HECKE ALGEBRAS FOR SET-THEORETICAL SOLUTIONS TO THE YANG–BAXTER EQUATION

EDOUARD FEINGESICHT

Abstract. We define a concept of Hecke algebra for structure groups of set-theoretical solutions to the Yang–Baxter equation. As a comparison to Artin–Tits groups of spherical type, we study some properties of this construction, while also highlighting some differences that appear, which shows a difference between finite Coxeter groups and the "Coxeter-like" group introduced by Dehornoy. We also relate this definition to known constructions on solutions (retractions). Finally, we study a particular case related to Torus Knot groups and Complex Reflexion groups.

Introduction

The study of involutive non-degenerate set-theoretical solutions to the Yang–Baxter equation ([13, 14]) involves many different algebraic structures: cycle sets ([26]), braces ([4]), I-structures ([16]), etc. The structure group of a solution ([14]), was shown to be a Garside group by Chouraqui ([6]). In [10], Dehornoy constructed a finite quotient of the structure group, which plays a role similar to finite Coxeter groups for Artin–Tits groups of spherical type ([2]). The construction of this finite quotient involves the existence of a positive integer associated to each solution, usually denoted d and which we call Dehornoy's class. In this article, we are interested in this finite "Coxeter-like" group, with the aim to understand both how it is similar and how it differs from finite Coxeter groups.

For an Artin–Tits group of spherical type A generated by S and with Coxeter group W, the generic Iwahori–Hecke algebra can be defined as a quotient of the group ring $\mathbb{Z}[q^{\pm 1}][A]$ by the relations $s^2 = (q-1)s + q$ for all s in S. This algebra has numerous interesting properties: it has dimension $|W|$, the generators are invertible, it is semi-simple under a suitable extension, etc. ([2, 17]). Here, we develop a theory of Hecke algebra for structure group of involutive non-degenerate set-theoretical solutions to the Yang–Baxter equation. We show that this algebra satisfies properties similar to the ones of Iwahori–Hecke algebras of Artin–Tits groups of spherical type, while also highlighting how and why the definition differs. To do so, we will rely on the fact that the structure group of a solution is a brace ([27, 4]), which in particular means that there exists an abelian structure on the structure group G such that $(G,+) \cong (\mathbb{Z}^X, +)$, and we denote by $x^{[k]}$ the element corresponding to $x + \cdots + x$ in $\mathbb{Z}^X$. We summarize our results from each section in the following:

Theorem. *Let (X, r) be an involutive non-degenerate set-theoretical solution to the Yang–Baxter equation of size n and Dehornoy's class d. Denote G the structure group of (X, r) and $\overline{G}_2 = G/\langle x^{[2d]}\rangle_{x\in X}$ its germ associated to $2d$ (two times Dehornoy's class). For any integral domain R, define the following $R[q^{\pm 1}]$-algebra:*

$$\mathcal{H} = R[q^{\pm 1}][G] \Big/ \left\langle \left(x^{[d]}\right)^2 = (q-1)\cdot x^{[d]} + q, \forall x \in X \right\rangle.$$

2020 *Mathematics Subject Classification.* 16T25, 20N02, 20C08.

Key words and phrases. Yang–Baxter equation, Hecke algebra, Cycle set, Brace.

Then the followings hold:

- *(Theorem 2.8)* $\mathcal{H}$ *is a free* $R[q^{\pm 1}]$*-module with basis indexed by* $\overline{G}_2$*. In particular,* $\mathcal{H}$ *has rank* $(2d)^n$*.*
- *(Corollary 3.4) If* T_g *denotes the generator of* $\mathcal{H}$ *associated to an element* g *of* $\overline{G}_2$*, then* T_g *is invertible.*
- *(Theorem 3.5) The anti-involution* $R[q^{\pm 1}] \to R[q^{\pm 1}]$ *that sends* q *to* q^{-1} *extends to a well-defined anti-involution of* $\mathcal{H}$ *that sends* T_g *to* T_g^{-1} *for any* $g \in \overline{G}_2$*.*
- *(Corollary 4.11) If* $R = \mathbb{C}$ *then* $\mathbb{C}(q) \otimes \mathcal{H}$ *is semi-simple, and there is bijection between the irreducible characters of* $\mathbb{C}(q) \otimes \mathcal{H}$ *and the irreducible characters of* $\mathbb{C}[\overline{G}_2]$*.*

In this explicit version of our results, we chose the polynomial $P(X) = X^2-(q-1)X-q$ to remind of the generic Iwahori–Hecke algebra of Coxeter groups, but our results hold for any polynomial whose leading and constant coefficients are invertible.

In the first section we introduce the necessary definitions on braces that we will need.

In the second section the define of the Hecke algebra is introduced and we show it has the expected dimension (equal to the cardinal of a Coxeter-like group).

In the third section, we explicitly construct an anti-involution on the Hecke algebras, as is known for the case Iwahori–Hecke algebra for Coxeter groups.

In the fourth section, we provide an application of Tits' Deformation Theorem, relating Hecke algebras and group rings of Coxeter-like groups over a suitable field extension.

Finally, in the fifth section, we focus on a particular example where the naive definition does work, and relate it to known results about Complex Reflection Groups (a generalization of finite Coxeter groups).

Moreover, in Appendix A, we explain how our definition of the Hecke algebra arises, and why, in general, the naive definition (adapting the definition for Artin–Tits groups of spherical type) doesn't provide the expected properties.

1. Preliminaries

The goal of this section is to provide the basic definitions of the approaches used in this article: cycle sets ([26]) and braces ([4]). We also give several technical lemmas that will be used in the construction and the study of the Hecke algebras.

1.1. Cycle sets

Our basis object to study non-degenerate involutive set-theoretical solutions to the Yang–Baxter equation are cycle sets, which were introduced by Rump ([26]).

Definition 1.1 ([26])**.** *A cycle set is a set* S *endowed with a binary operation* $*\colon S\times S \to S$ *such that for all* s *in* S *the map* $\psi(s)\colon t \mapsto s*t$ *is bijective and for all* s,t,u *in* S*:*

$$(s*t)*(s*u) = (t*s)*(t*u). \tag{1}$$

When S *is finite of size* n*,* $\psi(s)$ *can be identified with a permutation in* $\mathfrak{S}_n$*.*

When the diagonal map is the identity (i.e. for all $s \in S$*,* $s*s = s$*),* S *is called square-free.*

From now, we fix a cycle set $(S,*)$.

Definition 1.2 ([26])**.** *The group* G_S *associated with* S *is defined by the presentation:*

$$G_S \coloneqq \langle S \mid s(s*t) = t(t*s),\ \forall s \neq t \in S\rangle\,. \tag{2}$$

Similarly, we define the associated monoid M_S by the presentation:

$$M_S \coloneqq \langle S \mid s(s*t) = t(t*s),\ \forall s \neq t \in S\rangle^+ .$$

They will be called the structure group (resp. monoid) of S.

Example 1.3. *Let $S = \{s_1, \dots, s_n\}$, $\sigma = (12\dots n) \in \mathfrak{S}_n$. The operation $s_i * s_j = s_{\sigma(j)}$ makes S into a cycle set, as for all s, t in S we have $(s*t)*(s*s_j) = s_{\sigma^2(j)} = (t*s)*(t*s_j)$.*

The structure group of S then has generators $s_1, \dots, s_n$ and relations $s_i s_{\sigma(j)} = s_j s_{\sigma(i)}$ (which is trivial for $i = j$).

In particular, for $n = 2$ we find $G = \langle s, t \mid s^2 = t^2\rangle$.

When the context is clear, we will write G (resp. M) for G_S (resp. M_S).

We also assume S to be finite and fix an enumeration $S = \{s_1, \dots, s_n\}$.

Remark 1.4. *By the definition of $\psi\colon S \to \mathfrak{S}_n$ we have that $s_i * s_j = s_{\psi(s_i)(j)}$, which we will also write $\psi(s_i)(s_j)$ for simplicity.*

1.2. **Braces**

The structure group of a brace has an extra "ring-like" structure, which was first introduced by Rump in [27] as linear cycle sets. An equivalent definition was then introduced by Cedó, Jespers and Okniński in [5] and then in a large survey again by Cedó in [4]. We will use their definition of a (left) brace throughout this article.

Definition 1.5 ([27, 4])**.** *A brace is a triple $(B, +, \cdot)$ such that $(B, +)$ is an abelian group, $(B, \cdot)$ is a group and for all a, b, c in B:*

$$a(b + c) + a = ab + ac.$$

$(B, +)$ will be called the additive group and $(B, \cdot)$ the multiplicative group of the brace B.

We now fix B a brace.

Remark 1.6. *Note that, if 0 is the additive identity and 1 the multiplicative identity, then taking $a = 1, b = c = 0$ yields $1 * (0 + 0) + 1 = 1 * 0 + 1 * 0$, thus $1 = 0$.*

Example 1.7. *If $(G, +)$ is an abelian group then $(G, +, +)$ is a brace, called the trivial brace.*

Taking $(B, +) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with $(a, b) \cdot (c, d) = \begin{cases}(a + c, b + d), & a + b = 0 \ mod\ 2\\ (a + d, b + c), & a + b = 1 \ mod\ 2\end{cases}$ can be checked to be a left-brace, and obviously $(0, 0)$ is the identity of $(B, \cdot)$.

Proposition-Definition 1.8 ([4])**.** *For any a in B, the map $\lambda : (B, \cdot) \to Aut(B, +)$ defined by $\lambda_a(b) = ab - a$ for all a, b in B, is a well-defined morphism.*

This also gives $ab = a + \lambda_a(b)$. This will be used everywhere to switch between products and sum of elements.

Example 1.9. *From the previous example we have respectively $\lambda_g = id_G$ for all g in G, and in $(B, +, \cdot)$ $\lambda((a, b)) = \sigma^{a+b}$ where σ permutes the two coordinate of $(B, +)$, and obviously $(0, 0)$ is the identity of $(B, \cdot)$.*

Lemma 1.10 ([4])**.** *For any a, b in B we have:*

1. *$\lambda_a \lambda_b = \lambda_{a+\lambda_a(b)}$.*
2. *$ab^{-1} = -\lambda_{ab^{-1}}(b) + a$*
3. *If $\lambda_a = \lambda_b$ then $ab^{-1} = a - b$*

Proof. This first one follows from $gh = g + \lambda_g(h)$.
For the second one, $-\lambda_{ab^{-1}}(b) + a = -ab^{-1}b - ab^{-1} + a = ab^{-1}$.
And then, $\lambda_{ab^{-1}} = \lambda_a\lambda_b^{-1} = \lambda_a\lambda_a^{-1} = \mathrm{id}_B$. □

Lemma 1.11. *For any a, b in B, we have $a\lambda_a^{-1}(b) = b\lambda_b^{-1}(a)$.*
Moreover, $\lambda^{-1}_{\lambda_a^{-1}(b)}\lambda_a^{-1} = \lambda^{-1}_{\lambda_b^{-1}(a)}\lambda_b^{-1}$.

Proof. Firstly,

$$a\lambda_a^{-1}(b) = a(a^{-1}b - a^{-1}) = b - 1 + a = b - 0 + a = b + a = a + b = b\lambda_b^{-1}(a).$$

Then from the fact that $\lambda\colon (B, \cdot) \to \mathrm{Aut}(B, +)$ is a morphism we have that $\lambda_{ab}^{-1} = \lambda_b^{-1}\lambda_a^{-1}$ so

$$\lambda^{-1}_{\lambda_a^{-1}(b)}\lambda_a^{-1} = \lambda^{-1}_{a\lambda_a^{-1}(b)} = \lambda^{-1}_{b\lambda_b^{-1}(a)} = \lambda^{-1}_{\lambda_b^{-1}(a)}\lambda_b^{-1}.$$

□

The following is implicit in [4]:

Lemma 1.12 ([4])**.** *Let S be a subset of a brace $(B, +, \cdot$ such that $\lambda_s(S) \subseteq S$ for any s in S. Then $(S, +)$ is a subgroup of $(B, +)$ if and only if it is a subgroup of $(B, \cdot)$.*

Proof. This follows from the identity $ab = a + \lambda_a(b)$ (or equivalently $a + b = a\lambda_a^{-1}(b)$). □

Definition 1.13 ([4])**.** *Let $(B, +, \cdot)$ be a brace.*

- *$S \subseteq B$ is a subbrace if it is a subgroup of both $(B, +)$ and $(B, \cdot)$.*
- *$L \subseteq B$ is a left ideal if it is a subgroup of $(B, +)$ and $\lambda_a(I) \subseteq I$ for all a in B.*
- *$I \subseteq B$ is an ideal if it is a normal subgroup of $(B, \cdot)$ and $\lambda_a(I) \subseteq I$ for all a in B.*

Proposition 1.14 ([4])**.** *Let $(B, +, \cdot)$ be a brace and $I \subseteq B$.*

- *I is an ideal $\Rightarrow$ I is a left ideal $\Rightarrow$ I is a subbrace.*
- *If I is an ideal then the multiplicative quotient B/I has an induced brace structure $(B/I, +, \cdot)$.*
- *$Soc(B) = Ker(\lambda) = \{a \in B \mid \forall b \in B, ab = a + b\}$ is an ideal called the Socle of B.*

In [14], it was shown that there exists a bijective 1-cocyle $\Pi\colon \mathbb{Z}^S \to G$, i.e.a bijective map such that $\Pi(gh) = \Pi(g) \cdot \lambda_g^{-1}(\Pi(h))$ for any $g, h \in \mathbb{Z}^S$. This so called "I-structure" was shown in [27, 4] to be equivalent to the following:

Theorem 1.15 ([14, 4])**.** *The structure group G of a finite cycle set S has a brace structure given by $(\mathbb{Z}^S, +, \cdot)$ such that G with the usual multiplication is isomorphic to $(\mathbb{Z}^S, \cdot)$.*
Moreover, for any s, t in S, we have $\lambda_s^{-1}(t) = \psi(s)(t)$.

From the I-structure mentioned above we can write any element of G as $g = \sum_{s\in S} g_s s$ where $g_s \in \mathbb{Z}$. Then for any h in G, we have $\lambda_h(g) = \sum_S g_s\lambda_h(s)$ with $\lambda_h(s)$ in S.

