell| \leq 1$ satisfying the following. Let M' be the monoid presented by*

$$M' = \bigl\langle A, B \bigm| [A, B; k] = [A, B; k+1] = [B, A; \ell] = [B, A; \ell + 1] \bigr\rangle.$$

Then there exists an isomorphism $f \colon M' \longrightarrow M$ such that $f(A) = a$ and $f(B) = b$.

(c) *After interchanging a, b if necessary there exists $k \geq 2$ such that M admits one of the following presentations:*

$$M = \langle a, b \mid [a, b; k] = [b, a; k] \rangle, \text{ or} \tag{2}$$
$$M = \langle a, b \mid [a, b; k] = [a, b; k+1] = [b, a; k+1] \rangle. \tag{3}$$

The Hasse diagram of M is defined to be the directed graph with vertex set M and which has an arrow labelled s from x to xs whenever $s \in \{a, b\}$ and $x \neq xs$. If (b) holds with $k = 3$ and $\ell = 4$ then it looks as follows.

$$\begin{tikzcd}
 & a \arrow[r, "b"'] & ab \arrow[drr, "a"'] & & \\
1 \arrow[ur, "a"'] \arrow[dr, "b"] & & & & aba = baba \\
 & b \arrow[r, "a"] & ba \arrow[r, "b"] & bab \arrow[urr, "a"] &
\end{tikzcd}$$

Proof. Note that if (b) holds and $\ell = k + 1$ then M is presented by (3). The equivalence (b) $\Leftrightarrow$ (c) is now clear.

Proof of (a) $\Rightarrow$ (b). Since $(M, \leq)$ is a lattice there exists a join Δ of $\{a, b\}$. There are $k, \ell \geq 1$ such that

$$[a, b; k] = \Delta = [b, a; \ell]$$

because a, b are idempotents and M is generated by a, b and $\Delta \in aM$ and $\Delta \in bM$. Choose k, ℓ minimal with the above properties. Note $k, \ell \geq 2$ because neither $a \leq b$ nor $b \leq a$.

After interchanging a, b if necessary we may assume $k \leq \ell$.

We have

$$[a, b; k] \leq [a, b; \ell + 1] = a\,[b, a; \ell] = a\Delta = a\,[a, b; k] = [a, b; k]$$

so equality holds throughout, proving $[a, b; k] = [a, b; k+1]$. It follows that $\Delta = \Delta a = \Delta b$ (because a, b are idempotents) and therefore $[a, b; \ell] = [a, b; \ell + 1]$.

We shall next prove $\ell \leq k + 1$. Suppose to the contrary $\ell \geq k + 2$. Put $x = [a, b; \ell - k - 2]$ if k is odd and $x = [b, a; \ell - k - 2]$ if k is even. Then

$$[b, a; \ell] = b\,[a, b; k+1]\,x = b\,[a, b; k]\,x = b\,[a, b; k] = [b, a; k+1]$$

whence $\ell \leq k + 1$ because ℓ was chosen minimal. This is a contradiction and proves $\ell \leq k + 1$.

We have proved that there exists a unique surjective homomorphism $f\colon M' \to M$ such that $f(A) = a$ and $f(B) = b$. It remains to prove that f is injective. Suppose $x, y \in M$ are distinct with $f(x) = f(y)$. We need to derive a contradiction.

Let $\leq$ be the relation of left division in M' and $0 = [A, B; k] = [B, A; \ell]$. Note $0u = u0 = 0$ for all $u \in M'$.

Suppose first $A \leq x$, $B \leq y$, say, $x = [A, B; p]$ and $y = [B, A; q]$. Then $[a, b; p] = [b, a; q]$. But a, b have a join and k, ℓ are minimal so $k \leq p$ and $\ell \leq q$. The definition of M' now implies $x = 0 = y$, a contradiction.

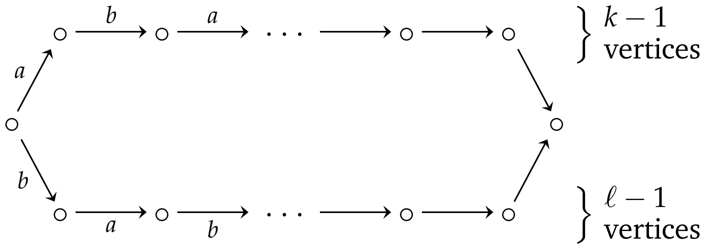
Suppose next $A \leq x$, $A \leq y$, say, $x = [A, B; p]$, $y = [A, B; q]$. Also assume $p < q$. Then $[a, b; p] = [a, b; q]$. But $\leq$ is an ordering so $[a, b; r]$ is independent of r as long as $p \leq r \leq q$. In particular $[a, b; p] = [a, b; p + 1]$. But a, b are idempotents so $f(x) = f(x)a = f(x)b$. So $[a, b; p] = \Delta$. Since k was chosen to be minimal we have $k \leq p < q$. Hence $x = [A, B; p] = [A, B; q] = y$. This is the required contradiction.

Suppose now $1 = x$, $A \leq y$. Then $1_M < a = f(A) \leq f(y) = f(x) = 1_M$. This contradicts our assumption that $\leq$ is an ordering.

Up to interchanging a with b or x with y or both this covers all cases. This proves that f is injective and thereby (a) $\Rightarrow$ (b).

Proof of (a) $\Leftarrow$ (b). Write $\Delta = [a, b; k] = [b, a; \ell]$. Note that Δ is a sink, that is, $x\Delta y = \Delta$ for all $x, y \in M$. Therefore every element of $M \smallsetminus \{1, \Delta\}$ can uniquely be written $[a, b; p]$ $(0 < p < k)$ or $[b, a; q]$ $(0 < q < \ell)$.

Conversely, $[a, b; p] \neq \Delta$ and $[b, a; q] \neq \Delta$ if $p < k$ and $q < \ell$ because $|k - \ell| \leq 1$. Therefore the Hasse diagram of M is



which proves that $\leq$ is an ordering and a lattice ordering. This finishes the proof of (a) $\Leftarrow$ (b). ☐

3 CI monoids and AI monoids

Definition 4. A *CI matrix* (C for Coxeter, I for idempotent) consists of a set S and a map $m\colon S \times S \to \mathbb{Z}_{\geq 1} \cup \{\infty\}$ such that:

- $m(a, b) = 1$ if and only if $a = b$.
- $m(a, b) = \infty$ if and only if $m(b, a) = \infty$.
- $|m(a, b) - m(b, a)| \leq 1$ for all $a, b \in S$.

With a CI matrix (S, m) we associate the *CI monoid* M presented by generating set S and relations

- $a^2 = a$ for all $a \in S$. (5)

- ∘ $[a,b;m(a,b)] = [b,a;m(b,a)]$ whenever $m(a,b) \neq \infty$. (6)
- ∘ $[a,b;m(a,b)] = [a,b;m(a,b)+1]$ whenever $m(a,b) \neq \infty$. (7)

Moreover we associate an *AI monoid* A (A for Artin, I for idempotent) presented by generating set S and relations (6).

It is easy to show that the natural map $S \to M$ is injective. We shall consider S as a subset of M and A. Clearly there is a unique homomorphism $A \to M$ which is the identity on S.

A pair (M', S') is called a *CI system* if M' is a monoid and there exists an isomorphism $M \to M'$ (with M as above) taking S to S'. Likewise, a pair (A', S') is called an *AI system* if A' is a monoid and there exists an isomorphism $A \to A'$ taking S to S'.

The number $\#S$ is called the *rank* of M and A. □

So part (b) of proposition 1 says that $(M, \{a,b\})$ is a CI system of rank 2.

Consider definition 4 and suppose that m is symmetric, that is, $m(a,b) = m(b,a)$ for all $a,b \in S$. Then the definition reduces to the following well-known things. Firstly, (S,m) is then known as a Coxeter matrix and A is called an Artin monoid. Likewise we shall call M a Coxeter monoid though this terminology is not common. More commonly studied is the *Coxeter group* W which is by definition the quotient of A by the additional relations $a^2 = 1$ for all $a \in S$ (provided m is symmetric).

The CI graph or diagram associated with a CI matrix (S,m) is the graph with vertex set S and the following edges:

- ∘ If $m(a,b) = m(b,a) > 2$ then there is an unoriented edge between a,b labelled $2m(a,b) = m(a,b) + m(b,a)$.
- ∘ If $m(a,b) + 1 = m(b,a)$ then there is an arrow from a to b labelled $m(a,b) + m(b,a)$.

