Normandie Université

UNIVERSITÉ CAEN NORMANDIE

THÈSE

Pour obtenir le diplôme de doctorat

Spécialité **MATHEMATIQUES**

Préparée au sein de l'**Université de Caen Normandie**

Representations of structure group of set-theoretical solutions to the Yang-Baxter equation

Présentée et soutenue par

EDOUARD FEINGESICHT

Thèse soutenue le 11/10/2024

devant le jury composé de :

M. EDDY GODELLE	Professeur des universités - Université de Caen Normandie	Directeur de thèse
M. IVAN MARIN	Professeur des universités - UNIVERSITE AMIENS PICARDIE JULES VERNE	Président du jury
MME VICTORIA LEBED	Maître de conférences - Université de Caen Normandie	Membre du jury
M. LEANDRO VENDRAMIN	Maître de conférences - UNIVERSITE VRIJE BRUSSEL BELGIQUE	Membre du jury
M. ADOLFO BALLESTER-BOLINCHES	Professeur - VALENCE - UNIVERSIDAD DE VALENCIA	Rapporteur du jury
M. LOÏC POULAIN D'ANDECY	Maître de conférences HDR - UNIVERSITE REIMS CHAMPAGNE ARDENNE	Rapporteur du jury

Thèse dirigée par **EDDY GODELLE** (Laboratoire de Mathématiques 'Nicolas Oresme' (Caen))

Résumé

Dans cette thèse nous nous intéressons à l'étude des solutions ensemblistes de l'équation de Yang–Baxter. Le point de départ de notre approche sont les travaux de Patrick Dehornoy, qui a établi des parallèles entre les groupes de structures des solutions et la théorie des groupes d'Artin–Tits. Nous étudions donc les groupes des structures d'un point de vue de la théorie de Garside, à travers des représentations monomiales, dans le but d'améliorer la compréhension des solutions pour amener à leur éventuelle classification. Dans ce sens, nous étudions les bornes et les valeurs d'une constante définie par Dehornoy pour chaque solution. Nous nous intéressons ensuite à l'irréductibilité des représentations monomiales de ces solutions. Enfin, nous construisons et étudions des algèbres de Hecke pour les solutions, en soulignant les points communs et les différences avec la théorie connue des algèbre de Hecke pour les groupes d'Artin–Tits.

Abstract

In this thesis we are interested in set-theoretical solutions to the Yang–Baxter equation. The starting point of our approach is the work of Patrick Dehornoy, who established parallels between the structure groups of solutions and the theory of Artin–Tits groups. We thus study the structure groups from a Garside theory perspective, through monomial representations, with the aim of improving our understanding of solutions and eventually classifying them. In this sense, we study the bounds and values of a constant defined by Dehornoy for each solution. We then focus on the irreducibility of the monomial representations of these solutions. Finally, we construct and study Hecke algebras for solutions, highlighting the similarities and differences with the known theory of Hecke algebra for Artin–Tits groups.

Remerciements/Acknowledgements

First of all, I would like to thank the referees and members of my Jury for accepting to accompany me in the end of this enriching journey, it is an honor to have you there.

Je tiens évidemment à remercier Eddy pour la chance de faire cette Thèse, pour m'avoir aidé à découvrir ces sujets fascinants tout en me laissant la liberté d'explorer mes propres directions, d'avoir su me guider dans le début d'une carrière dans la recherche à travers de nombreuses intéressantes discussions, d'avoir pris le temps de corriger et m'aider à améliorer mon travail, et enfin de m'inciter à raccourcir mes phrases pour plus de lisibilité (sauf celle-ci).

Merci à mon Comité de suivi de thèse (CSI), Jérôme et Nicolas, pour votre présence et vos conseils, si tout s'est bien passé c'est aussi grâce à vous.

Merci à toutes les personnes rencontrées en conférence, les maths sont toujours plus agréables quand on a des personnes avec qui les partager tout en passant de bons moments.

Arne, Carsten, Eric, Leandro, Senne, Sylvia, Thomas, and all the amazing people at VUB, thank you so much for your hospitality at VUB, working with you is such an amazing experience, hopefully I can come visit some time soon.

Merci à Marie de l'École doctorale pour tes réponses à toutes nos inquiétudes, tu facilites tellement nos vie. Merci à Anita, Carole et Vanessa, pour votre accompagnement (pas seulement administratif) et nous avoir aidés à sortir de nos bureaux (pour des conférences, ou juste aller parler avec vous). Merci également à tous les personnels de l'université, de l'entretien au service informatique, qu'on ne me remercie pas assez mais sans qui tout cela serait impossible.

Merci également à toutes les personnes du LMNO, pour les conseils, les échanges mathématiques, les discussions moins mathématiques. C'est la vie de laboratoire qui rend la recherche si belle.

Il va de soi que ces trois années n'auraient pas été aussi formidables sans tous les camarades de Caen (et parfois maintenant d'ailleurs), merci à vous pour les soirées inoubliables, les pauses déjeuners, les discussions plus ou moins mathématiques, les découvertes de nouvelles activités, les conseils, les conférences, les fous rires, et tout le reste. Les autres laboratoires devraient nous envier ce délirant petit groupe caennais.

Enfin mais surtout, merci à ma famille et mes proches pour votre soutien infaillible, votre présence rassurante, votre confiance, je n'y serais jamais parvenu sans vous. Maxime, Papa et Maman, je sais que je pourrai toujours compter sur vous, merci mille fois pour tout.

Pour l'enfant, amoureux de cartes et d'estampes,
L'univers est égal à son vaste appétit.
Ah ! que le monde est grand à la clarté des lampes !
Aux yeux du souvenir que le monde est petit !

Charles Baudelaire, Le Voyage I (1861)

Contents

Nomenclature **5**

Introduction **7**
Coxeter groups . . . 7
Artin–Tits and Coxeter groups . . . 7
Garside theory . . . 10
Iwahori-Hecke algebras . . . 11
The Yang–Baxter equation . . . 12
A physical model . . . 12
The mathematical approach . . . 17
Thesis' content . . . 17

1 Set-theoretical solutions to the Yang–Baxter equation **21**
1.1 Yang–Baxter equation . . . 21
1.2 Cycle sets . . . 24
1.3 Dehornoy's calculus . . . 25
1.4 Monomial matrices . . . 30
1.5 The monomial representation . . . 30
1.6 Braces . . . 38

2 On Dehornoy's constructions **43**
2.1 Garsideness . . . 44
2.2 Dehornoy's class . . . 47
2.3 Non-degeneracy . . . 53
2.4 Bounding the class . . . 55
2.5 Zappa-Szép product and Sylows . . . 61

3 Irreducibility of the monomial representations **69**
3.1 Indecomposability and Irreducibility . . . 69
3.2 Estimating the size of $\mathcal{G}(X)$ . . . 71
3.3 Inducing the representations . . . 73

4 Hecke algebras for set-theoretical solutions to the Yang–Baxter equation **77**
4.1 Finding the correct definition via a diagrammtic approach 77
4.2 Defining the Hecke algebra 82
4.3 Anti-involution on the Hecke algebra 87
4.4 Semi-simplicity 89
4.5 Two-generated Cyclic group 92

A Histograms for Dehornoy's class **97**

Index **109**

Bibliography **109**

Nomenclature

$\varnothing$	The empty set
$\mathbb{N}$	Monoid of non-negative integers
$\mathbb{Z}$	Group of integers
$\mathbb{Q}$	Field of fractions of integers
$\mathbb{R}$	Field of real numbers
$\mathbb{C}$	Field of complex numbers
$\langle S \mid R \rangle$	Group generated by S up to the relations R
G/H	Quotient of a group G by a normal subgroup H
$\mathfrak{S}_n$	Symmetric group on n elements
$M_n(R)$	Group of square matrices of size n over a ring R
$\mathrm{GL}_n(R)$	Group of invertible square matrices of size n over a ring R
$\mathrm{Tr}(A)$	Trace of a matrix A
$R[G]$	Algebra of a group G over a ring R
$R[X]$	Ring of polynomials in X over ring R
$R[X^{\pm 1}]$	Ring of Laurent series in X over a ring R
$K(X)$	Field of rational functions over a field K
$X \times Y$	Direct product of sets
$N \otimes_R M$	Tensor product of R-modules
$\mathrm{rad}(A)$	Radical of an algebra

$a \mid b$	a divides b in $\mathbb{N}$
$\mathrm{lcm}(a_1, \ldots, a_n)$	Least common multiple of the positive integers a_i
$\gcd(a_1, \ldots, a_n)$	Greatest common divisor of the positive integers a_i
$\pi(n)$	Set of primes dividing an integer
$v_p(n)$	p-valuation of an integer
$\mathrm{char}(K)$	Characteristic of a field K

Introduction

Coxeter groups

Artin–Tits groups and Coxeter groups

Braids group were first introduced and studied by E. Artin in [Art25]. They are better seen diagrammatically: a n-braid is a set of n strands which can cross over and under, up to ambient isotopy (moving the strands without crossing them). The operation on two n-braids is then given by just stacking the first one on top of the other.

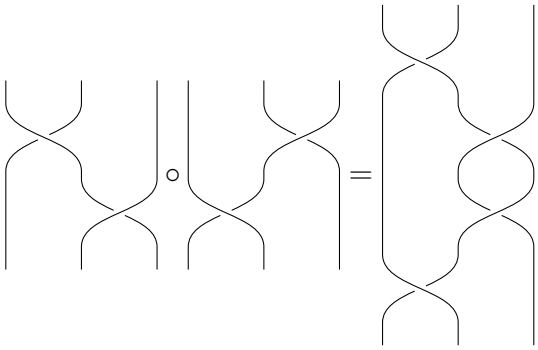


Figure 1: Example on 3-braids

Then, in [Art47, Theorem 16] a presentation of the n-braid group B_n is given as

$$B_n = \left\langle \sigma_1, \dots, \sigma_{i-1} \;\middle|\; \begin{array}{c} \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \\ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| \geq 2 \end{array} \right\rangle$$

where σ_i corresponds to a "positive" exchange of the i-th and $i+1$-th strands, the commutativity relation $\sigma_i\sigma_j = \sigma_i\sigma_i$ holds for strands far enough, and the so-called "braid relation" holds for close strands.

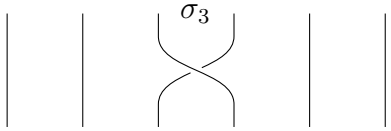
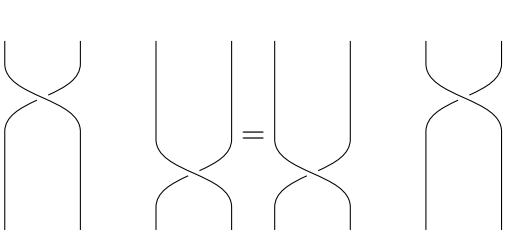
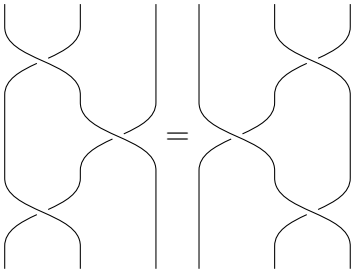


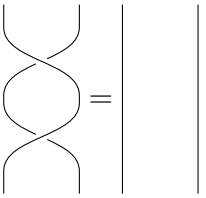
Figure 2: A generator of B_6



(a) Far commutativity relation



(b) Braid relation



(c) Inverse relation

Figure 3: The relations of B_n

For any braid, looking at the final position of each strand (from top to bottom) yields a morphism from B_n to the symmetric group $\mathfrak{S}_n$. This surjection amounts to adding to B_n the relation σ_i^2 for all σ_i. For instance the generator σ_i is associated to the transposition $(i \quad i+1)$.

Those groups were then generalized by J. Tits in [Tit66] to what are now called Artin–Tits groups as follows: consider a set S and for any $s \neq t$ in S take a number $m_{s,t}$ in $\mathbb{N}_{\geq 2} \cup \{\infty\}$ with $m_{s,t} = m_{t,s}$, the group is then defined by the presentation

$$A \coloneqq \langle S \mid \underbrace{ststst\ldots}_{m_{s,t}} = \underbrace{tstsst\ldots}_{m_{s,t}}, \forall s \neq t \in S \text{ when } m_{s,t} \neq \infty \rangle.$$

The associated Coxeter group W is then defined by adding to the presentation the relations $s^2 = 1$ for all s in S. The couple (W, S) is usually called a Coxeter system. For example, the braid groups correspond to the case $m_{\sigma_i,\sigma_j} = \begin{cases} 3, \text{ if } |i-j| = 1 \\ 2, \text{ otherwise} \end{cases}$.

A Coxeter system (W, S) can be represented by a so-called Dynkyn diagram as follows: each vertex is a generator, and each edge between vertices s_i and s_j is labeled by m_{s_i,s_j}, where for simplicity $m = 2$ is represented as no edge and $m = 3$ is represented as an unlabeled edge. So the Coxeter group associated to $S = \{s_1, s_2, s_3\}$ with $m_{s_1,s_2} = 3$ and $m_{s_1,s_3} = m_{s_2,s_3} = 2$ is

$$\langle s_1, s_2, s_3 \mid s_1^2 = s_2^2 = s_3^2 = 1, s_1s_2s_1 = s_2s_1s_2, s_1s_3 = s_3s_1, s_2s_3 = s_3s_2 \rangle$$

and corresponds to the diagram

A Coxeter group is called irreducible when its Dynkyn diagram is connected. Finite irreducible Coxeter groups have been classified in [Cox35, Theorem ‡]. This classification involves 4 infinite families (among which the braid groups) and 6 exceptional groups. We present the classification in the following Figure 4, where the parameters of the infinite families A, B, D, I_2 correspond to the number of vertices.

Name	Diagram
$A_n \quad (n \geq 1)$	
$B_n = C_n \quad (n \geq 2)$	
$D_n \quad (n \geq 4)$	
E_6	
E_7	
E_8	
F_4	
G_2	
H_2	
H_3	
H_4	
$I_2(p) \quad (p \geq 7)$	

Figure 4: Classification of finite irreducible Coxeter groups

For the particular cases of finite Coxeter groups, and their associated Artin groups which are called of spherical type, many properties are known, which will be the point of the next subsection of their Garside theory, as most of those properties can be deduced from the existence of a longest element ([Deh+15; DP99]). One easy thing to observe, which relates to the geometric origin of these groups is their geometric representation as reflection groups [Bou07; Tit74]:

Let S be a finite Coxeter system with finite Coxeter group W. Consider the finite dimensional vector space $V = \mathbb{R}^S$, with basis $(e_s)_{s \in S}$. We define a symmetric bilinear

form on V by setting

$$B(e_s, e_t) = -\cos(\frac{\pi}{m_{s,t}}),$$

and then for each s in S we define a reflection on V by

$$\sigma_s(x) = x - 2B(e_s, x)e_s.$$

The representation ρ obtained from these reflections happens to be faithful, and is called the geometric representation of a Coxeter group, allowing for a geometric approach to Coxeter groups, via reflection groups (finite groups generated by reflections of an euclidean space).

Explicitly, we equip the dual space V^* with the contragradient action of W such that, for all (x, y) in $(V^* \times V)$, $\langle \sigma_s(x), y\rangle = \langle x, \sigma_s(y)\rangle$, the hyperplanes $M_s = \{x \in V^* \mid \langle x, e_s\rangle = 0\}$ and their orbits by W are called walls. The cone defined by $C = \{x \in V^* \mid \forall s \in S, \langle x, e_s\rangle > 0\}$ is called the fundamental chamber and its W-orbits the chambers of V.

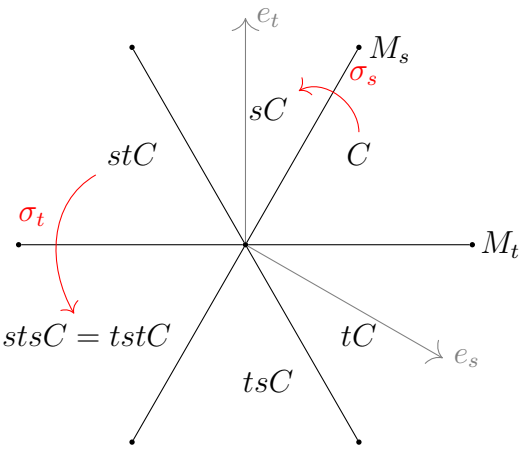


Figure 5: Walls and chambers for $A_2 = \mathfrak{S}_3 = \langle s, t \mid s^2 = t^2 = 1, sts = tst\rangle$

In Figure 5, we chose two unit vectors (e_s and e_t) separated by an angle of $\frac{\pi}{m_{s,t}} = \frac{\pi}{3}$ and their corresponding hyperplanes M_s and M_t. Then C is the fundamental chamber, between the positive part of these two walls. To go from C to another chamber, we can reflect through one wall to attain sC or tC, for our example say we chose sC. Then, one can again do a reflection with another wall of the chamber: choosing s will result in going back to C, will choosing t will lead to tsC. The relation $sts = tst$ then corresponds to the fact that $stsC = tstC$ obtained step-by-step (reflection-by-reflection).

Garside theory

The conjugacy problem (deciding when two words represent conjugate elements in a group) for the braid groups was solved by Garside in [Gar69]. His approach was generalized to spherical type Artin–Tits groups, that is for which the associated Coxeter

group is finite, by Brieskorn–Saito in [BS72] and Deligne in [Del72]. In [DP99] Dehornoy and Paris introduced the definition of a Garside group, and many algorithmical and combinatorial properties were deduced from this (solution to the word and conjugacy problems, biautomaticity, normal forms, etc.).

The fundamental aspect of this structure on Artin–Tits groups is the existence of a longest element in the Coxeter group; for instance, for the type A_n where $W = \mathfrak{S}_{n+1}$ is generated by adjacent transpositions, the longest element is

$$w_0 = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix} = \Pi_n \Pi_{n-1} \dots \Pi_1$$

where $\Pi_k = s_1 s_2 \dots s_k$ with $s_i = \begin{pmatrix} i & i+1 \end{pmatrix}$.

This special element, when lifted to the Artin–Tits group is called a Garside element, usually denoted Δ, and is seen as the least common multiple of the generators, which leads to numerous interesting properties: it induces an automorphism (from $s\Delta = \Delta\tau(s)$), the Artin–Tits group is the group of fractions of the Artin–Tits monoid (in particular the monoid is cancellative and embeds in the group).

We say that a word in S of length r is reduced in W if it is a minimal length decomposition of the element it represents ((s) is always reduced, (s, s, t) is not because $sst = t$). Another fundamental property of finite Coxeter groups is the so-called Exchange lemma: consider a reduced word $(s_1, \dots, s_r)$ and an element s in S, then either $(s, s_1, \dots, s_r)$ is reduced or $s_1 \dots s_r = s s_1 \dots \hat{s_i} \dots s_r$ in W for some removed element s_i).

In [Deh+15] a large review of current knowledge of Garside groups, and a generalization to Garside categories is made.

Iwahori-Hecke algebras

For a given Coxeter system (W, S) and a commutative ring R, one has the group algebra of W but also the group algebra of the Artin–Tits groups A associated to (W, S). The surjection $A \twoheadrightarrow W$ then extends to an algebra morphism $R[A] \twoheadrightarrow R[W]$ where R is the chosen coefficient ring. The aim of a Iwahori-Hecke algebra ([GP00; Bou07]) is to deform the finite-dimensional algebra $R[W] = R[A]/\langle s^2 = 1 \rangle$ (whenever W is finite) to retain some information of the quotient: to do so, in the generic version, a parameter q is introduced. Consider a quotient of $R[q^{\pm 1}][A]$ by deforming the relation $s^2 = 1 \Leftrightarrow (s-1)(s+1) = 0$ to $(s-q)(s+1) = 0 \Leftrightarrow s^2 = (q-1)s + q$. Thus the so-called generic Iwahori-Hecke algebra associated to W is defined as ([GP00])

$$\mathcal{H}_q(W) = R[q^{\pm 1}]\langle T_s, s \in S \mid \underbrace{T_s T_t T_s \dots}_{m_{s,t}} = \underbrace{T_t T_s T_t \dots}_{m_{s,t}},\ T_s^2 = (q-1)T_s + q \rangle.$$

For instance, in the braids groups, this allows to work in something similar to $R[\mathfrak{S}_n]$ (which is finite) while the parameter q "keeps track" of the information lost when quotienting; this leads to the definition of some invariants of knots (which are tightly related to braids, see [Ale23]) by Jones in [Jon87].

For this, consider the Iwahori-Hecke algebra $\mathcal{H}_n$ of $\mathfrak{S}_n$ over a field with two variables $k(q', q'')$ with the parameter $q = -\frac{q'}{q''}$, and with the new generating family given by $\tilde{s} = -q''s$, it follows that $\tilde{s}^2 = S\tilde{s} - P$ where $S = q' + q''$ and $P = q'q''$. Then, there

exists a unique Markov Trace over $\sqcup_{n\geq 1}\mathcal{H}_n$ ([Dig]), that is a collection of linear forms $\tau_n\colon \mathcal{H}_n \to R$ such that $\tau_{n+1}(\tilde{s}_n h) = \tau_n(h)$ for all $h \in \mathcal{H}_n$ and with s_n the last generator of $\mathfrak{S}_{n+1}$, and $\tau_1(1) = 1$. The Alexander polynomial ([Ale23]) is obtained by setting $q' = t^{\frac{1}{2}}$ and $q'' = -t^{-\frac{1}{2}}$, the Jones polynomial by setting $q' = t^{\frac{3}{2}}$ and $q'' = -t^{\frac{1}{2}}$ ([Jon87]), and their generalization the HOMFLY polynomial $R[x,t]$ by setting $S = tx$ and $P = -t^2$ ([Fre+85]).

Hecke algebras have a strong importance for the study of representation of algebraic groups. Let us focus on $G = \mathrm{GL}_n(\mathbb{F}_q)$, the general linear group of degree n over a finite field with $q = p^k$ elements. Consider the Borel subgroup $B \subset G$ of upper triangular matrices, it follows from Bruhat decomposition that $G = \sqcup_{\sigma\in\mathfrak{S}_n} B\sigma B$ ([Bou07]. It was shown by Iwahori that $\mathrm{End}_{\mathbb{F}_q[G]}(\mathbb{F}_q[G/B]) = \mathcal{H}_n(\mathfrak{S}_n)$ ([Iwa64]). This was then used by Lusztig in his book [Lus16] to construct all irreducible characters of G.

Some essential properties of an Iwahori-Hecke algebra $\mathcal{H}$ are the following: $\dim \mathcal{H} = \dim R[W] = |W|$, the generators are invertible, under a suitable extension of R the algebra is semi-simple.

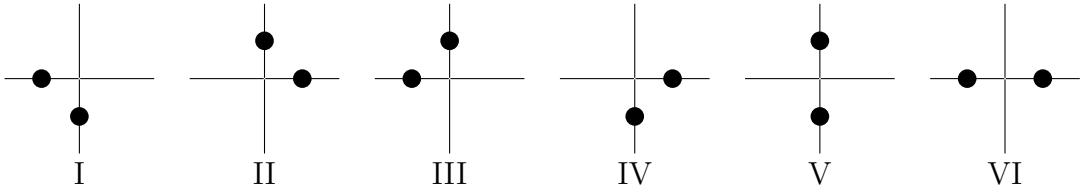
In particular, for instance over a large enough field K (such as $\mathbb{C}(\sqrt{q})$, [GP00]), we have a bijection between the irreducible characters of the algebras $K\mathcal{H} = K \otimes \mathcal{H}$ and $\mathbb{C}[W]$.

The Yang–Baxter equation

A physical model

First occurrences of the Yang–Baxter equation were in physics, specifically its name comes from the work of Yang on quantum mechanic ([Yan67]) and Baxter on statistical mechanic ([Bax72]), an extensive review of its origin and occurrences in different domains of physics can be found in [PA06; Jim89]. We provide one example of how the equation appears: square lattice vertex models, more specifically the 6- and 8-vertex models, the latter being the one studied by Baxter. For details, the reader can refer to [Eck19].

First consider a square lattice, representing the crystal structure of ice (H_2O), where each vertex represents an oxygen atom, and has in its neighborhood two hydrogen atoms, leading to 6 possible local configurations as represented in the following, where the center is the Oxygen atom and the two • represent the Hydrogen atoms.



A common alternative representation is with arrows to the vertex, where incoming arrows correspond to the presence of Hydrogen. The ice rule then being that there must be exactly 2 incoming arrows representing the two Hydrogen atoms.

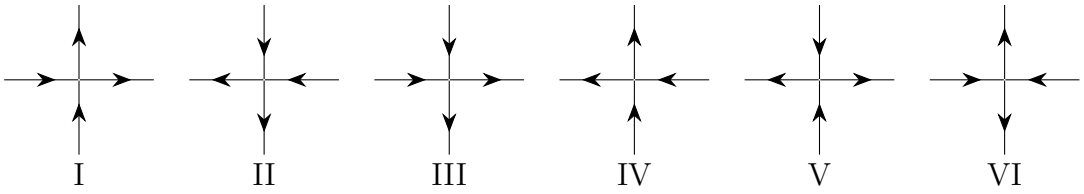


Figure 6: The six configurations of the ice-type model

This model was then generalized to the 8-vertex model, which Baxter studied, by relaxing the ice rule to having an even number of incoming arrows to each vertex, thus allowing two extra configurations:

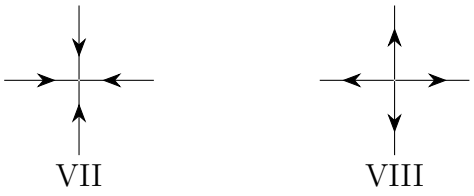
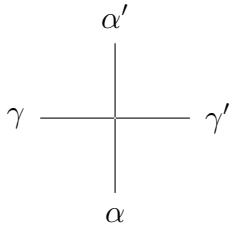


Figure 7: The two extra configurations of the 8-vertex model

Up to arrow reversing, those configurations can be grouped in 4 groups of two in the order they are written (I and II, III and IV, V and VI, VII and VIII), and those are named respectively $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ and $\mathfrak{d}$.