Because we will work over group rings $R[G]$, we will use Dehornoy's notation from [10] to denote $s^{[k]} = ks$ for any $k \in \mathbb{Z}$ (to avoid confusion with the element $k \cdot s \in R[G]$).

In [10], Dehornoy constructed a finite quotient of the structure group, which he calls a "Coxeter-like" group:

Theorem 1.16 ([10, 15])**.** *Let S be a finite non-trivial cycle set. Then there exists a positive integer d such that $dS \subset Soc(G)$.*
Moreover, for any positive integer l, the quotient $\overline{G}_l \coloneqq G/\langle (ld)s\rangle$ admits a quotient brace structure given by $((\mathbb{Z}/ld\mathbb{Z})^S, +, \cdot)$.

In particular, this means that the bijective 1-cocycle $\Pi\colon \mathbb{Z}^S \to G$ induces a bijective 1-cocycle $\overline{\Pi}\colon (\mathbb{Z}/ld\mathbb{Z})^S \to \overline{G}_l$.

The smallest positive integer satisfying the condition of Theorem 1.16 is called the Dehornoy's class of S, and the set of positive integers that will satisfy the condition are the multiple of d.

We denote by T the diagonal map of S defined by $T(s) = s{*}s$. The following Proposition will be useful:

Proposition 1.17 ([15]). *The followings hold:*

(i) Let o be the order of T and k any positive integer. Consider the euclidean division of k by o to write $k = o \cdot q + r$, then we have $ks = sT(s)T^2(s)\dots T^{k-1}(s) = (os)^q(rs)$.

(ii) The order o of T divides d. In particular, for any integer k and any s in S, we have $\lambda_{ks}^{-1}(s) = T^k(s)$ and $kds = \left(sT(s)\dots T^{o-1}(s)\right)^k$.

As in Coxeter group, we can consider reduced word and state an Exchange lemma (see [22] for the case of Coxeter groups):

Remark 1.18. *Consider a word $w = s_{i_1}\cdots s_{i_k}$ over S, and let g be the associated element of $\overline{G}_l$. Then we can write $g = \sum_S g_s s$ with $0 \le g_s < ld$. Thus the word w is a minimal expression of g iff $k = \sum_S g_s$.*

So for any g in $\overline{G}_l$ we denote $\ell(g) = \sum_S g_s$. Then we say that a word w is reduced if $k = \ell(g)$ when w represents $g \in \overline{G}_l$.

Lemma 1.19 (Exchange Lemma). *Let s be in S and g in $\overline{G}$. Write $g = \sum\limits_{s\in S} g_s s$ with $0 \le g_s < d$. Then either sg is reduced ($\ell(gs) = \ell(g)+1$) or $g_{s*s} = d-1$ (i.e.$(d-1)(s*s)$ left-divides g). Moreover, if it is not reduced, then $sg = \sum\limits_{\substack{t\in S\\ t\neq s}} g_{s*t}t$.*

Moreover, we can go from one reduced expression to another only using the quadratic relations $s(s*t) = t(t*s)$.

Proof. As the given expression of g is reduced, we know $\ell(g) = k$, i.e. $\sum\limits_{s\in S} g_s = k$. Now, by Proposition-Definition 1.8 $sg = s + \lambda_s(g) = s + \sum\limits_{t\in S} g_t\lambda_s(t)$. Reindexing the sum by setting $t = \lambda_s^{-1}(u) = s*u$ for some $u \in S$, we have $g = s + \sum\limits_{u\in S} g_{s*u}u$.

This is reduced if and only if $(sg)_u < d$ for all u. Because g is reduced, we have $g_{s*u} < d$, so this sg is reduced if and only if $1 + g_{s*s} < d$. Meaning that this is not reduced precisely when $g_{s*s} = d-1$. In this case, then $(sg)_s = d$, and we conclude by $ds = 0$.

Moreover, assume we have two reduced expressions as $g = s_{i_1}\cdots s_{i_k}$ and $g = s_{j_1}\cdots s_{j_k}$. Using Proposition-Definition 1.8, we can rewrite both expressions as $g = \sum\limits_{s\in S} g_s s$ and this is unique by the commutativity of $(\overline{G}, +)$. This rewriting only involves $st = s + \lambda_s(t) = \lambda_s(t) + s = \lambda_s(t)\lambda_{\lambda_s(t)}^{-1}(s)$ which preserves length. Moreover, by Theorem 1.15, we have that the quadratic relations $s_1(s_1 * s_2) = s_2(s_2 * s_1)$ are equivalent to $s_1\lambda_{s_1}^{-1}(s_2) = s_2\lambda_{s_2}^{-1}(s_1)$. Letting $s = s_1$ and $s_2 = \lambda_s(t)$, we see that $st = \lambda_s(t)\lambda_{\lambda_s(t)}^{-1}(s)$ allows us to go from one reduced expression to the other only with the quadratic relations. ∎

We conclude the preliminaries by the following technical lemma:

Lemma 1.20. *For any $s, t \in S$ the followings hold:*

(i) There exists ρ_s with $\ell(\rho_s) = d-1$ such that $s^{[d]} = s\rho_s$. Moreover $\rho_s = (s*s)^{[d-1]}$.

(ii) $\psi(\rho_s) = \psi(s)^{-1}$
(iii) $s^{[kd]} = (s\rho_s)^k$
(iv) $s^{[d]}t = t(t*s)^{[d]}$
(v) $\rho_s t = (s*t)\rho_{t*s}$
(vi) $\rho_{s*t}\rho_s = \rho_{t*s}\rho_t$
(vii) $(s*t)^{[d]}\rho_s = \rho_s t^{[d]}$

For simplicity we will write $\gamma_s^k = \rho_s s^{[(k-1)d]} = (s*s)^{[kd-1]}$ *(giving* $s\gamma_s^k = s^{[kd]}$*).*

h) $\gamma_s^k t = (s*t)\gamma_{t*s}^k$
i) $\gamma_{s*t}^{k_1}\gamma_s^{k_2} = \gamma_{t*s}^{k_2}\gamma_t^{k_1}$

In particular, when writing $s^{[kd]} = sg$ *we have* $g = (s*s)^{[kd-1]} = \rho_s s^{[(k-1)d]} = \rho_s(s\rho_s)^{k-1}$*. This implies that, if* $s^{[d]} = s_1 \dots s_d$ *then* $(s^{[i]})^{[d]} = s_i \dots s_d s_1 \dots s_{d-1}$*.*

Moreover, as all those equalities are true in G*, they respect length and also hold in* $\overline{G}_k$*.*

Proof. (i) is follows from Proposition 1.8: $s^{[d]} = s + (d-1)s = s\lambda_s^{-1}((d-1)s)$.

(ii) follows from $1 = \psi(s^{[d]}) = \psi(s\rho_s) = \psi(s)\psi(\rho_s)$.

(iii) and (iv) follow from the definition of d as we have: $s^{[kd]} = (kd)s = k(ds) = ds\lambda_{ds}^{-1}(ds)\dots\lambda_{(k-1)ds}^{-1}(ds) = (ds)(ds)\dots(ds) = (ds)^k$, and $s^{[d]}t = ds + \lambda_{ds}(t) = t + ds = t\cdot(d\lambda_t^{-1}(s)) = t\cdot d(t*s) = t(t*s)^{[d]}$.

For (v) we have $s\rho_s t = s^{[d]}t = t(t*s)^{[d]} = t(t*s)\rho_{t*s}$, applying $t(t*s) = s(s*t)$ and canceling the s gives the result.

For (vi) we have $\rho_{s*t}\rho_s = \rho_{s*t} + \lambda\rho_{s*t}(\rho_s) = \rho_{s*t} + (d-1)\psi^{-1}(s*t)(s*s) = \rho_{s*t} + (d-1)\psi(s*t)(s*s)$, from the cycle set equation, we have $\psi(s*t)(s*s) = \psi(t*s)(t*s)$, thus $\rho_{s*t}\rho_s = \rho_{s*t} + (d-1)\psi(s*t)(s*s) = \rho_{s*t} + (d-1)\psi(t*s)(t*s) = \rho_{s*t} + \rho_{t*s}$. By symmetric, we conclude that this is equal to $\rho_{t*s}\rho_t$.

(vii) comes from (iv) applied on $\rho_t = (t*t)^{[d-1]}$ and $\psi(\rho_t) = \psi(t)^{-1}$.

(viii) is deduced from the previous ones: $\gamma_s^k t = \rho_s s^{[kd]}t = \rho_s t(t*s)^{[kd]} = (s*t)\rho_{t*s}(t*s)^{[kd]} = (s*t)\gamma_{t*s}^k$

Similarly for (ix): $\gamma_{s*t}^{k_1}\gamma_s^{k_2} = \rho_{s*t}(s*t)^{[k_1d]}\rho_s s^{[k_2d]} = \rho_{s*t}\rho_s t^{[k_1d]}s^{[k_2d]} = \rho_{t*s}\rho_t s^{[k_2d]}t^{[k_1d]} = \rho_{t*s}(t*s)^{[k_2d]}\rho_t t^{[k_1d]} = \gamma_{t*s}^{k_2}\gamma_t^{k_1}$. □

2. Defining the Hecke algebra

We fix a cycle set $(S,*)$ of size n, of Dehornoy's class d, with structure group G and germ $\overline{G}_l = G/\langle lds\rangle$ for some positive integer l.

Recall that, by Theorem 1.15 we have a set bijection, more precisely a bijective 1-cocycle, $\mathrm{cp}\colon G \to \mathbb{Z}^n$. The inverse of this bijective 1-cocycle is also a bijective 1-cocycle $\mathrm{cp}^{-1} = \Pi\colon \mathbb{Z}^n \to G$: we have $\Pi(gh) = \Pi(g)\lambda_{\Pi(g)}^{-1}(\Pi(h))$. In particular, if $\psi(\Pi(g)) = 1$, then $\Pi(gh) = \Pi(g)\Pi(h)$. Moreover, by Theorem 1.16 Π induces a bijective 1-cocycle $\overline{\Pi}\colon (\mathbb{Z}/ld\mathbb{Z})^n \to \overline{G}_l$

Let R be a ring, and note that $R[\mathbb{Z}^n] = R[X_1^{\pm 1},\dots,X_n^{\pm 1}]$ by identifying the generator $e_i = (0,\dots,0,1,0,\dots,0)$ with X_i. The set map Π extends linearly to $R[X_1^{\pm 1},\dots,X_n^{\pm 1}] \to R[G]$, sending $\sum_i r_i X_1^{i_1}\dots X_n^{i_n}$ to $\sum_i r_i\Pi(s_1,\dots,s_1,\dots,s_n,\dots,s_n)$ for some finite indices i and corresponding integers $i_1,\dots,i_n$ and coefficients r_i.

We now proceed to construct the Hecke algebra as hinted before: we pick a polynomial, apply it to $s^{[d]}$ and use the 1-cocycle $\mathbb{Z}^n \to G$ to show that we have a basis by showing that the quotients of the associated group rings by appropriate ideals have the same dimensions.

From now on, fix a polynomial $P \in R[X]$ of degree $l > 0$ and set $P(X) = \sum_{k=0}^{l} a_k X^k$.

Remark 2.1. *Recall that given an algebra A and $R \subseteq A$, elements of the two sided ideal generated by R are of the form $\sum a_i r_i b_i$, a finite sum where $a_i, b_i \in A, r_i \in R$.*

Lemma 2.2. *Consider the two-sided ideals $I_P = \left(P(X_1^d), \dots, P(X_n^d)\right) \subset R[\mathbb{Z}^n]$ and $J_P = \left(P(s_1^{[d]}), \dots, P(s_n^{[d]})\right) \subset R[G]$. Then Π induces a bijection $I_P \to J_P$.*

Proof. First remark that P sends a set of generators of I_P to a set of generators of J_P:

$$\Pi(P(X_i^d)) = \Pi\left(\sum a_k X_i^{kd}\right) = \sum a_k \Pi\left(X_i^{kd}\right) = \sum a_k s_i^{[kd]} = \sum a_k (s_i^{[d]})^k = P(s_i^{[d]})$$

where we use that S is of class d with Proposition 1.17 to have $s_i^{[kd]} = (s_i^{[d]})^k$.

As $\Pi\colon \mathbb{Z}^n \to G$ is bijective, its linearization $\Pi\colon R[X_1, \dots, X_n] \to R[G]$ is bijective. But Π is not a morphism (only a bijective 1-cocycle), so we can't deduce that $\Pi(P(X_i^d)) = P(s_i^{[d]})$ to obtain $\Pi(I_P) \subseteq J_P$. However, we'll use that Π is a 1-cocycle and S is of class d, to deduce that, for any $1 \leq i \leq n$ and any $f \in R[\mathbb{Z}^n]$, we have $\Pi(X_i^d f) = \Pi(X_i^d) \cdot \lambda^{-1}_{\Pi(X_i^d)}(\Pi(f)) = s_i^{[d]}\Pi(f)$.

We'll prove that $\Pi(I_P) = J_P$ by double inclusion:

Let $Q_1, Q_2 \in R[\mathbb{Z}^n]$. By the commutativity of $R[\mathbb{Z}^n] = R[X_1, \dots, X_n]$, we have that $Q_1 P(X_i^d) Q_2 = P(X_i^d) Q_1 Q_2$ for any $1 \leq i \leq n$. Moreover, as S is of class d and Π is a 1-cocycle, we have $\Pi\left(X_i^d(X_1^{b_1} \dots X_n^{b_n})\right) = s_i^{[d]}\Pi(X_1^{b_1} \dots X_n^{b_n})$. Thus $\Pi(Q_1 P(X_i^d) Q_2) = \Pi(P(X_i^d))\Pi(Q_1 Q_2) = P(s_i^{[d]})\Pi(Q_1 Q_2)$, which is in J_P as J_P is an ideal. So we have $\Pi(I_P) \subseteq J_P$.