So m is symmetric if and only if all edge labels in the Coxeter graph are even. Warning: If all labels are even then our definition of Coxeter graph differs from the usual one because our labels are twice the usual labels. Labels equal to 6 are suppressed as usual.

Coxeter groups and Artin monoids have been studied extensively. A good introduction is [Hu]. Proposition 1 is our main motivation for generalising Artin monoids to AI monoids.

If M, N are monoids then a map $\phi\colon M \to N$ is called an *anti-homomorphism* if $\phi(xy) = \phi(y)\,\phi(x)$ for all $x, y \in M$.

Lemma 8. *Let (M,S) be a CI monoid. Assume that no edge label is in $1 + 4\mathbb{Z}$. That is, $m(a,b) + m(b,a) \notin 1 + 4\mathbb{Z}$ for all $a,b \in S$. Then there exists a unique anti-automorphism ϕ of M such that $\phi(a) = a$ for all $a \in S$.*

Proof. We may assume $\#S = 2$, say, $S = \{a,b\}$. Write $k = m(a,b)$, $\ell = m(b,a)$. After interchanging a,b if necessary we may also assume $k \leq \ell$.

If $k = \ell$ the result is clear. We are left to consider the case $k < \ell$. Then $\ell = k+1$ and k is odd. By definition M is presented by generating set $\{a,b\}$

and relations $a^2 = a$, $b^2 = b$ and

$$\begin{aligned} [a, b; k] &= [b, a; k+1] \qquad (9)\\ [a, b; k] &= [a, b; k+1] \qquad (10)\\ [b, a; k+1] &= [b, a; k+2]. \qquad (11) \end{aligned}$$

Note that (11) is a formal consequence of (9) and (10) and can therefore be supressed. The effect of reversing the multiplication is to interchange (9) and (10) because k is odd. The result follows. ☐

4 A linear representation for any CI monoid

The following proposition gives a linear representation of any CI monoid. It looks a bit like the well-known faithful representation of any Coxeter group [Hu]. We don't know if our representations are faithful.

Proposition 12. *Let (M, S) be a CI system and let m be the associated CI matrix. Let R be the associative ring presented by generators x_{ab} whenever $a, b \in S$ are distinct and relations*

$$[x_{ab}, x_{ba}; m(a, b) - 1] = 0 \qquad (13)$$

whenever $a, b \in S$ are distinct. Let V be a free left R-module with basis $(e_a \mid a \in S)$. Then there exists an M-action on V given by

$$e_a\, a = 0, \qquad e_b\, a = e_b + x_{ba}\, e_a$$

whenever $a, b \in S$ are distinct.

Proof. For $a \in S$ consider the R-linear map $T_a \colon V \to V$ defined by

$$e_a\, T_a = 0, \qquad e_b\, T_a = e_b + x_{ba}\, e_a$$

whenever a, b are distinct. Until further notice we shall not use the relations (13) between the x_{ab}.

We begin by proving that T_a is idempotent. Firstly $e_a\, T_a^2 = 0 = e_a\, T_a$. Moreover if $b \neq a$ then $e_b\, T_a^2 = (e_b + x_{ba}\, e_a) T_a = e_b\, T_a$ thus proving that T_a is idempotent.

Fix distinct $a, b, c \in S$. For $n \in \mathbb{Z}$ write

$$\big(a(n), b(n)\big) = \begin{cases} (a, b) & \text{if } n \text{ is even,} \\ (b, a) & \text{if } n \text{ is odd.} \end{cases}$$

By induction on n we shall prove

$$e_b\, [T_a, T_b; n] = [x_{ba}, x_{ab}; n-1]\, e_{a(n)} + [x_{ba}, x_{ab}; n]\, e_{b(n)} \quad \text{if } n \geq 1. \qquad (14)$$

For $n = 1$ this is given. If it is true for n then

$$\begin{aligned} &e_b\, [T_a, T_b; n+1] = e_b\, [T_a, T_b; n]\, T_{a(n)} \\ &\quad = \big([x_{ba}, x_{ab}; n-1]\, e_{a(n)} + [x_{ba}, x_{ab}; n]\, e_{b(n)}\big) T_{a(n)} \end{aligned}$$

$$\begin{aligned}&= [x_{ba}, x_{ab}; n]\, e_{b(n)} T_{a(n)} = [x_{ba}, x_{ab}; n]\, (e_{b(n)} + x_{b(n),a(n)}\, e_{a(n)}) \\ &= [x_{ba}, x_{ab}; n]\, e_{b(n)} + [x_{ba}, x_{ab}; n+1]\, e_{a(n)} \\ &= [x_{ba}, x_{ab}; n]\, e_{a(n+1)} + [x_{ba}, x_{ab}; n+1]\, e_{b(n+1)}.\end{aligned}$$

This proves (14).

Since T_a, T_b are idempotents

$$\begin{aligned}&[T_a, T_b; p+1] - [T_b, T_a; p+1] \\ &\quad = \big([T_a, T_b; p] - [T_b, T_a; p]\big)(T_a + T_b - 1)\end{aligned} \tag{15}$$

for all $p \geq 1$.

By induction on n we shall prove

$$\begin{aligned}e_c\big([T_a, T_b; n] - [T_b, T_a; n]\big) &= x_{ca}[x_{ab}, x_{ba}; n-1]\, e_{b(n)} \\ &\quad - x_{cb}[x_{ba}, x_{ab}; n-1]\, e_{a(n)} \quad \text{if } n \geq 1.\end{aligned} \tag{16}$$

It holds for $n = 1$ because

$$e_c(T_a - T_b) = (e_c + x_{ca}\, e_a) - (e_c + x_{cb}\, e_b) = x_{ca}\, e_a - x_{cb}\, e_b.$$

If it is true for $n-1$ then by (15)

$$\begin{aligned}&e_c\big([T_a, T_b; n] - [T_b, T_a; n]\big) \\ &= e_c\big([T_a, T_b; n-1] - [T_b, T_a; n-1]\big)(T_a + T_b - 1) \\ &= \big(x_{ca}[x_{ab}, x_{ba}; n-2]\, e_{a(n)} - x_{cb}[x_{ba}, x_{ab}; n-2]\, e_{b(n)}\big)(T_a + T_b - 1) \\ &= x_{ca}[x_{ab}, x_{ba}; n-2]\, e_{a(n)}(T_{b(n)} - 1) \\ &\quad - x_{cb}[x_{ba}, x_{ab}; n-2]\, e_{b(n)}(T_{a(n)} - 1) \\ &= x_{ca}[x_{ab}, x_{ba}; n-2]\, x_{a(n),b(n)}\, e_{b(n)} - x_{cb}[x_{ba}, x_{ab}; n-2]\, x_{b(n),a(n)}\, e_{a(n)} \\ &= x_{ca}[x_{ab}, x_{ba}; n-1]\, e_{b(n)} - x_{cb}[x_{ba}, x_{ab}; n-1]\, e_{a(n)}.\end{aligned}$$

This proves (16).

We are ready to use the relations (13) in the ring R. Write $k = m(a,b)$ and $\ell = m(b,a)$.

First suppose $k = \ell$. Write

$$X = [T_a, T_b; k], \qquad Y = [T_b, T_a; k].$$

We must prove $X = Y$. Well, (14) shows that all among e_aX, e_bX, e_aY, e_bY are zero. Also (16) shows that $e_c(X - Y) = 0$. This settles the case $k = \ell$.

Finally suppose $\ell = k+1$ and write

$$X = [T_a, T_b; k], \qquad Y = [T_b, T_a; k+1], \qquad Z = [T_a, T_b; k+1].$$

We must prove $X = Y = Z$. Well, (14) proves $e_aU = 0 = e_bU$ for all $U \in \{X, Y, Z\}$. Moreover (16) shows that $e_c(Y - Z) = 0$.

Applying $[T_a, T_b; k]$ to both sides of the equation $e_c(T_b - 1) = x_{cb}\, e_b$ yields

$$e_c\,\big([T_b, T_a; k+1] - [T_a, T_b; k]\big) = x_{cb}\, e_b\, [T_a, T_b; k]$$

so $e_c(Y - X) = 0$ by (14). This finishes the case $\ell = k+1$. The proof is complete. $\square$

5 An AI monoid not satisfying the cube condition

It is known that if two elements of an Artin monoid have a common upper bound then they have a join. For AI monoids this is false in general as we shall now show.