However, it is more convenient for mathematical purposes to identify an arrow with a sign as follows: $\begin{cases} \uparrow = +1 = \rightarrow \\ \downarrow = -1 = \leftarrow \end{cases}$, and we label a vertex with $\alpha, \alpha', \gamma, \gamma'$ in $\{-, +\}$ in the following way:



The ice rule, i.e. that every vertex has exactly two incoming edges, can be checked to being equivalent to $\alpha + \gamma = \alpha' + \gamma'$.

Then, a lattice is said to be valid if it locally corresponds to one of the 8 allowed configurations. So two configurations can be joined together when the sign where they are joined matched (for instance, to join two configurations from left to right, γ' of the left one must equal γ of the right one).

Now, to each of the 8 configurations we can associate an energy ϵ_j ($j \in \{\mathrm{I}, \ldots, \mathrm{VIII}\}$) and a corresponding positive number $v_j = e^{-\beta\epsilon_j}$, representing its statistical weight, where β is the inverse of the temperature of the system. If we have n_j vertices of configuration $j \in \{\mathrm{I}, \ldots, \mathrm{VIII}\}$ in a finite lattice (with the conditions above), the total energy is given by $\mathcal{E} = \sum_{j=1}^{8} n_j \epsilon_j$.

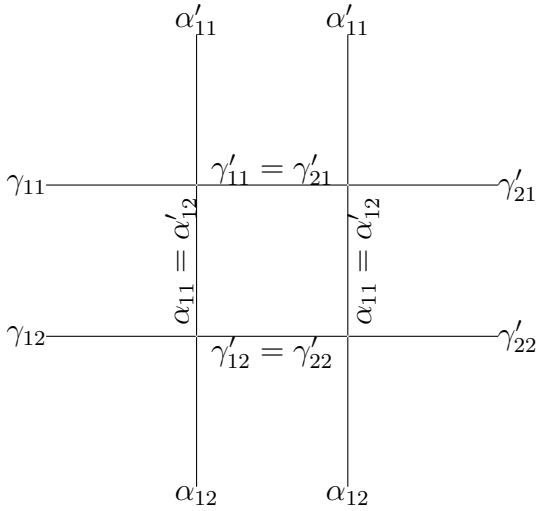


Figure 8: Conditions for a valid 2×2 lattice

The main interest, the partition function, is then defined as a sum over valid lattices

$$Z = \sum_{\text{valid lattices}} e^{-\beta \mathcal{E}}.$$

For a given configuration, we denote $R_\alpha^{\alpha'}(\gamma, \gamma')$ both the configuration itself and the associated statistical weight, as the context will be clear to determine which one is involved. Then, two vertex configurations $R_{\alpha_1}^{\alpha'_1}(\gamma_1, \gamma'_1)$ and $R_{\alpha_2}^{\alpha'_2}(\gamma_2, \gamma'_2)$ can be put next to each other, say left to right (resp. top to bottom), if $\gamma'_1 = \gamma_2$ (resp. $\alpha_1 = \alpha'_2$). If we consider the statistical weight of a row with N configurations, with the cylindrical condition $\gamma_1 = \gamma'_N$, we find it is equal to

$$T_{(\alpha),(\alpha')} = \sum_{\gamma_1,\dots,\gamma_N = \pm} R_{\alpha_1}^{\alpha'_1}(\gamma_1, \gamma_2) R_{\alpha_2}^{\alpha'_2}(\gamma_2, \gamma_3) \cdots R_{\alpha_N}^{\alpha'_N}(\gamma_N, \gamma_1).$$

which only depends on $(\alpha) = (\alpha_1, \dots, \alpha_N)$ and $(\alpha') = (\alpha'_1, \dots, \alpha'_N)$.

As $R_{\alpha_i}^{\alpha'_i}(\gamma_i, \gamma'_i)$ is the statistical weight of a local configuration, we have that the statistical weight of a row is given by $R_{\alpha_1}^{\alpha'_1}(\gamma_1, \gamma_2) \cdots R_{\alpha_N}^{\alpha'_N}(\gamma_N, \gamma_1)$. Thus $T_{(\alpha),(\alpha')}$ is the partition function of a single row.

We then put each of the weights $T_{(\alpha),(\alpha')}$ inside a $2^N \times 2^N$ matrix with row (resp. columns) indexed by the possible values of $\alpha_1, \dots, \alpha_N$ (resp. with primes), denoted T and called the transfer matrix.

Then, if we stack M rows on top of each other with the compatibility conditions and the toroidal condition $\alpha_1 = \alpha'_M$, we obtain obtain another expression for the partition function as

$$Z = \sum_{(\alpha_1),\dots,(\alpha_M)} T_{(\alpha_1),(\alpha_2)} T_{(\alpha_2),(\alpha_3)} \dots T_{(\alpha_N),(\alpha_1)}.$$

This expression of Z is also exactly the trace of T^m. Thus, to understand Z, we can try to find the eigenvalues of T.

In the most general case, there is 16 possible configurations (two states for each edge), and some have been studied (we still refer to [Eck19] for more details and references).

This leads to the definition of the R-matrix, a 4×4 matrix with coefficients $R_\alpha^{\alpha'}(\gamma, \gamma')$, where the rows (resp. columns) are indexed by (α, γ) (resp. with primes) in the order $1 = (+,+), 2 = (+,-), 3 = (-,+)$ and $4 = (-,-)$. For the 8-vertex model considered by Baxter, by assuming all the symmetries by arrows reversal (for instance identifying I$= R_{+,+}(+,+)$ and II$= R_{-,-}(-,-)$), the R-matrix is given by

$$R_{8v} = \begin{pmatrix} \mathfrak{a} & 0 & 0 & \mathfrak{d} \\ 0 & \mathfrak{b} & \mathfrak{c} & 0 \\ 0 & \mathfrak{c} & \mathfrak{d} & 0 \\ \mathfrak{d} & 0 & 0 & \mathfrak{a} \end{pmatrix}$$

and for the 6-vertex model of ice, we add that $\mathfrak{d} = 0$. To highlight the symmetries of such a matrix, it is common and convenient to make use of the Pauli matrices (and adding the identity) to write $R_{8v} = \sum_{j=1}^{4} w_j \sigma_j \otimes \sigma_j$, where the coefficients w_j can be deduced by solving an easy linear system of 4 equations (their values do not matter for this explanation); and in general we write $R = \sum\limits_{i,j=1}^{4} w_{ij} \sigma_i \otimes \sigma_j$ by solving a linear system of 16 equations.

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \sigma_4 = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Figure 9: The 3 Pauli matrices and the identity

For the 6-vertex model, the diagonalization was obtained using the "Bethe ansatz", but this method cannot be extended to the 8-vertex model (see [Eck19; Bax85]) and Baxter had to introduce a new approach, which leads to one of the first occurrences of the Yang–Baxter equation. Baxter's idea, extracted from Bethe ansatz, is to study the commutativity of transfer matrices: that is, given any two sets of Boltzmann weights v_j and v'_j for a $N \times M$ lattice, understanding when their respective transfer matrices T and T' commute. He showed how, under the assumption of their commutativity (and some extra others), any transfer matrix can be diagonalized. This method can be applied in a more general context, although then solving the Yang–Baxter equation is not always possible:

Now consider the so-called monodrony matrix, obtained like the transfer matrix of a row but without the cylindrical conditions:

$$\mathcal{T} = T_{(\alpha),(\alpha')}(\gamma, \gamma') = \sum_{\gamma_2, \dots, \gamma_N = \pm} R_{\alpha_1}^{\alpha'_1}(\gamma, \gamma_2) R_{\alpha_2}^{\alpha'_2}(\gamma_2, \gamma_3) \dots R_{\alpha_N}^{\alpha'_N}(\gamma_N, \gamma')$$

and regarded as a 2×2 matrix with coefficients the four $2^N \times 2^N$ matrices $\mathcal{T}(\gamma, \gamma')$. The transfer matrix can then be re-obtained as $T = \mathrm{Tr}(\mathcal{T}) = \mathcal{T}(+,+) + \mathcal{T}(-,-)$ (the other two coefficients don't satisfy the toroidal conditions). This monodrony matrix, although it looks more complicated than the transfer matrix, admits a nice "local description":

Recall that the 4×4 R-matrix can be expressed as $R = \sum\limits_{i,j=1}^{4} w_{ij} \sigma_i \otimes \sigma_j$ using the Pauli matrices. For all $1 \leq n \leq N$, we define the $2^{N+1} \times 2^{N+1}$ L-operator by $L_n =$

$\sum_{i,j=1}^{4} w_{ij}\sigma_i \otimes \sigma_j^{(n)}$, where $\sigma_j^{(n)} = \overbrace{I_2 \otimes I_2 \otimes \cdots \otimes \underbrace{\sigma_j}_{n} \otimes I_2 \otimes \cdots \otimes I_2}^{N}$. These matrices can be seen as a local version of the R-matrix, and one can show that $\mathcal{T} = L_1 L_2 \dots L_N$.

Now the commutativity of $T = \mathrm{Tr}(\mathcal{T})$ and $T' = \mathrm{Tr}(\mathcal{T}')$ can be obtained from the existence of an invertible 4×4 matrix M such that $M(\mathcal{T} \otimes \mathcal{T}') = (\mathcal{T}' \otimes \mathcal{T})M$; indeed, we would have $TT' = \mathrm{Tr}(\mathcal{T})\mathrm{Tr}(\mathcal{T}') = \mathrm{Tr}(\mathcal{T} \otimes T') = \mathrm{Tr}(M^{-1}(\mathcal{T}' \otimes \mathcal{T})M) = \mathrm{Tr}(T' \otimes T) = \mathrm{Tr}(T')\mathrm{Tr}(T) = T'T$. From examples, it is expected that in fact M can be obtained from another R-matrix, say R'' for a third set of Boltzmann weights v_j'', by taking

$$M = \tilde{R}'' = \mathcal{P}R'' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} R.$$

The equation $\tilde{R}''(\mathcal{T} \otimes \mathcal{T}') = (\mathcal{T}' \otimes \mathcal{T})\tilde{R}''$ can be written locally as $\tilde{R}''(L_n \otimes L_n') = (L_n' \otimes L_n)\tilde{R}''$ or with R-matrices $\tilde{R}''(R \otimes R') = (R' \otimes R)\tilde{R}''$. Explicitly, if we denote for clarity $R = R(w), R' = R(w')$ and $R'' = R(w'')$, this expands as

$$\sum_{\alpha'',\beta'',\gamma''} R_{\alpha''}^{\alpha'}(\gamma,\gamma'')(w) R_{\beta''}^{\beta'}(\gamma'',\gamma')(w') R_{\alpha}^{\alpha''}(\beta,\beta'')(w'') =$$

$$\sum_{\alpha'',\beta'',\gamma''} R_{\alpha''}^{\alpha'}(\beta'',\beta')(w'') R_{\beta}^{\beta''}(\gamma,\gamma'')(w') R_{\alpha}^{\alpha''}(\gamma'',\gamma')(w).$$

Going back to the 8 (or 6) vertex case, each R-matrix can be seen as an operator $V \otimes V \to V \otimes V$ where $V = (\uparrow \mathbb{C}) \oplus (\to \mathbb{C})$, and if instead we consider the operator $R_{ij} \colon V \otimes V \otimes V \to V \otimes V \otimes V$, the equation $\tilde{R}''(R \otimes R') = (R' \otimes R)\tilde{R}''$ can be rewritten as

$$R_{12}'' R_{13} R_{23}' = R_{23}' R_{13} R_{12}''$$

It can moreover be shown that, in those the 6-vertex case, this equation can be simplified by the introduction of "spectral parameters" u_1, u_2 and u_3 as

$$R_{12}(u_1 - u_2)R_{13}(u_1 - u_3)R_{23}(u_2 - u_3) = R_{23}(u_2 - u_3)R_{13}(u_1 - u_3)R_{12}(u_1 - u_2)$$

where the 3 original R-matrices have been reparameterized as operators $(\alpha\mathbb{C} \oplus \gamma\mathbb{C})^{\otimes 2} \to (\alpha'\mathbb{C} \oplus \gamma'\mathbb{C})^{\otimes 2}$. Forgetting the parameters, we arrive at the "quantum Yang–Baxter equation" $R_{12}R_{13}R_{23} = R_{23}R_{13}R_{12}$; if we define $\tau \colon V \otimes \to V \otimes V$ by $\tau(x \otimes y) = y \otimes x$, then R is a solution of the quantum Yang–Baxter equation if and only if τR is a solution of the "Yang–Baxter equation" $R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}$ (often also written $R_1R_2R_1 = R_2R_1R_2$, resembling the braid equation).

For the 8 vertex case, the solution was obtained by Baxter. In general, a solution does not necessarily exist. This is for instance the case of the 16-vertex model ([Eck19]). Thus, it is enough to find solutions to the Yang–Baxter equation (in its appropriate form) to obtain the partition function of the model, but this problem is in general very difficult.

The mathematical approach

In 1992 Drinfeld ([Dri92]) posed the question of classifying the "easier" case of set-theoretical solutions to the (quantum) Yang–Baxter equation, that is when considering R-matrices that leave invariant a basis of the vector space V. Explicitly, they are given by pairs (X, r) where X is a set, $r\colon X \times X \to X \times X$ a bijection satisfying $r_1 r_2 r_1 = r_2 r_1 r_2$ where r_i acts on the i and $i+1$ component of $X \times X \times X$. In [ESS99], the authors propose to study solutions which are involutive ($r^2 = \mathrm{id}_{X\times X}$) and non-degenerate (if $r(x, y) = (\lambda_x(y), \rho_y(x))$ then for any $x \in X$, λ_x and ρ_x are bijective), we will simply call those "solutions".

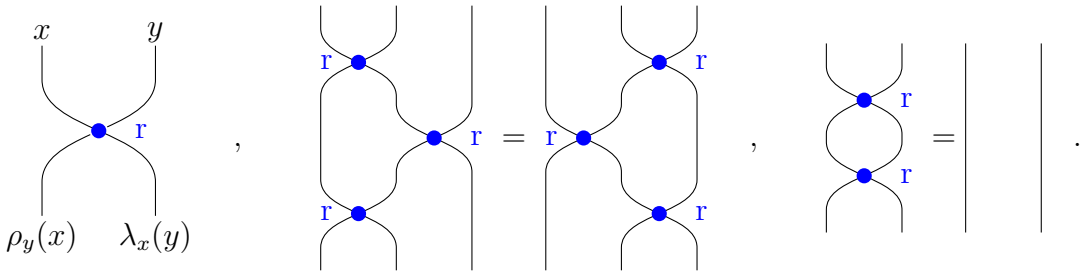


Figure 10: Representation of properties of solutions

Since then, many advances have been made on this question and objects introduced: structure group ([ESS99]), I-structure ([GV98]), etc. Many equivalent objects are known, but in particular here we are interested in cycle sets, introduced by Rump ([Rum05]). Dehornoy ([Deh15]) then studied the structure group (from cycle sets) seen from a Garside perspective (divisibility, word problem, ...),

In particular, Dehornoy defined an integer associated to a solution, which we call Dehornoy's class and usually denote d, which is to put in parallel to the number 2 for spherical Artin–Tits groups whose Coxeter groups are defined by quotienting by $s^2 = 1$ for all generators s. In this sense, quotienting the structure group by a sort of "twisted d-th power" of every generator yields a quotient, called a germ, playing a role similar to Coxeter groups.

Moreover, Dehornoy introduced a faithful representation of the structure group, and this representation specializes to a faithful representation of the germ. This representation of the structure group involves monomial matrices (where each row and column has a unique non-zero coefficient), allowing for the easy computer implementation of algorithmical tools to study the germ (a finite matrix group).

Thesis' content

The principal idea of this Thesis is to follow on Dehornoy's 2015 article ([Deh15]), where he studied structure group of set-theoretical solutions to the Yang–Baxter equation with technics coming from Artin–Tits groups and Coxeter groups. Most importantly, he constructed a quotient of the structure group that plays a role similar to the one finite Coxeter groups play for their associated Artin–Tits group of spherical type. In this sense, we will try to provide a better understanding of this "Coxeter-like" quotient, as well as highlighting the similarities and differences with finite Coxeter groups.

In the first section of this thesis, we will introduce the basic objects that we will study: set-theoretical solutions, cycle sets, braces. Our main interest will be a monomial representation introduced by Dehornoy, which we will use as a way to give a combinatorial and algorithmical approach to well-known results, such as the I-structure. We also explicit the equivalences between Dehornoy's calculus, brace theory and our monomial matrix approach.

The second section has three interests: Firstly, we answer a question of Dehornoy's on retrieving the Garside structure without a theorem of Rump, and then retrieving Rump's theorem. Both the Garside structure and Rump's theorem are obtained independently just using the I-structure. We then focus on Dehornoy's construction of the Coxeter-like groups, obtained from associating an integer (Dehornoy's class) to every solution. On the one hand, we focus on bounding the integer, with conjectures and partial results. On the other hand, we study a way to decompose the Coxeter-like group as a Zappa–Szép product of its Sylows, with the aim to try to reduce the classification problem to more "elementary" solutions (those were Dehornoy's class is a power of a prime). The main statements of this section are the followings conjecture and theorem, where we call a "finite involutive non-degenerate solution of the Yang–Baxter equation" just a "solution".

Conjecture (2.4.0.8)**.** *Let (X, r) be a solution of size n. Then the Dehornoy class d of (X, r) is bounded above by the "maximum of different products of partitions of n into distinct parts" and the bound is minimal, i.e.*

$$d \leq \max\left(\left\{\prod_{i=1}^{k} n_i \middle| k \in \mathbb{N}, 1 \leq n_1 < \cdots < n_k, n_1 + \cdots + n_k = n\right\}\right).$$

In Proposition 2.4.0.9, we prove the conjecture in a particular case: when (X, r) is square-free (i.e. $r(x, x) = (x, x)$ for all x in X) and has abelian permutation group.

Theorem (2.5.0.13)**.** *Any solution can be constructed from the Zappa–Szép product of the germs of solutions whose Dehornoy classes are powers of primes.*

Taking decomposability into account (writing a solution as union of solutions), one can consider that some "basic" cycle sets are the ones whose size and Dehornoy's class are powers of the same prime.

In the third section, we study the relation between the indecomposability of a solution and the irreducibility of the monomial representations defined by Dehornoy. To avoid a problem on particular values of Dehornoy's class, we study a larger germ obtained by considering a multiple of Dehornoy class ld and call it the l-germ. Moreover, we show that the monomial representations of indecomposable cycle sets are induced by a character of an explicit subgroup (the stabilizer of any element of X). The main result is the following:

Theorem (Proposition 3.1.0.1)**.** *Consider a integer $l > 1$ and let (X, r) be a solution. Then the following are equivalent:*

(i) *(X, r) is indecomposable*

(ii) *The monomial representation of the structure group of (X, r) is irreducible*

(iii) *The monomial representation of the l-germ of (X, r) is irreducible*

For $l = 1$, we show (Theorem 3.2.0.7) that if (X, r) is indecomposable and $d \notin \{2, 6\}$ then the monomial representation of the germ is irreducible.

In the fourth section, we define and study Hecke algebras for structure groups of solutions, still in parallel to finite Coxeter groups. The general definition, although less easy to manipulate than the Coxeter one, allows for many parameters: for instance, we are not limited by quadratic relations. Moreover, our definition happens to be slightly different from the generic Iwahori-Hecke approach to Coxeter groups. We explain why this difference occurs and where our definition comes from. We then study some properties of this Hecke algebra of solutions. As in the third section, our approach involves the l-germ of a solution (with $l > 1$), obtained by taking a multiple of Dehornoy's class.

We summarize the results in the following example:

Example (Example 4.2.0.11)**.** *Let (X, r) be the solution where $X = \{x_1, \ldots, x_n\}$ and $r(x_i, x_j) = (x_{j+1}, x_{i-1})$ where the indices are taken modulo n. This solution has Dehornoy's class $d = n$. Denote G the structure group of (X, r) and $\overline{G}_2$ its germ associated to $2n$ (two times Dehornoy's class). Then, for any integral domain R, define the following $R[q^{\pm 1}]$-algebra:*

$$\mathcal{H} = R[q^{\pm 1}][G] \Big/ \left\langle \left(x_i^{[n]}\right)^2 = (q-1) \cdot x_i^{[n]} + q, 1 \leq i \leq n \right\rangle$$

where $x_i^{[n]} = x_i x_{i+1} \cdots x_{i+n-1}$ with indices taken modulo n.

Then the followings hold:

- *(Theorem 4.2.0.8) $\mathcal{H}$ is a free $R[q^{\pm 1}]$-module with basis indexed by $\overline{G}_2$. In particular, $\mathcal{H}$ has rank $(2n)^n$.*
- *(Corollary 4.3.0.4) If T_g denotes the generator of $\mathcal{H}$ associated to an element g of $\overline{G}_2$, then T_g is invertible.*
- *(Theorem 4.3.0.5) 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 4.4.0.11) 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 $\mathbb{C}[\overline{G}_2]$.*

CHAPTER 1

Set-theoretical solutions to the Yang–Baxter equation

The goal of this section is to introduce the different approaches to study set-theoretical solutions to the Yang–Baxter equation, and also to retrieve well known results about their structure groups.

More precisely, we will define the objects to be studied: set-theoretical solutions to the Yang–Baxter equation ([Dri92; ESS99]), cycle sets ([Rum05; Deh15]) and braces ([Rum07; Ced18]). One of our main objects for this thesis is the monomial representation of structure groups introduced by Dehornoy ([Deh15]), which he obtained after retrieving the I-structure. We instead start from the representation to retrieve the I-structure, and will use this approach in the next Section (Section 2) to answer a question of Dehornoy. We also use the monomial representation to encompass both Dehornoy's calculus and Brace theory.

As the fact that structure groups are braces follows from the I-structure, we will start without the brace structure. Thus the plan for this section is the following: define our main objects, introduce Dehornoy's calculus, use a monomial representation to understand Dehornoy's calculus and deduce the I-structure, finally define braces and give their correspondance in terms of Dehornoy's calculus.

1.1 Yang–Baxter equation

As mentioned in the introduction, the Yang–Baxter equation (usually shortened YBE) is a fundamental equation on linear maps occurring in many topics in physics. In 1992, Drinfeld posed the question of restricting to linear maps that stabilize a basis, thus trying to find "set-theoretical solutions". This problem have been shown to be very difficult and many different approaches have been made, for which we will try to give an overview. A seminal paper by Etingof, Schedler and Solovier ([ESS99]), restricting to particular cases of such solutions and defining some group structures, allowed for many advances leading to some results in classification for special cases (see for instance [DPT24; CJO22; CPR20]).

Definition 1.1.0.1 ([Dri92])**.** *A set-theoretical solution to the Yang–Baxter equation is a couple (X, r) with X a set and $r\colon X \times X \to X \times X$ a bijection such that, on $X \times X \times X$ we have*

$$r_1 r_2 r_1 = r_2 r_1 r_2$$

where $r_1 = (r \times id)$ and $r_2 = (id \times r)$.

The main example that was known by Drinfeld, which he attributed to Lyubashenko is the following:

Example 1.1.0.2. *Let X be a set, and consider two maps $f, g\colon X \to X$. Then $r\colon X \times X \to X \times X$ defined by $r(x, y) = (f(y), g(x))$ is a solution if and only if $fg = gf$. Indeed, we have, for any $x, y, z \in X$,*

$$r_1 r_2 r_1(x, y, z) = r_1 r_2(f(y), g(x), z) = r_1(f(y), f(z), g^2(x)) = (f^2(z), g(f(y)), g^2(x))$$

and

$$r_2 r_1 r_2(x, y, z) = r_2 r_1(x, f(z), g(y)) = r_2(f^2(z), g(x), g(y)) = (f^2(z), f(g(y)), g^2(x)).$$

Which are equal if and only if $f(g(y)) = g(f(y))$ for all y in X.

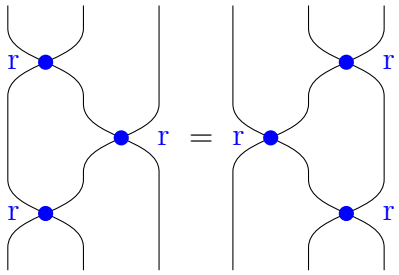


Figure 1.1: Graphical representation of the YBE

Finding all solutions of a given size is a very difficult problems, as a very naive and inefficient approach would try, for set-theoretical solutions of size $|X| = n$, all $(n^2)!$ possibilities. But having a better understanding of the behaviour of set-theoretical solutions would certainly help progress on the more general case in physics where we instead study couples (V, R) where V is a vector space and $R\colon V \otimes V \to V \otimes V$ is a linear map.

Definition 1.1.0.3. *A morphism of solutions $(X, r) \to (Y, s)$ is a map $f\colon X \to Y$ such that $(f \times f)r = s(f \times f)$. If such a map is bijective, then we say that it is an isomorphism of solutions.*

Example 1.1.0.4. *Given any solution (X, r) with $|X| = n$, for any permutation $\sigma \in \mathfrak{S}_X$ the solution defined by (X, r_σ) where $r_\sigma = (\sigma \times \sigma)r(\sigma^{-1} \times \sigma^{-1})$ is (possibly trivially) isomorphic to (X, r). Indeed, if we take $f = \sigma$, then we have*

$$r_\sigma(\sigma \times \sigma) = (\sigma \times \sigma)r(\sigma^{-1} \times \sigma^{-1})(\sigma \times \sigma) = (\sigma \times \sigma)r.$$

Drinfeld originally mentioned the restriction to involutive solutions, that is when $r^2 = \mathrm{id}_{X\times X}$, which greatly simplifies the problem. Indeed, if we write $r(x,y) = (\sigma_x(y), \tau_y(x))$, the involutivity is equivalent to $\sigma_x(y) = \tau^{-1}_{\tau_y(x)}(y)$, meaning that only "one side" of the map r defines the solution. Moreover, Etingof–Schedler–Soloviev ([ESS99]) proposed to restrict to non-degenerate solutions: when σ_x and τ_x are bijective maps for all x in X. If only one of those is required to be bijective, the solution is called left non-degenerate if it's σ_x that is bijective, and right non-degenerate if it's τ_x. Rump showed that, for finite involutive solutions, left and right non-degeneracy are equivalent ([Rum05, Theorem 2]), and we provide an alternative proof of this fact and its implications in Section 2.3 (answering a question of Dehornoy in [Deh17, Questions Slide 18] to re-obtain his results of [Deh15] without Rump's theorem).