Now let $f, g \in G$. Then, by Lemma 1.11, we have for all $g \in G$ that $gs^{[d]} = \lambda_g(s^{[d]})\lambda_{s^{[d]}}(g) = \psi(g)(s^{[d]})g$. Thus, in $R[G]$, we have

$$fP(s_i^{[d]})g = \sum a_k f s_i^{[dk]} g = \sum a_k (\psi(f)^{-1}(s_i))^{[dk]} fg.$$

Write $t = (\psi(f)^{-1}(s_i))$ and let $Y \in \{X_1, \dots, X_n\}$ be such that $\Pi(Y) = t$. As S is of class d, we have $\Pi^{-1}(fP(s_i^{[d]})g) = \sum a_k \Pi^{-1}(fs^{[dk]}g) = \sum a_k Y^{dk}\Pi^{-1}(fg) = P(Y^d)\Pi^{-1}(fg)$, which is in I_P by Remark 2.1. We conclude that $J_P \subseteq \Pi(I_P)$. ☐

Example 2.3. *Let $P(X) = 1 + X$, $g \in G$ and $s \in S$. Write $\Pi(X) = s, Q = \Pi^{-1}(g)$, $t = \psi(g)^{-1}(s)$ and $Y = \Pi^{-1}(t)$. Then $(1+g)(1+s^{[d]}) = 1+s^{[d]}+g+gs^{[d]} = 1+s^{[d]}+g+t^{[d]}g = (1+s^{[d]})+(1+t^{[d]})g = P(s^{[d]})+P(t^{[d]})g = \Pi(P(X^d))+\Pi(Y^d)\Pi(Q) = \Pi(P(X^d)+P(Y^d)Q)$.*

Thus $(1+g)(1+s^{[d]})$ is an element of $(P(s)) \subset J_P$, with preimage $P(X^d) + P(Y^d)Q$ in $(P(X^d), P(Y^d)) \subset I_P$.

The following examples highlight why we need to take polynomials in X^d:

Example 2.4. *Let $(S, *)$ be the cycle set, with $S = \{s, t, u\}$ and $\psi(s) = \psi(t) = \psi(u) = (stu) = \sigma$. Then S is of class 3 and $s^{[3]} = stu, t^{[3]} = tus, u^{[3]} = ust$. Write $R[\mathbb{Z}^3] = R[X, Y, Z]$ where $\Pi(X) = s, \Pi(Y) = t, \Pi(Z) = u$. Let $P(x) = 1 + x^2$ and consider the ideals $I = (P(X^2), P(Y^2), P(Z^2))$ and $J = (P(s^{[2]}), P(t^{[2]}), P(u^{[2]}))$.*

Note that, for $T_i \in \{X, Y, Z\}$ with $1 \leq i \leq k$,

$$\Pi(T_1 \cdots T_k) = \Pi(T_1) \cdot \sigma(\Pi(T_2)) \cdot \dots \cdot \sigma^{k-1}(\Pi(T_k))$$

as Π is a 1-cocycle. Or equivalently, for $t_i \in \{s, t, u\}$,

$$\Pi^{-1}(t_1 \dots t_k) = \Pi^{-1}(t_1)\Pi^{-1}(\sigma^{-1}(t_2)) \cdots \Pi^{-1}(\sigma^{-k+1}(t_k)).$$

Now the element $f = tt + tstt = t(1+st)t \in R[G]$ is in J, as $P(s^{[2]}) = 1 + s^{[2]} = 1 + st$. However, $\Pi^{-1}(tt) = \Pi^{-1}(t)\Pi^{-1}(\sigma^{-1}(t)) = \Pi^{-1}(t)\Pi^{-1}(s) = YX$, and similarly $\Pi^{-1}(tstt) = t\Pi^{-1}(u)\Pi^{-1}(u)\Pi^{-1}(t) = YZZY$. Thus $\Pi^{-1}(f) = YX + YZZY = XY + Y^2Z^2$, and we claim that this is not an element of J.

To check that $XY + Y^2Z^2 \notin J$, suppose $XY + Y^2Z^2 = a(1+X^2) + b(1+Y^2) + c(1+Z^2)$ with $a, b, c \in R[X, Y, Z]$. As we have no X^2 terms, we deduce $a = 0$, thus $XY + Y^2Z^2 = b(1+Y^2) + c(1+Z^2)$. We have a XY which contains no square term, meaning that XY appears in b or c. But there is no X in Y^2Z^2, a contradiction.

We took polynomials in X^2 instead of X^3, and now an element of I does not come from J. Thus the use of polynomials in X^d.

On the other hand , if instead of st we had an element g with trivial permutation (such as $g = stu$), we would have $\Pi^{-1}(t(1+g)t) \in J$. Indeed, $t(1+g)t = tt + tgt$, and as g has trivial permutation, the preimage of the blue t would have been the same as the preimage of the red t, allowing for factorization by $\Pi^{-1}(tt)$. But with st, the blue t gets acted on, preventing a factorization.

From now on, we fix P in $R[X]$ of degree $l > 0$. We furthermore assume that a_l, the leading coefficient of P, is invertible. We also fix the ideals $I_P \subset R[\mathbb{Z}^n]$ and $J_p \subset R[G]$ as in Lemma 2.2.

Let $\mathcal{H}(S, P) = R[G]/J_P$. In $\mathcal{H}(S, P)$ we thus have that

$$\mathcal{H}(S, P) = R[G]/\left(T_{s^{[ld]}} = \sum_{k=0}^{l-1} \frac{-a_k}{a_l} T_{s^{[kd]}}\right). \tag{3}$$

To distinguish between elements of G and their corresponding generator of the algebra, we will write $R[G] = R\langle T_g, g \in G \mid T_g T_h = T_{gh}\rangle$.

Lemma 2.5. *The followings hold:*

(i) We have the isomorphism $R[G] \cong R\langle T_s, s \in S \mid T_s T_{s*t} = T_t T_{t*s}, \forall s, t \in S\rangle$
(ii) For any $\overline{g} \in \overline{G}_l$, there is a well-defined element $T_{\overline{g}} \in \mathcal{H}(S, P)$ such that $T_{\overline{g}} = T_{s_{i_1}} \cdots T_{s_{i_r}}$ whenever $s_{i_1} \cdots s_{i_r}$ ($s_i \in S$) is a reduced expression of $\overline{g}$ in $\overline{G}_l$.
(iii) For any $g \in G$ with image $\overline{g} \in \overline{G}$, if $\ell(g) = \overline{\ell}(\overline{g})$, then the projection $R[G] \to \mathcal{H}(S, P)$ sends T_g to $T_{\overline{g}}$.

Proof. (i) follows from the definition of the group ring $R[G]$ as the free module with basis G such that $T_g T_h = T_{gh}$ for any g, h in G.

For (ii), the Exchange Lemma 1.19 tells us that we can go from one reduced expression to another only using the quadratic relations. By (i) those quadratic relations are also the defining relations of a presentation of $\mathcal{H}(S, P)$. Thus T_g does not depend on the choice of a reduced expression.

Finally, for (iii), let $g \in G$ and write $g = s_{i_1} \cdots s_{i_r}$ so that $\ell(g) = r$. Let $\overline{g}$ be the projection of g in $\overline{G}$, and assume that $\ell(g) = \overline{\ell}(\overline{g}) = r$. Then $\overline{s_{i_1}} \cdots \overline{s_{i_r}}$ is a reduced expression of $\overline{g}$ in $\overline{G}$. Thus, by (ii), $T_{\overline{g}} = T_{\overline{s_{i_1}}} \cdots T_{\overline{s_{i_r}}}$ is the projection of T_g. □

Recall that,by Lemma 1.20, we have $s^{[ld]} = s \cdot (s * s)^{[ld-1]}$. Thus, Equation (3) means that, in $\mathcal{H}(S, P)$ we have

$$T_s T_{s*s}^{[ld-1]} = \sum_{k=0}^{l-1} \frac{-a_k}{a_l} T_{s^{[kd]}}. \tag{4}$$

Even though $T_s^{[ld]}$ is not defined in $\mathcal{H}(S, P)$ from Lemma 2.5, we will often abuse notation and write $T_s^{[ld]}$ instead of $T_s T_{s*s}^{[ld-1]}$ in $\mathcal{H}(S, P)$.

Lemma 2.6. *As an R-module, $\mathcal{H}(S,P)$ is generated by $\{T_g\}_{g\in\overline{G}_l}$.*

In particular, this means that $\mathcal{H}(S,P)$ is finite dimensional, and that its dimension is bounded above by $\#\overline{G}_l = (ld)^n$.

Proof. Let $s \in S$ and $g \in \overline{G}_l$. By Remark 1.18, either sg is reduced and then $T_sT_g = T_{sg}$, or it is not reduced and $(s*s)^{[ld-1]} \prec g$ ($g = (s*s)^{[ld-1]}h$ is reduced in $\overline{G}$) by Lemma 1.19. Thus, if sg is not reduced, by Equation -4), we have $T_sT_g = T_sT_{s*s}^{[ld-1]}T_h = \sum_{k=0}^{l-1}\frac{-a_k}{a_l}T_{s^{[kd]}h}$, where $s^{[kd]}h$ is reduced in $\overline{G}_l$ as $k < l$ and $g = s^{[ld-1]}h$ is reduced. □

Lemma 2.7. *The quotient algebra $R[\mathbb{Z}^n]/I$ is a free R-module of dimension $(ld)^n$ and basis $X_1^{j_1}\dots X_n^{j_n}$ with $0 \le j_1,\dots,j_n < ld$.*

Moreover, the linearization of $\overline{\Pi}$ provides a bijection between this basis and $\overline{G}_l$.

The bijection Π allows us to write an abuse of notation: by $T_s^{[d]}$ we will mean $T_{s^{[d]}}$.

Proof. When quotienting $R[X_1,\dots,X_n]$ by $P(X_i^d)$, we can reduce all polynomials of degree strictly greater than $ld-1$. Meaning that $R[\mathbb{Z}^n]/I_P$ has a basis given by $X_1^{j_1}\cdots X_n^{j_n}$ with $0 \le j_i < ld$.

By considering the powers of such a monomial, this basis is in bijection with $(\mathbb{Z}/ld\mathbb{Z})^n$. By Theorem 1.16, $\overline{\Pi}$ gives a bijection $(\mathbb{Z}/ld\mathbb{Z})^n \to \overline{G}_l$, finishing the proof. □

Theorem 2.8. *$\mathcal{H}(S,P)$ is a free R-module with basis $\{T_g \mid g \in \overline{G}_l\}$, in particular it has dimension $(ld)^n$.*

Proof. From Lemma 2.5 we know that $\{T_g \mid g \in \overline{G}_l\}$ generates $\mathcal{H}(S,P)$ as an R-module, so in particular $\dim\mathcal{H}(S,P) \le (ld)^n$. We just have to show this family is free, but this follows from Lemmas 2.2 and 2.7:

Suppose we have a linear combination $\sum_{\overline{g}\in\overline{G}_l} a_{\overline{g}}T_{\overline{g}} = 0$ in $\mathcal{H}(S,P)$. By lifting the elements $\overline{g} \in \overline{G}_l$ to $g \in G$ we have $\sum_{\overline{g}\in\overline{G}_l} a_{\overline{g}}T_g \in J_P$. Then, applying Π^{-1} we obtain $\sum_{\overline{g}\in\overline{G}_l} a_{\overline{g}}\Pi^{-1}(T_g) \in I_P$. Projecting to $R[\mathbb{Z}^n]/I_P$, this means that $\sum_{\overline{g}\in\overline{G}_l} a_{\overline{g}}\Pi^{-1}(T_{\overline{g}}) = 0 \in R[\mathbb{Z}^n]/I_P$. From Lemma 2.7 the family $\Pi^{-1}(T_{\overline{g}})$ is a basis of $R[\mathbb{Z}^n]/I_P$, so we must have $a_{\overline{g}} = 0$ for all $\overline{g} \in \overline{G}_l$. □

Remark 2.9. *Note that in the above proofs we can take a different polynomial P for each orbit of S under the action of G, as in proof of Lemma 2.2 we just need that two elements are in the same orbit to obtain that $\Pi(J) \subseteq I$. If we denote such polynomials by $\underline{P} = (P_i)_{1\le i\le n} \in R[X]^n$ with deg $P_i = l_i$ and such that $P_i = P_j$ whenever s_i and s_j are in the same orbit by the action of $\mathcal{G}$, we obtain the Hecke algebra $\mathcal{H}(S,\underline{P})$ with dimension equal to $\prod_{i=1}^n(l_id)$ which is the same as the order of the finite group $G/\langle s_i^{[l_id]}\rangle_{1\le i\le n}$.*

With the same reasoning we can also take a different d for each of those orbits, see for instance [20], but this will not be used in this thesis.

It was chosen to not consider those generalizations (except in Section 4) to avoid heavy notation and make the proofs easier to read.

Corollary 2.10. *Taking $P(X) = X^2 - pX - q$ with $p, q \in R$ we obtain a definition of an Hecke algebra for cycle sets with relations of the form*

$$T_s^{[2d]} = pT_s^{[d]} + q$$

Example 2.11. *Take $S = \{s_1,\dots,s_n\}$, $\sigma \in \mathfrak{S}_n$ and $\psi(s_i) = \sigma$. Then S is of class $d = o(\sigma)$ (the order of the permutation), and taking $P(X) = X^2 - X - 1$ we get*

$$\mathcal{H}(S,P) = R\left\langle s_1,\dots,s_n \;\middle|\; \begin{matrix} s_is_{\sigma(j)} = s_js_{\sigma(i)}, & 1 \le i < j \le n \\ (s_is_{\sigma(i)}\cdots s_{\sigma^{d-1}(i)})^2 = s_is_{\sigma(i)}\cdots s_{\sigma^{d-1}(i)} + 1, & 1 \le i \le n \end{matrix}\right\rangle$$

Remark 2.12. *For all $g \in G$, by Proposition-Definition 1.8, we have $\lambda_g(s^{[d]}) = (\lambda_g(s))^{[d]}$. So the action of G on $R[G]$ stabilizes J the ideal generated by the $P(s^{[d]})$, meaning that G acts on $\mathcal{H}(S,P)$. As $ldG \subset Soc(G)$, the action of dG on J is trivial and thus $\overline{G}_l$ acts on $\mathcal{H}(S,P)$.*

Remark 2.13. *We see one important difference between Hecke algebras for Coxeter groups and for Structure group of solutions: for a finite Coxeter group W with associated Artin–Tits group A, one can view the Hecke algebra as a deformation of the quotient $R[A] \to R[W]$. However, with our approach for solutions, we have to consider the deformation of a larger quotient $R[G] \to R[\overline{G}_l]$ with $l > 1$ (if $l = 1$ then the relations are of the form $T_s^{[d]} = -\frac{a_0}{a_l}$, which is not an interesting deformation).*

Moreover, It was shown by Coxeter in [7] that the quotient $B_n/\langle s^k\rangle$ is finite if and only if $\frac{1}{n} + \frac{1}{k} > \frac{1}{2}$, thus for $n \geq 6$ the quotient is finite only for $k = 2$ (the symmetric group). This means that, in the case of Coxeter groups, we can only expect similar definitions of Hecke algebra with polynomials of degree 2.