Consider the AI monoid A of diagram

$$\begin{tikzcd} a \arrow[r, dash, "6"] & b \arrow[r, "7"] & c. \end{tikzcd}$$

This monoid is presented by

$$A = \langle a,b,c \mid aba = bab,\ bcb = cbcb,\ ac = ca \rangle. \tag{17}$$

Consider the ordering $\leq$ of left-division on A, that is, $x \leq y \Leftrightarrow y = xz$ for some z.

A *congruence* on a monoid N is an equivalence relation $\sim$ on N such that there exists a (necessarily unique) structure of monoid on the set $N/{\sim}$ of equivalence classes such that the natural map $N \to N/{\sim}$ is a homomorphism of monoids.

Let F be the free monoid on $\{a,b,c\}$ and $\sim$ the congruence generated by the relations in (17), so that $A = F/{\sim}$. For $x \in F$ let $[x]$ denote the equivalence class of $\sim$ containing x.

Put $p = [bcb]$, $q = [cabcbab]$ and note

$$cabcbab \sim acbcbab \sim abcbab \sim abcaba \sim abacba \sim babcba.$$

We have

$$p = [bcb] = [cbcb], \quad q = [cabcbab] = [babcba]$$

so p, q are two upper bounds of $\{[b],[c]\}$.

The proof of the following proposition doesn't use any background on Garside theory.

Proposition 18.

(a) *The set of all words in a,b,c representing p is $\{c^k\,b\,c\,b \mid k \geq 0\}$.*

(b) *p is a minimal upper bound of $\{[b],[c]\}$. Here minimal means that if r is an upper bound of $\{[b],[c]\}$ with $r \leq p$ then $r = p$.*

(c) *The set of all words representing q is contained in*

$$\begin{gathered}\{c^k\,b\,c^\ell\,a\,c^m\,b\,c\,b\,a \mid k,\ell,m \geq 0\} \cup \{c^k\,a\,c^\ell\,b\,a\,c\,b\,a \mid k,\ell \geq 0\} \\ \cup \{c^k\,a\,c^\ell\,b\,c\,b\,a\,b \mid k,\ell \geq 0\} \cup \{c^k\,a\,c^\ell\,b\,c\,a\,b\,a \mid k,\ell \geq 0\}.\end{gathered}$$

(d) *q is not an upper bound of p.*

(e) *$\{[b],[c]\}$ has an upper bound but no join.*

Proof. Parts (a)–(c) are straightforward. By (c) no word for q starts with bcb and so (d) follows. Part (e) follows from (b) and (d). ☐

There is also a mechanical method for proving that A contains two elements with a common upper bound but without join. To do this one proves that A fails to satisfy the so-called *cube condition.* See [D1] or [D2] for the necessary background including the $\backslash$ operation. One finds

$$(a\backslash b)\backslash(a\backslash c) = cba, \qquad (b\backslash a)\backslash(b\backslash c) = cbab$$

but cba, $cbab$ represent distinct elements of A.

6 A CI graph

From now we shall deal with the CI monoid and the AI monoid of diagram

$$\underset{x_1}{\circ} \xrightarrow{7} \underset{x_2}{\circ} \xrightarrow{7} \cdots \xrightarrow{7} \circ \xrightarrow{7} \underset{x_n.}{\circ} \tag{19}$$

Fix a natural number n. Let F_n be the free monoid on a set $X_n = \{x_1, \ldots, x_n\}$ of n elements. An element of F_n is called a *word* and an element of X a *letter.*

Definition 20.

(a) Let $=_B$ be the least congruence on F_n such that

$$x_a\, x_b =_B x_b\, x_a \qquad \text{whenever } |a-b| > 1. \tag{21}$$

(b) Let $=_A$ be the least congruence on F_n containing $=_B$ such that

$$x_a\, x_{a-1}\, x_a\, x_{a-1} =_A x_{a-1}\, x_a\, x_{a-1} \qquad \text{whenever } 2 \le a \le n. \tag{22}$$

(c) Let $=_M$ be the least congruence on F_n containing $=_A$ such that

$$\begin{aligned} x_a\, x_a &=_M x_a && \text{for all } a \\ x_{a-1}\, x_a\, x_{a-1}\, x_a &= x_{a-1}\, x_a\, x_{a-1} && \text{whenever } 2 \le a \le n. \end{aligned}$$

An equivalence class with respect to the equivalence relation $=_B$ is called a B-class. If $x =_B y$ then we also say that x and y are B-equivalent. The B-class of x is written $[x]_B$. Likewise for A or M instead of B. We write $m_a = [x_a]_M$ and $p_a = [x_a]_A$.

We put

$$A = A_n := (F_n/{=_A}), \qquad M = M_n := (F_n/{=_M}).$$

Then A is an AI monoid of diagram (19) and M a CI monoid of the same diagram.

7 M_n-actions on X^{n+1}

Let X be a set and write X^k for the Cartesian k-th power of X. Let $f\colon X^2 \to X^2$ be a map. Define maps $f_1, f_2\colon X^3 \to X^3$ by $f_1 = f \times \mathrm{id}_X$ and $f_2 = \mathrm{id}_X \times f$. Assume:

$$f^2 = f, \qquad f_1 f_2 f_1 = f_2 f_1 f_2 f_1 = f_1 f_2 f_1 f_2.$$

Then there exists an M_n-action on X^{n+1} by making $m_a = [x_a]_M$ act as

$$(\mathrm{id}_X)^{a-1} \times f \times (\mathrm{id}_X)^{n-a}.$$

This simple observation (and the fact that M_n has a sink, see proposition 67) is at the basis of Garside theory. See [D2], [He], [O]. This motivates us to focus on M_n and A_n.

8 The diamond lemma

Lemma 23 (Diamond lemma)**.** *Let $\to$ be a relation on a set S. Let $\twoheadrightarrow$ denote its transitive closure and $\sim$ the equivalence relation generated by $\to$. Assume:*

- ○ *(Well-founded). There is no infinite sequence $x_1 \to x_2 \to \cdots$ with $x_i \in S$ for all i.* (24)
- ○ *(Confluence). Let $u, v, w \in S$ and assume $u \to v$ and $u \to w$. Then there exists $x \in S$ such that $v \twoheadrightarrow x$ and $w \twoheadrightarrow x$.* (25)

An element $v \in S$ is called reduced if there is no w with $v \to w$. Then every equivalence class for $\sim$ contains a unique reduced element.

Proof. See for example [C, Lemma 1.4.1 and exercise 1.4.2]. ☐

9 A rewriting system for A_n

Write $(x_a, x_b] := x_{a-1} x_{a-2} \cdots x_b$ provided $a \geq b$. In particular $(x_a, x_a] = 1$. Note also $(x_a, x_b](x_b, x_c] = (x_a, x_c]$.

Definition 26. Let $\xrightarrow[0]{A}$ be the least relation on F_n such that

$$x_a\, x_b \xrightarrow[0]{A} x_b\, x_a \tag{27}$$

whenever $a - b \geq 2$ and

$$x_{a-1}^{c(1)} [x_{a-2}^{c(2)} \cdots x_{a-b}^{c(b)}]\, (x_a, x_{a-b}] \xrightarrow[0]{A} [x_{a-2}^{c(2)} \cdots x_{a-b}^{c(b)}]\, (x_a, x_{a-b}] \tag{28}$$

whenever $c(i) \geq 1$ for all i and $b \geq 2$. If $u \xrightarrow[0]{A} v$ then we call u an A-standard word. We call the move (27) a commutation move.

Note that if $u \xrightarrow[0]{A} v$ and $u \xrightarrow[0]{A} w$ then $v = w$. Also, if u and xuy are A-standard ($u, x, y \in F_n$) then $x = y = 1$.

Definition 29.

(a) Let $\xrightarrow{A}$ be the least relation on F_n containing $\xrightarrow[0]{A}$ and such that

$$(u \xrightarrow{A} v) \Rightarrow (xuy \xrightarrow{A} xvy)$$

for all $u, v, x, y \in F_n$.

(b) We define $\overset{A}{\twoheadrightarrow}$ to be the least transitive relation on F_n containing $\xrightarrow{A}$.