Problem 1.1.0.5 ([Dri92, Theorem 9])**.** *Classify all (finite) set-theoretical solutions to the Yang–Baxter equation (up to isomorphism).*

What about involutive? Non-degenerate? Both?

All involutive non-degenerate solutions of size up to 8 were first obtained in [ESS99], and then [AMV22] improved the classification up to size 10.

To approach this question, the notion of a structure group was introduced to try to shift the problem from combinatorics to algebra.

Definition 1.1.0.6 ([ESS99])**.** *If (X,r) is a solution we define its structure group (resp. monoid) by the presentation*

$$\langle X \mid xy = x'y' \text{ where } r(x,y) = (x',y')\rangle.$$

Example 1.1.0.7. *The trivial solution $(\{a,b\}, r(x,y) = (y,x))$ has structure group given by $\langle a,b \mid ab = ba\rangle \simeq \mathbb{Z}^2$.*

The solution $(\{a,b\}, r(x,y) = (\sigma(y), \sigma(x))$ where σ exchanges a and b, explicitly given as $\begin{cases} r(a,b) = (a,b), & r(a,a) = (b,b) \\ r(b,a) = (b,a), & r(b,b) = (a,a) \end{cases}$, has structure group $\langle a,b \mid a^2 = b^2\rangle$.

Those are the only two solutions of size 2 that are involutive and non-degenerate, as the identity of X^2 is degenerate ($r(x,y) = (x,y)$ implies $\sigma_x y = x$).

Many properties and constructions have been obtained for the structure group (see for instance [ESS99; Rum07; Cho10; GV98]), and we aim here to retrieve some of them with combinatorial and algorithmical technics inspired by [Deh15].

From now on, we will say "a solution" to mean a finite non-degenerate involutive set-theoretical solution of the Yang–Baxter equation.

Remark 1.1.0.8. *In the mathematical literature, the Quantum Yang–Baxter equation (QYBE) also appears ([Yan67; ESS99]), and is used almost interchangeably with the classical case. This equation can be written as*

$$r_{12}r_{13}r_{23} = r_{23}r_{13}r_{12}$$

where r_{ij} acts on the i and j components of $X \times X \times X$.

It is easily seen that one can go from a classical to a quantum solution by composing with the flip $\tau(x,y) = (y,x)$, and vice versa, that is: r is a solution to the YBE if and only if τr is a solution to the QYBE. Moreover, this equivalence preserves finiteness, involutivity and non-degeneracy.

1.2 Cycle sets

Rump introduced in [Rum05] a new object, which he calls cycle sets (and Dehornoy will call "Right-cyclic system") to study solutions. These have the advantage of having a "simpler" and shorter condition compared to the one obtained by expanding the Yang–Baxter equation with $r(x,y) = (\sigma_x(y), \tau_y(x))$ which is quite heavy. The unique condition defining a cycle set comes from, first using that r is involutive to relate $\sigma_x(y)$ and $\tau_y(x)$, then using clever changes of variables to reduce the 3 conditions to 1 (see [Rum05; Bha+21]).

Definition 1.2.0.1 ([Rum05])**.** *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:*

$$(s*t)*(s*u) = (t*s)*(t*u). \tag{1.1}$$

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

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

Analogously to set-theoretical solutions, we have a notion of morphism:

Definition 1.2.0.2. *A morphism of cycle sets $(S,*) \to (T,\star)$ is a map $f\colon S \to T$ such that, for any s_1, s_2 in S, $f(s_1 * s_2) = f(s_1) \star f(s_2)$.*

From now, and all along this thesis, we fix a cycle set $(S,*)$.

As for solutions, we associate to a cycle set a structure group, and a structure monoid, with quadratic relations as follows:

Definition 1.2.0.3 ([Rum05])**.** *The group G_S associated with $(S,*)$ is defined by the presentation:*

$$G_S \coloneqq \langle S \mid s(s*t) = t(t*s),\ \forall s \neq t \in S \rangle\,. \tag{1.2}$$

and called the structure group associated to $(S,*)$. Similarly, we define the structure monoid M_S associated to $(S,*)$ 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 1.2.0.4. *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), and call it the structure group associated to S (omitting the $*$).

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

Remark 1.2.0.5. *By the definition of $\psi\colon S \to \mathfrak{S}_n$ we have that $s_i * s_j = s_{\psi(s_i)(j)}$. For simplicity we will also write $s_{\psi(s_i)(j)}$ as $\psi(s_i)(s_j)$, by the identification between $\mathfrak{S}_n$ and $\mathfrak{S}_S$.*

Obviously, the interest of this object is that it provides an alternative definition of a solution:

Theorem 1.2.0.6 ([Rum05])**.** *There is a bijective correspondence between finite cycle sets and finite involutive left non-degenerate solutions.*

Moreover, this correspondence respects the definition of both structure groups.

Remark 1.2.0.7. *The proof relies in a series of clever change of variables, which Rump does not do in full details: the Yang–Baxter equation involves three identities, and he focuses on one, only mentioning that the last two are equivalent, which in fact requires a bit of work. A complete proof of this statement can be found in [Bha+21, Theorem 3.2.2].*

1.3 Dehornoy's calculus

Recall that we fixed $(S, *)$ a finite cycle set of size n with structure monoid (resp. group) M (resp. G).

In the following, we introduce the basics of Dehornoy's Calculus, which will be easily understood in section 1.5 by directly looking at the representation introduced in the same paper [Deh15]. We then use the representation to retrieve the well-known I-structure of the structure monoid ([GV98]). The goal of this approach is to provide a combinatorial and algorithmical way to work on words in the structure monoid by deriving relations from the quadratic relations defining the monoid.

Although all these results are already stated in [Deh15], their provided proofs are very technical, whereas using monomial matrices will greatly simplify proofs and allow for more intuition while improving the readability (as the notations are lighter). The representation approach, because it mixes the combinatorial techniques of Dehornoy with some brace theory (see Section 1.6), leads to an easier computer implementation to study structure groups.

Definition 1.3.0.1 ([Deh15])**.** *For a positive integer k, we define inductively the formal expression Ω_k by $\Omega_1(x_1) = x_1$ and*

$$\Omega_k(x_1, \dots, x_k) = \Omega_{k-1}(x_1, \dots, x_{k-1}) * \Omega_{k-1}(x_1, \dots, x_{k-2}, x_k). \tag{1.3}$$

We then define another formal expression Π_k by:

$$\Pi_k(x_1, \dots, x_k) = \Omega_1(x_1) \cdot \Omega_2(x_1, x_2) \cdot \ \dots \ \cdot \Omega_k(x_1, \dots, x_k). \tag{1.4}$$

For a cycle set S, $\Omega_k(t_1, \dots, t_k)$ will be the evaluation in S of $\Omega_k(x_1, \dots, x_k)$ at $(t_1, \dots, t_k)$ in S^k. Similarly, $\Pi_k(t_1, \dots, t_k)$ will be the evaluation in M_S of $\Pi_k(t_1, \dots, t_k)$ with the symbol $\cdot$ identified with the product of elements in M_S.

Remark 1.3.0.2. *For $k = 1$ we have $\Omega_1(t) = t$ and $\Pi_1(t) = t$. For $k = 2$ we have $\Omega_2(s, t) = s * t$ and thus $\Pi_2(s, t) = s(s * t)$, which correspond to one of the term of the quadratic relations $s(s * t) = t(t * s)$. Then for $k \geq 3$, Π_k can be thought of as a generalization of the terms of the quadratic relations and Ω_k; the point will be to use those expressions to study words in the structure monoid via a "natural" way to apply relations, and the following statements aim to highlight this.*

The best way to understand this calculus is to look at the Cayley graph of M:
First, the defining relations $s(s*t) = t(t*s)$ can be written as $\Pi_2(s,t) = \Pi_2(t,s)$, or equivalently $\Omega_1(s)\Omega_2(s,t) = \Omega_1(t)\Omega_2(t,s)$.

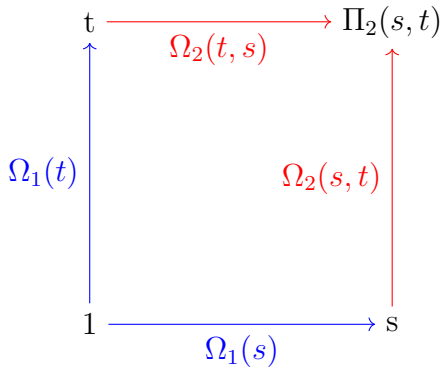
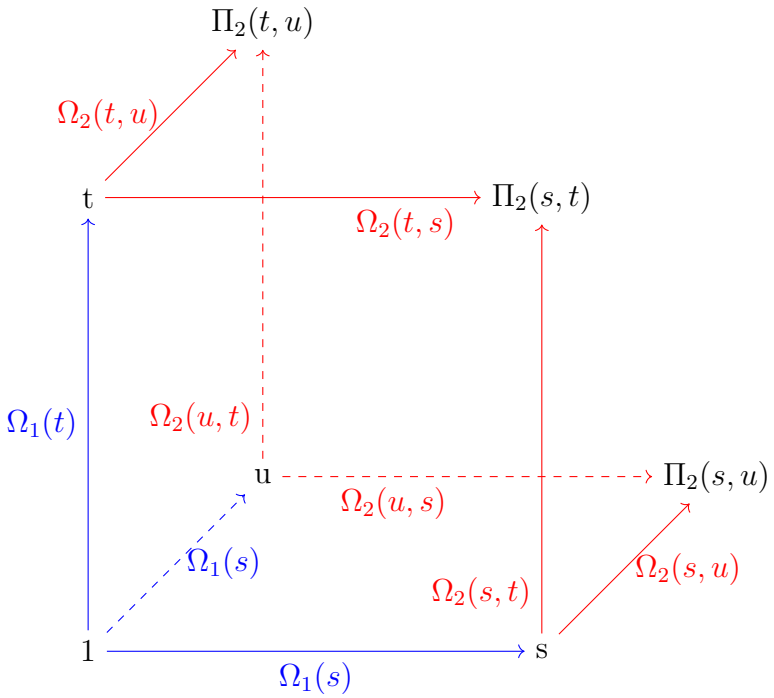


Figure 1.2: Defining relations in the Cayley graph

One of the goal of Dehornoy's calculus is to re-obtain the I-structure, which can be stated as the fact that the Cayley graph of M is isometric to the one of $\mathbb{Z}^n$ ([Deh15]), which is a n dimensional cube lattice.
If we add a third generator u to the square above, we can then "complete" the faces of $(1,s,u)$ and $(1,t,u)$.



From there, we can again complete the faces $(t,\Pi_2(t,u),\Pi_2(s,t))$, $(s,\Pi_2(s,u),\Pi_2(s,t))$, and $(u,\Pi_2(s,u),\Pi_2(t,u))$. The I-structure then corresponds to the fact that those 3 faces

intersect at exactly one point, which is $\Pi_3(s,t,u) = \Pi_3(t,u,s) = \Pi_3(u,t,s)$. *And Dehornoy's calculus allows for a combinatorial approach to this fact.*

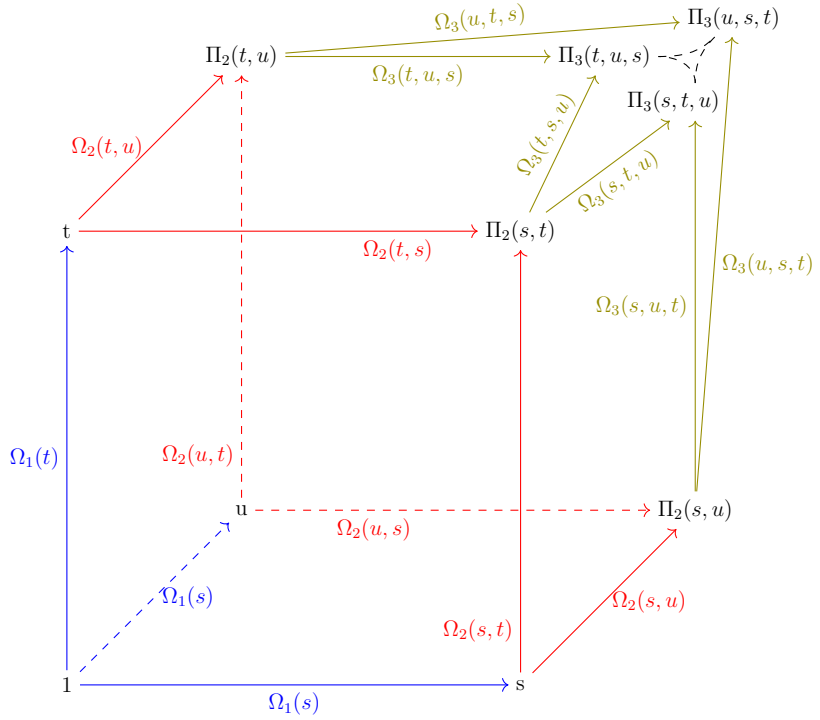


Figure 1.3: Graphical representation of Dehornoy's calculus

This cube will be seen again in Remark 2.1.0.13 (Figure 2.1), giving its name to Cube condition that makes M *a Garside monoid.*

Remark that for any s,t,u in S, $\Omega_3(s,t,u) = \Omega_2(s,t) * \Omega_2(s,u) = (s*t)*(s*u)$. By the definition of a cycle set (Equation (1.1)), we then have $\Omega_3(s,t,u) = (s*t)*(s*u) = (t*s)*(t*u) = \Omega_(t,s,u)$. The following lemma generalizes this property. And this corresponds, in the cube of Figure 1.3, to the fact that two edges Ω_3 that start from the same point, are identified.

Lemma 1.3.0.3 ([Deh15])**.** *The element* $\Omega_k(t_1,\dots,t_k)$ *of* S *is invariant by permutation of the first* $k-1$ *entries.*

Proof. For $k=1$ and $k=2$ there is only the identity permutation and for $k=3$ this is precisely the condition the cycle set equation (1.1):

$$\Omega_3(s,t,u) = \Omega_2(s,t) * \Omega_2(s,u) = (s*t)*(s*u) = (t*s)*(t*u) = \Omega_3(t,s,u).$$

Assume $k \geq 4$ and proceed by induction. Since the transpositions $\sigma_i = \begin{pmatrix} i & i+1 \end{pmatrix}$ generate $\mathfrak{S}_k$, we only have to look at σ_i with $i \leq k-2$. We have, by definition,

$$\Omega_k(t_1,\dots,t_k) = \Omega_{k-1}(t_1,\dots,t_{k-1}) * \Omega_{k-1}(t_1,\dots,t_{k-2},t_k).$$

If $i \neq k-2$, By the induction hypothesis, both Ω_{k-1} occurring here are invariant by σ_i as it does not affect the last term. Remains the case $i = k-2$, for which we have:

$\Omega_k(t_1,\dots,t_{\sigma_{k-2}(r-2)},t_{\sigma_{k-2}(r-1)},t_k) = \Omega_k(t_1,\dots,t_{k-3},t_{k-1},t_{k-2},t_k)$
$= \Omega_{k-1}(t_1,\dots,t_{k-3},t_{k-1},t_{k-2}) * \Omega_{k-1}(t_1,\dots,t_{k-3},t_{k-1},t_k)$ (Expanding)
$= (\Omega_{k-2}(t_1,\dots,t_{k-3},t_{k-1}) * \Omega_{k-2}(t_1,\dots,t_{k-3},t_{k-2}))$ (Expanding)
$\quad * (\Omega_{k-2}(t_1,\dots,t_{k-3},t_{k-1}) * \Omega_{k-2}(t_1,\dots,t_{k-3},t_k))$
$= (\Omega_{k-2}(t_1,\dots,t_{k-3},t_{k-2}) * \Omega_{k-2}(t_1,\dots,t_{k-3},t_{k-1}))$ (cycle set Equation)
$\quad * (\Omega_{k-2}(t_1,\dots,t_{k-3},t_{k-2}) * \Omega_{k-2}(t_1,\dots,t_{k-3},t_k))$
$= \Omega_{k-1}(t_1,\dots,t_{k-3},t_{k-2},t_{k-1}) * \Omega_{k-1}(t_1,\dots,t_{k-3},t_{k-2},t_k)$ (Collapsing)
$= \Omega_k(t_1,\dots,t_{k-2},t_{k-1},t_k).$ (Collapsing)
□

The defining relations of the monoid can be written as $\Pi_2(s,t) = \Pi_2(t,s)$, and the next propositions generalizes this property. In particular, in Figure 1.3, this leads to the cube "closing" , with the identification of the 3 top-right vertices.

Proposition 1.3.0.4. *The element $\Pi_k(t_1,\dots,t_k)$ of M_S is invariant by permutation of the entries.*

Proof. For $k=1$ there is nothing to prove. For $k=2$ we find $\Pi_2(t_1,t_2) = t_1(t_1 * t_2)$ which is identified with $t_2(t_2 * t_1) = \Pi_2(t_2,t_1)$ by the defining relations of M in 1.2.

Now assume $k \geq 3$ and, as in the proof of the previous lemma; restrict to the transpositions $\sigma_i = \begin{pmatrix} i & i+1 \end{pmatrix}$ with $1 \leq i < k$. Recall that, by definition

$$\Pi_k(t_1,\dots,t_k) = \Omega_1(t_1) \cdot \Omega_2(t_1,t_2) \cdot \cdots \cdot \Omega_k(t_1,\dots,t_k).$$

Clearly, the first $i-1$ terms remain unchanged by σ_i. And by the previous Lemma 1.3.0.3, for $k > i+1$ the terms Ω_k are invariant by σ_i. Thus we only have to look at the product:
$\Omega_i(t_1,\dots,t_{i-1},t_{i+1}) \cdot \Omega_{i+1}(t_1,\dots,t_{i-1},t_{i+1},t_i)$
$= \Omega_i(t_1,\dots,t_{i-1},t_{i+1}) \cdot (\Omega_i(t_1,\dots,t_{i-1},t_{i+1}) * \Omega_i(t_1,\dots,t_{i-1},t_i))$ (Expanding)
$= \Omega_i(t_1,\dots,t_{i-1},t_i) \cdot (\Omega_i(t_1,\dots,t_{i-1},t_1) * \Omega_i(t_1,\dots,t_{i-1},t_{i+1}))$ (Relations of M)
$= \Omega_i(t_1,\dots,t_{i-1},t_i) \cdot \Omega_{i+1}(t_1,\dots,t_{i-1},t_i,t_{i+1}).$ (Collapsing)
Which shows that Π is invariant by permutation of the entries. □

Now having better understood the generalization of the relations, we will show that any element can be seen as one those. Thus, applying relations to a word in M will be seen as using the above properties. The idea of the following lemma is that, the Cayley graph of M will always locally look like Figure 1.3. More precisely, if we start at any vertex of the Cayley graph, we have the same cube up to a permutation of the labels.

Lemma 1.3.0.5. *For any positive integer k, and any $s,t_1,\dots,t_k$ in S, the map $s \mapsto \Omega_{k+1}(t_1,\dots,t_k,s)$ is bijective.*

Proof. We proceed by induction: for $k=1$ there is nothing to prove, for $k=2$ this is part of the definition of a cycle set. So consider $k \geq 2$ and suppose that the property holds for $k-1$. We have

$$\Omega_{k+1}(t_1,\dots,t_k,s) = \Omega_k(t_1,\dots,t_k) * \Omega_k(t_1,\dots,t_{k-1},s),$$

by induction hypothesis $s \mapsto \Omega_{t_1,\dots,t_{k-1},s}$ is bijective, and as $\Omega_k t_1,\dots,t_k$ is an element of S, its left action is bijective, which concludes the proof. □

From this lemma, we can deduce that any edge of the Cayley graph (equivalently any element of M) can be reached by taking step-by-step $\Omega_\bullet$ from the origin, and this written as a $\Pi_\bullet$.

Proposition 1.3.0.6. *Let f be in M. Then there exists $(t_1, \dots, t_k)$ in S^k such that $f = \Pi_k(t_1, \dots, t_k)$.*

In the sequel, for any $f \in M$, by a "Π-expression of f" we mean choosing any $(t_1, \dots, t_k)$ in S^k such that $f = \Pi_k(t_1, \dots, t_k)$.

Proof. Take a decomposition of f as a product of elements of S:

$$f = t'_1 t'_2 \dots t'_k.$$

Let $t_1 = t'_1$, because S is a cycle set, the map $t' \mapsto t_1 * t'$ is bijective, so there exists t_2 such that $t'_2 = t_1 * t_2$ (explicitly $t_2 = \psi(t_1)^{-1}(t'_2)$), i.e.:

$$f = t_1(t_1 * t_2)t'_3 \dots t'_k = \Omega_1(t_1)\Omega_2(t_1, t_2)t'_3 \dots t'_k = \Pi_2(t_1, t_2)t'_3 \dots t'_k.$$

We proceed by induction on k: suppose that we have $t_1, \dots, t_{k-1}$ such that $t'_1 \dots t'_{k-1} = \Pi_{k-1}(t_1, \dots, t_{k-1})$, i.e. $t'_i = \Omega_k(t_1, \dots, t_i)$ for $i < k$. By the previous lemma the map $s \mapsto \Omega_k(t_1, \dots, t_{k-1}, s)$ is bijective, so there exists t_k such that

$$t'_k = \Omega_k(t_1, \dots, t_k).$$

By induction, this gives the existence of $t_1, \dots, t_k$ such that

$$f = \Omega_1(t_1) \dots \Omega_k(t_1, \dots, t_k) = \Pi_k(t_1, \dots, t_k).$$

□

Example 1.3.0.7. *Take $S = \{s_1, s_2, s_3, s_4\}$ with*

$$\psi(s_1) = (1234) \qquad \psi(s_3) = (24)$$
$$\psi(s_2) = (1432) \qquad \psi(s_4) = (13).$$

And consider the element $f = s_1 s_2 s_3 s_4$. We have $\psi(s_1)^{-1}(s_2) = s_1$, so $f = s_1(s_1 * s_1)s_3 s_4 = \Pi_2(s_1, s_1)s_3 s_4$.

Similarly, $\psi(s_2)^{-1}(s_3) = s_4$, so $s_3 = s_2 * s_3 = (s_1 * s_1) * s_4$, as $\psi(s_1)^{-1}(s_4) = s_3$, we have $s_3 = (s_1 * s_1) * (s_1 * s_3) = \Omega_3(s_1, s_1, s_3)$. So $f = \Pi_3(s_1, s_1, s_3)s_4$.

Finally, for s_4, we first write $s_4 = s_3 * a$, then $a = s_2 * b$ and $b = s_1 * c$ (going through the letters of $f = s_1 s_2 s_3 s_4$ from right to left), so that $s_4 = s_3 * (s_2 * (s_1 * c)))$. Replacing s_3, s_2 and s_1 by their previously found expressions gives

$$s_4 = ((s_1 * s_1) * (s_1 * s_3)) * ((s_1 * s_1) * (s_1 * c)) = \Omega_4(s_1, s_1, s_3, c).$$

Here we find $c = s_2$ so

$$f = \Pi_4(s_1, s_1, s_3, s_2).$$

One can also check for instance that $s_4 = \Omega_4(s_1, s_1, s_3, s_2)$ also equals $\Omega_4(s_3, s_1, s_1, s_2)$ and so $f = \Pi_4(s_3, s_1, s_1, s_2)$.

1.4 Monomial matrices

In the next section, we will introduce the representation of Dehornoy from [Deh15] that will be used to study solutions, but first we need the basics on monomial matrices. We recall the definition and some properties: A matrix is said to be monomial if each row and each column has a unique non-zero coefficient. We denote by $\mathfrak{Monom}_n(R)$ the set of monomial matrices over a ring R. To a permutation $\sigma \in \mathfrak{S}_n$ we associate the permutation matrix P_σ where the i-th row contains a 1 on the $\sigma(i)$-th column, for instance $P_{(123)} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$. We then have $P_\sigma \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} v_{\sigma(1)} \\ \vdots \\ v_{\sigma(n)} \end{pmatrix}$ and thus, if e_i is the i-th canonical basis vector, $P_\sigma(e_i) = e_{\sigma^{-1}(i)}$. Moreover, for $\sigma, \tau \in \mathfrak{S}_n$ we find $P_\sigma P_\tau = P_{\tau\sigma}$. It is well known that a monomial matrix admits a unique (left) decomposition as a diagonal matrix right-multiplied by a permutation matrix. Thus, if m is monomial, D_m will denote the associated diagonal matrix, and P_m the associated permutation matrix, i.e. $m = D_m P_m$, and by $\psi(m)$ we will denote the permutation associated with the matrix P_m. Let D be a diagonal matrix and P a permutation matrix. We denote the conjugate matrix PDP^{-1} as ${}^P D$, and if σ is the permutation associated with P we will also write ${}^\sigma D$. The following statements are well-known. As they will be essential throughout this paper, we state them explicitly:

Lemma 1.4.0.1. *Let D be a diagonal matrix and P a permutation matrix. Then ${}^P D$ is diagonal.*

Moreover, the i-th row of D is sent by conjugation to the $\sigma^{-1}(i)$-th row.

In particular, this implies that, $P_\sigma D = {}^\sigma D P_\sigma$ giving a way to alternate between left and right (unique) decomposition of monomial matrices.

Corollary 1.4.0.2. *Let m and m' be monomial matrices. Then we have the identities $D_{mm'} = D_m \left({}^{\psi(m)}D_{m'}\right)$ and $\psi(mm') = \psi(m') \circ \psi(m)$.*

To simplify notations we will sometimes only write ${}^m D_{m'}$ for ${}^{\psi(m)}D_{m'}$.