However here, we can work over any degree, which highlights the different behaviours of the germs and associated Hecke algebra for Coxeter groups and structure groups of solutions.

We conclude the construction of the Hecke algebra for solutions by relating the Hecke algebra of a solution with the Hecke algebra of its retraction. As in Proposition-Definition 2.16, we denote by S' the retraction of S. Then the class d' of S' divides the class d of S by Lemma 2.17. We deduce the following:

Proposition 2.14. *We have a surjective algebra morphism*

$$\mathcal{H}(S,P(X)) \to \mathcal{H}\left(S', P\left(X^{\frac{d}{d'}}\right)\right).$$

Proof. The morphism $G \to G'$ linearly extends to $R[G] \to R[G']$. By Theorem 1.17, for any $s \in S$ and any positive integer k, we have $(s^{[d]})^k = s^{[kd]}$. Moreover, by Proposition 2.17 we know that d' divides d, so $(\underline{s}^{[d']})^{\frac{d}{d'}} = \underline{s}^{[d]}$. Thus we get $\mathcal{H}\left(S', P\left(X^{\frac{d}{d'}}\right)\right) = R[G']/\left(P\left((\underline{s}^{[d']})^{\frac{d}{d'}}\right)\right) = R[G']/\left(P\left(\underline{s}^{[d]}\right)\right)$. Thus $R[G] \to \mathcal{H}(S', P(X^{\frac{d}{d'}}))$ factors through $H(S,P)$. ☐

Example 2.15. *If S is of class 4, S' of class 2, and we take $P(X) = X^2 + X + 1$, then we have a morphism $\mathcal{H}(S, X^8 + X^4 + 1) \to \mathcal{H}(S', X^8 + X^4 + 1)$.*

The retraction of a set-theoretical solution to the Yang–Baxter equation was introduced in [14]. Here, we relate the Hecke algebra of a solution ahd the Hecke algebra of its retraction.

Proposition-Definition 2.16 ([14, 26])**.** *The retraction of S is the quotient set S' by the equivalence relation $s \sim t \Leftrightarrow \psi(s) = \psi(t)$.*

The cycle set structure on S naturally induces a cycle set structure on S'. Moreover, we also obtain a morphism of cycle sets $S \to S'$, and a morphism of braces $G \to G'$ from the structure brace of S to the one of S'.

Lemma 2.17. *Let d (resp. d') be the Dehornoy's class of S (resp. S'). Then d' divides d.*

Proof. Let $\underline{s}$ be the equivalence classes in S' of $s \in S$. Then, from the fact that $G \to G'$ is a morphism of brace and that S is of class d, we have in G'

$$\lambda_{d\underline{s}}(\underline{t}) = d\underline{s} \cdot \underline{t} - d\underline{s} = \underline{ds \cdot t - ds} = \underline{\lambda_{ds}(t)} = \underline{t}.$$

This means that for all s, we have that $d\underline{s}$ is in the socle of $G_{S'}$. So d is a multiple of d' (the smallest integer such that $dG' \subset \mathrm{Soc}(G')$). ☐

Example 2.18. *Consider $S = \{s_1, s_2, s_3, s_4\}$ with $\psi(s_1) = \psi(s_3) = (12)(34)$ and $\psi(s_2) = \psi(s_4) = (14)(23)$. Then S' has two elements: $t_1 = \{s_1, s_3\}$ and $t_2 = \{s_2, s_4\}$, and both t_1 and t_2 act on S' by the permutation (12). For instance, $t_1 * t_2 = \underline{s_1} * \underline{s_4} = \underline{s_1 * s_4} = \underline{s_3} = t_1$, and this computation does not depend on the choice of representatives for t_1 and t_2.*

Proposition 2.19. *We have a surjective algebra morphism*

$$\mathcal{H}(S, P(X)) \to \mathcal{H}\left(S', P\left(X^{\frac{d}{d'}}\right)\right).$$

Proof. The morphism $G \to G'$ linearly extends to $R[G] \to R[G']$. As d is the Dehornoy's class of S, for any $s \in S$ and any positive integer k, we have $(s^{[d]})^k = s^{[kd]}$. Moreover, by Proposition 2.17 we know that d' divides d, so $(\underline{s}^{[d']})^{\frac{d}{d'}} = \underline{s}^{[d]}$. Thus we get $\mathcal{H}\left(S', P\left(X^{\frac{d}{d'}}\right)\right) = R[G']/\left(P\left((\underline{s}^{[d']})^{\frac{d}{d'}}\right)\right) = R[G']/\left(P\left(\underline{s}^{[d]}\right)\right)$. Thus $R[G] \to \mathcal{H}(S', P(X^{\frac{d}{d'}}))$ factors through $H(S, P)$. ☐

Example 2.20. *If S is of class 4, S' of class 2, and we take $P(X) = X^2 + X + 1$, then we have a morphism $\mathcal{H}(S, X^8 + X^4 + 1) \to \mathcal{H}(S', X^8 + X^4 + 1)$.*

3. Anti-involution on the Hecke algebra

Recall that we fixed a cycle set $(S, *)$ of size n, of Dehornoy's class d, with structure group G and germ $\overline{G}_l = G/\langle lds \rangle$. We fix a polynomial P in $R[x]$, written as $P(X) = \sum_{k=0}^{l} a_k X^k$ with a_l invertible. We have previously defined the Hecke algebra for cycle sets $\mathcal{H}(S, P)$. In this section, the goal is to endow $\mathcal{H}(S, P)$ with an anti-involution derived from the inversion in the group $\overline{G}_l$, in parallel to what is known for finite Coxeter groups (see [17, Exercise 4.8] for instance).

Proposition 3.1. *Suppose a_0, a_l are invertible in R. Then*

$$T_s^{-1} = \sum_{k=1}^{l} \frac{-a_k}{a_0} T_{s*s}^{[kd-1]}.$$

Moreover $(T_s^{-1})^{[d]} = (T_{s*s}^{[d]})^{-1}$.

Proof. From Lemma 1.17 we have, for any positive integer k, $s^{[k]} = s \cdot (s * s)^{[k]}$. We will use this to check that $\sum_{k=1}^{l} \frac{-a_k}{a_0} T_{s*s}^{[kd-1]}$ is indeed the inverse of T_s:

Firstly, $T_s\left(\sum_{k=1}^{l} \frac{-a_k}{a_0} T_{s*s}^{[kd-1]}\right) = \sum_{k=1}^{l-1} \frac{-a_k}{a_0} T_s^{[kd]} + \frac{-a_l}{a_0} T_s T_{s*s}^{[ld-1]}$. By Equation (4) we have $T_s T_{s*s}^{[ld-1]} = \sum_{k=0}^{l-1} \frac{-a_k}{a_l} T_{s^{[kd]}}$. We conclude that

$$T_s\left(\sum_{k=1}^{l} \frac{-a_k}{a_0} T_{s*s}^{[kd-1]}\right) = \frac{-a_l}{a_0}\frac{-a_0}{a_l} + \sum_{k=1}^{l-1}\left(\frac{-a_k}{a_0} + \frac{a_l}{a_0}\frac{a_k}{a_l}\right) T_s^{[kd]} = 1.$$

Then, let $X, Y \in \mathbb{R}[\mathbb{Z}^n]$ be such that $P(X) = s$ and $\Pi(Y) = s * s$. This means that, for $Y' = \sum_{k=1}^{l} \frac{-a_k}{a_0} Y^{kd-1}$, we have $\Pi(Y') = T_s^{-1}$ and $\Pi(Y'^d) = (T_s^{-1})^{[d]}$. By Lemma 1.20, we have $\psi(\Pi(Y^{kd-1})) = \psi((s * s)^{[kd-1]}) = \psi(\rho_s (s * s)^{[(k-1)d]}) = \psi(\rho_s) = \psi(s)^{-1}$. Thus, in the sum for T_s^{-1}, all the terms have the same permutation. Now, by Proposition 1.17 we can write $s^{[d]} = t_1 \dots t_d$ where $t_i = t_{i-1} * t_{i-1}$ and $s = t_1 = t_d * t_d$ (and so $t_2^{[d]} = t_2 \dots t_d t_1$). By Theorem 1.15, we know that Π is a 1-cocycle, meaning that $\Pi(Y'Y') = \Pi(Y')\lambda_{\Pi(Y')}(\Pi(Y')) = \Pi(Y')\psi(s)^{-1}(\Pi(Y'))$. As $\psi(s)^{-1}(s*s) = s$, we have $\psi(s)^{-1}(T_{s*s}^{[kd-1]}) = T_s^{[kd-1]} = T_{t_d*t_d}^{[kd-1]}$. Thus $\Pi(Y'Y') = T_{t_1}^{-1}T_{t_d}^{-1}$. By induction, we then have $\Pi(Y'^d) = T_{t_1}^{-1}T_{t_d}^{-1}T_{t_{d-1}}^{-1} \dots T_{t_2}^{-1} = (T_{t_2} \dots T_{t_d}T_{t_1})^{-1} = (T_{t_2}^{[d]})^{-1}$. □

Remark 3.2. *One has to be careful that $T_s^{-1} \neq T_{s^{-1}}$. Indeed, by Lemma 1.20 and Proposition 1.17, we have $T_{s^{-1}} = T_{\rho_s} = T_{s*s}^{[ld-1]}$, which is only one of the terms occurring in T_s^{-1}.*

Example 3.3. *Take $R = \mathbb{Z}[q^{\pm 1}]$ and the polynomial $P(X) = X^2 - (q-1)X - q = (X-q)(X+1)$, which satisfies the hypotheses of Proposition 3.1. Then*

$$T_s^{-1} = \frac{1-q}{q} T_{s*s}^{[d-1]} + \frac{1}{q} T_{s*s}^{[2d-1]}.$$

Corollary 3.4. *For any g in $\overline{G}_l$, T_g has an inverse in $\mathcal{H}(S,P)$.*

Proof. If $g = t_1 \dots t_r$ then the inverse of $T_g = T_{t_1} \cdots T_{t_r}$ is $T_g^{-1} = T_{t_r}^{-1} \cdots T_{t_1}^{-1}$. □

In a group G, the map ι sending an element to its inverse is an anti-involution, that is: $\iota(gh) = \iota(h)\iota(g)$ and $\iota(\iota(g)) = g$. This anti-involution is known to extend to the generic Iwahori–Hecke algebra in the case of Coxeter groups [17, Exercise 4.8]. We show that the same holds for Hecke algebra of structure groups of solutions to the Yang–Baxter equation, where the algebra is associated to the polynomial $P(X) = \sum_{k=0}^{l} a_k X^k$ with a_l invertible and $l > 0$.

Theorem 3.5. *If P splits over R with invertible roots $\alpha_1, \dots, \alpha_l$ (not required to be distinct), and if there exists an anti-involution $\iota : R \to R$ sending each α_i to α_i^{-1}.*

Then ι extends to an anti-involution of $\mathcal{H}(S,P)$ by sending T_g to T_g^{-1} for g in $\overline{G}_l$.

Proof. Denote by $\tilde{\iota}$ the map $\mathcal{H}(S,P) \to \mathcal{H}(S,P)$ defined by $\tilde{\iota}(\sum_{g \in \overline{G}_l} c_g T_g) = \sum_{g \in \overline{G}_l} \iota(c_g) T_g^{-1}$.

We will need that ι must send $1 \in R$ to 1: $\alpha_1^{-1} = \iota(\alpha_1) = \iota(1 \cdot \alpha_1) = \iota(\alpha_1)\iota(1) = \alpha_1^{-1}\iota(1)$, thus $\iota(1) = 1$.

By the hypothesis that P is split we have

$$P(T_s^{[d]}) = 0 \iff a_l \prod_{k=1}^{l} (T_s^{[d]} - \alpha_k) = 0 \tag{5}$$

For the constant coefficient of P we have $a_0 = (-1)^l a_l \prod_{k=1}^{l} \alpha_k$, so $\frac{a_l}{a_0} = (-1)^l \prod_{k=1}^{l} \alpha_k^{-1}$.

Multiplying Equation (5) by $\frac{a_0}{a_l}\left((T_s^{[d]})^{-1}\right)^l$ yields

$$a_l \prod_{k=1}^{l} (-\alpha_k^{-1})(T_s^{[d]})^{-1}(T_s^{[d]} - \alpha_k) = 0 \iff a_l \prod_{k=1}^{l} \left((T_s^{[d]})^{-1} - \alpha_k^{-1}\right) = 0.$$

This means precisely that $\tilde{\iota}(P(T_s^{[d]})) = 0$.

Recall from Lemma 1.20 the notation $\gamma_s^k = (s*s)^{[kd-1]}$ and that $\gamma_{s*t}^{k_1}\gamma_s^{k_2} = \gamma_{t*s}^{k_2}\gamma_t^{k_1}$. Thus, by Proposition 3.1 we have

$$T_{s*t}^{-1}T_s^{-1} = \left(\sum_{k=1}^{l} \frac{-a_k}{a_0} T_{\gamma_{s*t}^k}\right)\left(\sum_{k=1}^{l} \frac{-a_k}{a_0} \gamma_s^k\right) = \left(\sum_{k=1}^{l} \frac{-a_k}{a_0} \gamma_{t*s}^k\right)\left(\sum_{k=1}^{l} \frac{-a_k}{a_0} \gamma_t^k\right) = T_{t*s}^{-1}T_t^{-1}$$

So $\tilde{\iota}(T_s T_{s*t}) = (T_s T_{s*t})^{-1} = T_{s*t}^{-1}T_s^{-1} = T_{t*s}^{-1}T_t^{-1} = \tilde{\iota}(T_t T_{t*s})$.