Lemma 30. *The congruence on F_n generated by $\xrightarrow{A}$ equals $=_A$.*

Proof. Let $\sim$ denote the congruence generated by $\xrightarrow{A}$.

In (28) set $b = 2$, $c(1) = c(2) = 1$. We get

$$x_{a-1}\, x_{a-2}\, x_{a-1}\, x_{a-2} \sim x_{a-2}\, x_{a-1}\, x_{a-2}.$$

Together with (21) these generate precisely $=_A$. This proves that $(x =_A y) \Rightarrow (x \sim y)$ for all $x, y \in F_n$. It remains to prove the converse.

Let x be the left-hand side in (28) and y the right-hand side. Let $P(b)$ denote the statement $x =_A y$ for all choices of the parameters different from b. We will be finished if we can prove $P(b)$ for all $b \geq 2$.

Let $a \in \{2, \ldots, n\}$. By induction on ℓ we shall prove

$$x_a\, x_{a-1}^{\ell}\, x_a\, x_{a-1} =_A x_{a-1}^{\ell}\, x_a\, x_{a-1} \tag{31}$$

for all $\ell \geq 1$. For $\ell = 1$ this is (22). In the following, something in curly brackets is next to be rewritten. Assuming it to be true for $\ell - 1$ we find

$$\begin{aligned}
& x_a \left\{x_{a-1}^{\ell}\right\} x_a\, x_{a-1} \\
&= x_a\, x_{a-1}^{\ell-1} \left\{x_{a-1}\, x_a\, x_{a-1}\right\} \\
&= \left\{x_a\, x_{a-1}^{\ell-1}\, x_a\, x_{a-1}\right\} x_a\, x_{a-1} && \text{by (22)} \\
&= x_{a-1}^{\ell-1} \left\{x_a\, x_{a-1}\, x_a\, x_{a-1}\right\} && \text{by the induction hypothesis} \\
&= \left\{x_{a-1}^{\ell-1}\, x_{a-1}\right\} x_a\, x_{a-1} && \text{by (22)} \\
&= x_{a-1}^{\ell}\, x_a\, x_{a-1}.
\end{aligned}$$

We have proved (31). Using (31) and an obvious induction on k we find

$$x_a^k\, x_{a-1}^{\ell}\, x_a\, x_{a-1} =_A x_{a-1}^{\ell}\, x_a\, x_{a-1}$$

for all $k \geq 1$ and $\ell \geq 1$. This says that $P(2)$ holds.

We prove $P(b)$ by induction on b. Assume $P(b-1)$ and $a-d=b$ and $r(i) \geq 1$ for all $i \in \{a-1, a-2, \dots, d\}$. We simplify notation by writing e instead of x_e. We find

$$\begin{aligned}
&(a-1)^{r(a-1)} \cdots d^{r(d)} \{(a,d]\} \\
&= (a-1)^{r(a-1)} \cdots (d+1)^{r(d+1)} \{d^{r(d)} (a, d+2]\} (d+2, d] \\
&=_A (a-1)^{r(a-1)} \cdots (d+1)^{r(d+1)} (a, d+2] \{d^{r(d)} (d+2, d]\} \\
&=_A (a-1)^{r(a-1)} \cdots (d+1)^{r(d+1)} \\
&\qquad\qquad \{(a, d+2] (d+1)\} d^{r(d)} (d+2, d] \quad \text{by (31)} \\
&= \{(a-1)^{r(a-1)} \cdots (d+1)^{r(d+1)} (a, d+1]\} d^{r(d)} (d+2, d] \\
&=_A (a-2)^{r(a-2)} \cdots (d+1)^{r(d+1)} \\
&\qquad \{(a, d+1]\}\, d^{r(d)} (d+2, d] \quad \text{by the induction hypothesis} \\
&= (a-2)^{r(a-2)} \cdots (d+1)^{r(d+1)} (a, d+2] \{(d+1)\, d^{r(d)} (d+2, d]\} \\
&=_A (a-2)^{r(a-2)} \cdots (d+1)^{r(d+1)} \{(a, d+2]\, d^{r(d)}\} (d+2, d] \quad \text{by (31)} \\
&=_A (a-2)^{r(a-2)} \cdots (d+1)^{r(d+1)}\, d^{r(d)} \{(a, d+2] (d+2, d]\} \\
&= (a-2)^{r(a-2)} \cdots (d+1)^{r(d+1)}\, d^{r(d)} (a, d].
\end{aligned}$$

This proves $P(b-1) \Rightarrow P(b)$ and the proof is complete. $\square$

Lemma 32. *The following is the complete list of triples (q, r, s) of nontrivial words such that qr and rs are A-standard.*

(a) *A triple (q, r, s) given by*

$$\begin{aligned}
q &= x_{a-1}^{r(a-1)} x_{a-2}^{r(a-2)} \cdots x_b^{r(b)} (x_a, x_c] \\
r &= (x_c, x_b] \\
s &= x_{b-1}^{s(b-1)} x_{b-2}^{s(b-2)} \cdots x_d^{s(d)} (x_c, x_d]
\end{aligned}$$

whenever

$$a \geq c > b \geq d, \qquad a-b \geq 2, \qquad c-d \geq 2$$

and $r(i) \geq 1$ for all $i \in \{a-1, a-2, \dots, b\}$ and $s(j) \geq 1$ for all $j \in \{b-1, b-2, \dots, d\}$.

(b) *A triple (q, r, s) given by*

$$\begin{aligned}
q &= x_c \\
r &= x_{a-1} \\
s &= [x_{a-1}^{r(1)-1} x_{a-2}^{r(2)} \cdots x_{a-b}^{r(b)}] (x_a, x_{a-b}]
\end{aligned}$$

whenever $r(i) \geq 1$ for all i and $b \geq 2$ and $c-a \geq 1$.

(c) *A triple* (q, r, s) *given by*

$$q = \left[x_{a-1}^{r(1)} x_{a-2}^{r(2)} \cdots x_{a-b}^{r(b)}\right](x_a, x_{a-b+1}]$$

$$r = x_{a-b}$$

$$s = x_c$$

whenever $r(i) \geq 1$ *for all* i *and* $b \geq 2$ *and* $a - b - c \geq 2$.

(d) *A triple* $(q, r, s) = (x_a, x_b, x_c)$ *where* $a - b \geq 2$ *and* $b - c \geq 2$.

Proof. This is obvious. □

Lemma 33. *Let* $u, v, w \in F_n$ *and assume* $u \xrightarrow{A} v$ *and* $u \xrightarrow{A} w$. *Then there exists* $x \in F_n$ *such that* $v \overset{A}{\twoheadrightarrow} x$ *and* $w \overset{A}{\twoheadrightarrow} x$.

$$\begin{tikzcd}
u \arrow[r, "A"'] \arrow[d, "A"'] & v \arrow[d, twoheadrightarrow, "A"] \\
w \arrow[r, twoheadrightarrow, "A"] & x
\end{tikzcd}$$

Proof. Throughout the proof we remove the index A from the arrows.

First suppose there is no overlap, that is,

- there are $p, q, r, s, t, q', s' \in F_n$ such that $u = pqrst$, $v = pq'rst$, $w = pqrs't$, $q \xrightarrow[0]{} q'$, $s \xrightarrow[0]{} s'$. (34)

Then $x := pq'rs't$ has the required properties.

$$\begin{tikzcd}
pqrst \arrow[r] \arrow[d] & pq'rst \arrow[d, twoheadrightarrow] \\
pqrs't \arrow[r, twoheadrightarrow] & pq'rs't
\end{tikzcd}$$

We are left to consider the case of overlap, that is, there are words p, q, r, s, t, v_0, w_0 such that

$$u = p\,q\,r\,s\,t \qquad q\,r \xrightarrow[0]{} v_0 \qquad r\,s \xrightarrow[0]{} w_0$$

$$r \neq 1 \qquad v = p\,v_0\,s\,t \qquad w = p\,q\,w_0\,t.$$

We may assume $v \neq w$. It follows that $q \neq 1$ and $s \neq 1$.

We may also assume $p = t = 1$.

The possible triples (q, r, s) have been listed in lemma 32. We shall deal with them one by one.