As a final example, let $m = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix}$, $m' = \begin{pmatrix} 0 & 0 & x \\ 0 & y & 0 \\ z & 0 & 0 \end{pmatrix}$, which decomposes with $D_m = \mathrm{diag}(a, b, c)$, $D_{m'} = \mathrm{diag}(x, y, z)$ and $\psi(m) = (123)$, $\psi(m') = (13)$. We find $\psi(m') \circ \psi(m) = (13) \circ (123) = (12)$ and

$$D_m \left({}^{\psi(m)}D_{m'}\right) = \mathrm{diag}(a, b, c)\, {}^{(123)}\mathrm{diag}(x, y, z) = \mathrm{diag}(a, b, c)\mathrm{diag}(y, z, x) = \mathrm{diag}(ay, bz, cx)$$

and indeed $mm' = \begin{pmatrix} 0 & ay & 0 \\ bz & 0 & 0 \\ 0 & 0 & cx \end{pmatrix} = \mathrm{diag}(ay, bz, cx) P_{(12)}$.

1.5 The monomial representation

We can now define and study Dehornoy's representation ([Deh15]), which will allow for a simplification and a better understanding of his proofs. This representation is a monomial representation, which will allow the use of particular techniques following from the

previous section. In particular, the fact that this representation is monomial relies on the I-structure of the structure group ([GV98; Deh15]) and provides an alternative description of this structure. A similar representation, one dimension higher, also appears in a work of Chouraqui ([Cho23]).

Recall that we fix $(S, *)$ a finite cycle set of size n with $S = \{s_1, \dots, s_n\}$ and with structure monoid (resp. group) M (resp. G).

Proposition 1.5.0.1 ([Deh15])**.** *Let z be an indeterminate and consider the matrix group $\mathfrak{Monom}_n(\mathbb{Q}(z)$, denote $D_{s_i} = diag(1, \dots, z, \dots, 1)$ the $n \times n$ diagonal matrix with a z on the i-th row.*

The map Θ defined on S by

$$\Theta(s_i) \coloneqq D_{s_i} P_{\psi(s_i)} \tag{1.5}$$

extends to a representation $G \to \mathfrak{Monom}_n(\mathbb{Q}(z))$ and similarly to a morphism $M \to \mathfrak{Monom}_n(\mathbb{Q}[z])$.

Proof. We have to show that Θ respects the defining relations of G (and M). Let s_i, s_j be in S and define $g = \Theta(s_i)\Theta(s_i * s_j)$ and $g' = \Theta(s_j)\Theta(s_j * s_i)$. By Corollary 1.4.0.2 we have $D_g = D_{s_i}{}^{\psi(s_i)} D_{s_i * s_j} = D_{s_i}{}^{\psi(s_i)} D_{\psi(s_i)(s_j)}$ and the latter is equal to $D_{s_i} D_{s_j}$ by Lemma 1.4.0.1. By symmetry and commutativity of diagonal matrices, we deduce $D_g = D_{g'}$.

On the other hand, again by Corollary 1.4.0.2, we have $\psi(g)(t) = \psi(s_i * s_j) \circ \psi(s_i)(t) = (s_i * s_j) * (s_i * t)$ for all $t \in S$. By symmetry and as S is a cycle set we deduce that $\psi(g) = \psi(g')$ and so $g = g'$. □

For simplicity, we will write $\Theta(g) = D_g P_g$ to mean $\Theta(g) = D_{\Theta(g)} P_{\Theta(g)}$.

Remark 1.5.0.2. *The image of G by Θ lies in the subgroup of $\mathfrak{Monom}_n(\mathbb{Q}(z)$ consisting of matrices such that the non-zero coefficients (i.e. the diagonal part of the decomposition) consists only of powers of z (including $z^0 = 1$). We denote this subgroup by Σ_n. By Σ_n^+ we denote the submonoid of $\mathfrak{Monom}_n(\mathbb{Q}[z])$ consisting of matrices whose non-zero coefficients are non-negative powers of z only, and by D_i the matrix $diag(1, \dots, z, \dots, 1)$ with a z in the i-th place.*

Let G^+ be the submonoid of G of positive words. As M and G^+ have the same generators, their images in their respective representations Θ coincide. Thus, when working in $\mathfrak{Monom}_n(\mathbb{Q}(z)$, we will not distinguish between $\Theta(M)$ and $\Theta(G^+)$. Later, we will see that in fact G is the group of fractions of M and $M = G^+$.

Example 1.5.0.3. *Set $S = \{s_1, s_2, s_3\}$ and $\psi(s_i) = (123)$ for all i.*

$$\Theta(s_1) = \begin{pmatrix} z & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & z & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

and similarly

$$\Theta(s_2) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & z \\ 1 & 0 & 0 \end{pmatrix} \quad \Theta(s_3) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ z & 0 & 0 \end{pmatrix}.$$

As a direct consequence of Lemma 1.4.0.1 we have the following, which will be useful for going from left to right monomial decompositions.

Proposition 1.5.0.4. *For all $s, t \in S$:*

$$P_s D_t = {}^{\psi(s)}D_t P_s = D_{\psi(s)^{-1}(t)} P_s.$$

In particular, $P_s D_{s*t} = D_t P_s$.

Because the representation is monomial, we are interested in the non-zero coefficient of each row of a matrix, which will be a power of z. Moreover, as the monoid only has quadratic relations, we can define a length on words from these powers (as each generators contributes by one power of z).

Definition 1.5.0.5. *For an element $g \in \Sigma_n$, we define its "coefficient-powers tuple" $cp(g)$ to be the unique n-tuple of integers $(c_1, \ldots, c_n)$ such that $D_g = diag(z^{c_1}, \ldots, z^{c_n})$.*

We set $\ell(g) \coloneqq \sum_{i=0}^{n} \mid c_i \mid$.

For $\sigma \in \mathfrak{S}_n$, by ${}^{\sigma}(c_1, \ldots, c_n)$ we denote $(c_{\sigma(1)}, \ldots, c_{\sigma(n)})$.

Example 1.5.0.6. *If* $g = \begin{pmatrix} z^2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & z^{-1} \\ 0 & z & 0 & 0 \end{pmatrix}$, *then* $cp(g) = (2, 0, -1, 1)$ *and* $\ell(g) = 2 + 0 + 1 + 1 = 4$.

Proposition 1.5.0.7. *For all $g, h \in \Sigma_n$ we have:*

$$cp(gh) = cp(g) + {}^{\psi(g)}cp(h). \tag{1.6}$$

Moreover, if $g, h \in \Theta(M)$, then $\ell(gh) = \ell(g) + \ell(h)$.

Proof. The first equality is a direct consequence of Corollary 1.4.0.2 applied to the representation. The second follows from the fact that the defining relations of the structure monoid respects the length of words. □

Set $\Omega' = \Theta \circ \Omega$ and $\Pi' = \Theta \circ \Pi$ the evaluation in the representation of the constructions from Section 1.3, that is $\Pi'_k(t_1, \ldots, t_k) = \Theta(\Pi(t_1, \ldots, t_k))$. The following proposition and corollary shows how Dehornoy's calculus works very well with the monomial representation, and how we can deduce a Pi-expression for any element in the monoid.

Proposition 1.5.0.8. *Let $t_1, \ldots, t_k$ be in S, then*

$$D_{\Pi'_k(t_1,\ldots,t_k)} = D_{t_1} \cdots D_{t_k}$$

and

$$P_{\Pi'_k(t_1,\ldots,t_k)} = P_{\Omega'_1(t_1)} \cdots P_{\Omega'_k(t_1,\ldots,t_k)}.$$

Or, equivalently for all s in S, $\psi(\Pi'_k(t_1, \ldots, t_k))(s) = \Omega'_{k+1}(t_1, \ldots, t_k, s)$.

Proof. We proceed by induction: for $r = 1$, $\Pi_1(t_1) = t_1$ and there is nothing to prove. Assume $r \geq 1$ and the property true for $r-1$. Then, by definition we have $\Pi(t_1, \ldots, t_k) = \Pi_{k-1}(t_1, \ldots, t_{k-1}) \cdot \Omega_k(t_1, \ldots, t_k)$. So, by the induction hypothesis

$$\Pi'_k(t_1, \ldots, t_k) = \left(D_{t_1} \ldots D_{t_{k-1}} P_{\Omega'_1(t_1)} \ldots P_{\Omega'_{k-1}(t_1, \ldots t_{k-1})}\right) \left(D_{\Omega'_k(t_1, \ldots, t_k)} P_{\Omega'_k(t_1, \ldots, t_k)}\right)$$

Note that $\Omega'_k(t_1, \ldots, t_k) = \Omega'_{k-1}(t_1, \ldots, t_{k-1}) * \Omega'_{k-1}(t_1, \ldots, t_{k-2}, t_k)$. So by Proposition 1.5.0.4 we get

$$\begin{aligned} P_{\Omega'_{k-1}(t_1, \ldots t_{k-1})} D_{\Omega'_k(t_1, \ldots, t_k)} &= P_{\Omega'_{k-1}(t_1, \ldots t_{k-1})} D_{\Omega'_{k-1}(t_1, \ldots, t_{k-1}) * \Omega'_{k-1}(t_1, \ldots, t_{k-2}, t_k)} \\ &= D_{\Omega'_{k-1}(t_1, \ldots, t_{k-2}, t_k)} P_{\Omega'_{k-1}(t_1, \ldots t_{k-1})}. \end{aligned}$$

We can then repeat this process for all the permutation matrices $P_{\Omega'_{k-2}(t_1, \ldots t_{k-2})}, \ldots, P_{\Omega'_1(t_1)}$ and get

$$P_{\Omega'_1(t_1)} \ldots P_{\Omega'_{k-1}(t_1, \ldots t_{k-1})} D_{\Omega'_k(t_1, \ldots, t_k)} = D_{t_k} P_{\Omega'_1(t_1)} \ldots P_{\Omega'_{k-1}(t_1, \ldots t_{k-1})}.$$

Thus we find

$$\Pi'_k(t_1, \ldots, t_k) = (D_{t_1} \ldots D_{t_k}) \left(P_{\Omega'_1(t_1)} \ldots P_{\Omega'_k(t_1, \ldots, t_k)}\right).$$

As $P_\sigma P_\tau = P_{\tau\sigma}$, we have $\psi(\Pi'_k(t_1, \ldots, t_k))(s) = \psi(\Omega'_k(t_1, \ldots, t_k)) \circ \cdots \circ \psi(\Omega'_1(t_1))(s)$. Then $\psi(\Omega'_1(t_1))(s) = t_1 * s = \Omega_2(t_1, s)$, which in turns gives $\psi(\Omega'_2(t_1, t_2)) \circ \psi(\Omega'_1(t_1))(s) = \psi(\Omega_2(t_1, t_2))(\Omega_2(t_1, s)) = \Omega_2(t_1, t_2) * \Omega_2(t_1, s) = \Omega_3(t_1, t_2, s)$. By induction, this gives the last statement. □

Corollary 1.5.0.9. *Any tuple of non-negative integers $(c_1 \ldots, c_n) \in \mathbb{N}^n$ can be realized as the coefficient-powers tuple of a matrix in $\Theta(M_S)$.*

Proof. Let $l = \sum_i c_i$ and take the l-tuple containing c_i times the element s_i. By the previous Proposition 1.5.0.8, we know that Π'_l applied to this tuple gives the expected result. □

Example 1.5.0.10. *As in 1.3.0.7 take $S = \{s_1, s_2, s_3, s_4\}$ with*

$$\psi(s_1) = (1234) \qquad \psi(s_3) = (24) \qquad \psi(s_2) = (1432) \qquad \psi(s_4) = (13).$$

The tuple $(2, 1, 1, 0)$ can be obtained from $\Pi_4(s_1, s_1, s_3, s_2) = s_1 s_2 s_3 s_4 = f$ as, in the induction of the proof of Proposition 1.5.0.8 we did:

$$\begin{aligned} P_{s_1} P_{s_2} P_{s_3} D_{s_4} &= P_{s_1} P_{s_2} D_{\psi(s_3)^{-1}(s_4)} P_{s_3} = P_{s_1} D_{\psi(s_2)^{-1} \circ \psi(s_3)^{-1}(s_4)} P_{s_2} P_{s_3} \\ &= D_{\psi(s_1)^{-1} \circ \psi(s_2)^{-1} \circ \psi(s_3)^{-1}(s_4)} P_{s_1} P_{s_2} P_{s_3} \end{aligned}$$

to obtain the last s_2 in $\Pi_4(s_1, s_1, s_3, s_2)$.

Computing $\psi(s_1)^{-1} \circ \psi(s_2)^{-1} \circ \psi(s_3)^{-1}(s_4) = s_2$ precisely retrieves the Example 1.3.0.7.

Corollary 1.5.0.11. *Any $f \in M$ is uniquely determined by $D_{\Theta(f)}$.*

Moreover, this diagonal part can be read as the entries when taking a Π-expression of f, i.e. if $D_{\Theta(f)} = D_{s_1}^{a_1} \cdots D_{s_n}^{a_n}$ then $f = \Pi_{a_1 + \cdots + a_n}(s_1, \ldots, s_1, \ldots, s_n, \ldots, s_n)$ where s_i occurs a_i times.

From Proposition 1.5.0.8 the diagonal part is determined by the entries of a Π-expression, which is invariant by permutations of those entries by Proposition 1.3.0.4. This implies that the representation Θ is injective when restricted to the monoid.

Proof. This follows from the previous proposition and Proposition 1.3.0.6. Take $\Theta(f) = D_f P_f \in M$ with $D_f = D_{s_1}^{a_1} \dots D_{s_k}^{a_k}$. By Proposition 1.3.0.6 there exist $t_1, \dots, t_k \in S$ such that $f = \Pi_k(t_1, \dots, t_k)$. By Proposition 1.5.0.8, we have $D_{\Theta(f)} = D_{t_1} \dots D_{t_k}$, this gives the second statement. By the unicity of the monomial decomposition, we must have a_i times s_i in the tuple $(t_1, \dots, t_k)$ and by Proposition 1.3.0.4 the orders of the t_i's does not matter.

Thus if $g \in M$ is such that $D_{\Theta(g)} = D_{\Theta(f)}$, by the same argument we must have $g = \Pi_k(t_1, \dots, t_k) = f$. □

Denote $\mathfrak{D}_n$ (resp. $\mathfrak{D}_n^+$) the subset of diagonal matrices of Σ_n (resp. Σ_n^+). We have an obvious inclusion $\mathfrak{D}_n^+ \hookrightarrow \mathfrak{D}_n$, and a faithful representation $\mathbb{N}^n \xrightarrow{\sim} \mathfrak{D}_n^+$.

We now focus on extending the results from the structure monoid to the structure group:

Corollary 1.5.0.12. *The natural morphism $M \to G$ sending each generator $s_i \in M$ to $s_i \in G$ is injective.*

Proof. We have shown that there is a (set) bijection $\Pi\colon \mathbb{N}^n \xrightarrow{\sim} M$. Then we have the following commutative diagram:

$$\begin{array}{ccccc} \mathbb{N}^n & \xrightarrow[\Pi]{\sim} & M & \longrightarrow & G \\ \downarrow{\scriptstyle \sim} & & & & \downarrow \\ \mathfrak{D}_n^+ & & \hookrightarrow & & \mathfrak{D}_n \end{array}$$

Because the composition $\mathbb{N}^n \to \mathfrak{D}_n^+ \to \mathfrak{D}_n$ is injective, and as $\Pi\colon \mathbb{N}^n \to M$ is bijective, the composition $M \to G \to \mathfrak{D}_n$ must be injective, so necessarily M injects in G. □

A word $t_1 \dots t_k$ over S representing an element g in M is said to be reduced if its length k is minimal among the representative words of g.

Proposition 1.5.0.13. *Any element $g \in G$ can be decomposed as a reduced left-fraction in M, that is:*

$$\exists f, h \in M, g = fh^{-1} \text{ with } \ell(g) = \ell(f) + \ell(h)$$

where ℓ denotes the length as a $S \cup S^{-1}$-word.

Proof. Let $g \in G$, and write a reduced decomposition of g as product of elements in $S \cup S^{-1}$. If this expression is of length 1, this is trivial. If the length is 2, we have 4 cases with $s, t \in S$: st, $s^{-1}t^{-1}$, st^{-1} and $s^{-1}t$. The first 3 cases are of the desired form. For the last one, the defining relations of G give

$$s(s * t) = t(t * s) \iff s^{-1}t = (s * t)(t * s)^{-1}.$$

For arbitrary length, we can inductively use the same relation $s^{-1}t = (s * t)(t * s)^{-1}$ to "move" all inverses of the generators to the right in a decomposition of g, which gives the desired form. □

We will soon state a similar result for right-fractions (Corollary 1.5.0.16).

Corollary 1.5.0.14. *Any element in G can be decomposed as a left-fraction fh^{-1} in M such that D_h commutes with all permutation matrices (more precisely that D_h is a power of $D_{s_1} \dots D_{s_n}$).*

Proof. Take a Π-expression $\Pi_k(t_1, \dots, t_k)$ of h. Up to permuting the entries, by Proposition 1.3.0.4, we can assume that $h = \Pi_k(s_1, \dots, s_1, \dots, s_n, \dots, s_n)$, where for $1 \leq i \leq n$ each s_i occurs a_i times and $a_1 + \dots + a_n = k$. Let j be such that a_j is (one of) the biggest of the a_i's, then if for some i we have $a_i < a_j$ we can consider a new element $\Pi_{k+1}(s_1, \dots, s_1, \dots, s_n, \dots, s_n, s_i) = h \cdot \Omega_{k+1}(s_1, \dots, s_1, \dots, s_n, \dots, s_n, s_i)$, where s_i occurs $a_i + 1$ times and that is obtained from h by right-multiplying by an element in S. Doing so, until all s_i occurs a_j times, provides an element $\overline{h}$ which is obtained from h by right-multiplication by some $h' \in M$ and such that $D_{\overline{h}} = (D_{s_1} \dots D_{s_n})^{a_j}$.

Let P_σ be a permutation matrix, then $P_\sigma D_{\overline{h}} = {}^{\sigma}D_{\overline{h}} P_\sigma = D_{\overline{h}} P_\sigma$ where the last equality is because all the diagonal terms in $D_{\overline{h}}$ are equal so are invariant by σ. Finally $fh'(\overline{h})^{-1} = fh^{-1}$, so replacing (f, h) by (fh', hh') gives us the result. □

Example 1.5.0.15. *Take $S = \{s_1, s_2, s_3\}$ and $\psi(s_i) = (123)$ for all i. Consider $g = s_3^{-1}s_2^{-1}s_3$, the relation $s_2s_1 = s_3s_3$ (i.e. $s_1s_3^{-1} = s_2^{-1}s_3$) gives $g = s_3^{-1}s_1s_3^{-1}$; similarly $s_3s_2 = s_1s_1$ (i.e. $s_2s_1^{-1} = s_3^{-1}s_1$) yields $g = s_2s_1^{-1}s_1^{-1}$.*

Let $f = s_2$ and $h = s_1s_1$ so that $g = fh^{-1}$, we have $h = s_1(s_1 * s_3) = \Pi_2(s_1, s_3)$, thus $D_h = D_{\Theta(h)} = D_{s_1}D_{s_3}$, which is not stable under permutation (as we have ${}^{(123)}D_h = D_{s_{(123)^{-1}(1)}}D_{s_{(123)^{-1}(2)}} = D_{s_3}D_{s_2} \neq D_h$). To complete h so that it commutes, we must add D_{s_3}, so we take $h' = \Pi_3(s_1, s_2, s_3) = hs_1$ and $f' = fs_1$. Now $D_{h'} = D_{s_1}D_{s_2}D_{s_3}$ commutes with permutation matrices, and $f'h'^{-1} = fs_1s_1^{-1}h^{-1} = fh^{-1} = g$.

Corollary 1.5.0.16. *Any element in G can be decomposed as a reduced right-fraction in the submonoid $G^+ = M$, that is:*

$$\forall g \in G, \exists f, h \in M, g = h^{-1}f \text{ with } \ell(g) = \ell(f) + \ell(h).$$

In particular, G is the group of fractions of M.

Proof. From Proposition 1.5.0.13, start with a reduced left-fraction of g as fh^{-1} such that D_h commutes with all permutation matrices. Then $g = fh^{-1} = D_fP_fP_h^{-1}D_h^{-1} = D_h^{-1}D_fP_fP_h^{-1}$. So $hg = D_hP_hg = P_hD_hg = P_hD_hD_h^{-1}D_fP_fP_h^{-1} = P_hD_fP_fP_h^{-1} = {}^hD_fP_hP_fP_h^{-1} = f'$. As $f \in M$, so does f', and thus $g = h^{-1}f'$. Reducing this expression if necessary finishes the proof. □

In [ESS99, Proposition 2.5] and then [GV98; Deh15] it is shown that the structure group G of a finite cycle set S of size n has an I-structure: G embeds in $\mathbb{Z}^n \rtimes \mathfrak{S}_n$ such that projecting on the first coordinate is a bijection. Moreover, the structure monoid M embeds in G and corresponds to first coordinates in $\mathbb{N}^n$. We've already seen that M embeds in G, we now prove in the following statements a matricial equivalent of the I-structure:

Theorem 1.5.0.17 ([Deh15])**.** *Let S be a finite cycle set of cardinal n. Then Θ is a faithful representation of G.*

Proof. Let $g \in G$, from Proposition 1.5.0.13 we know that there exist $f, h \in M$ such that $g = fh^{-1}$. Thus as Θ is a representation:

$$\Theta(g) = \mathrm{Id}_n \iff \Theta(f) = \Theta(h)$$

By Corollary 1.5.0.12, $\Theta(f) = \Theta(h) \iff f = h$, thus Θ is faithful. □

From now on, we assume that S is a finite cycle set with $S = \{s_1, \ldots, s_n\}$. We identify G with its image by the (faithful) representation Θ. We can as well identify Ω (resp. Π) with its image Ω' (resp. Π') by Θ.

Definition 1.5.0.18. *A subgroup of Σ_n is called permutation-free if the only permutation matrix it contains is the identity.*

Proposition 1.5.0.19. *G is permutation-free.*

Proof. Suppose P_σ is a permutation matrix (associated with $\sigma \in \mathfrak{S}_n$) that is in G. Then by Proposition 1.5.0.13, there exists $f, g \in M$ such that $P_\sigma = fg^{-1}$, i.e. $D_f P_f = P_\sigma D_g P_g$. And by Corollary 1.5.0.14 we can moreover assume that D_g commutes with permutation matrices ($P_\sigma D_g = D_g P_\sigma$), so $D_f P_f = D_g P_\sigma P_g$. By the unicity of the monomial decomposition, we must have $D_f = D_g$ and $P_f = P_\sigma P_g$, so by Proposition 1.5.0.11 $f = g$ and thus P_σ =Id (and σ =id). □

Corollary 1.5.0.20. *An element $g \in G$ is uniquely determined by D_g.*

Proof. Suppose for $g, h \in G$ we have $D_g = D_h$. Then

$$g^{-1}h = (D_g P_g)^{-1}(D_h P_h) = P_g^{-1} D_g^{-1} D_g P_h = P_g^{-1} P_h \in G$$

We have $P_g^{-1} P_h$ is a permutation matrix G, so it must be the identity. Thus $P_g = P_h$ and thus $g = h$. □

Corollary 1.5.0.21. *An element g in G is in M if and only if it has only non-negative powers of z as non-zero coefficients (i.e $g \in \Sigma_n^+$).*

Proof. From Proposition 1.3.0.6 we know that $g \in M$ implies $g \in \Sigma_n^+$ (where we identified G with its image $\Theta(G)$). Reciprocally, suppose $g \in G$ is such that $\Theta(g) = D_g P_g \in \mathfrak{M}_n^+$ (i.e $D_g \in \mathfrak{D}_n^+$). From Corollary 1.5.0.9, we know there exists $f \in M$ such that $D_f = D_g \in \mathfrak{D}_n^+$. Then $g^{-1}f = P_g^{-1} D_g^{-1} D_f P_f = P_g^{-1} P_f$ is a permutation matrix. By Proposition 1.5.0.19, this permutation matrix must be trivial, so $g = f$ is in M. □

We relate Proposition 1.5.0.19 to the two usual ways to present the I-structure: an embedding and a 1-cocycle. A 1-cocycle associated to an action $\phi \colon G \to \mathrm{Aut}(H)$ is a map $f \colon G \to H$ such that $f(gg') = f(g)\phi(g)(f(g'))$ for all g, g' in G.

Corollary 1.5.0.22 ([ESS99; GV98])**.** *G embeds as a subgroup of $\mathbb{Z}^n \rtimes \mathfrak{S}_n$ such that the restriction to the first coordinate is bijective (i.e $G \cap \{1\} \rtimes \mathfrak{S}_n = \{1\}$).*

Equivalently, we have a bijective 1-cocycle $cp \colon G \to \mathbb{Z}^n$ associated to the action given by ψ^{-1}.

Moreover, in this embedding, M is identified with $G \cap (\mathbb{N}^n \rtimes \mathfrak{S}_n)$.

Proof. Consider the map $f\colon G \to \mathbb{Z}^n \rtimes \mathfrak{S}_n$ defined by $f(g) = (\mathrm{cp(g)}, \psi^{-1}(g))$. Then, by Proposition 1.5.0.7, $f(gh) = (\mathrm{cp}(g) + {}^{\psi(g)}\mathrm{cp}(h), \psi^{-1}(gh))$. Corollary 1.4.0.2 implies that $\psi(gh) = \psi(h)(g)$, thus $\psi^{-1}(gh) = \psi^{-1}(g)\psi^{-1}(h)$. Also note that if $(a_1, \dots, a_n) \in \mathbb{Z}^n$ and $\sigma \in \mathfrak{S}_n$, then the action of σ is given by $\sigma \cdot (a_1, \dots, a_n) = (a_{\sigma^{-1}(1)}, \dots, a_{\sigma^{-1}(n)}) = {}^{\sigma^{-1}}(a_1, \dots, a_n)$. So we find

$$f(g)f(h) = (\mathrm{cp}(g), \psi^{-1}(g)) \cdot (\mathrm{cp}(h), \psi^{-1}(h)) = (\mathrm{cp}(g) + {}^{\psi(g)}\mathrm{cp}(h), \psi^{-1}(g)\psi^{-1}(h)) = f(gh).$$

Meaning that f is a morphism.