This shows that $\tilde{\iota}$ is a well-defined anti-morphism $\mathcal{H}(S,P) \to \mathcal{H}(S,P)$.

It remains to show that $\tilde{\iota}$ is an involution. For this, we will show that $\tilde{\iota}(\tilde{\iota}(T_g))$ is an inverse of $\tilde{\iota}(T_g) = T_g^{-1}$, which will imply that $\tilde{\iota}(\tilde{\iota}(T_g)) = T_g$. As $\tilde{\iota}$ is an anti-morphism, we have $\tilde{\iota}(\tilde{\iota}(T_g))\tilde{\iota}(T_g) = \tilde{\iota}(T_g\tilde{\iota}(T_g)) = \tilde{\iota}(T_gT_g^{-1}) = \tilde{\iota}(1) = 1$. So $\tilde{\iota}(\tilde{\iota}(T_g)) = T_g$ by unicity of the inverse.

Moreover, by Theorem 2.8, $(T_g)_{g\in\overline{G}}$ is a basis of $\mathcal{H}(S,P)$. We conclude that $\tilde{\iota}$ is an anti-automorphism. Thus ι is an anti-involution. □

Remark 3.6. *In the above proof, one has to be careful that $T_g^{-1} \neq T_{g^{-1}}$ as mentioned in Remark 3.2. For instance, for the involutivity of $\tilde{\iota}$, it is not enough to write $\tilde{\iota}(\tilde{\iota}(T_g) = \tilde{\iota}(T_g^{-1}) = (T_g^{-1})^{-1} = T_g$. Indeed, for $g = s \in S$, we have $\tilde{\iota}(T_s^{-1}) = \sum_{k=1}^{l} \iota(\frac{-a_k}{a_0})\tilde{\iota}(T_{s*s}^{[kd-1]}) = \sum_{k=1}^{l} \iota(\frac{-a_k}{a_0})\tilde{\iota}(T_{s*s}^{[kd-1]})$, which does not so obviously simplify to T_s.*

Example 3.7. *Consider $R = \mathbb{Z}[q_1^{\pm 1}, \dots, q_l^{\pm 1}, c^{\pm 1}]$. Let $P(X) = c(X - q_1)\dots(X - q_l)$ which satisfies the hypothesis of the theorem. It is an analogue of the "generic Hecke algebra" of a Coxeter group ([17]).*

Taking as $S = \{s,t\}, \psi(s) = \psi(t) = 12$ with $P(X) = (X+1)(X-q) = X^2-(q-1)X-q$, we have $T_s^{-1} = \frac{1-q}{q}t^{[1]} + \frac{1}{q}t^{[3]}$.

We find $(T_s^{-1})^{[2]} = \frac{1}{q}T_t^{[2]} + \frac{1-q}{q}$ and $(T_s^{-1})^{[4]} = \frac{1-q}{q^2}T_t^{[2]} + \frac{q^2-q+1}{q^2}$.

Thus

$$(T_s^{-1})^{[4]} - (\frac{1}{q} - 1)(T_s^{-1})^{[2]} - \frac{1}{q} = 0$$

4. Semi-simplicity

This section is based on [8, 9, 17] and inspired from the lecture notes [12, 21]. For details on character theory we refer to [8]. In this section we fix a commutative integral domain R with field of fractions F, K a field with an algebraic closure $\overline{K}$, $f\colon R \to K$ a ring morphism. Let $\mathcal{H} = \mathcal{H}(S,\underline{P})$ be the Hecke algebra of a cycle set S, as in Remark 2.9, with $\underline{P} = (P_i)_{1\leq i\leq n} \in R[X]^n$, $P_i(X) = \sum_{i=0}^{l_i} a_{i,k}X^i$ such that $P_i = P_j$ whenever s_i and s_j are in the same $\mathcal{G}$-orbit. From Theorem 2.8, This algebra dimension is equal to the order of the quotient group $\overline{G}_{\underline{l}} = G/\langle s_i^{[l_i d]}\rangle$.

Definition 4.1. *Let A be a non-trivial K-algebra. Then A is called,*

(i) simple if it contains no proper two-sided ideal,
(ii) semi-simple if it is isomorphic to a direct sum of simple algebras,
(iii) separable if for any extension L/K, $L \otimes A$ is a semi-simple algebra,
(iv) split if it is semi-simple and it is isomorphic to a finite sum of matrix algebras over K.

An ideal I of an algebra is called nilpotent if there exists a positive integer n such that $I^n = 0$, i.e. any product of n elements of I is 0. The following proposition helps us characterizing semi-simple algebras:

Proposition 4.2 ([1, Section 9])**.** *Let A be a finite dimensional K-algebra. Then there exists a unique largest nilpotent two-sided ideal, called the radical of A and denoted rad(A).*

Moreover, the followings hold:

(i) rad(A) is the set of elements of A acting as 0 on every simple A-module (modules without proper submodules)
(ii) rad(A) is the intersection of all maximal left ideals of A

(iii) A is semi-simple if and only if rad$(A) = \{0\}$

In the literature $\mathrm{rad}(A)$ is also often called the Jacobson radical of A.

If A is a finite-dimensional K-algebra and a is an element of A, then we denote by $\mathrm{Tr}_{A/K}(a)$ the trace of the left-multiplication operator $A \to A$ defined by $b \mapsto ab$.

If L/K is a field extension, we denote by A^L the L-algebra $L \otimes A$.

Lemma 4.3 ([8])**.** *Let A be a finite dimensional K-algebra, L/K a field extension. Then for any a in A, $Tr_{A^L/L}(1 \otimes a) = Tr_{A/K}(a)$.*

Moreover, $Tr_{A^L/L}$ is equal to $id \otimes Tr_{A/K}$ defined by sending $l \otimes a$ to $l\,Tr_{A/K}(a)$.

Proof. Let (e_i) be a basis of A, so that $(1 \otimes e_i)$ is a basis of A^L. For a in A, write $ae_i = \sum_j c_{ij} e_i$, so that $\mathrm{Tr}_{A/K}(a) = \sum_i c_{ii}$. Then $(1 \otimes a)(1 \otimes e_i) = 1 \otimes ae_i = \sum_j c_{ij}(1 \otimes e_i)$, meaning that $\mathrm{Tr}_{A^L/L}(1 \otimes a) = \sum_i c_{ii} = \mathrm{Tr}_{A/K}(a)$.

Moreover, for any $x \in L$, we then have $(x \otimes a)(1 \otimes e_i) = \sum_j c_{ij}(x \otimes e_i) = \sum c_{ij} x(1 \otimes e_i)$. Thus $\mathrm{Tr}_{A^L/L}(x \otimes a) = x \sum_i c_{ii} = x\mathrm{Tr}_{A/K}(a)$. □

The following lemma will be useful to restrict to the base field K when studying the trace:

Lemma 4.4. *Let A be a finite-dimensional K-algebra such that the bilinear map $T \colon A \times A \to K$ defined by $T(a, b) = Tr_{A/K}(ab)$ is non-degenerate. Then for any field extension L/K the bilinear map $T^L \colon A^L \otimes A^L$ defined by $T^L((l_1 \otimes a), (l_2 \otimes b)) = Tr_{A^L/L}(l_1 l_2 \otimes ab)$ is non-degenerate.*

Proof. Let $l \otimes a \in L \otimes A$. As T is non-degenerate, there exists $b \in A$ such that $T(a, b) \neq 0$. Then, by Lemma 4.3, we have $T^L((l \otimes a), (1 \otimes b)) = T^L(l \otimes ab) = l\mathrm{Tr}_{A/K}(ab) \neq 0$. Thus T^L is non-degenerate. □

Proposition 4.5 ([8, Exercice 7.6])**.** *Let A be a finite dimensional K-algebra. If the bilinear form $T \colon A \times A \to K$ defined with the usual trace $T(a, b) = Tr_{A/K}(ab)$ is non-degenerate, then A is separable (and thus semi-simple).*

Proof. First we know that non-degeneracy is stable by field extension by Lemma 4.4.

So it is enough to show that A is semi-simple. As A is finite dimensional, by Proposition 4.2 A is semi-simple iff $\mathrm{rad}(A)$ is trivial. Also from Proposition 4.2, $\mathrm{rad}(A)$ is the largest nilpotent ideal, so any element in it has trivial trace (any element is nilpotent). Thus as $\mathrm{rad}(A)$ is an ideal, if $a \in \mathrm{rad}A$ then, for any $b \in A$ we have $ab \in \mathrm{rad}(A)$ and so $\mathrm{Tr}_{A/K}(ab) = 0$. If T is non-degenerate, this implies that $a = 0$, finishing the proof. □

Definition 4.6. *A trace over a K-algebra A is a map $\tau \colon H \to K$ such that $\tau(ab) = \tau(ba)$ for any a, b in K. A trace τ is said to be symmetrizing if the map $(a, b) \mapsto \tau(ab)$ is non-degenerate.*

The following statement is a generalization of Lemma 4.4:

Proposition 4.7 ([3, Proposition 8.7])**.** *If A is a finite-dimensional algebra over a field K and if τ is a symmetrizing trace over A that is a linear combination of characters, then A is separable.*

In particular, if $Tr_{A/K}$ is symmetrizing, then A is separable.

Corollary 4.8 ([12, Exemple 2.10])**.** *Let G be a group and K a field such that char(K) does not divide $|G|$. Then the map $\tau\colon K[G]\to K$ defined by $\tau(\sum_{g\in G} r_gT_g)=r_1$ (where T_g is the standard basis of $K[G]$) is a symmetrizing trace and $K[G]$ is separable.*

Proof. We have that $\tau(\sum_{g\in G} r_gT_g)(\sum_{h\in G} r'_hT_h)=\tau(\sum_{g,h\in G} r_gr'_hT_gT_h)=\sum_{g\in G} r_gr'_{g^{-1}}=\sum_{h\in G} r'_hr_{h^{-1}}$, so $\tau(ab)=\tau(ba)$. Moreover, $\tau(T_gT_g^{-1})=\tau(T_1)=1$, so $\tau((\sum_{g\in G} r_gT_g)T_h^{-1})=r_h$ is zero for every h if and only if $r_h=0$ for every $h\in G$. Thus τ is non-degenerate, and so it is indeed a symmetrizing trace.

Then, the trace of the algebra $K[G]$ is given on the basis (T_g) by

$$\mathrm{Tr}_{K[G]/K}(T_h\mapsto T_{gh})=\#\{h\mid T_{gh}=T_h\}=\begin{cases}\#G, \text{ if } g=1\\ 0, \text{ otherwise}\end{cases}=\#G\cdot\tau(T_g).$$

Thus $\mathrm{Tr}_{K[G]/K}=\#G\tau$, which is not zero as char K does not divide $\#G$. So $\tau=\frac{\mathrm{Tr}_{K[G]/K}}{\#G}$ is a linear combination of character and finally, by Proposition 4.7, $K[G]$ is separable. □

Our goal is to be able to apply the following theorem:

Theorem 4.9 ([9, Tits Deformation Theorem 68.17])**.** *Let A be a finite dimensional R-algebra, recall that we chose $F=Frac(R)$ and $f:R\to K$. If $K\otimes_R A$ and $F\otimes_R A$ (defined by f) are separable, then they have the same numerical invariants.*

Moreover, let $\overline{R}$ be an integral closure of R in $\overline{K}$ and $\overline{f}:\overline{R}\to\overline{K}$ be an extension of f. Then $\overline{f}$ induces a bijection of irreducible characters $Irr(\overline{K}\otimes A)\to Irr(\overline{F}\otimes A)$.

Theorem 4.10. *Let K be a field of characteristic p. Suppose that p does not divide d, and p does not divide l_i for any i (the degrees of each polynomial). Let $\underline{q}=(q_{i,k})_{1\le i\le n,0\le k\le l_i}$ be a family of indeterminates such that $q_{i,k}=q_{j,k}$ whenever s_i and s_j are in the same orbit and $P_i(X)=\sum_i a_{i,k}X^k\in K[\underline{q}][X]$. Then $K(\underline{q})\otimes\mathcal{H}(S,\underline{P})$ is separable and has the same numerical invariants as $K[\overline{G}_{\underline{l}}]$.*

Proof. Consider the context of Theorem 4.9 with $A=\mathcal{H}(S,\underline{P})$, $R=K[\underline{q}]$, $F=\mathrm{Frac}(R)=K(\underline{q})$. We define $f:R\to K$ by $f(q_{i,0})=f(q_{i,l_i})=1$ and otherwise $f(q_{i,k})=0$, so that the specialization given by f yields the algebra $K[\overline{G}_{\underline{l}}]=K[G]/(T_{s_i}^{[l_id]}-1)$.

First, by Corollary 4.8, $K\otimes A=K[G_{\underline{l}}]$ is separable when char(K) does not divide $\#\overline{G}_{\underline{l}}=\prod_{i=1}^{n}(l_id)$.

Then, as R is an integral domain, $F=\mathrm{Frac}(R)$ is a field, so $F\otimes A=K(\underline{q})\otimes\mathcal{H}(S,\underline{P})$. We want to show that $\mathrm{Tr}_{F\otimes A/F}$ is symmetrizing, so that we can apply 4.7 to have that $F\otimes A$ is separable. By Theorem 2.8, $(T_g)_{g\in\overline{G}_l}$ is a basis of $A=\mathcal{H}(S,\underline{P})$. So $(1\otimes T_g)$ is a basis of $F\otimes A$. Moreover, $\mathrm{Tr}_{F\otimes A/F}$ specializes to $\mathrm{Tr}_{K[\overline{G}_{\underline{l}}]/K}$, which is symmetrizing by Corollary 4.8. We have $\mathrm{Tr}_{F\otimes A/F}((1\otimes T_g)(1\otimes T_h))=\mathrm{Tr}_{F\otimes A/F}(1\otimes T_gT_h)=1\otimes\mathrm{Tr}_{A/K}(T_gT_h)$ by Lemma 4.3. As $\mathrm{Tr}_{A/K}$ specializes to $\mathrm{Tr}_{K[\overline{G}_{\underline{l}}]/K}$ which is non-degenerate, $\mathrm{Tr}_{F\otimes A/F}$ is also non-degenerate and thus symmetrizing.