Suppose first that (q, r, s) is as in lemma 32(b). Then, not only can x_c (which is q) pass its neighbour x_{a-1} by a commutation move (27), but it can also go on to pass all remaining letters. This shows

$$v = v_0\,s \twoheadrightarrow r\,s\,q \longrightarrow w_0\,q.$$

Likewise, q can pass all letters in w_0 which shows

$$w = q\,w_0 \twoheadrightarrow w_0\,q.$$

We have shown that $x := w_0\,q$ has the required properties.

Cases (c) and (d) of lemma 32 are similar to case (b).

It remains to consider case (a) in lemma 32.

Write e instead of x_e. In the following, anything between curly brackets is to be rewritten next. On the one hand

$$\begin{aligned}
&\{qr\}s = \big\{(a-1)^{r(a-1)}\cdots b^{r(b)}(a,b]\big\}(b-1)^{s(b-1)}\cdots d^{s(d)}(c,d] \\
&\to (a-2)^{r(a-2)}\cdots b^{r(b)}(a,b](b-1)^{s(b-1)}\cdots d^{s(d)}(c,d] \\
&= (a-2)^{r(a-2)}\cdots b^{r(b)}(a,c]\big\{(c,b](b-1)^{s(b-1)}\cdots d^{s(d)}(c,d]\big\} \\
&\to (a-2)^{r(a-2)}\cdots b^{r(b)}\big\{(a,c](c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}\big\}(c,d] \\
&\twoheadrightarrow (a-2)^{r(a-2)}\cdots b^{r(b)}(c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,c](c,d] \\
&= (a-2)^{r(a-2)}\cdots(c-1)^{r(c-1)}\big\{(c-2)^{r(c-2)}\cdots b^{r(b)}(c-1,b]\big\} \\
&\cdot (b-1)^{s(b-1)}\cdots d^{s(d)}(a,d] =: z.
\end{aligned}$$

Here the last term is abbreviated z. On the other hand

$$\begin{aligned}
&q\{rs\} = (a-1)^{r(a-1)}\cdots b^{r(b)}(a,c]\big\{(c,b](b-1)^{s(b-1)}\cdots d^{s(d)}(c,d]\big\} \\
&\to (a-1)^{r(a-1)}\cdots b^{r(b)}\big\{(a,c](c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}\big\}(c,d] \\
&\twoheadrightarrow (a-1)^{r(a-1)}\cdots b^{r(b)}(c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,d] =: y.
\end{aligned}$$

If $c-b \geq 3$ then

$$\begin{aligned}
&z \to \big\{(a-2)^{r(a-2)}\cdots(c-1)^{r(c-1)}(c-3)^{r(c-3)}\cdots b^{r(b)}\big\} \\
&\cdot (c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,d] \twoheadrightarrow (c-3)^{r(c-3)}\cdots b^{r(b)} \\
&\cdot (a-2)^{r(a-2)}\cdots(c-1)^{r(c-1)}(c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,d]\,;
\end{aligned}$$

$$\begin{aligned}
&y = (a-1)^{r(a-1)}\cdots(c-1)^{r(c-1)}\big\{(c-2)^{r(c-2)}\cdots b^{r(b)}(c-1,b]\big\} \\
&\cdot (b-1)^{s(b-1)}\cdots d^{s(d)}(a,d] \to \big\{(a-1)^{r(a-1)}\cdots(c-1)^{r(c-1)} \\
&\cdot (c-3)^{r(c-3)}\cdots b^{r(b)}\big\}(c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,d] \\
&\twoheadrightarrow (c-3)^{r(c-3)}\cdots b^{r(b)} \\
&\big\{(a-1)^{r(a-1)}\cdots(c-1)^{r(c-1)}(c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,d]\big\} \\
&\to (c-3)^{r(c-3)}\cdots b^{r(b)} \\
&(a-2)^{r(a-2)}\cdots(c-1)^{r(c-1)}(c-1,b](b-1)^{s(b-1)}\cdots d^{s(d)}(a,d].
\end{aligned}$$

If $c-b = 2$ then

$$\begin{aligned}
&y = \big\{(a-1)^{r(a-1)}\cdots(b+1)^{r(b+1)}b^{r(b)+1}(b-1)^{s(b-1)}\cdots d^{s(d)}(a,d]\big\} \\
&\to (a-2)^{r(a-2)}\cdots(b+1)^{r(b+1)}b^{r(b)+1}(b-1)^{s(b-1)}\cdots d^{s(d)}(a,d] = z.
\end{aligned}$$

If $c - b = 1$ then

$$\begin{aligned} y &= \{(a-1)^{r(a-1)} \cdots b^{r(b)} (b-1)^{s(b-1)} \cdots d^{s(d)} (a,d]\} \\ &\to (a-2)^{r(a-2)} \cdots b^{r(b)} (b-1)^{s(b-1)} \cdots d^{s(d)} (a,d] = z. \end{aligned}$$

This proves the promised result in case (a) of lemma 32. The proof is complete. □

Definition 35.

(a) A word $u \in F_n$ is said to be *A-reduced* if there is no v satisfying $u \xrightarrow{A} v$.

(b) Let $x, y \in F_n$. We say that x is the *A-reduced form* of y if x is A-reduced and $x =_A y$.

Theorem 36. *Every $=_A$-class in F_n contains a unique A-reduced word.*

Proof. In lemma 23 (the diamond lemma) put $S := F_n$, $(\to) := (\xrightarrow{A})$. Then $\sim$ (as defined in the diamond lemma) equals $=_A$ by lemma 30.

Note that $u \to v$ implies $\ell(u) > \ell(v)$. Therefore there are no infinite chains $u_1 \to u_2 \to \cdots$. Confluence (25) is satisfied by lemma 33. This shows that the assumptions of the diamond lemma are satisfied. The result follows by the diamond lemma. □

Corollary 37. *Consider the AI monoid $A := (F_n/{=_A})$.*

(a) *There is a polynomial algorithm computing the A-reduced form for a word.*

(b) *There is a polynomial solution to the word problem in A.*

Proof. (a). Let $u_1 \in F_n$ be the input to our algorithm. The algorithm calculates words $u_2, u_3, \ldots, u_n$ such that

$$u_i \xrightarrow{A} u_{i+1}$$

for all i, and u_n is A-reduced. It is easy to show that each step can be carried out in polynomial time. For all i we have $\ell(u_i) > \ell(u_{i+1})$ so after polynomial time the process terminates, as promised, at some A-reduced word u_n. The result follows.

(b). This follows immediately from (a) and the fact that every element of A is represented by a unique A-reduced word (theorem 36). □

It would be interesting to know if the methods of this section apply to the better-known positive braid monoid.

10 A_n is left-cancellative

Lemma 38. *Let $x \in F_n$ be such that x is A-standard of length > 2, that is, x is the left-hand side of (28). Let $y \in F_n$ be B-equivalent to x. Then x has the same first letter as y, that is, $x = x_a\, u$ and $y = x_a\, v$ for some a, u, v.*

Proof. This is clear. ☐

Let us call a word *B-reduced* if it is not of the form $u\,x_a\,x_b\,v$ with $u, v \in F_n$ and $a - b \geq 2$. Clearly, every element of F_n is B-equivalent to a unique B-reduced word called its *B-reduced form.*

Proposition 39. *The AI monoid A_n is left-cancellative, that is, if $x, y, z \in F_n$ are such that $xy =_A xz$ then $y =_A z$.*

Proof. Recall that F_n is the free monoid on $X = \{x_1, \ldots, x_n\}$. We may assume $x \in X$.

We may also assume that y, z are A-reduced, because otherwise we replace them by their A-reduced forms.

Note that A-reduced words are B-reduced. What does the B-reduced form of xy look like? A moment's thought about this question shows that there are words a, b such that $y = ab$ and the B-reduced form of xab is axb and such that

- $ax =_B xa.$ (40)
- The letter x doesn't appear in a. (41)

Likewise there are words c, d such that $z = cd$ and the B-reduced form of xcd is cxd and such that

- $cx =_B xc.$ (42)
- The letter x doesn't appear in c. (43)

We shall prove that for all $k \geq 1$:

- If axb is A-reduced then the A-reduced form of $x^k y$ is $ax^k b$. (44)
- If axb is not A-reduced then the A-reduced form of $x^k y$ is ab. (45)

Indeed (44) is immediate. To prove (45), assume axb is not A-reduced. Then there are words $a_1, a_2, b_1, b_2 \in F_n$ such that $a = a_1\,a_2$, $b = b_1\,b_2$ and $a_2\,x\,b_1$ is A-standard. Using lemma 38 and (40) and (41) it follows that $a_2 = 1$. From (28) it now follows that

$$xb_1 \xrightarrow{A} b_1.$$

Since $\xrightarrow{A}$ generates $=_A$ as congruence by lemma 30, we have $xb =_A b$. An obvious induction shows $x^k b =_A b$ and hence $x^k y =_A ax^k b =_A ab$. But ab is A-reduced, and we have proved (45).