Corollary 1.5.0.20 says that an element of g is uniquely determined by its diagonal part, thus its cp-tuple. This implies that f is injective, and more precisely bijective when restricted to the first coordinate.

The 1-cocycle version is also given by Proposition 1.5.0.7, as shown in the first paragraph of this proof.

Corollary 1.5.0.21 precisely says that an element of M corresponds to elements with positive coefficient powers, i.e. M embeds in $\mathbb{N}^n \rtimes \mathfrak{S}_n$. □

Proposition 1.5.0.23. *For any tuple $a = (a_1, \dots, a_n)$ in $\mathbb{Z}^n$, there exists a unique $g \in G$ with $cp(g) = (a_1, \dots, a_k)$. In particular, the bijection $\Pi\colon \mathbb{N}^S \to M$ extends to a bijection $\Pi\colon \mathbb{Z}^S \to G$.*

Moreover, if all $a_i \geq 0$ then $g \in M$ has a Π-expression $g = \Pi_{\ell(a)}$ which is of length $\ell(a)$ over S and is minimal by additivity of ℓ.

Similarly, if $g \in G$, writing it as a reduced fraction in M also gives that the length of g over $S \cup S^{-1}$ is $\ell(g)$.

Proof. The existence of g is given by Corollary 1.5.0.9. For the unicity, if we had $a = \mathrm{cp}(g) = \mathrm{cp}(h)$ for some g, h in G, then $D_g = D_h = D_{s_1}^{a_1} \dots D_{s_n}^{a_n}$ and thus $g = h$ by the previous Corollary 1.5.0.20.

Moreover, Proposition 1.5.0.19 tells us that G is permutation-free, meaning that the cp-tuple uniquely determines an element of G, providing a bijection $\Pi\colon \mathbb{Z}^S \to G$.

If all a_i's are positive, then we apply Corollary 1.5.0.9 to get a Π expression in M. The minimality is the insured by Proposition 1.5.0.7 (each generators contributes by 1 to $\ell(g)$).

Finally if g is in G, we can take a reduced fraction $g = fh^{-1}$ from Proposition 1.5.0.13, which also tells us that the length is then exactly $\ell(g) = \ell(f) + \ell(h)$. □

We've seen that the structure group of a cycle set is permutation-free, we now state a reciprocal under a condition on the atom set of the submonoid:

Recall that we denote by Σ_n the group of monomial matrices with non-zero coefficients in $\{z^k, k \in \mathbb{Z}\}$, Σ_n^+ the submonoid of those with only non-negative powers, D_i the diagonal matrix $\mathrm{diag}(1, \dots, 1, z, 1, \dots, 1)$ and $\psi(m)$ the permutation associated to the permutation matrix of m in the decomposition $m = D_m P_m$.

Theorem 1.5.0.24. *Let G be a subgroup of Σ_n, denote $G^+ = G \cap \Sigma_n^+$ (the submonoid of positive elements). Suppose that the set of atoms $S = \{s_1, \dots, s_n\}$ of G^+ has cardinal n, generates G and there exists a positive integer k such that $D_{s_i} = D_i^k$. Let the operation $*$ be defined on S by $s_i * s_j = \psi(s_i)(s_j)$, then the following assertions are equivalent:*

(i) G is permutation-free

(ii) $s(s*t) = t(t*s)$ *for all* s, t *in* S

(iii) G *is the structure group of* S

Proof. First notice that $z \mapsto z^k$ provides an injective morphism $\Sigma_n \to \Sigma_n$, so up to a change of variable $z' = z^k$, we can assume $k = 1$.

(i) $\Rightarrow$ (ii): For $1 \leq i, j \leq n$, we have from Proposition 1.5.0.4:

$$s_i s_{\psi(i)(j)} = D_i P_{s_i} D_{s_i * s_j} P_{s_i * s_j} = D_i D_j P_{s_i} P_{s_i * s_j}$$

By symmetry, $s_j(s_j * s_i)$ will have the same diagonal part. Then

$$(s_i(s_i * s_j))^{-1} (s_j(s_j * s_i)) = P^{-1}_{s_i(s_i * s_j)} D^{-1}_{s_i(s_i * s_j)} D_{s_j(s_j * s_i)} P_{s_j(s_j * s_i)} = P^{-1}_{s_i(s_i * s_j)} P_{s_j(s_j * s_i)} \in G.$$

So by the assumption that G is permutation-free we deduce $s_i(s_i * s_j) = s_j(s_j * s_i)$.

(ii) $\Rightarrow$ (iii): Recall that $P_{s_i(s_i * s_j)} = P_{s_i} P_{s_i * s_j} = P_{\psi(s_i * s_j) \circ \psi(s_i)}$, so we find $\psi(s_i * s_j) \circ \psi(s_i) = \psi(s_j * s_i) \circ \psi(s_j)$. For $t \in S$, this means that $\psi(s_i * s_j) \circ \psi(s_i)(t) = \psi(s_j * s_i) \circ \psi(s_j)(t)$, i.e. $(s_i * s_j) * (s_i * t) = (s_j * s_i) * (s_j * t)$, so precisely that S is a cycle set. Then the generators of M correspond to the generators of M_S and both are submonoids of Σ_n, so $M = M_S$. Similarly, as S generates G we have $G_S = G$.

(iii)$\Rightarrow$ (i): This is Proposition 1.5.0.19. □

1.6 Braces

Braces were first introduced by Rump in [Rum07] through linear cycle sets to provide extra-structure on the structure group which is a commutative operation (denoted $+$) very close to being distributive over the group operation (thus resembles a ring). To obtain the brace structure on the structure group, the I-structure is needed; thus, although brace theory greatly simplifies proofs, it couldn't be used before. An equivalent definition was then introduced by Cedó, Jespers and Okniński in [CJO14] and then in a large survey again by Cedó in [Ced18]. We will use their definition of a (left) brace throughout this thesis.

Definition 1.6.0.1 ([Rum07; Ced18])**.** *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. The additive (resp. multiplicative) inverse of an element a in B is denoted $-a$ (resp. a^{-1}).

Remark 1.6.0.2. *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 1.6.0.3. *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 brace, and obviously $(0, 0)$ *is the identity of* $(B, \cdot)$*.*

Proposition-Definition 1.6.0.4 ([Ced18]). *For any a in a brace 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 1.6.0.5. *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 $(B, \cdot)$.*

Remark 1.6.0.6. *In [BCJ16, Theorem 3.1], the authors explicit a way to construct involutive non-degenerate set-theoretical solutions to the Yang–Baxter equation from a brace. There exists a generalization, introduced by Guarnieri and Vendramin in [GV17], to solutions that are not necessarily involutive: skew braces. Skew braces are defined in a similar fashion to braces, with the difference that $(B, +)$ is not supposed to be abelian. Thus, in the definitions, one has to be careful of the non-commutativity of addition, for instance the defining condition of a skew brace is $a(b + c) = ab - a + ac$, which coincides with the one for a brace when addition is commutative. Similarly, the λ-map is defined by $\lambda_a(b) = -a + ab$ to be a morphism $(B, \cdot) \to Aut((B, +))$.*

However, structure groups of non-involutive solutions can have torsion, so they are not always Garside groups, thus the reason why we restrict to only defining braces. For instance, consider the solution (from [Jes+21]), over $X = (\mathbb{Z}/3\mathbb{Z})$ defined by $r(x, y) = (2y, x + 2y)$. Then on $X \times \times X$ we have $r_1 r_2 r_1(x, y, z) = (z, 2y + z, x + 2y + 2z) = r_2 r_1 r_2(x, y, z)$, so r satisfies the Yang–Baxter equation. Moreover, $r^{-1}(x, y) = (y+2x, 2x)$, so r is bijective. And if we write $r(x, y) = (\sigma_x(y), \tau_y(x))$, then both σ_x and τ_y are always bijective (the first one because 2 is invertible, the second for the same reason plus a translation). In the end, we have a non-involutive non-degenerate solution, whose structure group is given by $G = \langle x, y, z \mid xy = yx = z^2, xz = zx = y^2 \rangle$, and using that $z = y^2 x^{-1}$ we see that this presentation is equivalent to $G \cong \langle x, y \mid xy = yx, x^3 = y^3 \rangle \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, which has non-trivial torsion.

Lemma 1.6.0.7 ([Ced18]). *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 1.6.0.8. *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 [Ced18]:

Lemma 1.6.0.9 ([Ced18])**.** *Let S be a subset of a brace $(B,+,\cdot)$. Assume that $\lambda_s(S) \subseteq S$ for any s in S. Then $(S,+)$ is a subgroup of $(B,+)$ if and only if $(S,\cdot)$ is a subgroup of $(B,\cdot)$.*

Proof. By Proposition-Definition 1.6.0.4, we have $ab = a + \lambda_a(b)$, or equivalently $a + b = a\lambda_a^{-1}(b)$. If S is stable by the action of any λ_s with s in S, then it is stable under $+$ if and only if it is stable under $\cdot$. By Remark 1.6.0.2, the identities of both laws are the same. Finally, we deduce from $ab = a + \lambda_a(b)$ that $-a = \lambda_a(a^{-1})$, thus S is stable under inversion for $+$ if and only if it is stable under inversion for $\cdot$. □

Definition 1.6.0.10 ([Ced18])**.** *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 $\lambda_a(L) \subseteq L$ 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 1.6.0.11 ([Ced18])**.** *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.*

Going back again at the I-structure of [ESS99; GV98; Deh15], we obtain in a matricial way the brace structure of the structure group.

Theorem 1.6.0.12 ([Ced18])**.** *The structure group G of a finite cycle set S has a brace structure with the usual multiplication, addition given by $g+h$ as the unique element with $D_{g+h} = D_gD_h$, and such that $(G,+) \simeq \mathbb{Z}^S$.*

In particular, if g and h are in M, so is $g+h$.

Moreover, $Soc(G) = \{g \in G \mid P_g = Id\}$.

Proof. Let g, h and k be in G. Then $g(h+k) = D_gP_g(D_hD_kP_{h+k}) = D_g\,{}^gD_h\,{}^gD_kP_gP_{h+k}$, so that $D_{g(h+k)+g} = D_g^2\,{}^gD_h\,{}^gD_k$. As $D_{gh} = D_g\,{}^hD_h$, we deduce that $D_{g(h+k)+g} = D_{gh+gk}$ and thus, from Theorem 1.5.0.19 $g(h+k)+g = gh+gk$. □

Remark 1.6.0.13. *Note that for any g in G, $Id_n = D_{g-g} = D_gD_{-g}$ thus*

$$D_{-g} = D_g^{-1},$$

while $0 = g^{-1}g = g^{-1} + \lambda_g^{-1}(g)$ thus

$$D_{g^{-1}} = D^{-1}_{\psi(g)(g)} = {}^gD_g^{-1}.$$

Corollary 1.6.0.14. *For any s, t in S we have $\lambda_s(t) = \psi(s)^{-1}(t)$, or equivalently $\lambda_s^{-1}(t) = s * t$.*

Moreover, this implies that for any g in G and s in S, $\lambda_g(s) = \psi(g)^{-1}(s)$. In particular, $\lambda_g|_S$ is a bijection.

Proof. $\lambda_s(t) = st - s = D_sP_sD_tP_t - D_sP_s = D_sD_{\psi(s)^{-1}(t)}P_sP_t - D_sP_s$ which, from the previous theorem, is the unique element with diagonal part $(D_sD_{\psi(s)^{-1}(t)})D_s^{-1} = D_{\psi(s)^{-1}(t)}$ (as $D_{-s} = D_s^{-1}$, thus $\lambda_s(t) = \psi(s)^{-1}(t)$.

In general, if $g = t_1 \dots t_k \in G$ with $t_i \in S$ for all $1 \leq i \leq k$, then by Proposition-Definition 1.6.0.4 $\lambda_g = \lambda_{t_1} \dots \lambda_{t_k} = \psi(t_1)^{-1} \dots \psi(t_k)^{-1} = (\psi(t_k) \dots \psi(t_1))^{-1}$. From Corollary 1.4.0.2, we know that $\psi(g)^{-1} = \psi(t_1 \dots t_k)^{-1} = (\psi(t_k) \dots \psi(t_1))^{-1}$, finishing the proof. □

From the previous theorem we can deduce a brace equivalent to Dehornoy's calculus:

Corollary 1.6.0.15. *The following identities hold for any $t_1, \dots, t_k$ in S:*

$$\Pi_k(t_1, \dots, t_k) = t_1 + \dots + t_k$$

$$\Omega_k(t_1, \dots, t_k) = \lambda^{-1}_{t_1+\dots+t_{k-1}}(t_k).$$

In particular, $\Theta(t_1 + \dots + t_k) = D_{t_1} \cdots D_{t_k} P_{t_1+\dots+t_k}$.

Proof. We proceed by induction: For $k = 1$, we have $\Omega_1(s) = s = \lambda_1^{-1}(s)$ and $\Pi_1(s) = s$.

Now suppose the statements hold for $k \geq 1$, then we have $\Omega_{k+1}(t_1, \dots, t_k, s) = \Omega_k(t_1, \dots, t_k) * \Omega_k(t_1, \dots, t_{k-1}, s) = \lambda^{-1}_{t_1+\dots+t_{k-1}}(t_k) * \lambda^{-1}_{t_1+\dots+t_{k-1}}(s)$ by the induction hypothesis. From Corollary 1.6.0.14, we know that for $g, h \in g$ $\lambda_g^{-1}(h) = \psi(g)(h)$ (and in S $\lambda_s^{-1}(t) = s * t$). So we obtain $\Omega_{k+1}(t_1, \dots, t_k, s) = \lambda^{-1}_{\lambda^{-1}_{t_1+\dots+t_{k-1}}(t_k)}(\lambda^{-1}_{t_1+\dots+t_{k-1}}(s))$. Then, we will apply Lemma 1.6.0.7 that tells us that for any a, b in G, $\lambda_b^{-1}\lambda_a^{-1} = \lambda^{-1}_{a+\lambda_a(b)}$. Taking $b = \lambda^{-1}_{t_1+\dots+t_{k-1}}(t_k)$ and $a = t_1 + \dots + t_{k-1}$, we have $\lambda_a(b) = \lambda_{t_1+\dots+t_{k-1}}\lambda^{-1}_{t_1+\dots+t_{k-1}}(t_k) = t_k$, and so $a + \lambda_a(b) = t_1 + \dots + t_k$. We then arrive at $\Omega_{k+1}(t_1, \dots, t_k, s) = \lambda^{-1}_{t_1+\dots+t_k}(s)$.

Finally, by Definition 1.3.0.1 $\Pi_{k+1}(t_1, \dots, t_k, s) = \Pi_k(t_1, \dots, t_k)\Omega_{k+1}(t_1, \dots, t_k, s)$, so applying the induction hypothesis and the result for Ω_{k+1} we obtain $\Pi_{k+1}(t_1, \dots, t_k, s) = (t_1 + \dots + t_k)\lambda^{-1}_{t_1+\dots+t_k}(s)$. Recall that, again by Proposition-Definition 1.6.0.4, $ab = a + \lambda_a(b)$, thus $\Pi_{k+1}(t_1, \dots, t_k, s) = (t_1 + \dots + t_k) + \lambda_{t_1+\dots+t_k}\lambda^{-1}_{t_1+\dots+t_k}(s) = t_1 + \dots + t_k + s$, finishing the proof.

Finally, by Proposition 1.5.0.8 we have

$$\Theta(t_1 + \dots + t_k) = \Theta(\Pi_k(t_1, \dots, t_k)) = D_{t_1} \cdots D_{t_k} P_{t_1+\dots+t_k}.$$

□

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.

CHAPTER 2

On Dehornoy's constructions

In this section, we focus on Dehornoy's construction of a Garside germ for structure groups of cycle sets. They should be thought of as an analogue to what finite Coxeter groups are to their associated Artin–Tits group. In this sense, Dehornoy called the germ of structure group "Coxeter-like groups".

To construct this germ as in [Deh15], one associates to a cycle set an integer called the Dehornoy's class and usually denoted d. This class in then used to construct the "Coxeter-like group" (or germ), and relate this quotient to the Garside structure of the structure monoid. In the following chapters, multiples of the class and their associated germs will play an important role.

In the first half of this section, we start by answering a question of Dehornoy ([Deh17, Questions, Slide 18]). He wondered if one could obtain the Garside structure without a theorem of Rump ([Rum05, Theorem 2]) and then retrieving said theorem from the Garside structure. We obtain the Garside structure just with the monomial representation (as a way to see the I-structure). We then retrieve Rump's theorem, only using the I-structure (thus not needing the Garside structure).

Then we focus on bounding Dehornoy's class d for a fixed size of cycle sets n, with or without extra-hypotheses on the cycle sets. The point is that this will give a restriction on which braces to consider, as the best bound known so far is $d \leq n!$ which is very much larger than numerical evidences suggests, as shown in Appendix A. We give a conjecture on the bound of d, along with a proof under some hypotheses.

Finally we focus on the primes dividing d: in a similar fashion to [Bac18; CCS20], we will highlight how the Sylows of the germs are related to the prime decomposition of Dehornoy's class d, and the way this can be reversed to construct new solutions. In particular, this further reduces the problem of classifying solutions to those with class a prime power. In the indecomposable case, this further reduces to the classification of solutions whose class and size are powers of the prime.

We fix a finite cycle set $(S, *)$ of size n with structure monoid (resp. group) M (resp. G).

This work appears in [Fei24].

2.1 Garsideness

In [Deh15], Dehornoy used Rump's result on the non-degeneracy of finite cycle sets to obtain the Garside structure of the structure group (first proved in [Cho10, Theorem 2] and also appearing in [Rum15, Theorem 2]). In [Deh17, Questions Slide 18] Dehornoy asked whether the opposite could be done and the objective of the next sections is to provide a positive answer to this question. We will first obtain the Garside structure without using Rump's theorem, and then recover Rump's result (without even using the Garside structure). Both the Garsideness and Rump's theorem will be directly deduced from the I-structure alone. This section will mostly use the monomial matrix approach, but in Section 2.3 we will give a brace equivalent of some statements (although requiring the use of a consequence of Rump's theorem).

Recall that we fix $(S, *)$ a finite cycle set of size n with structure brace G and monoid of positive elements M. Moreover, as the defining relations of the presentation of G are homogeneous (quadratic), we have a well-defined length function $\ell : G \to \mathbb{Z}$, which restricts to $M \to \mathbb{N}$.

Definition 2.1.0.1. *Let g_1, g_2 be elements of M. We say that g_1 left-divides (resp. right-divides) g_2, that we note $g_1 \preceq g_2$ (resp. $g_1 \preceq_r g_2$) if there exists some $h \in M$ such that $g_2 = g_1 h$ (resp. $g_2 = h g_1$) and $\ell(g_2) = \ell(g_1) + \ell(h)$.*

An element $g \in M$ is called balanced if the set of its left-divisors $Div(g)$ and the set of its right-divisors $Div_r(g)$ coincide.

Note that, as $g_1 = P_{g_1}\, {}^{g_1}D_{g_1}$, its matricial transpose is given by $g_1^t = P_{g_1}^t D_{g_1} = P_{g_1}^{-1} D_{g_1} = {}^{g_1}D_{g_1} P_{g_1}^{-1}$, thus the coefficient on the i-th column of g_1 is the coefficient on the i-th row of g_1^t.

Proposition 2.1.0.2. *Let g, h be in M.*

Then g left-divides h if and only if for each row of g the power of z on this row is smaller than the corresponding one of h.

Similarly, g right-divides h if and only if for each column of g the power of z on this column is smaller than the corresponding one of h.

We will give an alternative brace proof and an interpretation of this statement in section 2.3, but it will use Rump's theorem (after reproving it).

Proof. Write $g_i = D_{g_i} P_{g_i} = P_{g_i}\, {}^{g_i}D_{g_i}$. For left-divisibility, consider in G the element $h = g_1^{-1} g_2 = P_{g_1}^{-1} D_{g_1}^{-1} D_{g_2} P_{g_2}$. From Corollary 1.5.0.21, $h \in M$ iff $D_{g_1}^{-1} D_{g_2}$ contains only non-negative powers of z (to lie in $\mathbb{N}^n \subseteq \mathbb{Z}^n$ the additive group of the brace), precisely meaning that the power on each row of g_1 is less than the one of g_2.

Similarly, for right divisibility, let $h' = g_2 g_1^{-1} = P_{g_2}\, {}^{g_2}D_{g_2} \left({}^{g_1}D_{g_1}\right)^{-1} P_{g_1}^{-1}$, which is in M iff ${}^{g_2}D_{g_2} \left({}^{g_1}D_{g_1}\right)^{-1}$ contains only non-negative powers of z, which is the same criterion on the columns. □

Example 2.1.0.3. *Taking $S = \{s_1, s_2\}$ with $\psi(s_1) = \psi(s_2) = (12)$, we can see that:*

$\begin{pmatrix} 0 & z^3 \\ 1 & 0 \end{pmatrix}$ *left-divides* $\begin{pmatrix} z^4 & 0 \\ 0 & 1 \end{pmatrix}$ *(as $3 \leq z_4$ on the first line and $0 \leq z0$ on the second since $1 = z^0$), but does not right divide it (as $3 > 0$ on the second column).*

Corollary 2.1.0.4. *Let g, h be in M. The left-gcd (resp. left-lcm) of g and h, denoted $g_1 \wedge g_2$ (resp. $g_1 \vee g_2$) is given by the unique element such that the coefficient-power on each row is the minimum (resp. maximum) of those of g_1 and g_2.*

For right-gcd (resp. right-lcm) it is the same but for each column.

Example 2.1.0.5. *Consider $S = \{s_1, s_2, s_3, s_4\}$ with*

$$\psi(s_1) = (1234) \qquad \psi(s_3) = (24)$$
$$\psi(s_2) = (1432) \qquad \psi(s_4) = (13)$$

We have

$$\begin{pmatrix} 0 & z & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & z \\ 0 & 0 & 1 & 0 \end{pmatrix} \wedge \begin{pmatrix} 0 & 0 & 0 & z \\ 0 & 0 & z & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & z & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Which is given by $gcd(s_1 + s_3, s_1 + s_2) = s_1$.

Similarly:

$$\begin{pmatrix} 0 & z & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & z \\ 0 & 0 & 1 & 0 \end{pmatrix} \vee \begin{pmatrix} 0 & 1 & 0 & 0 \\ z & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & z & 0 \end{pmatrix} = \begin{pmatrix} z & 0 & 0 & 0 \\ 0 & z & 0 & 0 \\ 0 & 0 & z & 0 \\ 0 & 0 & 0 & z \end{pmatrix}$$

Which is given by $lcm(s_1 + s_3, s_2 + s_4) = s_1 + s_2 + s_3 + s_4$.

For the right gcd and lcm, the explicit versions will be given in the next section using Rump's result (after reproving it).

Corollary 2.1.0.6. *An element such that the non-zero terms of its i-th row and i-th column are equal for all $1 \leq i \leq n$ is balanced.*

Definition 2.1.0.7. *An element of M is called a Garside element if it is balanced, $Div(g)$ is finite and generates M.*

Proposition 2.1.0.8 ([Deh15])**.** *The element $\Delta = \sum_S s$ is a Garside element of M.*

Proof. Because all the non-zero coefficients of Δ are equal, it is balanced.

Its set of divisors is the set of elements with non-zero coefficients 1 or z and so is finite and has cardinal 2^n, and it contains all the generators s so also generates M. □

Remark 2.1.0.9. *The powers of Δ, which are given by $\Delta^k = \sum_S ks$, are also Garside elements by the same reasoning.*

More generally, Garside elements are precisely the balanced elements g such that $g_s \geq 1$.

Definition 2.1.0.10 ([Deh+15])**.** *A monoid is said to be a Garside monoid if:*

(i) It is cancellative, i.e. if for every element g_1, g_2, h, k, $hg_1k = hg_2k \Rightarrow g_1 = g_2$.

(ii) There exists a map ℓ to the integers such that $\ell(g_1g_2) \geq \ell(g_1) + \ell(g_2)$ and $\ell(g) = 0 \Rightarrow g = 1$.

(iii) Any two elements have a gcd and lcm relative to $\preceq$ (resp. $\preceq_r$).

(iv) It possesses a Garside element Δ.

The group of fraction of a Garside monoid is called a Garside group.

Proposition 2.1.0.11 ([Deh15])**.** *M is a Garside monoid.*

Proof. The length of words (as the relations of G respects length) satisfies (ii) as an equality.

For (iii) we have Corollary 2.1.0.4 and for (iv) Proposition 2.1.0.8.

We are left to prove (i), which is a direct consequence of the fact that M injects in G. We can see also this from restricting the representation to M and as the elements are monomial matrices, we deduce the cancellative property. □

Corollary 2.1.0.12. *G is a Garside group.*

Proof. This follows from the fact that G is the group of fraction of the Garside monoid M. □

Remark 2.1.0.13. *In essence, the fact that M is left-cancellative and admits left-lcm relies on the so-called Cube condition ([Deh+15, Definition 4.14]):*

Let M be a monoid with presentation $\langle X \mid x\theta(x,y) = y\theta(y,x)\rangle$ with θ is (potentially partially defined) from $X \times X$ to X. Suppose that, for all x, y, z in X, either both $\theta(\theta(x,y),\theta(x,z))$ and $\theta(\theta(y,x),\theta(y,z))$ are undefined, or they are equal. Then M is left-cancellative and admits left-lcm. In our case, $\theta(x,y) = x * y$ satisfies the cube condition by Lemma 1.3.0.3.