The conditions of Theorem 4.9 are satisfied, meaning that $F\otimes A=K(\underline{q})\otimes\mathcal{H}(S,\underline{P})$ and $K\otimes A=K[\overline{G}_{\underline{l}}]$ have the same numerical invariants. □

Corollary 4.11. *If $\mathcal{H}(S,\underline{P})$ is defined over $\mathbb{C}[\underline{q}]$, then $\mathbb{C}(\underline{q})\otimes\mathcal{H}(S,\underline{P})$ and $\mathbb{C}[\overline{G}_{\underline{l}}]$ have the same numerical invariants.*

Moreover, we have a bijection $Irr(\mathbb{C}[\overline{G}_{\underline{l}}])\to Irr\Big(\overline{\mathbb{C}(\underline{l})}\otimes\mathcal{H}(S,\underline{P})\Big)$.

Proof. We apply Theorem 4.9 with: $R = \mathbb{C}[\underline{q}]$, $A = \mathcal{H}(S, \underline{P})$, $F = \mathbb{C}(\underline{q})$, $K = \mathbb{C} = \overline{K}$ and $K \otimes A = \mathbb{C}[\overline{G}_{\underline{l}}]$. Theorem 4.10 already tells us that $\mathbb{C}(\underline{q}) \otimes \mathcal{H}(S, \underline{P})$ and $\mathbb{C}[\overline{G}_{\underline{l}}]$ have the same numerical invariants. Moreover, as $K = \mathbb{C} = \overline{K}$, the last part of Theorem 4.9 says that the specialization $\mathcal{H}(S, \underline{P}) \to \mathbb{C}[\overline{G}_{\underline{l}}]$ induces a bijection $\mathrm{Irr}(\mathbb{C}[\overline{G}_{\underline{l}}]) \to \mathrm{Irr}(\overline{\mathbb{C}(\underline{l})} \otimes \mathcal{H}(S, \underline{P}))$. □

5. Two-generated Cyclic group

At the beginning of Section A, we mentioned how the naive definition of a Hecke algebra does not work in general, and we developed a different approach that provides the expected results. However, we also mentioned that the naive approach does work for a very particular solution of size. For this solution, the structure group is $\langle a, b \mid a^2 = b^2 \rangle$ and the germ is $\langle a, b \mid a^2 = b^2, ab = ba = 1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ with algebra $R\langle T_a, T_b \mid T_a^2 = T_b^2, T_aT_b = T_bT_a = p(T_a + T_b) + q \rangle$ with some p, q in R. The goal of this section is to prove that in this particular case, the Hecke algebra has a basis indexed by the germ.

Moreover, we study a family of groups for which this approach works: torus knot group, which are the only knot groups (fundamental groups of complements of knots in the 3-sphere) which are Garside groups ([11, 19, 18]). For n and m integers strictly greater than 1, the n, m-torus knot monoid (resp. group) is defined by the presentation $\mathcal{T}_{n,m} = \langle a, b \mid a^n = b^m \rangle$, and has as a Garside element $\Delta = a^n = b^m$.

The goal of this section is to show that $\mathcal{T}_{n,m}$ has a Garside germ given by $\overline{\mathcal{T}_{n,m}} = \mathcal{T}_{n,m}/\langle ab = ba = 1 \rangle \simeq \mathbb{Z}/(n+m)\mathbb{Z}$, and show that we have a Hecke algebra $\mathcal{H}_{n,m}(p, q) = R\langle T_a, T_b \mid T_a^n = T_b^m, T_aT_b = T_bT_a = p(T_a + T_b) + q \rangle$, i.e. that $(T_g)_{g \in \overline{\mathcal{T}_{n,m}}}$ is a basis of $\mathcal{H}_{n,m}(p, q)$.

Proposition 5.1. *$\mathcal{T}_{n,m}$ is a Garside group with germ $\overline{\mathcal{T}_{n,m}} \cong \mathbb{Z}/(n+m)\mathbb{Z}$.*

Proof. It is shown in [11, Example 4] that, with the given presentation, $\mathcal{T}_{n,m}$ is a Garside group, with a Garside element $\Delta = a^n = b^m$ and

$$\mathrm{Div}(\Delta) = \{1, a, \dots, a^n = b^m, b^{m-1}, b^{m-2}, \dots, b\}.$$

The additive length $\ell \colon \mathcal{T}_{n,m} \to \mathbb{N}$ can be obtained by setting $\ell(a) = m, \ell(b) = n$, so that $\ell(a^n) = nm = \ell(b^m)$.

On the other hand,

$$\begin{aligned}\overline{\mathcal{T}_{n,m}} &\simeq \langle \overline{a}, \overline{b} \mid \overline{a}^n = \overline{b}^m, \overline{a}\overline{b} = \overline{b}\overline{a} = 1 \rangle \simeq \langle \overline{a}, \overline{b} \mid \overline{a}^n = \overline{b}^m, \overline{a} = \overline{b}^{-1} \rangle \simeq \langle \overline{a} \mid \overline{a}^n = \overline{a}^{-m} \rangle \\ &\simeq \mathbb{Z}/(n+m)\mathbb{Z} = \{1, \overline{a}, \dots, \overline{a}^n = \overline{b}^m, \overline{b}^{m-1}, \overline{b}^{m-2}, \dots, \overline{b}\}.\end{aligned}$$

Thus we have a bijection $\mathrm{Div}(\Delta) \to \overline{\mathcal{T}_{n,m}}$ sending a (resp. b) to $\overline{a}$ (resp. $\overline{b}$).

Let $\overline{\ell}$ be the induced map of ℓ in $\overline{\mathcal{T}_{n,m}}$, i.e. $\overline{\ell}(\overline{a}) = m, \overline{\ell}(\overline{b}) = n$.

To show that $\overline{\mathcal{T}_{n,m}}$ is a Garside germ of $\mathcal{T}_{n,m}$, we need to show that

$$\mathcal{T}_{n,m} \cong \langle \overline{\mathcal{T}_{n,m}} \mid \forall g, h \in \overline{\mathcal{T}_{n,m}}, g \cdot h = gh \text{ when } \overline{\ell}(gh) = \overline{\ell}(g) + \overline{\ell}(h) \rangle.$$

We will prove the isomorphism by showing that the presentation on the right reduces to the presentation of $\mathcal{T}_{n,m}$ as $\langle a, b \mid a^n = b^m \rangle$.

As $\{\overline{a}, \overline{b}\} \subset \overline{\mathcal{T}_{n,m}}$, $\overline{\mathcal{T}_{n,m}}$ generates $\mathcal{T}_{n,m}$. Now for the relations, we have to consider the products $\overline{a}^i\overline{a}^j, \overline{b}^i\overline{b}^j$ and $\overline{a}^i\overline{b}^j$:

We have $\overline{\ell}(\overline{a}^i) + \overline{\ell}(\overline{a}^j) = im + jm = (i+j)m$ for $1 \leq i, j \leq n$. If $i + j \leq n$, then $\overline{\ell}(\overline{a}^i\overline{a}^j) = \overline{\ell}(\overline{a}^{i+j}) = (i+j)m$. Thus we can omit $\overline{a}^i$ for $2 \leq i \leq n$ from the generators. The same holds for $\overline{b}^j$, as $\overline{\ell}(\overline{b}^i) + \overline{\ell}(\overline{b}^j) = in + jn = (i+j)n = \overline{\ell}(\overline{b}^{i+j})$, if $i + j \leq m$. Thus we can omit $\overline{b}^i$ for $2 \leq i \leq m$ from the generators. The particular case of $\overline{b}\overline{b}^{m-1} = \overline{b}^m = \overline{a}^n$ with $\overline{\ell}(\overline{b}^m) = nm = \overline{\ell}(\overline{a}^n)$ recovers the relation $\overline{a}^n = \overline{b}^m$.

However, the longest length in $\overline{\mathcal{T}_{n,m}}$ is $\overline{\ell}(\overline{a}^n) = \overline{\ell}(\overline{b}^m) = nm$. So if $i+j > n$, $\overline{\ell}(\overline{a}^i)+\overline{\ell}(\overline{a}^j) = in + jn = (i+j)m > nm$, so there is no relation for this case. The same also holds for $\overline{b}$ whenever $i + j > m$.

Finally, $\overline{\ell}(\overline{a}^i) + \overline{\ell}(\overline{b}^j) = im + jn$ for $1 \leq i \leq n, 1 \leq j \leq m$. But $\overline{a} = \overline{b}^{-1}$, so $\overline{\ell}(\overline{a}^i\overline{b}^j) = \begin{cases} \overline{\ell}(\overline{a}^{i-j}) = (i-j)m, & \text{if } i \geq j \\ \overline{\ell}(\overline{b}^{j-i}) = (j-i)n, & \text{if } i < j \end{cases}$. In both cases this is smaller than $im + jn$, so there is no relation.

From this, we conclude that the only relation left that occurs from $\overline{\mathcal{T}_{n,m}}$ is $\overline{a}^n = \overline{b}^m$, showing the desired result. □

Now consider $\mathcal{H}_{n,m}(p,q) = R\langle T_a, T_b \mid T_a^n = T_b^m, T_aT_b = T_bT_a = p(T_a + T_b) + q\rangle$ for some p, q in R.

Lemma 5.2. *The followings hold:*

(i) In $\mathcal{H}_{n,m}(p,q)$ we have,

(a) $T_aT_b^k = p^{k-1}q + p^kT_a + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}T_b^i + pT_b^k$, for $1 \leq k \leq m$

(b) $T_bT_a^k = p^{k-1}q + p^kT_b + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}T_a^i + pT_a^k$, for $1 \leq k \leq n$

(ii) $(T_g)_{g\in\overline{\mathcal{T}_{n,m}}}$ generates $\mathcal{H}_{n,m}(p,q)$

Proof. For (i) we proceed by induction on k. If $k = 1$, then $T_aT_b = q+pT_a+pT_b = p^{1-1}q+p^1T_a + pT_b^1$ (and the sum is empty). Now assume the equality holds for some $1 \leq k < m$, then we have $T_aT_b^{k+1} = (T_aT_b^k)T_b = (p^{k-1}q + p^kT_a + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}T_b^i + pT_b^k)T_b = p^{k-1}qT_b + p^kT_aT_b + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}T_b^{i+1} + pT_b^{k+1}$. We have $p^kT_aT_b = p^k(pT_a + pT_b + q) = p^{k+1}T_a + p^{k+1}T_b + p^kq$ and we can rewrite $\sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}T_b^{i+1} = \sum_{i=2}^{k}(p^2+q)p^{(k+1)-i-1}T_b^i$. Thus, rearranging the terms, we obtain $T_aT_b^{k+1} = p^kq + p^{k+1}T_a + p^{k-1}qT_b + p^{k+1}T_b + \sum_{i=2}^{k}(p^2+q)p^{(k+1)-1-i}T_b^i + pT_b^{k+1} = p^kq + p^{k+1}T_a + \sum_{i=1}^{k}(p^2+q)p^{(k+1)-i-1}T_b^i + pT_b^{k+1}$. A totally symmetric argument holds for $T_bT_a^k$.

For (ii), we can use that $T_a^{n+1} = T_aT_a^n = T_aT_b^m$ (resp. $T_b^{m+1} = T_bT_b^m = T_bT_a^n$) and the apply the relations of (1) to reduce terms of high enough exponents. Thus, with the relations of (1), any product of generators can be reduced to linear combinations of the family $(T_g)_{g\in\overline{\mathcal{T}_{n,m}}}$. □

Theorem 5.3. *The family $(T_g)_{g\in\overline{\mathcal{T}_{n,m}}}$ is a basis of $\mathcal{H}_{n,m}(p,q)$. In particular $\mathcal{H}_{n,m}(p,q)$ has dimension $n+m$.*

The proof will follow a common strategy for Hecke algebra of finite Coxeter groups, see [17, Theorem 4.4.6].

Proof. Consider E the free R-module with basis $(e_g)_{g\in\overline{\mathcal{T}_{n,m}}}$. We are going to show that we have an action of $\mathcal{H}_{n,m}(p,q)$ over E induced by $T_ge_1 = e_g$ and this will be enough. Indeed, assuming we have a linear combination $\sum_{g\in\overline{\mathcal{T}_{n,m}}} r_gT_g = 0$ then $0 = (\sum_{g\in\overline{\mathcal{T}_{n,m}}} r_gT_g)e_1 = \sum_{g\in\overline{\mathcal{T}_{n,m}}} r_ge_g$ and since E is free over (e_g) we deduce that $r_g = 0$ for all g.

We define the following action of $\overline{\mathcal{T}_{n,m}}$ on E, and show that it induces an action of $\mathcal{H}_{n,m}(p,q)$ on E:

- $T_a e_{a^k} = e_{a^{k+1}}$, for $0 \leq k \leq n-1$
- $T_a e_{b^k} = p^{k-1} q e_1 + p^k e_a + \sum_{i=1}^{k-1} (p^2+q) p^{k-i-1} e_{b^i} + p e_{b^k}$, for $1 \leq k \leq m$
- $T_b e_{b^k} = e_{b^{k+1}}$, for $0 \leq k \leq m-1$
- $T_b e_{a^k} = p^{k-1} q e_1 + p^k e_b + \sum_{i=1}^{k-1} (p^2+q) p^{k-i-1} e_{a^i} + p e_{a^k}$, for $1 \leq k \leq n$

In particular, $T_a e_{a^n} = T_a e_{b^m} = p^{m-1} q e_1 + p^m e_a + \sum_{i=1}^{m-1} (p^2+q) p^{m-i-1} e_{b^i} + p e_{b^m}$.

We will to show that this action respect the defining relations of $\mathcal{H}_{n,m}(p,q)$.