Comparison of (44)–(45) with the analogous statement for (y, c, d) instead of (x, a, b) (in fact the range $k \in \{1, 2\}$ is enough) proves that either both axb and cxd are A-reduced, or neither is.

Assume now that axb and cxd are both A-reduced. But $axb =_A xy =_A xz =_A cxd$ and an A-class doesn't contain more than one A-reduced word by theorem 36. Therefore $axb = cxd$. Also the letter x doesn't appear in a or c by (41) and (43). It follows that $a = c$ and $b = d$ and $y = ab = cd = z$. This proves the result if both axb and cxd are A-reduced.

Assume finally that axb and cxd are not A-reduced. By (45), y is the A-reduced form of xy. Likewise z is the A-reduced form of xz. But $xy =_A xz$ so theorem 36 yields $y = z$. This settles the case where neither axb nor cxd is A-reduced. The proof is complete. □

11 A Garside element in A_n

Definition 46. A *Garside element* in a monoid N is an element $\Delta \in N$ such that:

- ◦ For all $x \in N$ there exist $k \geq 0$ and $y \in N$ such that $xy = \Delta^k$.
- ◦ There exists an endomorphism ϕ of N such that $x\Delta = \Delta\phi(x)$ for all $x \in N$.

In this section we shall prove that the AI monoid $A_n = (F_n/{=_A})$ has a Garside element.

Definition 47. We define the elements

$$\begin{aligned} Y_n &:= (x_3, x_1] \cdots (x_{n+1}, x_1] \\ \nabla_n &:= x_1\, Y_n = (x_2, x_1](x_3, x_1] \cdots (x_{n+1}, x_1] \end{aligned}$$

of F_n and $\Delta_n = [\nabla_n]_A \in A_n$.

We consider F_{i-1} as a submonoid of F_i, for all i. Then $\nabla_a \in F_n$ whenever $1 \leq a \leq n$. Also $\nabla_n = \nabla_{n-1}(x_{n+1}, x_1]$.

Lemma 48. *We have $x_a\, \nabla_n =_A \nabla_n$ for all $a \in \{2, \ldots, n\}$.*

Proof. Induction on n. For $n = 1$ there is nothing to prove. Assume it is true for $n - 1$. For $2 \leq a \leq n - 1$ the induction hypothesis implies

$$x_a\, \nabla_n =_A x_a\, \nabla_{n-1}(x_{n+1}, x_1] =_A \nabla_{n-1}(x_{n+1}, x_1] =_A \nabla_n$$

thus proving the induction step whenever $2 \leq a \leq n - 1$. It remains to prove the same for $a = n$. Well,

$$\begin{aligned} x_n\{\nabla_n\} &=_A \{x_n \nabla_{n-2}\}(x_n, x_1](x_{n+1}, x_1] \\ &=_A \nabla_{n-2}\{x_n(x_n, x_1](x_{n+1}, x_1]\} \\ &=_A \{\nabla_{n-2}(x_n, x_1](x_{n+1}, x_1]\} \qquad \text{by (28) and lemma 30} \\ &=_A \nabla_n. \end{aligned}$$

This proves the induction step and thereby the lemma. □

Lemma 49. *We have $x_a\, x_1^r\, \nabla_n =_A x_1^r\, \nabla_n$ whenever $2 \leq a \leq n$ and $0 \leq r$.*

Proof. If $a = 2$ then

$$\begin{aligned} & x_a\, x_1^r\{\nabla_n\} \\ & =_A \{x_2\, x_1^r\, x_1\, x_2\, x_1\}\, (x_4, x_1] \cdots (x_{n+1}, x_1] \end{aligned}$$

$$
\begin{aligned}
&=_A x_1^r\{x_1\,x_2\,x_1\,(x_4,x_1]\cdots(x_{n+1},x_1]\} && \text{by (28) and lemma 30}\\
&=_A x_1^r\nabla_n.
\end{aligned}
$$

If $a \geq 3$ then

$$
\begin{aligned}
\{x_a\,x_1^r\}\nabla_n &=_A x_1^r\{x_a\,\nabla_n\}\\
&=_A x_1^r\,\nabla_n && \text{by lemma 48.} \qquad \square
\end{aligned}
$$

Definition 50. Let $\pi\colon F_n \to F_1$ be the homomorphism defined by $\pi(x_1) = x_1$ and $\pi(x_a) = 1$ for all $a > 1$.

Lemma 51. *For all $x \in F_n$ we have $x\,\nabla_n =_A \pi(x)\,\nabla_n$.*

Proof. For $x \in F_n$, let $k(x) := \ell(x) - \ell(\pi x)$. This is the number of letters in x different from x_1. Let $P(n)$ be the statement that the lemma holds whenever $k(x) \leq n$. Then $P(1)$ holds by lemma 49.

We prove $P(n)$ by induction on n. Assume $P(n-1)$ and let $k(x) = n$. Then we can write $x = yz$ such that $k(y)$ and $k(z)$ are both less than n. Then also $k(y\,\pi(z)) = k(y) < n$. Using the induction hypothesis we find

$$
\begin{aligned}
x\,\nabla_n &=_A y(z\,\nabla_n) =_A (y\,\pi(z))\nabla_n\\
&=_A \pi(y\,\pi(z))\nabla_n =_A \pi(yz)\nabla_n =_A \pi(x)\nabla_n. \qquad \square
\end{aligned}
$$

Lemma 52. *Let $x \in F_n$. Then there exist $k \geq 0$ and $y \in F_n$ with $xy =_A \nabla_n^k$.*

Proof. We may assume $n > 0$. Then $\pi(\nabla_n) \neq 1$. Therefore there are $z \in F_n$ and ℓ such that $\pi(xz) = \pi(\nabla_n^\ell)$. By lemma 51 then

$$
xz\nabla_n =_A \pi(xz)\nabla_n =_A \pi(\nabla_n^\ell)\nabla_n =_A \nabla_n^{\ell+1}. \qquad \square
$$

Definition 53. We define an endomorphism $\lambda_n\colon F_n \to F_n$ by $\lambda_n(x_a) = 1$ for all $a \in \{2,\dots,n\}$ and $\lambda_n(x_1) = (x_{n+1},x_n]$.

Lemma 54. *For all $x \in F_n$ we have $x\,\nabla_n =_A \nabla_n\,\lambda_n(x)$.*

Proof. It is clear that we only need to prove this for $\ell(x) = 1$. If $x = x_a$ with $a > 1$ it follows from lemma 48. It remains to prove it for $x = x_1$ in which case it states

$$
x_1\,\nabla_n =_A \nabla_n\,(x_{n+1},x_n].
$$

We prove this by induction on n. For $n = 1$ this is clearly true. Assume it to hold for $n-1$. Then

$$
\begin{aligned}
&\nabla_n\,(x_{n+1},x_n] =_A \nabla_{n-1}\,(x_{n+1},x_n]^2\\
&=_A \nabla_{n-1}\,(x_n,x_n](x_{n+1},x_n] && \text{by (28) and lemma 30}\\
&=_A x_1\,\nabla_{n-1}\,(x_{n+1},x_n] && \text{by the induction hypothesis}\\
&=_A x_1\,\nabla_n.
\end{aligned}
$$

This proves the induction step and thereby the lemma. $\square$

Lemma 55. *If $x, y \in F_n$ are such that $x =_A y$ then $\lambda_n(x) =_A \lambda_n(y)$.*

Proof. It is enough to prove this if (x, y) is a generator of the congruence $=_A$, that is, x is the left-hand side in (a) or (b) of definition 20 and y the right-hand side. The result is now a simple observation. □

Lemma 55 implies that there exists a unique endomorphism ϕ_n of $A_n = (F_n/{=_A})$ such that $\phi_n([x]_A) = [\lambda_n(x)]_A$ for all $x \in F_n$.