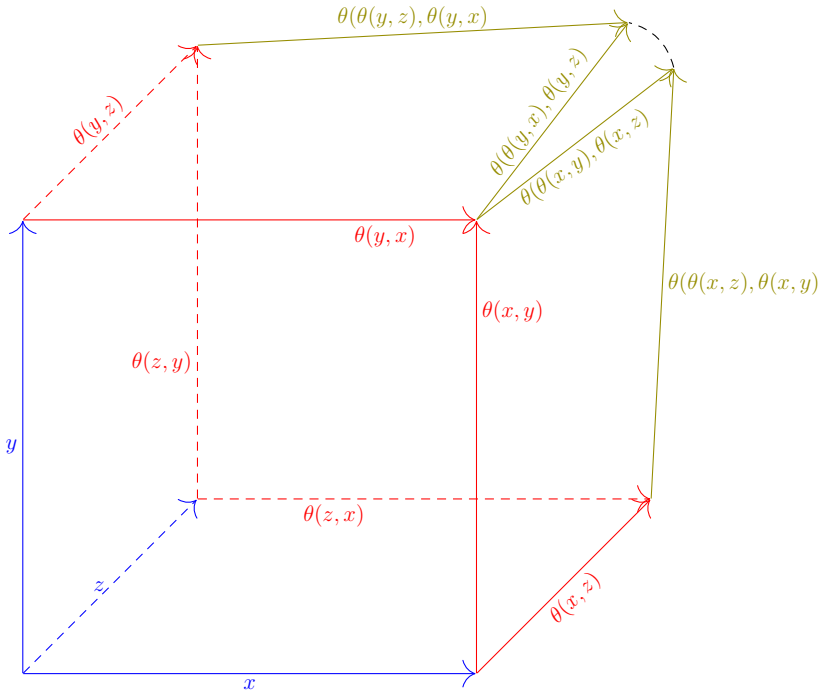


Figure 2.1: The cube condition

In Figure 2.1, each edge represents a generator from X, each face corresponds to a relation $x\theta(x,y) = y\theta(y,x)$, and the cube condition is the fact that (when defined) the cube closes at the top right, at the intersection of the top and right faces.

2.2 Dehornoy's class

In the introduction we mentioned that a special class of Artin–Tits groups (spherical type) have finite quotients, Coxeter groups, obtained by adding to the usual group presentation the fact that every generator is involutive ($s^2 = 1$), and that this quotient corresponds nicely with the Garside structure of the group (in particular the divisors of the Garside element are in bijection with the Coxeter group). This quotient is then fundamental in a lot of works as it allows to work in a finite group and then "lift" the results to the Garside group (as first introduced in [Deh+15; BS72]), thus deserving the name of a Germ ([Deh+15]).

We have seen that structure group of solutions are Garside groups, which was first proved by Chouraqui in [Cho10]. Thus, the question of finding a quotient playing a similar role appeared naturally. It was first obtained for special cases of solutions in [CG14, Proposition 3.8] and then generalized in [Deh15] by constructing an integer d and adding the relation $ds = 1$ (in the other notation $s^{[d]} = 1$), the special case first obtained then corresponding to $d = 2$.

The goal here is to follow the construction of the germ from [Deh15] mixing a brace and monomial approach.

Fix a finite cycle set $(S, *)$ of size n with structure monoid (resp. group) M (resp. G). Recall from Proposition 1.6.0.11 that $\mathrm{Soc}(G) = Ker(\lambda) = \mathrm{Ker}(\psi)$ is an ideal of the brace G, in particular $(\mathrm{Soc}(G), +) = (\mathrm{Soc}(G), \cdot)$.

Proposition 2.2.0.1. *There exists a positive integer d such that for all s in S, ds is diagonal, i.e. $ds \in Soc(G)$.*

In particular, for any positive integer k, $k(ds) = (ds)^k$.

Remark 2.2.0.2. *The smallest positive integer satisfying this condition is called the Dehornoy's class of S, and all the others will be multiples of this class. Our results will be stated for the class, but they would work for any multiples. In this section we restrict to Dehornoy's class, however in Sections 3 and 4 considering a multiple ld of d with $l > 1$ will be crucial.*

In [Deh15] the elements ks are denoted $s^{[k]}$ and, although the notation ks is nicer, we will sometimes later have to use the power notation to avoid confusion when working in the group ring $\mathbb{Z}[G]$.

Proof. First fix $s \in S$. The map sending ks to $\psi(ks)$ is a map from an infinite (countable) set to a finite one ($\mathbb{N}^* \to \mathfrak{S}_n$), therefore it is not injective. So there exists $k_1 \neq k_2 \in \mathbb{N}$ such that $\lambda_{k_1 s} = \lambda_{k_2 s}$. We can assume $k_1 > k_2$ without loss of generality. Then from Lemma 1.6.0.7 we get $(k_1 s) \cdot (k_2 s)^{-1} = k_1 s - k_2 s = (k_1 - k_2)s \in \mathrm{Soc}(G)$

Doing this for all $s \in S$, we get the existence of $d_s \in \mathbb{N}^*$ such that $d_s s$ is diagonal. By Proposition 1.6.0.11 $\mathrm{Soc}(G)$ is an ideal, so we must have for all $k \in \mathbb{N}$ $k(d_s s) \in \mathrm{Soc}(G)$. Taking $d = \mathrm{lcm}(d_s)_{s \in S}$ we have for all s the existence of $d'_s > 0$ such that $d = d_s d'_s$, we find that for all s, $ds = d'_s(d_s s) \in \mathrm{Soc}(G)$.

W show by induction that $k(ds) = (ds)^k$: for $k = 1$ this is trivial. Then, as ds is in $\mathrm{Soc}(G) = \mathrm{Ker}(\lambda) = \{g \in G \mid \forall h \in G, gh = g + h\}$, we have $(k+1)(ds) = ds + k(ds) = ds + (ds)^k = ds \cdot (ds)^k = (ds)^{k+1}$, finishing the proof. □

Remark 2.2.0.3. *In [Deh15, Lemma 5.4], the author obtained a bound on the class of a cycle set as $d \leq (n^2)!$. Here, we obtain a first better bound $d \leq (n!)^n$ given by the previous proof (as $d = lcm(d_1, \ldots, d_n)$ with $d_i \leq n!$). Improving this bound will be the focus of Section 2.*

Proposition 2.2.0.4. *Let d be the class of S and denote by dG the subgroup of $(G, \cdot)$ generated by all the ds. Then dG is an ideal of G.*

Proof. From Proposition 1.6.0.11 we have the ideal $\mathrm{Soc}(G) = \mathrm{Ker}(\lambda) = \{g \in G \mid \forall h \in G, gh = g + h\}$ for which the group laws $+$ and $\cdot$ coincides, so in particular $(\mathrm{Soc}(G), \cdot)$ is abelian. As dG is a subgroup of $(\mathrm{Soc}(G), \cdot)$, and the latter is abelian, dG is a normal subgroup. Moreover, by definition $\lambda_{ds} = \mathrm{id}$ so $\lambda_h = \mathrm{id}$ for any $h \in dG$, in particular $\lambda_h(dG) = dG$. □

Thus we obtain a quotient brace $\overline{G} = G/dG$.

Proposition 2.2.0.5 ([Deh15])**.** *The following hold:*

1. *A presentation of $\overline{G}$ can be obtained by adding to the presentation of G the relations $ds = 1$.*
2. *Matricially, quotienting is the same as specializing at $z = \exp(\frac{2i\pi}{d})$, which we will denote ev_z.*
3. *The quotient brace $\overline{G}$ has additive group $(\mathbb{Z}/d\mathbb{Z})^S$*
4. *$\overline{G}$ embeds as a subgroup of $(\mathbb{Z}/d\mathbb{Z})^n \rtimes \mathfrak{S}_n$, such that restricting to the first coordinate is bijective. Equivalently we have a bijective 1-cocycle $\overline{G} \to (\mathbb{Z}/d\mathbb{Z})^n$ associated to the action of ψ^{-1}.*
5. *The bijection $\Pi \colon \mathbb{Z}^n \to G$ induces a bijection $\overline{\Pi} \colon (\mathbb{Z}/d\mathbb{Z})^n \to \overline{G}$.*

Proof. The first point is the definition of $\overline{G}$.

For the second one, we know by definition that dG is generated by the ds which are in the socle, so they have trivial permutation. Thus quotienting by them just amounts to setting $D_s^d = 1$, or equivalently $z^d = 1$.

The third point then follows from the facts that $(G, +) \simeq \mathbb{Z}^S$ (Theorem 1.6.0.12) and $(dG, +)$ identifies with $(d\mathbb{Z})^S$ inside $\mathbb{Z}^S$, thus $(\overline{G}, +) = (G, +)/(dG, +) \cong \mathbb{Z}^S/(d\mathbb{Z})^S = (\mathbb{Z}/d\mathbb{Z})^S$.

Then, by Corollary 1.5.0.22 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. Moreover, in this embedding, dG is sent to $(d\mathbb{Z})^n \rtimes \{1\}$. As $(\mathbb{Z}^n \rtimes \mathfrak{S}_n)/((d\mathbb{Z})^n \rtimes \{1\}) \cong (\mathbb{Z}/d\mathbb{Z})^n \rtimes \mathfrak{S}_n$, this finishes the proof.

Finally let $\overline{\Pi}$ be the composition of Π with the projection $G \to \overline{G}$. As $\Pi \colon \mathbb{Z}^S \to G$ is a bijection by Proposition 1.5.0.23, $\overline{\Pi}$ is surjective. By (iii) we have $\#\overline{G} = d^n$ which is also equal to $\#(\mathbb{Z}/d\mathbb{Z})^S$, thus $\overline{\Pi}$ is bijective. □

Remark 2.2.0.6. *If $d = 1$ then $dG = G$ so $\overline{G}$ is trivial. However, $d = 1$ means that all the generators s are diagonal, i.e. $s * t = t$ for all s, t in S: this is just the special case of the trivial cycle set. But the case $d = 1$ can be included as all our results hold for any multiples of the class (thus any positive integer for $d = 1$).*

Example 2.2.0.7. *Let $S = \{s_1, \dots, s_n\}$ with $\psi(s_i) = (12 \dots n) = \sigma$ for all i. Then for any $s \in S$, $k \in \mathbb{Z}$: $ks_i = D_s^k P_{\sigma^k}$. Thus Dehornoy's class of S is equal to n. Let $\zeta_n = \exp(\frac{2i\pi}{n})$, then $\overline{G}$ is generated by the $\overline{s_i} = diag(1, \dots, \zeta_n, \dots, 1)P_\sigma$.*

From now on and everywhere in this thesis, we assume $d \geq 2$.

Denote by $\zeta_d = \exp(\frac{2i\pi}{d})$ a primitive d-th root of unity and $\mu_d = \{\zeta_d^i \mid 0 \leq i < d\}$. Let Σ_n^d be the subgroup of $\mathfrak{Monom}_n(\mathbb{C})$ with non-zero coefficients in $\{0\} \cup \mu_d$. Given $k \geq 1$, there is natural embedding $\iota_d^{dk} \colon \Sigma_n^d \to \Sigma_n^{dk}$ sending ζ_d to ζ_{dk}^k (as $\zeta_{dk}^k = \exp(\frac{2ik\pi}{dk}) = \zeta_d$). From the previous proposition, we deduce the following result:

Corollary 2.2.0.8. *The quotient group $\overline{G}$ is a subgroup of Σ_n^d.*

Recall that if S has Dehornoy's class d, then for any positive integer k we have that kds is in the Socle, thus we could also consider the germ $G/\langle kds \rangle_{s \in S}$. The embedding $\iota_d^{dk}(\overline{G})$ can then be seen as embedding the germ $\overline{G}$ in this bigger quotient group.

Definition 2.2.0.9. *[Deh15] If (M, Δ) is a Garside monoid with atom set S and G is the group of fractions of M, a group $\overline{G}$ with a surjective morphism $\pi \colon G \to \overline{G}$ is said to provide a Garside germ for (G, M, Δ) if there exists a map $\chi \colon \overline{G} \to M$ such that $\pi \circ \chi = Id_{\overline{G}}$, $\chi(\overline{G}) = Div(\Delta)$ and M admits the presentation*

$$\langle \chi(\overline{G}) \mid \chi(fg) = \chi(f)\chi(g) \text{ when } ||fg||_{\overline{S}} = ||f||_{\overline{S}} + ||g||_{\overline{S}} \rangle$$

where $|| \cdot ||_{\overline{S}}$ denote the length of an element over $\overline{S} = \pi(S)$.

Proposition 2.2.0.10 ([Deh15])**.** *The specialization ev_d that imposes $z = \exp(\frac{2i\pi}{d})$ provides a Garside germ of (G, M, Δ^{d-1}).*

Proof. Consider the map $\chi \colon \overline{G} \to M$ defined by sending $\exp(\frac{2i\pi \cdot k}{d})$ to $z^k \in \mathbb{Q}[z]$ for $1 \leq k < d$. As ev_d is defined by sending z to $\exp(\frac{2i\pi}{d})$, we deduce $\mathrm{ev}_d \circ \chi = \mathrm{Id}_{\overline{G}}$. The image of χ is the set of elements of M such that each non-zero coefficient is a power of z strictly less than d, and thus identifies with $\mathrm{Div}(\Delta^{d-1})$ by the characterization of left-divisibility (Proposition 2.1.0.2). And the presentation amounts to forgetting that z is a root of unity, thus generating M as required. □

To work over $\overline{G}$, we will use the following corollary to restrict to classes of equivalence over the structure monoid.

Corollary 2.2.0.11. *The projection $ev_d \colon M \to \overline{G}$ is surjective.*

Proof. G is generated by all the elements of S, so its quotient $\overline{G}$ is also generated by S. Moreover, as $\overline{G}$ is finite, inverses can be constructed from only positive generators, thus the restriction $G \to \overline{G}$ to M. □

Example 2.2.0.12. *Let $S = \{s_1, \dots, s_n\}$ with $\psi(s_i) = (12 \dots n) = \sigma$ for all i. Then for any $s \in S$, $k \in \mathbb{Z}$: $ks_i = D_s^k P_{\sigma^k}$. The Dehornoy's class of S is n and $\overline{G}$ is generated by the $\overline{s_i} = diag(1, \dots, \zeta_n, \dots, 1)P_\sigma$ where $\zeta_n = \exp(\frac{2i\pi}{n})$.*

To recover G from $\overline{G}$, one simply takes all the elements of $\overline{G}$ and forget that z is a root of unity in the following sense: when computing the product of two elements and finding a

coefficient z^a with $a > d$, we do not use that $z^d = 1$ and just consider it as a new element. So for instance in $\langle \chi(\overline{G}) \rangle$ with $n = 4$:

$$\chi(\overline{3s_1})\chi(\overline{2s_4}) = \chi(3\overline{s_1})\chi(2\overline{s_4}) = \begin{pmatrix} 0 & 0 & 0 & z^3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & z^2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & z^5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 5s_1.$$

Because $5 > 4$, we obtain a new element different from $\chi(\overline{5s_1}) = \chi(\overline{s_1})$.

The quotient group $\overline{G}$ defined above is called a Coxeter-like group, it was first studied by Chouraqui and Godelle in [CG12] for $d = 2$ and generalized by Dehornoy in [Deh15].

Fix $\overline{G}$ a Coxeter-like group obtained from a cycle set S of cardinal n and class $d \geq 2$ (so that $\overline{G}$ is not trivial).

Definition 2.2.0.13. *We define a function $l_d \colon \{0, 1, \ldots, d-1\} \to \{0, 1, \ldots, \lfloor \frac{d}{2} \rfloor\}$ by:*

$$\forall k \in \{0, 1, \ldots, d-1\}, \overline{\ell}_d(k) = \begin{cases} k, & \text{if } k \leq \frac{d}{2} \\ k - d, & \text{if } k > \frac{d}{2}. \end{cases} \tag{2.1}$$

Note that $\overline{\ell}_d$ corresponds to ℓ with the projection $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ but with representatives in $]-\frac{d}{2}, \frac{d}{2}] \cap \mathbb{Z}$ instead of $[0, d-1[\cap\mathbb{Z}$. Because, if we have $z^6 = 1$, the shortest way to write z^2 is $z \cdot z$ but to write z^4 we should use $z^{-1} \cdot z^{-1}$ instead of $z \cdot z \cdot z \cdot z$.

Proposition 2.2.0.14. *Let $g = \sum_{s \in S} g_s s \in \overline{G}$ with $0 \leq g_s < d$. Let $\overline{S} = \pi(S)$.*

The length $\overline{\ell}$ of an element $g \in \overline{G}$ over $\overline{S}$ is given by $\sum_{s \in S} g_s$.

The length $\overline{\ell}_d$ of an element $g \in \overline{G}$ over $\overline{S} \cup \overline{S}^{-1}$ is given by $\sum_{s \in S} l_d(g_s)$.

Proof. First recall that by Proposition 2.2.0.5 $\overline{G}$ has additive brace structure $(\mathbb{Z}/d\mathbb{Z})^S$. Thus, an element of g has a unique expression $g = \sum_{s \in S} g_s s \in \overline{G}$ with $0 \leq g_s < d$.

Now, for the length over $\overline{S}$, we can use $s + t = s\lambda_s^{-1}(t)$ from Proposition-Definition 1.6.0.4 to go from an additive to a multiplicative expression. Thus the additive and multiplicative length are equal, and are the sum of the g_s.

For the length over $\overline{S} \cup \overline{S}^{-1}$, note that the shortest way to write k for $k \in \mathbb{Z}/d\mathbb{Z}$ using ± 1 is using $1 + \cdots + 1$ if $k \leq \frac{d}{2}$ and otherwise, as $d = 0$, we write it as $-1 - \cdots - 1$. Doing so for every term g_s of $g \in \overline{G}$, we obtain the result. □

Corollary 2.2.0.15. *For any g, h in $\overline{G}$, we have $\overline{\ell}(h) = \overline{\ell}(\lambda_g(h))$.*

Proof. If $h = \sum_{s \in S} h_s s$ with $0 \leq h_s < d$, then by Proposition-Definition 1.6.0.4, $\lambda_g(h) = \sum_{s \in S} h_s \lambda_g(s) = \sum_{t \in S} h_{\lambda_g^{-1}(t)} t$. By Corollary 1.6.0.14, $\lambda_g|_S$ is a bijection. Thus

$$\overline{\ell}(\lambda_g(h)) = \sum_{t \in S} h_{\lambda_g^{-1}(t)} = \sum_{s \in S} h_s = \overline{\ell}(h).$$

□

Definition 2.2.0.16. *We say that a word w over $\overline{S} = \pi(S)$ is reduced in $\overline{G}$ if it has length $\overline{\ell}(w)$ when seen as an element of $\overline{G}$.*

Remark 2.2.0.17. *This means that if $g = s_{i_1} \cdots s_{i_k}$ in $\overline{G}$, and we use Proposition-Definition 1.6.0.4 to rewrite it additively with $st = s + \lambda_s(t)$ so that $g = \sum_{s \in S} g_s s$, then the given expression is reduced when $0 \leq g_s < d$ for all s.*

Remark 2.2.0.18. *Corollary 2.2.0.11 tells us that M surjects in $\overline{G}$, and Proposition 2.2.0.5 says that $\Pi \colon \mathbb{Z}^S \to G$ induces a bijection $\overline{\Pi} \colon (\mathbb{Z}/d\mathbb{Z})^S \to \overline{G}$. Thus, we can adapt "taking a Π-expression of an element in M" to $\overline{G}$. We will say that we take a $\overline{\Pi}$-expression of $g \in \overline{G}$ to mean we chose any $(t_1, \ldots, t_k)$ in S^k such that $g = \overline{\Pi}_k(t_1, \ldots, t_k)$ with $\overline{\ell}(g) = k$.*

Definition 2.2.0.19. *For any g in $\overline{G}$, we define its support as $supp(g) = \{s \in S \mid g_s > 0$, where $g = \sum_{s \in S} g_s s$ with $0 \leq g_s < s$.*

Proposition 2.2.0.20. *For any g in $\overline{G}$, we have $\overline{\ell}(g^{-1}) = d \cdot |supp(g)| - \overline{\ell}(g)$.*

Proof. From Remark 2.2.0.17, write $g = \sum_{s \in S} g_s s$ with $0 \leq g_s < d$, so that $\overline{\ell}(g) = \sum_{s \in S} g_s$.Let $h = \sum_{s \in \mathrm{supp}(g)} (d - g_s)s \in \overline{G}$ meaning that $g + h = \sum_{s \in \mathrm{supp}(g)} ds = 0 \in \overline{G}$ and $\overline{\ell}(h) = d \cdot |\mathrm{supp}(g)| - \overline{\ell}(g)$. Using Proposition-Definition 1.6.0.4 to rewrite h multiplicatively, we obtain a reduced expression of h. Finally, $g + h = g\lambda_g^{-1}(h)$, and $\overline{\ell}(\lambda_g^{-1}(h)) = \overline{\ell}(h)$. □

For Coxeter groups, we have the so-called exchange lemma (see [Mic14, Theorem 4.2]): if (W, S) is a Coxeter system. We provide a similar result for Coxeter-like groups:

Lemma 2.2.0.21 (Exchange Lemma)**.** *Let s be in S and g in $\overline{G}$. Write $g = \sum_{s \in S} g_s s$ with $0 \leq g_s < d$. Then either sg is reduced ($\ell(sg) = \ell(g) + 1$) or $g_{s*s} = d - 1$ (i.e $(d-1)(s*s)$ left-divides g). Moreover, if it is not reduced, then $sg = \sum_{\substack{t \in S \\ t \neq s}} g_{s*t} t$.*

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 $\ell(g) = k$. Remark 2.2.0.17 then tells us that $\sum_{s \in S} g_s = k$. Now, by Proposition-Definition 1.6.0.4 $sg = s + \lambda_s(g) = s + \sum_{t \in S} g_t \lambda_s(t)$. Reindexing the sum by setting $t = \lambda_s^{-1}(u) = s * u$ for some $u \in S$, we have $g = s + \sum_{u \in S} g_{s*u} u$.

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 1.6.0.4, we can rewrite both expressions as $g = \sum_{s \in S} g_s s$ 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 Corollary 1.6.0.14, 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 this subsection with a technical lemma which will be especially useful in Section 4. We state it with the notation $s^{[d]} = ds$, as it will be used in Section 4 to avoid confusion in the group ring $\mathbb{Z}[G]$.

Lemma 2.2.0.22. *For any $s, t \in S$ the following 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 1.6.0.4: $s^{[d]} = s + (d-1)s = s\lambda_s^{-1}((d-1)s)$.

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

2.3 Non-degeneracy

As mentioned above (Theorem 1.2.0.6), finite cycle sets are in bijective correspondence with finite left non-degenerate involutive set-theoretical solutions. Rump showed ([Rum05, Theorem 2]) that finite left non-degenerate involutive set-theoretical solutions are also right non-degenerate by showing that the square map of a cycle set is bijective (logically called the non-degeneracy of a cycle set). Dehornoy used this result in [Deh15] to be able to transpose most results on right-multiplication to results on left-multiplication, which does not provide a very explicit construction. Above we have adapted Dehornoy's work without Rump's theorem, but we can also obtain said theorem.

Our proof, compared to Rump's, is fairly short and a direct consequence of the I-structure, whereas he needed several intermediate constructions (such as the retraction of a solution, which we'll mention later). We although use it to translate Dehornoy's left-multiplication statement into brace theory with explicit constructions.

Recall that we fix $(S, *)$ a finite cycle set of size n with structure monoid (resp. group) M (resp. G).

Definition 2.3.0.1. *A finite cycle set is called non-degenerate if the diagonal map T defined by $T(s) = s * s$ is a bijection of S.*

Lemma 2.3.0.2 ([Rum05])**.** *For any g, h in G, $\lambda_g^{-1}(g) = \lambda_h^{-1}(h)$ if and only if $g = h$.*

Proof. If $g = h$ then trivially $\lambda_g^{-1}(g) = \lambda_h^{-1}(h)$. Suppose $\lambda_g(g) = \lambda_h(h)$, we want to show $gh^{-1} = 1$. Also recall that, by Remark 1.6.0.2, in a brace, we have that $0 = 1$.

From Lemma 1.6.0.7 we find:

$$gh^{-1} = -\lambda_g(\lambda_{h^{-1}}(h)) + g = -\lambda_g(\lambda_{g^{-1}}(g)) + g = -\lambda_g(\lambda_g^{-1}(g)) + g = -g + g = 0 = 1.$$

□

From Lemma 2.3.0.2 we retrieve Rump's theorem ([Rum05, Theorem 2]):

Theorem 2.3.0.3 (Rump's theorem)**.** *Every finite cycle set is non-degenerate.*

Proof. Let S be a finite cycle set. By Corollary 1.6.0.14, for any $s \in S$ we have the equality $\lambda_s = \psi(s)^{-1}$. So by Lemma 2.3.0.2;

$$s * s = t * t \Leftrightarrow \psi(s)(s) = \psi(t)(t) \Leftrightarrow \lambda_s^{-1}(s) = \lambda_t^{-1}(t) \Leftrightarrow s = t.$$

This means that T is injective, and as S is finite, T is bijective. □

The following will be very useful to switch from working on the left to working on the right when looking at divisibility:

Proposition 2.3.0.4. *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 $kds = (sT(s) \dots T^{o-1}(s))^k$.

Proof. For the first point, as S is finite and T is injective by the previous lemma, it is bijective and so has finite order.

The second point follows directly from an induction and Lemma 1.6.0.7: $\lambda^{-1}_{(k+1)s}(s) = \lambda^{-1}_{ks+s}(s) = \lambda^{-1}_{\lambda^{-1}_{ks}(s)}(\lambda^{-1}_{ks}(s)) = \lambda^{-1}_{T^k(s)}(T^k(s)) = T^k(s) * T^k(s) = T^{k+1}(s)$. Then $(k+1)s = ks + s = ks \cdot \lambda^{-1}_{ks}(s) = ks \cdot T^k(s) = sT(s)\dots T^k(s)$. As T is of order o, we can consider the exponent i of $T^i(s)$ modulo o ($T^{i\pm o}(s) = T^i(o)$). Thus, if $k = o \cdot q + r$, then $(o \cdot q + r)s = (sT(s)\dots T^{o-1}(s))^q sT(s)\dots T^{r-1}(s)$.