To verify that the action is compatible with the relation $T_a T_b = p(T_a + T_b) + q$, we only need to consider the cases of $T_a T_b e_{b^k}$ and $T_a T_b e_{a^k}$, as the cases of $T_b T_a e_{b^k}$ and $T_b T_a e_{a^k}$ are obtained by symmetry. First assume that $k < m$, then, on one hand, $T_a T_b e_{b^k} = T_a e_{b^{k+1}} = p^k q e_1 + p^{k+1} e_a + \sum_{i=1}^{k} (p^2+q) p^{k-i} e_{b^i} + p e_{b^{k+1}}$. On the hand, $(pT_a + pT_b + q) e_{b^k} = pT_a e_{b^k} + q e_{b^k} + p e_{b^{k+1}} = p^k q e_1 + p^{k+1} e_a + \sum_{i=1}^{k-1} (p^2+q) p^{k-i} e_{b^i} + p^2 e_{b^k} + q e_{b^k} + p e_{b^{k+1}}$ and those are easily seen to be equal by just noticing $p^2 e_{b^k} + q e_{b^k} = (p^2+q) p^{k-k} e_{b^k}$.

Then, for $k < n$, we have $T_a T_b e_{a^k} = T_a (p^{k-1} q e_1 + p^k e_b + \sum_{i=1}^{k-1} (p^2+q) p^{k-i-1} e_{a^i} + p e_{a^k}) = p^{k-1} q e_a + p^k T_a e_b + \sum_{i=1}^{k-1} (p^2+q) p^{k-i-1} e_{a^{i+1}} + p e_{a^{k+1}}$ and a bit of rearranging the terms (and changing indices of sum) show that this is equal to $T_b e_{a^{k+1}} = T_b T_a e_{a^k}$ which, again by symmetry, finishes the case $k < n$.

Now for $k = m$ we have $T_a T_b e_{b^m} = T_a T_b e_{a^n} = T_a (p^{n-1} q e_1 + p^n e_b + \sum_{i=1}^{n-1} (p^2+q) p^{n-i-1} e_{a^i} + p e_{a^n})$, so

$$T_a T_b e_{b^m} = p^{n-1} q e_a + p^n T_a e_b + \sum_{i=1}^{n-1} (p^2+q) p^{n-i-1} e_{a^{i+1}} + p T_a e_{a^n}. \tag{6}$$

On the other hand,

$$(pT_a + pT_b + q) e_{b^m} = pT_a e_{b^m} + pT_b e_{b^m} + q e_{b^m}. \tag{7}$$

The last term of Equation (6) and the first term of Equation (7) match, as $a^n = b^m$. So we have to show

$$p^{n-1} q e_a + p^n T_a e_b + \sum_{i=1}^{n-1} (p^2+q) p^{n-i-1} e_{a^{i+1}} = pT_b e_{b^m} + q e_{b^n}.$$

On the left we expand $T_a e_b$ and on the right we expand $T_b e_{b^n} = T_b e_{a^n}$, where we respectively obtain

$$p^n q e_1 + p^{n+1} e_b + \sum_{i=1}^{n} (p^2+q) p^{(n+1)-i-1} e_{a^i}$$

and

$$p^n q e_1 + p^{n+1} e_b + \sum_{i=1}^{n-1} (p^2+q) p^{(n+1)-i-1} e_{a^i} + p^2 e_{a^n} + q e_{a^n}$$

which also match as $(p^2+q) e_{a^n} = (p^2+q) p^{(n+1)-n-1} e_a^n$.

For $T_b T_a e_{b^m}$ the computation is totally similar.

Then we can easily deduce that the relation $T_a^n = T_b^m$ is compatible with the action:

$$T_a^n e_{a^k} = T_a^k e_{a^n} = T_a^k e_{b^m} = T_a^k T_b^m e_1 = T_b^m T_a^k e_1 = T_b^m e_{a^k}$$

The first equality is obtained by $T_a e_{a^k} = e_{a^{k+1}}$ for $k < n$. The second one by $a^n = b^m$. The third equality is obtained by $T_b e_{b^k} = e_{b^{k+1}}$ for $k < m$. The fourth one follows from the fact that we've shown that $T_a T_b = T_b T_a$ is respected by the action.

Similarly, we have

$$T_a^n e_{b^k} = T_a^n T_b^k e_1 = T_b^k T_a^n e_1 = T_b^k e_{a^n} = T_b^k e_{b^m} = T_b^m e_{b^k}.$$

Showing that the action of $\mathcal{H}_{n,m}(p,q)$ on E is well-defined, and thus finishing the proof. □

We finish this section by relating this result with a well-known theory for Complex reflection groups (CRG), following [25]:

Definition 5.4. *Let V be a complex vector space of finite dimension r.*

A pseudo-reflection is a non-trivial element of $GL(V)$ that fixes an hyperplane in V.

A complex reflection group of rank r is a finite subgroup of $GL(V)$ generated by pseudo-reflections. Moreover, a complex reflection group is called irreducible if it does not stabilize any proper subspace of V.

The classification of all irreducible complex reflection groups was obtained by Shephard and Todd in [28], involving an infinite family $G(de, e, r)$ with d, e, r positive integers, and 34 exceptional cases $G_4, G_5, \ldots, G_{37}$. Moreover, the family of complex reflection groups whose elements are real matrices correspond to finite Coxeter groups. Thus, they are often seen as a natural generalization of finite Coxeter groups.

In [25], the authors give a topological definition of the Hecke algebra of a CRG. The authors then show that for the infinite family $G(de, e, r)$, the Hecke algebra admits a presentation with generators T_s associated to the pseudo-reflections generating the CRG, and relations of two types: "braid-like" relations, and relations of the form $(T_s - u_{s,0})(T_s - u_{s,1}) \cdots (T_s - u_{s,e_s})$ for some integer e_s.

As in the section we focused on the Garside group $\mathcal{T}_{n,m}$ of rank 2 with germ $\overline{\mathcal{T}_{n,m}} \cong \mathbb{Z}/(n+m)\mathbb{Z}$, we provide the statement of [25] for the case $G(k,1,1) \cong \mathbb{Z}/k\mathbb{Z}$:

Theorem 5.5 ([25, Propositions 4.22-4.24])**.** *For the Hecke algebra of $C_k \coloneqq \mathbb{Z}/k\mathbb{Z}$ we have*

$$\mathcal{H}(C_k) \cong \mathbb{Z}[u_1, \ldots, u_k] \left\langle T \mid (T-u_1)(T-u_2)\cdots(T-u_k) = 0 \right\rangle .$$

The specialization of u_j at $\exp\left(j\frac{2i\pi}{k}\right)$ induces a morphism $\mathcal{H}(C_k) \to \mathbb{C} \otimes \mathbb{Z}[C_k]$.

Moreover, $\mathcal{H}(C_k)$ is free of rank k, with basis $\{1, T, T^2, \ldots, T^{k-1}\}$.

Remark 5.6. *It was remarked by Loïc Poulain-d'Andecy ([23]) that, if $R = \mathbb{Z}$, then $\mathcal{H}_{n,m}(p,q)$ is a specialization of $\mathcal{H}(C_{n+m})$. Indeed, by Proposition 5.1 we have a bijection between their respective basis given by $T \mapsto T_a$ and $T^{n+m-1} \mapsto T_b$. The relation $T_a T_b = p(T_a + T_b) + q$ can then be rewritten as $T^{n+m} = pT^{n+m-1} + pT + q$. Taking a specialization of $(u_1, \ldots, u_k)$ at the complex roots of $X^{n+m} - pX^{n+m-1} - pX - q \in \mathbb{Z}[X]$ then induces a specialization $\mathcal{H}(C_{n+m}) \to \mathcal{H}_{n,m}(p,q)$.*

Appendix A. Finding the correct definition via a diagrammtic approach

The first attempts to adapt the definition from Artin–Tits groups to Yang–Baxter structure groups would be to quotient $R[G]$ by something of the form $T_{s^{[d]}} = a_{d-1}T_{s^{[d]}} + \cdots + a_1 T_s + a_0$. However, apart from a specific case mentioned in the following sections (the unique non-trivial solution of size 2), this does not really work. Using the GAP package *GBNP* to compute a non-commutative Gröbner Basis, shows that such quotient won't have the correct dimension (it collapses, almost always identifying all generators). For instance, the GAP code in Program 1 checks, for a chosen cycle set of both size and class 3, that no intuitive definition works.

```
#Setup
LoadPackage("GBNP");
A:=FreeAssociativeAlgebraWithOne(Integers,"a","b","c");
gens:=GeneratorsOfAlgebra(A);
e:=gens[1];a:=gens[2];b:=gens[3];c:=gens[4];
q:=100;
#Construct all subsets of elements of length < 3
words:=[e,a,b,c,a*a,a*b,b*b,b*c,c*a,c*c];
comb:=Combinations(words);
Remove(comb,1);
sComb:=String(comb);
sComb:=ReplacedString(ReplacedString(
        sComb,"(1)*",""),"<identity ...>","e");
sCombx:=ReplacedString(ReplacedString(
        ReplacedString(sComb,"a","x"),"b","y"),"c","z");
sCombB:=ReplacedString(ReplacedString(
        ReplacedString(sCombx,"x","b"),"y","c"),"z","a");
sCombC:=ReplacedString(ReplacedString(
        ReplacedString(sCombx,"x","c"),"y","a"),"z","b");
combA:=EvalString(sComb);
combB:=EvalString(sCombB);
combC:=EvalString(sCombC);
l:=Length(combA);
#Compute dimensions of each quotient algebras
for i in [1..l] do
Print("\r              ");
Print(i,"/",l);
x:=combA[i];y:=combB[i];z:=combC[i];
rels:=[a*c-b*b,b*a-c*c,c*b-a*a,
        a*b*c-(q-1)*Sum(x)-q*e,b*c*a-(q-1)*Sum(y)-q*e,
        c*a*b-(q-1)*Sum(z)-q*e];
KI:=GP2NPList(rels);
GB:=SGrobner(KI);
if DimQA(GB,0)=27 then
Print("\n");
Print(Sum(x));
Print("\n");
Print(Sum(y));
Print("\n");
Print(Sum(z));
Print("\n");
PrintNPList(GB);
Print("\n");
fi;
od;
```

Program 1. Checking dimensions of quotient algebras

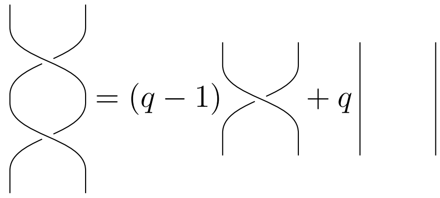
To do this verification for $S = \{s, t, u\}, \psi(s) = \psi(t) = \psi(u) = (stu) = \sigma$, we consider all relations of the form

$$T_{s^{[d]}} = 2T_1 + \sum_{\substack{g \in \overline{G} \\ 1 \leq \ell(g) \leq 2}} a_{s,g} T_g, \quad a_{s,g} \in \{0, 1\} \subset \mathbb{Q}$$

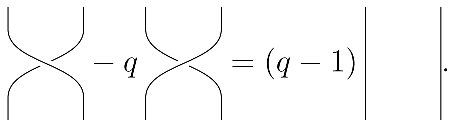
and $T_{t^{[d]}} = \sigma(T_{s^{[d]}})$,$T_{u^{[d]}} = \sigma^2(T_{s^{[d]}})$ to retain the symmetry. Note that we chose a particular specialization of the coefficients a_i, as we expect the definition of the Hecke algebra to work for all specializations. We then use the *GBNP* package functions to compute the size of the quotient algebra (deduced from a non-commutative Gröbner basis). We are interested in quotient algebras which are free of rank $\#\overline{G} = 3^3 = 27$, so that we can have $(T_g)_{g \in \overline{G}}$ as a basis. The only relation for which this happen is $T_{s^{[d]}} = 2T_1$, i.e. a non-interesting deformation of the group ring $\mathbb{Z}[\overline{G}]$. It is also worth to note that, in most cases, the quotient is small to the point that the generators $(T_s)_{s \in S}$ are identified.

This was tested for many small solutions, in particular the cyclic solutions such that $\psi(S) = \sigma \in \mathfrak{S}_n$, leading to the alternative approach of Section 5. Thus the approach had to be changed, and we are going to give a brief idea on how the current one was obtained. The following approach was inspired by a talk given by L. Poulain d'Andecy in Caen [24].

For the Braids groups B_n, whose Coxeter groups are $\mathfrak{S}_n$ (of type A_{n-1}), the generic Iwahori–Hecke algebra can be defined by the diagrammatic relations as follows:



which can also be written as



Intuitively, this means that we are "mostly" interested in the permutation associated to the braid, which is related to the fact that the Coxeter group is $\mathfrak{S}_n$. In what follows, we will explain the diagrammatical construction which gives the intuition of a "good" definition of Hecke algebra.

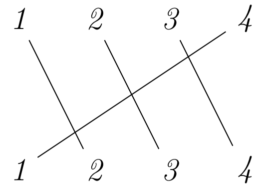
Definition A.1. *Let n be a positive integer. Consider the $2n$ points in $\mathbb{R}^2$ with coordinates $(1, 0), \ldots, (n, 0)$, $(1, 1), \ldots (n, 1)$. A family of n curves $(C_i \colon [0, 1] \to \mathbb{R}^2)_{1 \leq i \leq n}$ is called a n-strand permutation diagram if there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $C_i(0) = (i, 1)$ and $C_i(1) = (\sigma(i), 0)$.*

In this case, C_i is called the i-th strand.