Proposition 56. *The element Δ_n is a Garside element in A_n, with ϕ_n playing the role of ϕ in definition* 46.

Proof. This is the content of lemmas 52 and 54. □

We finish with a conjecture.

For $x, y \in A_n$ write $x \leq y$ if and only $y \in xA_n$. This is called the ordering of left division. Note that it is an ordering because A_n is left-cancellative by proposition 39.

Conjecture 57.

(a) *The ordered set $(A_n, \leq)$ is a lattice.*

(b) *Let p_a denote the image of x_a in A_n. Let $x \in A_n$. Then $x \leq \Delta_n$ if and only if there exist $z_a \in \langle p_2, p_3, \ldots, p_n \rangle$ for all $a \in \{1, \ldots, n\}$ such that*

$$x = z_n\,(p_1 \cdots p_n)\,z_{n-1}\,(p_1 \cdots p_{n-1}) \cdots z_2\,(p_1\,p_2)\,z_1\,p_1.$$

A *lower semi-lattice* is an ordered set such that any two elements have a meet.

A weak left-Garside monoid is a monoid with a Garside element and such that the ordering of left-division is a lower semi-lattice. Thus conjecture 57(a) implies that A_n is a weak left-Garside monoid. The adjective *weak* means to remind us that there may be infinitely many left-divisors of Δ, as is the case for A_n.

12 A rewriting system for M_n

Recall the MI monoid $M = M_n = (F_n/{=_M})$ of CI graph (19). We aim to solve the word problem in this monoid.

Definition 58. Let $\xrightarrow[0]{M}$ be the least relation on F_n such that the following hold.

(a) $x_a\,x_b \xrightarrow[0]{M} x_b\,x_a$ whenever $a - b \geq 2$.

(b) $(x_a, x_b](x_a, x_b] \xrightarrow[0]{M} (x_{a-1}, x_b](x_a, x_b]$ whenever $a - b \geq 1$. In particular, for $a = b$, we have

$$x_b\,x_b \xrightarrow[0]{M} x_b.$$

(c) Let $1 \leq a \leq b \leq n$. For $i \in \{a+1, \ldots, b\}$ let y_i be an element of the submonoid $\langle x_{i+1}, x_{i+2}, \ldots, x_n \rangle$ of F_n and $z_i \in \langle x_1, \ldots, x_{i-2} \rangle$. Then we have a rewrite rule

$$\begin{aligned} & x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b) x_b \\ \xrightarrow[0]{M} \; & x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b). \end{aligned} \tag{59}$$

In particular, for $a = b$, we have (again)

$$x_a\, x_a \xrightarrow[0]{M} x_a.$$

If $u \xrightarrow[0]{M} v$ then we call u an M-standard word.

Note that if $u \xrightarrow[0]{M} v$ and $u \xrightarrow[0]{M} w$ then $v = w$. Also, if u and xuy are M-standard ($u, x, y \in F_n$) then $x = y = 1$. As in the case of A_n we define the following.

Definition 60.

(a) Let $\xrightarrow{M}$ be the least relation on F_n containing $\xrightarrow[0]{M}$ and such that

$$(u \xrightarrow{M} v) \Rightarrow (xuy \xrightarrow{M} xvy)$$

for all $u, v, x, y \in F_n$.

(b) We define $\xrightarrow{M}\!\!\!\!\rightarrow$ to be the least transitive relation on F_n containing $\xrightarrow{M}$.

Lemma 61. *The congruence on F_n generated by $\xrightarrow{M}$ equals $=_M$.*

Proof. Let $\sim$ denote the congruence on F_n generated by $\xrightarrow{M}$. Let $x, y \in F_n$. We must prove

$$(x \sim y) \Leftrightarrow (x =_M y).$$

The implication $\Leftarrow$ is trivial. In order to prove $\Rightarrow$ we may assume $x \xrightarrow[0]{M} y$.

If $(x, y) = (x_a\, x_b, x_b\, x_a)$ as in part (a) of definition 58 then $x =_M y$ is clearly true.

Assume next $x = (x_a, x_b](x_a, x_b]$, $y = (x_{a-1}, x_b](x_a, x_b]$ as in part (b) of definition 58. Then $x \xrightarrow[0]{A} y$ by (28) so $x =_A y$ by lemma 30 so $x =_M y$.

Suppose finally that x is the left-hand side in (59) and y the right-hand side. Note first that the $=_B$-class (commutation class) of x and y doesn't change if we move the y_i all the way to the left and the z_j all the way to the right. Thus we may assume the y_i and z_j to be trivial as we now do.

Let ρ denote the anti-automorphism of F_n defined by $\rho(x_a) = x_a$ for all a. By lemma 8 ρ preserves $=_M$. Therefore we need only prove $\rho(x) =_M \rho(y)$.

Let u be the B-reduced form of $\rho(x)$ and v the B-reduced form of $\rho(y)$. Then $u = (x_b, x_a](x_b, x_a]$ and $v = (x_{b-1}, x_a](x_b, x_a]$. This is precisely a case we've already dealt with. It follows that $u =_M v$ whence $x =_M y$. The proof is finished. ☐

Lemma 62. *The following is the complete list of triples (q, r, s) of nontrivial words such that qr and rs are M-standard.*

(a) (x_a, x_b, x_c) *whenever* $a - b \geq 2$, $b - c \geq 2$.

(b) $\big(x_a, x_{b-1}, (x_{b-1}, x_c](x_b, x_c]\big)$ *whenever* $a - b \geq 1$, $b - c \geq 1$.

(c) $\big((x_a, x_b](x_a, x_{b+1}], x_b, x_c\big)$ *whenever* $a - b \geq 1$, $b - c \geq 2$.

(d) $\big(x_c, x_a, (y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b)x_b\big)$ *whenever* $c - a \geq 2$ *and the notation of* (c) *holds.*

(e) $\big(x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b), x_b, x_c\big)$ *whenever* $b - c \geq 2$ *and the notation of* (c) *holds.*

(f) $\big((x_a, x_b](x_a, x_c], (x_c, x_b], (x_b, x_d](x_c, x_d]\big)$ *whenever* $a \geq c > b \geq d$.

(g) $\big((x_c, x_a](x_c, x_{a+1}], x_a, (y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b)x_b\big)$ *whenever* $c - a \geq 1$ *and the notation of* (c) *holds.*

(h) $\big(x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b), x_b, (x_b, x_c](x_{b+1}, x_c]\big)$ *whenever* $b - c \geq 0$ *and the notation of* (c) *holds.*

(i) *Let* $1 \leq a < b < c \leq n$. *For* $i \in \{a+1, \ldots, c\}$ *let* y_i *be an element of the submonoid* $\langle x_{i+1}, x_{i+2}, \ldots, x_n\rangle$ *of* F_n *and* z_i *an element of* $\langle x_1, \ldots, x_{i-2}\rangle$. *Then we have a triple* (q, r, s) *with*

$$\begin{aligned} q &= x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b) \\ r &= x_b \\ s &= (y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c)x_c. \end{aligned}$$

(j) *Let* $1 \leq a < b \leq c \leq n$. *For* $i \in \{a+1, \ldots, c\}$ *let* y_i *be an element of the submonoid of* $\langle x_{i+1}, x_{i+2}, \ldots, x_n\rangle$ *and* z_i *an element of* $\langle x_1, \ldots, x_{i-2}\rangle$. *Then we have a triple* (q, r, s) *with*

$$\begin{aligned} q &= x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_{b-1}\, x_{b-1}\, x_{b-2}\, z_{b-1})y_b\, x_b \\ r &= x_{b-1}\, x_b \\ s &= x_{b-1}\, z_b(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c)x_c. \end{aligned}$$

Proof. This is easy. ☐

Lemma 63. *Let* $u, v, w \in F_n$ *and assume* $u \xrightarrow{M} v$ *and* $u \xrightarrow{M} w$. *Then there exists* $x \in F_n$ *such that* $v \overset{M}{\twoheadrightarrow} x$ *and* $w \overset{M}{\twoheadrightarrow} x$.

Proof. Throughout the proof we remove the index M from the arrows.