For the third point, $T^d(s) = \lambda^{-1}_{ds}(s) = s$ as $ds \in \mathrm{Soc}(G)$. □

This allows us to naturally obtain a cycle set structure on the transpose of the elements of G and transform all statement on right-multiplication to statements on the left-multiplication. In [Deh15] the statements with multiplication on the left are obtained by abstractly and non-explicitly "dualizing" the operations.

Corollary 2.3.0.5. *Let G^t be the set of transposes of the elements of G seen as matrices. Then G^t is the structure group of a cycle set structure on S^t, the set of the transposes of the elements of S seen as elements of Σ_n.*

Explicitly $\psi(s^t) = \psi^{-1}(T^{-1}(s))$.

Proof. First note that, because G is generated by S, G^t is generated by S^t. As T is a bijection, for each u the set S^t contains exactly one element s^t such that $D_{s^t} = D_u$, that is $s = T^{-1}(u)$. Moreover, as G is permutation-free, so is G^t. So by Theorem 1.5.0.24 it is the structure group of a cycle set S^t. □

Example 2.3.0.6. *Let $S = \{s_1, s_2, s_3\}$ with $\psi(s_1) = \psi(s_2) = \psi(s_3) = (123) = \sigma$. Then $s_i^t = (D_i P_\sigma)^t = P_\sigma^{-1} D_i = {}^\sigma D_i P_\sigma^2$, so for example*

$$s_2^t = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & z \\ 1 & 0 & 0 \end{pmatrix}^t = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & z & 0 \end{pmatrix} = D_3 P_{(132)} = D_{\sigma(2)} P_\sigma^{-1}.$$

In particular, this can be used to work on the columns in G: if we want an element of G with the coefficient $z^{a_1}, \dots, z^{a_n}$ read column by column, we can work in G^t, compute $\sum_{i=1}^{n} a_i T^{-1}(s_i)$ and transpose it to get the desired element in G.

Moreover, this also implies the easier characterization of divisibility in G:

Corollary 2.3.0.7. *Let g, h be in M. Write $g = \sum_{s\in S} g_s s$ and $h = \sum_{s\in S} h_s s$ with $g_s, h_s \in \mathbb{N}$.*

Then g left-divides h if and only if $g_s \le h_s$ for all s.

Similarly, g right-divides h if and only if $g^t_{s^t} \le h^t_{s^t}$ for all s, where $s^t = T^{-1}(s)$.

Corollary 2.3.0.8. *Let g, h be in M. Write $g = \sum_{s\in S} g_s s$ and $g = \sum_{s\in S} h_s s$ with $g_s, h_s \in \mathbb{N}$.*

Then $g \wedge h = \sum_{s\in S} min(g_s, h_s)s$ and $g \vee h = \sum_{s\in S} max(g_s, h_s)s$.

Similarly $g \wedge_r h = \left(\sum_{s\in S} min(g^t_{s^t}, h^t_{s^t})s^t\right)^t$ and $g \vee_r h = \left(\sum_{s\in S} max(g^t_{s^t}, h^t_{s^t})s^t\right)^t$.

Proposition 2.3.0.9. *For any $k \in \mathbb{N}$, $\psi(ks)(s) = T^k(s)$. In particular, the map $s \mapsto \psi(ks)(s)$ is a bijection of S.*

Proof. We proceed by induction: for $k = 0$, $T^0(s) = s = \psi(1)(s)$. For $k = 1$, $T(s) = s*s = \psi(s)(s)$ by definition. Then suppose the equality holds for $k \geq 1$. From Proposition 2.3.0.4 we know that $(k+1)s = ks \cdot T^k(s)$, so $\psi((k+1)s) = \psi(T^k(s)) \circ \psi(ks)$. Thus, $\psi((k+1)(s))(s) = \psi(T^k(s)) \circ \psi(ks)(s) = \psi(T^k(s))T^k(s)) = T^{k+1}(s)$. □

Corollary 2.3.0.10. *For any k in $\mathbb{N}$ and s in S, let $t = (T^k)^{-1}(s)$ then $-ks = (kt)^{-1}$.*

Proof. Let $t \in S$, we have

$$(kt)^{-1} = (D_t^k P_{kt})^{-1} = P_{(kt)}^{-1} D_t^{-k} = {}^{\psi(kt)^{-1}}D_t^{-k} P_{kt}^{-1} = D_{\psi(kt)(t)}^{-k} P_{kt}^{-1} = D_{T^k(t)}^{-k} P_{kt}^{-1}.$$

Thus, if $t = (T^k)^{-1}(s)$, we find $D_{(kt)^{-1}} = D_s^{-k}$.

From Proposition 2.3.0.4 we have $t = \lambda_{kt}(T^k(t))$, so

$$kt \cdot (-ks) = kt + \lambda_{kt}(-ks) = kt - k\lambda_{kt}(s) = kt - k\lambda_{kt}(T^k(t)) = kt - kt = 0 = 1.$$

□

Proposition 2.3.0.11 ([Deh15])**.** *The map $(s,t) \mapsto (s*t, t*s)$ is bijective.*

Proof. As S is finite, so is $S \times S$, so we only have to show injectivity. Assume $s*t = s'*t'$ and $t*s = t'*s'$ for some $s,t,s',t' \in S$. Then, from $s*t = s'*t'$ and $s+t = s(s*t)$, we have $\lambda_{s+t}\lambda_{s'+t'}^{-1} = \lambda_{s(s*t)}\lambda_{s'(s'*t')}^{-1} = \lambda_s\lambda_{s*t}\lambda_{s'*t'}^{-1}\lambda_{s'}^{-1} = \lambda_s\lambda_{s'}^{-1}$. Thus $\lambda_{s+t}\lambda_{s'+t'}^{-1}(s') = \lambda_s(s'*s')$. As $s+t = t+s = t(t*s)$ we have by symmetry $\lambda_{s+t}\lambda_{s'+t'}^{-1}(t') = \lambda_t(t'*t')$. Thus $(s+t)(s'+t')^{-1} = -\lambda_{s+t}\lambda_{s'+t'}^{-1}(s'+t') + (s+t) = -\lambda_s(s'*s') - \lambda_t(t'*t') + (s+t)$

On the other hand, as $s+t = s(s*t)$, we have $(s+t)(s'+t')^{-1} = s(s*t)(s'*t')^{-1}s'^{-1} = ss'^{-1} = -\lambda_s\lambda_{s'}^{-1}(s') + s = -\lambda_s(s'*s') + s$.

Combining the above equalities gives $-\lambda_s(s'*s') + s = (s+t)(s'+t')^{-1} = -\lambda_s(s'*s') - \lambda_t(t'*t') + (s+t)$, thus we deduce $t - \lambda_t(t'*t') = 0$, so $t*t = t'*t'$ and by the bijectivity of T we find $t = t'$. By the same symmetry argument we obtain $s = s'$, and this concludes the proof. □

2.4 Bounding the class

In this section, we study the behaviour of Dehornoy's class. We provide conjectures on the largest class for cycle sets of a fixed size, and prove it for particular cases. These conjectures were obtained by a numerical study of solutions, using a computer, and we provide our algorithms (in our case they were done using monomial matrices, as they allow for quick and simple implementations).

We also relate divisors of Dehornoy's class with other constants associated to a cycle set (size, order of the permutation group, order of the diagonal map).

From now on, we fix a cycle set S of size n, structure group G, germ $\overline{G}$ and Dehornoy's class d.

One important object to consider is the Permutation group of a solution, denoted G^0 in the seminal paper [ESS99].

Definition 2.4.0.1. *The permutation group $\mathcal{G}_S$ associated to a cycle set S is the subgroup of $\mathfrak{S}_n$ generated by $\psi(s_i), 1 \leq i \leq n$.*

When the context is clear we will simply write $\mathcal{G}$.

$\mathcal{G}$ is precisely the image of the map sending g in G to P_g. Note that, as $P_\sigma P_\tau = P_{\tau\sigma}$, we have that $\psi(gh) = \psi(h)\psi(g)$, thus an anti-morphism (by sending g to $\psi(g)^{-1}$ we obtain a morphism). Equivalently, it is the image of the morphism given by the restriction $\lambda|^S \colon (G, \cdot) \to \mathrm{Aut}(S)$ where we only consider the action of $\lambda(G)$ on S. The kernel of this restriction is the socle $\mathrm{Soc}(G)$, thus $\mathcal{G} = G/\mathrm{Soc}(G)$. By Proposition 2.2.0.4, dG is a subbrace of $\mathrm{Soc}(G)$, thus the quotient $G \to \mathcal{G}$ factors through $\overline{G}$.

As a consequence we obtain the following result:

Proposition 2.4.0.2 ([Ced18])**.** *The class d divides the order of $\mathcal{G}$. In particular d divides $n!$.*

Moreover, d is the lcm of the additive orders of $\psi(g)$ in $(\mathcal{G}, +)$.

Proof. For $s \in S$, the set $\{ks \mid k \in \mathbb{Z}\}$ is a subgroup of $(G, +)$, and the smallest integer d_s such that $d_s s$ is in the socle is exactly equal to the order of $\psi(s)$ in $(\mathcal{G}, +)$, which thus divides $|\mathcal{G}|$. Thus the lcm of the d_s also divides the order of $\mathcal{G}$.

As d is the lcm of all the $d_s, s \in S$, it also divides $|\mathcal{G}|$. □

The following is proved in [LRV22], allowing to restrict to orbits for computing the class of a solution:

Proposition 2.4.0.3 ([LRV22, Lemma 6.1])**.** *If s and t in S are in the same $\mathcal{G}$-orbit, then the additive orders of their permutations $\psi(s)$ and $\psi(t)$ are the same.*

A very important class of solutions are the "indecomposable" ones, which have been studied extensively and led to some classification results, such as it can be found in [ESS99; CPR20; DPT24; ESG01].

Definition 2.4.0.4 ([Bha+21])**.** *A subset X of S is said to be $\mathcal{G}$-invariant if for every $s \in S$, $\psi(s)(X) \subseteq X$.*

S is called decomposable if there exists a proper partition $S = X \sqcup Y$ such that X, Y are stable under $*$, i.e. $X * X = X$ and $Y * Y = Y$. In this case $(X, *_{|_X})$ and $(Y, *_{|_Y})$ are also cycle sets.

A cycle set that is not decomposable is called indecomposable.

Example 2.4.0.5. *For $S = \{s_1, s_2, s_3, s_4\}$ and $\psi(s) = (12)(34)$ for all s, we have $\mathcal{G} = \langle (12)(34) \rangle < \mathfrak{S}_n$. We see that $X = \{s_1, s_2\}$ and $Y = \{s_3, s_4\}$ are both $\mathcal{G}$-invariant and their respective cycle set structure are given by $\psi_X(s_1) = \psi_X(s_2) = (12)$ and $\psi_Y(s_3) = \psi_Y(s_4) = (34)$.*

Note that S has size 4 and class 2, and both X and Y have size and class 2.

The following statement will be be useful

Proposition 2.4.0.6 ([ESS99, Proposition 2.11])**.** *A cycle set S is indecomposable if and only if its permutation group $\mathcal{G}$ acts transitively on S.*

Using a python program based on the proof of Proposition 2.2.0.1 and the enumeration from [AMV22], we can find the following maximum values of the class of cycle sets of size n. We used the following algorithm to compute the class of a solution:

Algorithm 1 Computing the class of a solution

Input: A cycle set $(S, *)$.
Output: A couple $(S, *)$ with a binary operation $*$

```
Set d := 1
for each s in S do
    Set d_s := 1
    while λ_{dd_s s}|_S ≠ id_S do
        Set d_s := d_s + 1
    Set d := dd_s
return d.
```

The idea of Algorithm 1 is that, if $S = \{s_1, \ldots, s_n\}$, we find the smallest positive integer d_1 such that $d_1 s_1$ is diagonal (has trivial permutation). Then, for s_2 we look at all multiples of $d_1 s_2$, i.e. we look for the smallest positive integer d_2 such that $d_1 d_2 s_2$ is diagonal, and so on. Doing so for all solutions of a fixed size, we obtain the following values for the maximal class of solutions of a given size:

n	1	2	3	4	5	6	7	8	9	10
$d_{\max}$	1	2	3	4	6	8	12	15	24	30

Figure 2.2: Maximal class for solutions of a given size

The sequence in Figure 2.2 corresponds to the OEIS sequence A034893 *"Maximum of different products of partitions of n into distinct parts"*, studied in [Doš05] where the following is proved:

Lemma 2.4.0.7 ([Doš05, Theorem 3.1])**.** *Let $n \geq 2$ be written as $n = \mathcal{T}_m + l$ where $\mathcal{T}_m$ is the biggest triangular number ($\mathcal{T}_m = 1 + 2 + \cdots + m$) with $\mathcal{T}_m \leq n$ (and so $l \leq m$). Then the maximum value*

$$a_n = \max\left(\left\{\prod_{i=1}^{k} n_i \middle| k \in \mathbb{N}, 1 \leq n_1 < \cdots < n_k, n_1 + \cdots + n_k = n\right\}\right)$$

is given by

$$a_n = a_{\mathcal{T}_m + l} = \begin{cases} \frac{(m+1)!}{m-l}, & 0 \leq l \leq m-2 \\ \frac{m+2}{2} m!, & l = m-1 \\ (m+1)!, & l = m. \end{cases}$$

This leads to the following conjecture:

Conjecture 2.4.0.8. *If S is of size n, its class d is bounded above by a_n and the bound is minimal.*

The next value we would expect for $n = 11 = 10 + 1 = T_4 + 1$ (resp. $n = 12 = 10 + 2$ would be $d_{\max}(11) = \frac{(4+1)!}{4-1} = 40$ (resp. $d_{\max}(12) = 60$).

The landau function $g\colon \mathbb{N}^* \to \mathbb{N}^*$ ([Lan03]) is defined as the largest order of a permutation in $\mathfrak{S}_n$.

Recall, from [Rum05], that a cycle set S is called square-free when $s * s = s$ (i.e the diagonal map T is the identity).

Proposition 2.4.0.9. *If S is of size n and is square-free and $\mathcal{G}$ is abelian then $d \leq a_n$*

That is, under these conditions the bound part of Conjecture 2.4.0.8 holds.

Proof. If S is square-free, then for all $s \in S$ we have by definition $T(s) = s$, so by Proposition 2.3.0.4 for any $k \in \mathbb{Z}$, $ks = sT(s)\dots T^{k-1}(s) = s^k$. Thus $\{ks \mid k \in \mathbb{Z}\}$ is a subgroup of $(G, \cdot)$ and the smallest integer d_s such that $d_s s$ is in the socle corresponds to the order of $\psi(s)$ in $(\mathcal{G}, \cdot)$, which must divide $e(\mathcal{G})$ the exponent of $\mathcal{G}$ (the lcm of the orders of every element). So d will also divide $e(\mathcal{G})$.

As $\mathcal{G}$ is abelian and finite, there exists an element with order equal to its exponent, so the exponent is bounded by the maximal order of an element, i.e. $d \mid e(\mathcal{G}) \leq g(n)$.

By the decomposition of permutations in disjoint cycles, $g(n)$ is equal to the maximum of the lcm of partitions of n:

$$g(n) = \max\left(\{\mathrm{lcm}(n_1, \dots, n_k) | k \in \mathbb{N}, 1 \leq n_1 \leq \dots \leq n_k, n_1 + \dots + n_k = n\}\right)$$

Moreover, by properties of the lcm, if $1 \leq n_i = n_j$, as $\mathrm{lcm}(n_i, n_j) = n_i$, the max is unchanged by replacing n_j by only 1's. And as the lcm of a collection is bounded above by the product of the elements, we have $g(n) \leq a_n$. Thus $d \leq g(n) \leq a_n$. □

This result was then improved in [CR23]:

Proposition 2.4.0.10 ([CR23, Section 5])**.** *The following hold:*

- *If $\mathcal{G}$ is cyclic, $d \leq g(n)$*
- *If $\lambda_g(g) = g$ for all $g \in \overline{G}$ (equivalently for all $g \in G$), then $d \leq g(n)$*
- *If $(G, \cdot) \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ with non-necessarily distinct primes p_i and such all $p_i^{\alpha_i}$ are distinct, then $d \leq a_n$*
- *We always have $d \leq 24^{\frac{n-1}{3}}$*

In Appendix A) we will provide some histograms on the values of d for particular classes of solutions.

In personal communications with R. Sastriques-Guardiola, the following conjecture was mentioned:

Conjecture 2.4.0.11 ([Sas])**.** *If S is indecomposable of size n, then $d \leq n$.*

Note that, as in Example 2.2.0.7, taking $S = \{s_1, \dots, s_n\}$ with $\psi(s) = (12\dots n)$ for all s provides an indecomposable cycle set that attains this bound.

In this direction the following was obtained in [CR23]:

Proposition 2.4.0.12 ([CR23, Corollary 5.12])**.** *If S is indecomposable and $\mathcal{G}$ acts regularly on X (i.e without fixed point), then $d \leq n$.*

Moreover, if S is indecomposable and n is square-free, then $d = n$.

The following proposition, although a direct consequence of previous results, will provide useful relations between different integers associated to a solution.

Proposition 2.4.0.13. *We have the following divisibilities:*

(i) $o(T) \mid d$

(ii) $d \mid \#\mathcal{G}$

(iii) $\#\mathcal{G} \mid d^n$

where $o(T)$ *is the order of the diagonal permutation* T*,* $\#\mathcal{G}$ *denotes its order* $|\mathcal{G}|$ *(to avoid confusion with* $\mid$ *for divisibility).*

In particular, $G \to \mathcal{G}$ *factorizes through* $\overline{G}$*.*

Proof. (i) is Proposition 2.3.0.4 and (ii) is Proposition 2.4.0.2.

For the last one, by definition $dG \subset \mathrm{Soc}(G)$, so $\overline{G}$ is a quotient of G by elements with trivial permutation. Thus $G \twoheadrightarrow \mathcal{G}$ factorizes through $\overline{G}$, giving (iii). □

Example 2.4.0.14. *Let* $S = \{s_1, s_2, s_3, s_4\}$ *with* $\psi(s_1) = \psi(s_2) = (34)$ *and* $\psi(s_3) = \psi(s_4) = (12)$*. Then* $T = id$ *and* $\mathcal{G} = \langle (12), (34) \rangle$*. Moreover* S *is square-free so* $ks = s^k$ *for all* $s \in S$ *and* $k \in \mathbb{Z}$*. Thus* $o(T) = 1, d = 2$ *and* $\#\mathcal{G} = 4$*.*

For a positive integer k, denote by $\pi(k)$ the set of prime divisors of k. For instance $\pi(24) = \{2, 3\}$.

Corollary 2.4.0.15. *We have* $\pi(d) = \pi(\#\mathcal{G})$*.*

In particular, d *is a prime power iff* $\#\mathcal{G}$ *is a prime power.*

This means that our later results, which will involve the condition "d is a prime power" can also be restated for $\#\mathcal{G}$.

Proof. As d divides $\#\mathcal{G}$ (Proposition 2.4.0.2), any divisor of d is a divisor of $\#\mathcal{G}$. Conversely, if p is a prime divisor of $\#\mathcal{G}$ then it divides d^n and thus divides d. □

Lemma 2.4.0.16. *If* S *is indecomposable then* n *divides* $\#\mathcal{G}$*.*

In particular, $\pi(n) \subseteq \pi(\#\mathcal{G}) = \pi(d)$*, and thus if* d *is a prime power then* n *is also a power of the same prime.*

Proof. By Proposition 2.4.0.6, we know that S is indecomposable iff $\mathcal{G}$ acts transitively on S. By the orbit stabilizer theorem, for any s in S we have $\#\mathrm{Orb}(x) = \frac{\#\mathcal{G}}{\#\mathrm{Stab}(x)}$. So if S is indecomposable there is a unique orbit of size n so n divides $\#\mathcal{G}$. The last statements are a direct consequence of this divisibility and the previous corollary. □

Lemma 2.4.0.17. *If* S *is indecomposable and* $\mathcal{G}$ *is abelian, then* $n = |\mathcal{G}|$

Proof. [1] By Proposition 2.4.0.6, we know that S is indecomposable iff $\mathcal{G}$ acts transitively on S. Let $x_0 \in S$, by transitivity for all $x \in S$, there exists $\sigma \in \mathcal{G}$ such that $x = \sigma(x_0)$. Let $\tau \in \mathcal{G}$ be such that we also have $x = \tau(x_0)$, we will show that $\tau = \sigma$. For all $y \in S$, there exists $\nu \in \mathcal{G}$ such that $y = \nu(x)$, thus $\sigma(y) = \sigma(\nu(x)) = \sigma(\nu(\tau(x_0)) = \tau(\nu(\sigma(x_0)) = \tau(y)$. So an element of $\mathcal{G}$ is uniquely determined by its image of x_0, thus $|S| \geq |\mathcal{G}|$, and the other inequality follows by transitivity. □

[1] https://math.stackexchange.com/a/1316138

Let $k \geq 1$ and denote by kG the subgroup of $(G, \cdot)$ generated by $kS = \{ks \mid s \in S\}$. The following result appears simultaneously in [Fei24, Proposition 2.13] and [LRV22, Theorem B], the latter calling it "cabling":

Proposition 2.4.0.18. *For $k \geq 1$, kG is a left-ideal of G. Moreover, it induces a cycle set structure on kS.*

Explicitly, $\psi(ks)(kt) = k\lambda_{ks}^{-1}(t)$.

Proof. First note, as for any $s, t \in S$ and $g \in G$, by Proposition-Definition 1.6.0.4, $ks + kt = ks \cdot k\lambda_{ks}^{-1}(t) \in kG$ and $\lambda_g(ks) = k\lambda_g(s) \in kS$. Thus, kG is a left-ideal of G, in particular it is a subbrace by Proposition 1.6.0.11.

So we will construct the cycle set $(kS, \star)$ so that it has naturally as structure brace kG. Define $ks \star ts = \psi(ks)(t) = k\lambda_{ks}^{-1}(t) = \lambda_{ks}^{-1}(kt)$. We want to show that $(ks \star kt) \star (ks \star ku) = (kt \star ks) \star (kt \star ks)$.

We have $(ks \star kt) \star (ks \star ku) = \lambda_{ks}^{-1}(kt) \star \lambda_{ks}^{-1}(ku) = \lambda^{-1}_{\lambda_{ks}^{-1}(kt)}(\lambda_{ks}^{-1}(ku))$.

The conclusion then follows from Lemma 1.6.0.8:

$$(ks \star kt) \star (ks \star ku) = \lambda^{-1}_{\lambda_{ks}^{-1}(kt)}(\lambda_{ks}^{-1}(ku)) = \lambda^{-1}_{\lambda_{kt}^{-1}(ks)}(\lambda_{kt}^{-1}(ku)) = (kt \star ks) \star (kt \star ku).$$

□

We can explicitly know the class of the cabling of a solution:

Proposition 2.4.0.19. *Let k be a positive integer smaller than d, then $(kS, \star)$ is of class $\frac{d}{gcd(d,k)}$.*

Moreover, $((d+1)S, \star)$ is the same, as a cycle set, as $(S, *)$.

This means that this construction provides, at most, d different cycle sets.

Proof. By definition of $(G, +)$, for any integer j and k, we have $j(ks) = (jk)s$. Thus $a(ks)$ is in the socle for every s if and only if ak is a multiple of d. So we deduce that kS is of class $\frac{\text{lcm}(d,k)}{k} = \frac{d}{\text{gcd}(d,k)}$.

By definition of d, we have that $(dS, \star)$ is the trivial cycle set (all permutations are trivial), thus $\psi((d+1)S) = \psi(s)$. □

Example 2.4.0.20. *Consider $S = \{s_1, s_2, s_3, s_4\}$ with $\psi(s) = \sigma = (1234)$ for all s in S. Then kS is given by $ks_i \star ks_j = ks_{\sigma^k(j)}$, so that $2S$ has class 2 (all elements acts by $(13)(24)$)) and $4S$ is the trivial cycle set, while $3S$ has class 3 (all elements acts by $(1234)^{-1} = (4321)$) and is in fact isomorphic to S (by setting f that swaps (s_4, s_1) and (s_3, s_2)).*

Finally, we relate the class of a cycle set with the class of its retraction as defined in [ESS99]:

Proposition-Definition 2.4.0.21 ([ESS99; Rum05])**.** *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 2.4.0.22. *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 2.4.0.23. *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.*

2.5 Zappa-Szép product and Sylows

In [Bac18; CCS20], the matched product of braces is defined, which is a way to take two braces acting on each other by automorphism to construct a new one. In [BCJ16], a method is given to construct, given a brace B, all solutions (X, r) such that $\mathcal{G}_{(X,r)} \simeq B$. Combining these and classifying suitable families of braces could lead to a classification of solutions. Both methods are algorithmically complex: the first relies on knowing the automorphism group of a brace, the second on some parameters to be obtained in a brace (additively generating set, families of subgroups of stabilizers). Also note that the matched product is a brace version of the Zappa–Szép product ([Led73]), which is the terminology we'll use.

This approach can be improved by only considering braces that come from germs, i.e. those with additive group $(\mathbb{Z}/d\mathbb{Z})^n$. To do so, we explicitly algorithmically highlight how the Sylow subgroups of the germ decompose the cycle set into cycle set with prime power classes. Then, we are able to obtain a condition, a simplified version of the matched product condition, for which two germs can be multiplied to obtain a new solution with class a divisor of the product of the original classes.

Recall that Σ_n^k, for $k > 1$, denotes the group of monomial matrices with non-zero coefficients powers of ζ_k, and that ι_k^{kl} is the embedding $\Sigma_n^k \hookrightarrow \Sigma_n^{kl}$ sending ζ_k to ζ_{kl}^l. Given two subgroups $H, K < G$, their internal product subset is defined by $HK = \{hk \mid h \in H, k \in K\}$. If H and K have trivial intersection and $HK = KH$, the set product HK has a natural group structure called the Zappa–Szép product of H and K. We apply this to the Sylow-subgroups of the germs to obtain that any finite cycle set can be constructed from the Zappa–Szép product of the germs of cycle sets of class a prime power.