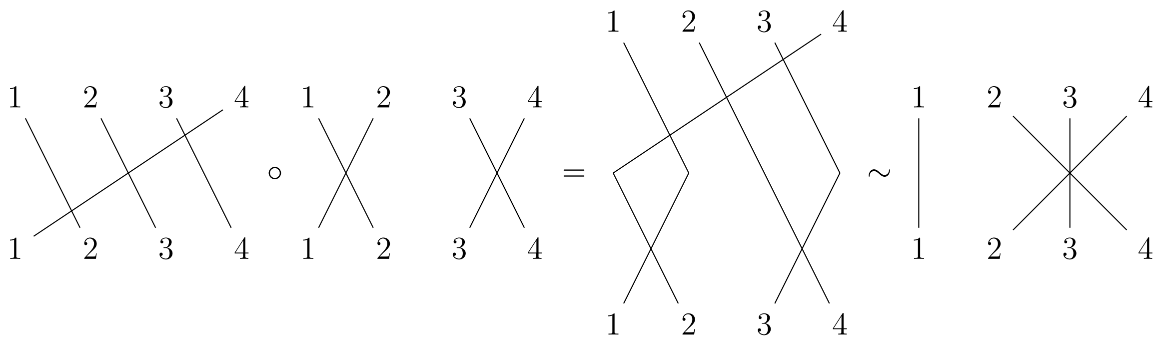
The inverse of σ will be called the permutation associated to the diagram. Equivalently, the associated permutation can be read as the permutation obtained looking at the diagram from bottom to top.

Two such diagrams are said to be equivalent if they define the same permutation.

Example A.2. *The following is a 4-strand permutation diagram with associated permutation* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$*:*



If we have two n-strand permutation diagrams, we can stack one on top of the other to obtain a new one (after rescaling vertically). This is illustrated in this example:



The associated permutation of the first (resp. second) diagram in the product is given by $(1234)^{-1} = (4321)$ (resp. $((12)(34))^{-1} = (12)(34)$). And the permutation of their stacking is $(24)^{-1} = (24)$, which is also equal to $(4321) \circ (12)(34)$. The fact that the permutation of the stacking is the product of the permutation holds in general, as indicated by the following:

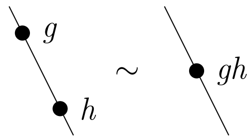
Proposition A.3. *There is an isomorphism between the group of n-strand permutation diagrams up to equivalence and $\mathfrak{S}_n$.*

Proof. Consider the stacking of two diagrams with associated permutations respectively σ and τ. The first diagram sends i to $\sigma(i)$, and the second one sends $\sigma(i)$ to $\tau(\sigma(i)$. So we obtain that the permutation of the stacking is the product of the permutation. This implies that, when considering diagrams up to equivalence (defining the same permutation), the stacking operation is a group law: associativity is clear, the identity is the equivalence class of diagrams with trivial permutation, and inverses are given by the equivalence class of diagram with the inverse permutation. In other words, the map sending a diagram to its associated permutation is a morphism.

Moreover, diagrams are considered up to the equivalence relation of defining the same permutation. Thus there is a unique equivalence class of diagrams with trivial permutation, and so this morphism is an isomorphism. □

Definition A.4. *Let Γ be a group. A Γ-marked permutation diagram is a permutation diagram where strands can be marked anywhere by elements of Γ. There can be multiple ordered elements for one strand. Moreover, a marking by $1 \in \Gamma$ is considered equivalent to no marking.*

Two markings of one strand are equivalent if they are identified by the group law as follows:

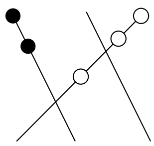


Example A.5. *We will later focus on $\mathbb{Z}$ and $\mathbb{Z}/d\mathbb{Z}$ markings. As those groups are cyclic, we can simplify the markings:*

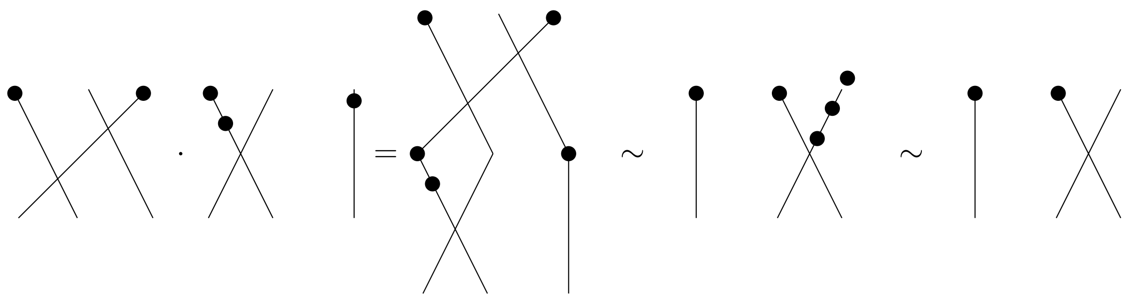
For $\mathbb{Z}$, associate to $+1$ the marking by $\bullet$ and to -1 the marking by $\circ$. A marking by a positive integer n then corresponds to n markings by $\bullet$, and similarly for negative integers with $\circ$.

For $\mathbb{Z}/d\mathbb{Z}$, we will only consider markings by $\bullet$ which corresponds to the class of $+1$.

The following is a $\mathbb{Z}$-marked 3-strand permutation diagram, where the strand 1 to 3 are respectively marked by 2, 0 and -3:



Remark A.6. *We can always move all the markings to the top (or bottom) of a strand. This also applies when stacking two diagrams, as illustrated in the following for $\mathbb{Z}/3\mathbb{Z}$-marked 3-strand permutation diagrams:*



where the equality is the stacking operation, the first equivalence is the equivalence of permutation diagram, and the second equivalence is the fact that we have a $\mathbb{Z}/3\mathbb{Z}$-marking (so $\bullet\bullet\bullet = 3\bullet = 0$)

Consider the action of $\mathfrak{S}_n$ on G^n by permuting the entries, i.e. σ sends the i-th entry to the $\sigma(i)$-th one, or, equivalently, $\sigma \cdot (g_1, \ldots, g_n) = (g_{\sigma^{-1}(1)}, \ldots, g_{\sigma^{-1}(n)})$.

Proposition A.7. *The group of Γ-marked n-strand permutation group is isomorphic to $\Gamma^n \rtimes \mathfrak{S}_n$, where $\mathfrak{S}_n$ acts by permuting the entries of Γ^n.*

Proof. Let $(g_1, \ldots, g_n, \sigma)$ be an element of $\Gamma^n \rtimes \mathfrak{S}_n$. Consider the map f sending such an element to the permutation diagram associated to σ and where the i-th strand is marked by g_i.

We have $f\left((g_1, \ldots, g_n, \sigma)(h_1, \ldots, h_n, \tau)\right) = f(g_1 h_{\sigma^{-1}(1)}, \ldots, g_n h_{\sigma^{-1}(n)}, \sigma\tau)$.

On the other hand, when stacking $f\left((g_1, \ldots, g_n, \sigma)\right)$ and $f\left((h_1, \ldots, h_n, \tau)\right)$ from bottom to top. The permutation associated to this diagram is $\sigma\tau$ by Proposition A.3. Moreover, the top diagrams has an i-th strand that is followed by the $\sigma^{-1}(i)$-th strand of the second diagram. Thus, the markings on the i-th strand of the diagram after stacking is $g_i h_{\sigma^{-1}(i)}$. From this, we deduce that f is a morphism.

Now, $f((g_1, \dots, g_n, \sigma))$ is trivial if and only if the diagram has trivial permutation and markings, so $\sigma = \mathrm{id}$ and $g_1 = \cdots = g_n = 1$. This means that f is injective.

Finally, consider a diagram with associated permutation σ and markings $g_1, \dots, g_n$. By the definition of f, the given diagram is equal to $f(g_1, \dots, g_n, \sigma)$, meaning that f is surjective. Thus f is an isomorphism. □

We can finally arrive at a diagrammatical representation of structure groups and germs of solutions, which corresponds to the I-structure of [14, 16] and Theorem 1.15.

Theorem A.8. *Let S be a cycle set of size n and class d. Then its structure group G (resp. germ $\overline{G}_l$) is isomorphic to a subgroup of $\mathbb{Z}$-marked (resp. $\mathbb{Z}/ld\mathbb{Z}$-marked) n-strand permutation diagrams. Moreover, an element is uniquely determined by its marking as a diagram.*

Proof. By Theorem 1.15, we know that G embeds as a subgroup of $\mathbb{Z}^n \rtimes \mathfrak{S}_n$ such that restricting to the first coordinate is bijective. Theorem 1.16 gives a similar embedding of $\overline{G}_l$ in $(\mathbb{Z}/ld\mathbb{Z})^n \rtimes \mathfrak{S}_n$. In both cases, we then apply Proposition A.7 to conclude. □

Remark A.9. *A way to interpret the quotient $G \to \overline{G}_l$ through the diagram is to visualize the strands as having thickness in 3-dimensions, and consider the markings as twists. In G, a marking as $\bullet = +1 \in \mathbb{Z}$ can be seen as a twists by $\frac{2\pi}{ld}$. Then, quotienting to $\overline{G}_l$ amounts to considering a full twist as trivial.*

Now going back to the analogy with Artin–Tits group, where the focus to obtain the Iwahori–Hecke algebra was the permutation associated to a braid. Here the permutation of the braid is an obstacle when we only care about the number of circles/twists (the Γ^n part). This is why we will consider deformations which only involves elements with trivial permutation. so in our case using $s^{[d]}$. For instance, the analogue of $s^2 = (q-1)s + q$ will be ${s^{[d]}}^2 = (q-1)s^{[d]} + q$ (where $(s^{[d]})^2 = s^{[2d]}$). This means we will consider bigger germs, like here $\overline{G}_2 = G/\langle s^{[2d]} \rangle$ to be able to obtain a Hecke algebra.

The visualization through marked permutation diagrams allows us to understand an important difference between the Garside structures of Artin–Tits groups and Structure groups of solutions to the Yang–Baxter equation. In particular, it yields the intuition on why the "correct" definition will involve elements with trivial permutation.

References

[1] N. Bourbaki. “Chapter VIII Semisimple Modules and Rings”. *Algebra: Chapter 8.* Ed. by N. Bourbaki. Cham: Springer International Publishing, 2022, 1–467.

[2] N. Bourbaki. *Groupes et algébras de Lie (Tome 4,5 et 6).* Berlin, Heidelberg: Springer, 2007.

[3] M. Broué. “Reflection Groups, Braid Groups, Hecke Algebras, Finite Reduction Groups”. *Curr. Dev. in Math.* 2000.1 (2000), 1–107.

[4] F. Cedó. “Left Braces: Solutions of the Yang-Baxter Equation”. *Advances in Group Theory and Applications* 5 (2018), 33–90.

[5] F. Cedó, E. Jespers, and J. Okniński. “Braces and the Yang–Baxter Equation”. *Commun. Math. Phys.* 327.1 (2014), 101–116.

[6] F. Chouraqui. “Garside Groups and Yang–Baxter Equation”. *Communications in Algebra* 38.12 (2010), 4441–4460.

[7] H. S. M. Coxeter. “Factor Groups of the Braid Group,” *Proceedings of the Fourth Cananadian Mathematical Congress* (1959), 95–122.
[8] C. W. Curtis and I. Reiner. *Methods of Representation Theory, Volume I.* New York: Wiley, 1990.
[9] C. W. Curtis and I. Reiner. *Methods of Representation Theory, Volume II.* New York: Wiley, 1990.
[10] P. Dehornoy. “Set-Theoretic Solutions of the Yang–Baxter Equation, RC-calculus, and Garside Germs”. *Advances in Mathematics* 282 (2015), 93–127.
[11] P. Dehornoy and L. Paris. “Gaussian Groups and Garside Groups, Two Generalisations of Artin Groups”. *Proceedings of the London Mathematical Society* 79.3 (1999), 569–604.
[12] F. Digne. *Algèbres de Hecke*. www.lamfa.u-picardie.fr/digne/hecke.pdf.
[13] V. G. Drinfeld. “On Some Unsolved Problems in Quantum Group Theory”. Vol. 1510. Lecture Notes in Mathematics. 1992, 1–8.
[14] P. Etingof, T. Schedler, and A. Soloviev. “Set-Theoretical Solutions to the Quantum Yang-Baxter Equation”. *Duke Mathematical Journal* 100 (1999), 169–209.
[15] E. Feingesicht. “Dehornoy’s Class and Sylows for Set-Theoretical Solutions of the Yang–Baxter Equation”. *Int. J. Algebra Comput.* 34 (2024), 147–173.
[16] T. Gateva-Ivanova and M. Van den Bergh. “Semigroups of I-Type”. *Journal of Algebra* 206 (1998), 97–112.
[17] M. Geck and G. Pfeiffer. *Characters of Finite Coxeter Groups and Iwahori-Hecke Algebras*. Clarendon Press, 2000.
[18] T. Gobet. “A New Garside Structure on Torus Knot Groups and Some Complex Braid Groups”. *J. Knot Theory Ramifications* 32.13 (Nov. 2023), 2350094.
[19] T. Gobet. “Toric Reflection Groups”. *Journal of the Australian Mathematical Society* 116.2 (Apr. 2024), 171–199.
[20] V. Lebed, S. Ramírez, and L. Vendramin. *Involutive Yang-Baxter: Cabling, Decomposability, Dehornoy Class*. 2022. arXiv: 2209.02041 [math].
[21] J. Michel. “Groupes de tresses, Groupes réductifs et algèbres de Hecke”. Lecture Notes. 1998.
[22] J. Michel. “Lectures on Coxeter Groups”. Beijing, 2014.
[23] L. Poulain d’Andecy. “Personnal Communications”.
[24] L. Poulain d’Andecy. “Algèbres de Hecke Fusionnées et Dualité de Schur–Weyl”. *Séminaire d’Algèbre et de Géométrie*. Caen, May 2023.
[25] R. Rouquier, G. Malle, and M. Broué. “Complex Reflection Groups, Braid Groups, Hecke Algebras”. *Crelles Journal* 1998.500 (July 1998), 127–190.
[26] W. Rump. “A Decomposition Theorem for Square-Free Unitary Solutions of the Quantum Yang-Baxter Equation”. *Advances in Mathematics* 193 (2005), 40–55.
[27] W. Rump. “Braces, Radical Rings, and the Quantum Yang–Baxter Equation”. *Journal of Algebra* 307.1 (Jan. 2007), 153–170.
[28] G. C. Shephard and J. A. Todd. “Finite Unitary Reflection Groups”. *Canadian Journal of Mathematics* 6 (Jan. 1954), 274–304.

Normandie Univ, UNICAEN, CNRS, LMNO, 14000 Caen, France
Email address: edouard.feingesicht@unicaen.fr