If there is overlap (34) this is proved the same way as in lemma 33. We are left to consider the case of overlap, that is, there are words p, q, r, s, t,

v_0, w_0 such that

$$\begin{array}{lll} u = p\,q\,r\,s\,t & q\,r \xrightarrow[0]{} v_0 & r\,s \xrightarrow[0]{} w_0 \\ r \neq 1 & v = p\,v_0\,s\,t & w = p\,q\,w_0\,t. \end{array}$$

We may assume $v \neq w$. It follows that $q \neq 1$ and $s \neq 1$.

We may also assume $p = t = 1$.

The possible triples (q, r, s) have been listed in lemma 62. We shall deal with them one by one.

Cases (a)–(e). In these cases the lemma is readily seen to hold.

Case (f). In case (f) we write a instead of x_a. On the one hand we have

$$\begin{aligned} &\{qr\}s = \big\{(a,b](a,c](c,b]\big\}(b,d](c,d] = \big\{(a,b](a,b]\big\}(b,d](c,d] \\ &\to (a-1,b](a,b](b,d](c,d] = (a-1,b](a,c]\big\{(c,d](c,d]\big\} \\ &\to (a-1,b]\big\{(a,c](c-1,d]\big\}(c,d] \twoheadrightarrow (a-1,b](c-1,d](a,c](c,d] \\ &= (a-1,c-1](c-1,b](c-1,b](b,d](a,d] =: y. \end{aligned}$$

On the other hand

$$\begin{aligned} &q\{rs\} = (a,b](a,c]\big\{(c,b](b,d](c,d]\big\} = (a,b](a,c]\big\{(c,d](c,d]\big\} \\ &\to (a,b]\big\{(a,c](c-1,d]\big\}(c,d] \twoheadrightarrow (a,b](c-1,d](a,c](c,d] \\ &= (a,b](c-1,d](a,d] =: z. \end{aligned}$$

If $c - b \geq 2$ then

$$\begin{aligned} &y \to (a-1,c-1](c-2,b](c-1,b](b,d](a,d] \\ &= \big\{(a-1,c-1](c-2,b]\big\}(c-1,d](a,d] \\ &\twoheadrightarrow (c-2,b](a-1,c-1](c-1,d](a,d] = (c-2,b](a-1,d](a,d]\,; \end{aligned}$$

$$\begin{aligned} &z = (a,c-1]\big\{(c-1,b](c-1,b]\big\}(b,d](a,d] \\ &\to \big\{(a,c-1](c-2,b]\big\}(c-1,b](b,d](a,d] \\ &\twoheadrightarrow (c-2,b]\big\{(a,c-1](c-1,b](b,d]\big\}(a,d] \\ &= (c-2,b]\big\{(a,d](a,d]\big\} \to (c-2,b](a-1,d](a,d]. \end{aligned}$$

If $c - b = 1$ then

$$z = (a,d](a,d] \to (a-1,d](a,d] = y.$$

Chaining and comparing the above results proves the lemma in case (f).

Case (g). This case the overlap is untouched, that is, there are words $v_1, w_1 \in F_n$ such that $v = v_1\,r\,s$, $w = q\,r\,w_1$. Then $x := v_1\,r\,w_1$ has the required properties.

Case (h). In this case $v = w$ so $x := v$ has the required properties.

Case (i). On the one hand we have

$$\begin{aligned}
&\{qr\}s \longrightarrow qs = \big\{x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c) x_c\big\} \\
&\longrightarrow x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c).
\end{aligned}$$

On the other hand

$$\begin{aligned}
&q\{rs\} \longrightarrow \big\{x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b)\, x_b\big\} \\
&(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c) \\
&\longrightarrow x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_b\, x_b\, x_{b-1}\, z_b) \\
&(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c) \\
&= x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c).
\end{aligned}$$

The result follows.

Case (j). On the one hand

$$\begin{aligned}
&\{qr\}s \longrightarrow q\, x_{b-1}\, s = x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_{b-1}\, x_{b-1}\, x_{b-2}\, z_{b-1}) \\
&y_b\, x_b\big\{x_{b-1}\, x_{b-1}\big\} z_b(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c)\, x_c \\
&\longrightarrow x_a(y_1\, x_{a+1}\, x_a\, z_1) \cdots (y_{b-1}\, x_{b-1}\, x_{b-2}\, z_{b-1})\, y_b\, x_b\, x_{b-1}\, z_b \\
&(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c)\, x_c \\
&= \big\{x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c)\, x_c\big\} \\
&\longrightarrow x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c).
\end{aligned}$$

On the other hand

$$\begin{aligned}
&q\{rs\} \longrightarrow \big\{x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_{b-1}\, x_{b-1}\, x_{b-2}\, z_{b-1}) \\
&y_b\, x_b\, x_{b-1}\, x_b\big\}\, x_{b-1}\, z_b(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c) \\
&\longrightarrow x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_{b-1}\, x_{b-1}\, x_{b-2}\, z_{b-1})\, y_b\, x_b \\
&\big\{x_{b-1}\, x_{b-1}\big\} z_b(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c) \\
&\longrightarrow x_a(y_{a+1}\, x_{a+1}\, x_a\, z_{a+1}) \cdots (y_{b-1}\, x_{b-1}\, x_{b-2}\, z_{b-1}) \\
&y_b\, x_b\, x_{b-1}\, z_b(y_{b+1}\, x_{b+1}\, x_b\, z_{b+1}) \cdots (y_c\, x_c\, x_{c-1}\, z_c) \\
&= x_a(y_1\, x_{a+1}\, x_a\, z_1) \cdots (y_c\, x_c\, x_{c-1}\, z_c).
\end{aligned}$$

This settles case (j). The lemma is proved. □

Definition 64.

(a) A word $u \in F_n$ is said to be *M-reduced* if there is no v satisfying $u \xrightarrow{M} v$.

(b) Let $x, y \in F_n$. We say that x is the *M-reduced form* of y if x is M-reduced and $x =_M y$.

Theorem 65. *Every $=_M$-class in F_n contains a unique M-reduced word.*

Proof. The proof is the same as for theorem 36. This time the ingredients are lemmas 61, 63 and 23. □

Corollary 66. *Consider the CI monoid* $M := (F_n/{=_M})$.

(a) *There is a polynomial algorithm computing the M-reduced form for a word.*

(b) *There is a polynomial solution to the word problem in M.*

Proof. The proof is the same as for corollary 37. ☐

A *sink* in a monoid N is an element 0 such that $x0y = 0$ for all $x, y \in N$.

It is known that a Coxeter monoid is finite if and only if it has a sink. This is false for CI monoids as our next and last two results show.

Proposition 67. *Let* $w_0 \in M_n$ *be the image of* ∇_n. *Then* $x\, w_0\, y = w_0$ *for all* $x, y \in M_n$.

Proof. Recall $m_a = [x_a]_M \in M_n$. By lemma 48 we have $m_a\, w_0 = w_0$ if $a \geq 2$. Also $m_1^2 = m_1$ and $w_0 \in m_1\, M_n$ so $m_1\, w_0 = w_0$ as well. Since M_n is generated by $\{m_1, \dots, m_n\}$, we find

$$x\, w_0 = w_0 \text{ for all } x \in M_n. \tag{68}$$

By lemma 8 there exists a unique anti-automorphism ϕ of M_n preserving m_a for all a. Note that $\phi(w_0) = w_0$. Applying ϕ to both sides of (68) we find $w_0\, y = w_0$ for all $y \in M_n$. The result follows. ☐

Proposition 67 was earlier proved in [He, proposition 2.3.14] and [D2].

Proposition 69. M_n *is infinite if* $n \geq 3$.

Proof. Note that $(x_2\, x_1\, x_2\, x_3)^k$ is M-reduced for all $k \geq 0$. By theorem 65(a), they represent distinct elements of M_n. ☐

References

[C] P.M. Cohn; Further algebra and applications. Springer–Verlag London, London, 2003.

[D1] Patrick Dehornoy; Braids and Self-Distributivity. Birkhäuser Verlag, Basel, 2000.

[D2] Dehornoy; Digne; Godelle; Michel; Garside Theory. Work in progress, 2012.

[He] Alexander Hess; Factorable Monoids: Resolutions and Homology via Discrete Morse Theory. Thesis, Bonn, 2012.

[Hu] James E. Humphreys; Reflection groups and Coxeter groups. Cambridge University Press, Cambridge, 1990.

[O] Viktoriya Ozornova; Factorability, Discrete Morse Theory and a Reformulation of $K(\pi, 1)$-conjecture. Thesis, Bonn, 2012.