Definition 2.5.0.1. *Let k, l be integers such that $k, l > 1$. Let m be a common multiple of k and l, with $m = ka = lb$ for some $a, b \geq 1$. Given two subgroups $G < \Sigma_n^k$, $H < \Sigma_n^l$ by $G \bowtie_m H$ we denote the subset $\iota_k^m(G)\iota_l^m(H)$ of Σ_n^m.*

Identifying G and H with their image in Σ_n^m, we say that they commute ([Led73]) if $GH = HG$ as sets, i.e. for any (g, h) in $G \times H$, there exists a unique (g', h') in $(G \times H)$ such that $gh = h'g'$.

Example 2.5.0.2. *Consider* $A = \begin{pmatrix} \zeta_2 & 0 \\ 0 & \zeta_2 \end{pmatrix} \in \Sigma_2^2$ *and* $B = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^2 \end{pmatrix} \in \Sigma_2^3$. *The least common multiple of 2 and 3 is 6, thus*

$$\iota_2^6(A)\iota_3^6(B) = \begin{pmatrix} \zeta_6^3 & 0 \\ 0 & \zeta_6^3 \end{pmatrix} \begin{pmatrix} \zeta_6^2 & 0 \\ 0 & \zeta_6^4 \end{pmatrix} = \begin{pmatrix} \zeta_6^5 & 0 \\ 0 & \zeta_6 \end{pmatrix} \in \Sigma_2^6$$

Remark 2.5.0.3. *This operation can be thought of as taking elements of* G *and* H*, changing appropriately the roots of unity (with* $\zeta_k = \zeta_m^a$ *and* $\zeta_l = \zeta_m^b$*) and taking every product of such elements (we embed* G *and* H *in* Σ_n^m *and take their product as subsets).*

When k *and* l *are coprime,* G *and* H *can be seen as subgroups of* Σ_n^m *with trivial intersection, and so if they commute we have that* $G \bowtie_m H$ *is a group called the Zappa–Szép product of* G *and* H *([Led73], Product Theorem).*

Let $(S, *_1), (S, *_2)$ be two cycle sets, over the same set S, of coprime respective classes d_1, d_2 and germs $\overline{G}_1, \overline{G}_2$. Let $d = d_1 d_2$ and $\overline{G} = \overline{G}_1 \bowtie_d \overline{G}_2$ (which, in general, is only a subset of Σ_n^d), and we identify each $\overline{G}_i$ with its image in $\overline{G}$.

Definition 2.5.0.4. S_1 *and* S_2 *are said to be* $\bowtie$*-compatible if* $\overline{G}$ *is a germ of the structure group of some cycle set which we'll denote* $S_1 \bowtie S_2$.

If $S_1 \bowtie S_2$ exists, let G be its structure group, d_s its Dehornoy class and $\overline{G}_s$ its germ. Note that we don't require that $\overline{G}$ is exactly $\overline{G}_s$. We only require that $d = d_1 d_2$ is a multiple of d_s.

In Algorithm 2 we construct a candidate $S_1 \bowtie_d S_2$ for which $\overline{G}$ could be the germ. This candidate is not, in general, a cycle set, but if it is, its class is a divisor of d. Then we will state the condition for it to be a cycle set.

For clarity, we will put a subscript to distinguish between the respective structures of S_1 and S_2: $\psi_1(s)$ will denote the permutation given by $*_1$ and similarly $\psi_2(s)$ for $*_2$.

Algorithm 2 Constructing $S_1 \bowtie_d S_2$

Input: A set S with two cycle sets structure $*_1, *_2$ on S of coprime classes d_1, d_2
Output: A couple $(S, *)$ with $*$ a binary operation

1: Compute (u, v) the solution to Bézout's identity $d_2 u + d_1 v = 1[d]$
2: **for** $i = 1$ to n **do**
3: Compute $g = us_i \in \overline{G}_1$
4: Let $\sigma = \psi_1(us_i)$
5: Compute $h = vs_{\sigma(i)} = v\lambda_g^{-1}(s_i) \in \overline{G}_2$
6: Let $\psi(s_i)$ be the permutation of $\iota_{d_1}^d(g_1)\iota_{d_2}^d(g_2)$
7: **return** $S_1 \bowtie_d S_2 = (S, *)$ with $s_i * s_j = s_{\psi(s_i)(j)}$.

Remark 2.5.0.5. *The heart of the algorithm is line* 5 *which relies on* $ks \cdot kt = ks + k\lambda_{ks}(t)$.

To obtain an element with diagonal part D_{s_i}*, we have to take* $t = s_{\sigma(i)} = \lambda_{ks}^{-1}(s_i)$ *with here* $\sigma = \psi(ks_i)$ *and as we apply* ι^d *on the elements (in* S_1 *this does* $z \mapsto z^{d_2}$ *and in* S_2 $z \mapsto z^{d_1}$*), we obtain* $D_{s_i} = D_i^{d_2 u + d_1 v} = D_i$ *from lign 1.*

Example 2.5.0.6. *Take two cycle sets of size* $n = 5$ *and class respectively* 2 *and* 3*, and apply Algorithm 2 providing a candidate for a cycle set of class* 6*:*

Let $S_1 = \{s'_1, \dots, s'_5\}$ and $S_2 = \{s''_1, \dots, s''_5\}$, with $(S_1, \psi_1), (S_2, \psi_2)$ given by:

$$\psi_1(s'_1) = \psi_1(s'_3) = (1234) \qquad \psi_1(s'_2) = \psi_1(s'_4) = (1432) \qquad \psi(s'_5) = id$$
$$\psi_2(s''_1) = \psi_2(s''_2) = (354) \qquad \psi_2(s''_3) = \psi_2(s''_4) = \psi_2(s''_5) = (345)$$

Where S_1 is of class $d_1 = 2$ and S_2 of class $d_2 = 3$.

Consider their respective germs $\overline{G}_1$ and $\overline{G}_2$ of order 2^5 and 3^5. Then we define $\overline{G} = \overline{G}_1 \bowtie_6 \overline{G}_2$ over the basis $S = \{s_1, \dots, s_5\}$. For instance we have:

$$\iota_2^6(s'_1) = \iota_2^6\left(\begin{pmatrix} 0 & \zeta_2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 0 & \zeta_6^3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\iota_3^6(s''_1) = \iota_3^6\left(\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_6^2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

To construct an element $g \in \overline{G}$ with $D_g = D_{s_3}$ we first solve Bézout's identity modulo 6: $3u + 2v = 1[6]$, a solution is given by $u = 1$ and $v = 2$, so we will multiply some $\iota_2^6(s'_i)$ and $\iota_2^6(2s''_j)$ so that their product has diagonal part $D^1_{s_3}(D^2_{s_3})^2 = D_{s_3} mod z^6$. Recall that:

$$ks \cdot kt = ks + k\lambda_{ks}(t).$$

Here we want $s = \lambda_{ks}(t) = s_3$, $k = 3u$ and $l = 2v$, so we take $s = 3$. As $\sigma = \psi(1s'_3) = \psi(s'_3) = (1234)$, we have $t = s''_{\sigma(3)} = s''_4$, and note that $2s''_4 = s''_4 s''_5$. Finally:

$$\iota_2^6(s'_3)\iota_3^6(2s''_4) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \zeta_6^{3\cdot 1} & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \zeta_6^{2\cdot 2} & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \zeta_6^{3+4} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & \zeta_6 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

This will be our candidate for s_3. Doing this for all the generators we find:

$$\psi(s_1) = (124)(35), \psi(s_2) = (1532), \psi(s_3) = (1254), \psi(s_4) = (132)(45), \psi(s_5) = (354).$$

Unfortunately, this isn't a cycle set: $(s_1 * s_2) * (s_1 * s_1) = s_4 * s_2 = s_1$ whereas $(s_2 * s_1) * (s_2 * s_1) = s_5 * s_5 = s_4$. This also means that $\overline{G}$ is not a brace, as for instance $s_1 + s_2 \neq s_2 + s_1$.

To verify that $S_1 \bowtie S_2$ is a cycle set, an extra condition is needed:

Proposition 2.5.0.7. *If $\overline{G}_1$ and $\overline{G}_2$ commute, then S_1 and S_2 are $\bowtie$-compatible.*

In this case, $\overline{G} = \overline{G}_1 \bowtie_d \overline{G}_2$ is the Zappa–Szép product of $\overline{G}_1$ and $\overline{G}_2$. Note that this would also work over any multiple of d, but we chose to restrict to d for simplicity (as mentioned under Proposition 2.2.0.1 which defines the class).

Proof. As d_1 and d_2 are coprime, it follows that $\overline{G}_1 \cap \overline{G}_2 = \{1\}$.

By ([Led73], Product Theorem), $\overline{G}$ is a subgroup of Σ_n^k if and only if $\overline{G}_1$ and $\overline{G}_2$ commute, i.e. $\overline{G} = \overline{G}_1 \bowtie_d \overline{G}_2 = \overline{G}_2 \bowtie_d \overline{G}_1$.

Now, d_1 and d_2 are coprime, so $\overline{G}_1$ and $\overline{G}_2$ have different (non-trivial) coefficient-powers. Thus a product $g_1 g_2$ of two non-trivial elements from $\iota_{d_1}^d(\overline{G}_1)$ and $\iota_{d_2}^d(\overline{G}_2)$ cannot be a permutation matrix.

With Algorithm 2, we can construct elements $s_1, \ldots, s_n$ of $\overline{G} < \Sigma_n^d$ such that $D_{s_i} = D_i = \mathrm{diag}(0, \ldots, 0, \zeta_d, 0, \ldots, 0)$. Now by Lemma 1.4.0.1 we have

$$s_i \cdot \psi(s_i)(s_j) = D_{s_i} P_{s_i} D_{\psi(s_i)(s_j)} P_{\psi(s_i)(s_j)} = D_i D_j P_{s_i} P_{\psi(s_i)(s_j)}.$$

Similarly, $s_j \cdot \psi(s_j)(s_i) = D_i D_j P_{s_j} P_{\psi(s_j)(s_i)}$. As $\overline{G}$ is permutation-free and $D_{s_i \cdot \psi(s_i)(s_j)} = D_{s_j \cdot \psi(s_j)(s_i)}$, this implies that $P_{s_i \psi(s_i)(s_j)} = P_{s_j \psi(s_j)(s_i)}$. This precisely means that $S_1 \bowtie S_2$ is a cycle set. □

Remark 2.5.0.8. *To check whether $\overline{G}_1$ and $\overline{G}_2$ commute, we can restrict to the generators and check that:*

$$\forall (s,t) \in S_1 \times S_2, \exists (s', t') \in S_1 \times S_2 \text{ such that } st = t's'.$$

Proposition 2.5.0.9. *If S_1 and S_2 satisfy the following "mixed" cycle set equation*

$$\forall s,t,u \in S, (s *_1 t) *_2 (s *_1 u) = (t *_2 s) *_1 (t *_2 u) \tag{2.2}$$

then S_1 and S_2 are $\bowtie$-compatible and $(S = S_1 \bowtie_d S_2, *)$ is a cycle set.

Let u, v be integers such that $d_2 u + d_1 v = 1[d_1 d_2]$. Explicitly, from Algorithm 2 gives that $\psi(s_i) = \psi_2\left(v s''_{\psi_1(u s'_i)(i)}\right) \circ \psi_1(u s'_i)$.

Proof. Here we will work over monomial matrices as we do not yet have a Brace structure on $\overline{G}$.

We will use the previous Proposition 2.5.0.7 and show how Equation (2.2) naturally arises from considering the commutativity of the germs. For clarity, although our two cycle sets have the same underlying set $S = \{s_1, \ldots, s_n\}$, we will distinguish where we see those elements by writing s' for $(S, *_1)$ and s'' for $(S, *_2)$.

Let $s'_i \in S_1, s''_j \in S_2$, then in $\overline{G}$:

$$s'_i s''_j = D_i^{d_2} P_{s'_i} D_j^{d_1} P_{s''_j} = D_i^{d_2} D^{d_1}_{\psi_1(s'_i)^{-1}(j)} P_{s'_i} P_{s''_j}.$$

We want some $s'_k \in S_1, s''_l \in S_2$ such that $s'_i s''_j = s''_l s'_k$, i.e:

$$D_i^{d_2} D^{d_1}_{\psi_1(s'_i)^{-1}(j)} P_{s'_i} P_{s''_j} = D_l^{d_1} D^{d_2}_{\psi_2(s''_l)^{-1}(k)} P_{s''_l} P_{s'_k}.$$

As d_1 and d_2 are coprime, they're in particular different, so we must have:

$$\begin{cases} D_i^{d_2} = D^{d_2}_{\psi_2(s''_l)^{-1}(k)} \\ D^{d_1}_{\psi_1(s'_i)^{-1}(j)} = D_l^{d_1} \\ P_{s'_i} P_{s''_j} = P_{s''_l} P_{s'_k}. \end{cases} \tag{2.3}$$

From which we first deduce: $k = \psi_2(s''_l)(i)$ and $j = \psi_1(s'_i)(l)$, or equivalently $s_k = s_l *_2 s_i$ and $s_j = s_i *_1 s_l$. So taking this k and l we get $D_{s'_i s''_j} = D_{s''_l s'_k}$. We are left with the last of the three conditions, which then becomes:

$$P_{s'_i} P_{s'_i *_1 s''_l} = P_{s''_l} P_{s''_l *_2 s'_i}.$$

As $P_\sigma P_\tau = P_{\tau\sigma}$, this is equivalent to

$$\psi_2(s'_i *_1 s''_l) \circ \psi_1(s'_i) = \psi_1(s''_l *_2 s'_i) \circ \psi_2(s''_l).$$

As $s''_l \in S_2$, $\psi_2(s'_i *_1 s''_l)$ is seen as the action of an element of S_2. Thus, the Equations 2.3 are equivalent to:

$$\forall s, t, u \in S, (s *_1 t) *_2 (s *_1 u) = (t *_2 s) *_2 (t *_2 u).$$

□

Remark 2.5.0.10. *The condition that the classes are coprime is used, with Bézout's identity, to have generators of the group $\overline{G}$ (elements with diagonal part D_i). Otherwise, say for instance that the classes are powers of the same prime, $d_1 = p^a$ and $d_2 = p^b$ with $b \leq a$. Then $\iota^d_{d_2}$ is the identity and $\iota^d_{d_1}$ will add elements with higher coefficient powers (or equal), thus we do not get any new generators (or too many in the case $a = b$).*

We've seen how to construct cycle sets from ones of the same size and coprime classes. Now we show that this is enough to get all cycle sets from just ones of prime-power class:

Let $d = p_1^{a_1} \dots p_r^{a_r}$ be the prime decomposition of p ($a_i > 0$ and $p_i \neq p_j$), and write $\alpha_i = p_i^{a_i}$ for simplicity. We use techniques inspired by [CJO22] to construct new cycle sets from two with coprime Dehornoy's class.

Fix again a cycle set S of size n and class $d > 1$, with germ $\overline{G}$. By Proposition 2.4.0.18, given $k > 0$ diving d, the subgroup $\overline{k}G$ generated by $kS = \{ks \mid s \in S\}$ is the germ of a structure group, and has for elements the matrices whose coefficient-powers are multiples of k.

Lemma 2.5.0.11. *Let $\beta_i = \frac{d}{\alpha_i}$ then*

(i) For each i, $\beta_i \overline{G}$ is a p_i-Sylow of $\overline{G}$.

(ii) Two such subgroups commute (i.e. $\beta_i \overline{G} \cdot \beta_j \overline{G} = \beta_j \overline{G} \cdot \beta_i \overline{G}$).

(iii) $\overline{G}$ is the product of all those subgroups.

Proof. (i) follows directly from the fact that $\beta_i\overline{G}$ is a left ideal of $\overline{G}$ (Proposition 2.4.0.18), and has order

$$\#\beta_i\overline{G} = \frac{\#\overline{G}}{(\beta_i)^n} = \frac{d^n}{\left(\frac{d}{\alpha_i}\right)^n} = \alpha_i^n = p_i^{na_i}.$$

This is indeed a p-Sylow as $\#\overline{G} = d^n = (p_1^{a_1}\dots p_r^{a_r})^n = p_1^{na_1}\dots p_r^{na_r}$.

For (ii), let $g, h \in G$ and consider $\beta_i g \cdot \beta_j h \in \beta_i\overline{G} \cdot \beta_j\overline{G}$. From Lemma 1.6.0.7 and Proposition-Definition 1.6.0.4, we have $\beta_i g \cdot \beta_j h = \beta_i g + \beta_j \lambda_{\beta_i g}(h)$ and denote $h' = \lambda_{\beta_i g}(h)$ for simplicity. Then $\beta_i g \cdot \beta_j h = \beta_i g + \beta_j h' = \beta_j h' + \beta_i g = \beta_j h' \cdot \beta_i \lambda_{\beta_j h'}(g) \in \beta_j\overline{G} \cdot \beta_i\overline{G}$. We conclude by symmetry to obtain the other inclusion $\beta_j\overline{G} \cdot \beta_i\overline{G} \subseteq \beta_i\overline{G} \cdot \beta_j\overline{G}$.

(iii) then follows by cardinality ($\#\overline{G} = \prod_{i=1}^{r} \#\beta_i\overline{G}$), as the $\beta_i\overline{G}$ are a family of commuting Sylows for each prime p_i dividing d. □

Example 2.5.0.12. *Checking the enumeration of solutions up to size* 10 *provided by [AMV22], we find that the first example where S is indecomposable but has class product of different primes is $n = 8, d = 6$ given by:*

$$\begin{aligned}
\psi(s_1) &= (12)(36)(47)(58), & \psi(s_2) &= (1658)(2347),\\
\psi(s_3) &= (1834)(2765), & \psi(s_4) &= (12)(38)(45)(67),\\
\psi(s_5) &= (1438)(2567), & \psi(s_6) &= (1856)(2743),\\
\psi(s_7) &= (16)(23)(45)(78), & \psi(s_8) &= (14)(25)(36)(78)
\end{aligned}$$

Here, $\overline{G}$ decomposes as the Zappa–Szép product $3\overline{G} \bowtie_6 2\overline{G}$ of its 2-Sylow and 3-Sylow. If we denote by (S_2, ψ_2) and (S_3, ψ_3) their respective cycle set structures then we find:

$$\begin{aligned}
\psi_2(s_1') = \psi_2(s_2') &= (1476)(2583),\\
\psi_2(s_3') = \psi_2(s_6') &= (18)(27)(36)(45),\\
\psi_2(s_4') = \psi_2(s_5') &= (1674)(2385),\\
\psi_2(s_7') = \psi_2(s_8') &= (12)(34)(56)(78)
\end{aligned}$$

and

$$\begin{aligned}
\psi_3(s_1'') = \psi_3(s_3'') = \psi_3(s_5'') = \psi_3(s_7'') &= (135)(264),\\
\psi_3(s_2'') = \psi_3(s_4'') = \psi_3(s_6'') = \psi_3(s_8'') &= (153)(246).
\end{aligned}$$

The associativity of multiplication of matrices ensure that the Zappa-Szép products of germs is associative (see [Bri05, Section 3.14] for the general case). Then, Lemma 2.5.0.11 can be rephrased as $\overline{G} = \beta_1\overline{G} \bowtie_d \dots \bowtie_d \beta_r\overline{G}$. As the germ can be used to reconstruct the structure group and thus the cycle set, the following theorem summarizes these results from an enumeration perspective, that is to construct all solutions of a given size.

Theorem 2.5.0.13. *Any finite cycle set can be constructed from the Zappa–Szép product of the germs of cycle sets of whose Dehornoy classes are powers of primes.*

Proof. Any cycle set is determined by its structure monoid (the atoms are the generators, with permutation equal to the left-action of the cycle set binary map $*$). And the structure monoid can be recovered from the germ by Proposition 2.2.0.10. By Lemma 2.5.0.11 and the above construction, the germ can be decomposed and reconstructed from its Sylows, which also determine cycle sets by Proposition 2.4.0.18. □

Remark 2.5.0.14. *As mentioned earlier, if one is able to construct all solutions in a given size with prime-power class, the solutions with the same size and non prime-power classes could then be constructed. This would still involve checking when two solutions are compatible and to consider each solution up to isomorphism (which is simpler than brace automorphism of the germ, as done in [Bac18]).*

Remark 2.5.0.15. *The class of the cycle set constructed will Algorithm 2 will, in general, only be a divisor of the product of the prime-powers. This happens because nothing ensures that, for instance, the cycle set obtained is not trivial: we only know that $d_1 d_2 s$ is diagonal, but it is not necessarily minimal.*

When restricting to indecomposable cycle sets, the classification problem can be further reduced:

Corollary 2.5.0.16. *Any cycle set is induced (in the sense of using the decomposability and Zappa–Szép product) by indecomposable cycle sets of smaller size and class, both powers of the same prime.*

More precisely, this "breaking down" of a cycle set, of size n and class $d = p_1^{a_1} \dots p_r^{a_r}$, is as follows: First using Theorem 2.5.0.13 to split it into cycle sets $(S_i)_{1 \leq i \leq r}$ of size n and class a power of p_i. Then using Lemma 2.4.0.16 to decompose each S_i into indecomposable cycle sets of size and class both a power of p_i (and the sum of their sizes equal to n).

Proof. From Theorem 2.5.0.13, let a cycle set S be obtained from its germ as an internal product of $S_1, \dots, S_r$ of classes respectively $p_1^{a_1}, \dots, p_r^{a_r}$ with distinct primes. Then, consider a decomposition of each S_i as indecomposable cycle sets: so up to a change of enumeration, the matrices in the structure group of S_i are diagonal-by-block with each block corresponding to a cycle set. Moreover, each of those cycle sets must have a class that divides the class of S_i, which is $p_i^{a_i}$, thus their class is a power of p_i. By Lemma 2.4.0.16, the size of those indecomposable cycle sets must also be powers of p_i. □

However, as far as the author knows, there is no "nice" way, given two cycle sets, to construct all cycle sets that decompose on those two, thus the above result is an existence result but not a constructive one, unlike the Zappa–Szép product previously used.

Remark 2.5.0.17. *Starting from a cycle set, we first write it as a Zappa–Szép product of its Sylows and then decompose each Sylow-subgroup if the associated cycle set is decomposable. If one proceeds the other way, first decomposing and then looking at the Sylows of each cycle set of the decomposition, we obtain less information. For instance, if $S = \{s_1, \dots, s_6\}$ with $\psi(s_i) = (1 \dots 6)$ for all i, then S is not decomposable, but the cycle sets obtained from its Sylows $2S$ and $3S$ are decomposable ($\psi_2(s_i) = (14)(25)(36)$ and $\psi_3(s_i) = (135)(246)$ for all i, having respectively 3 and 2 orbits).*

Example 2.5.0.18. *In Example 2.5.0.12, S_3 has to be decomposable as $n = 3$ does not divide $d = 8$. Indeed, it decomposes as $S_3 = \{s_1'', s_3'', s_5''\} \sqcup \{s_2'', s_4'', s_6''\} \sqcup \{s_7'', s_8''\}$.*

Using the enumeration of [AMV22] and Algorithm 1, for $n = 10$ we find that there is approximately 67% of cycle sets that have class a prime-power ($\sim$ 3.3millions out of $\sim$ 4.9 millions). We hope that this number greatly reduces as n increases (as hinted by the previous values, for $n = 4$ it is 99%), as more values of d are possible (See Conjecture 2.4.0.8).

CHAPTER 3

Irreducibility of the monomial representations

In this section, we study the relation between the indecomposability of a cycle set and the irreducibility of its monomial representation. Recall from Definition 2.4.0.4 that a cycle set S is said to be indecomposable if there exists no proper partition $S = S_1 \sqcup S_2$ such that $S_1 * S_1 = S_1$ and $S_2 * S_2 = S_2$. On the other hand for a group G, a ring R and a $R[G]$-module V, a representation $G \to \mathrm{GL}(V)$ is said to be irreducible if there exists no proper submodule W of V such that $G \cdot W \subseteq W$.

The motivation is that the representations of G and $\overline{G}$, defined in Section 1, are monomial. By [CR62, Corollary 50.4], any irreducible monomial representation is induced by a character of a subgroup. Our goal is thus to study the irreducibility of the representations Θ and $\overline{\Theta}$, and when they are induced by a character of a subgroup.

Here, we obtain that the indecomposability of a cycle set is equivalent to the irreducibility of the representation Θ. For the irreducibility of $\overline{\Theta}$ on the germ we have to restrict to the cases where the Dehornoy class is not 2 or 6. We provide a counterexample for $d = 2$, but the case of finding a counterexample for $d = 6$ remains open. Moreover, we show that when considering a larger germ, namely $\overline{G}_l = G/\langle lds \rangle$ there is an equivalence between irreducibility of the representation and indecomposability of the solution.

All along this section, we fix a cycle set $(S, *)$ of size n, of Dehornoy's class $d > 1$, with structure group G and germ $\overline{G} = G/\langle dS \rangle$.

The content of this section was obtained in joint work with C. Dietzel (LMNO, Caen) and S. Properzi (VUB, Brussels).

3.1 Indecomposability and Irreducibility

In this section, we study the equivalences between the indecomposability of a cycle set and the irreducibility of the monomial representations of its structure group and germs.

For any positive integer l, we denote by $\overline{G}_l$ the quotient $G/\langle (ld)S \rangle$ and call it the l-germ of G. In particular, we have $\overline{G}_1 = \overline{G}$. Recall that we have the monomial representation of the structure group $\Theta \colon G \to M_S(\mathbb{C}(z))$. By Proposition 2.2.0.5 we have that $\overline{G}_l$ is a brace

with additive structure $(\mathbb{Z}/ld\mathbb{Z})^S$ and we have a monomial representation $\overline{\Theta}_l \colon \overline{G}_l \to M_S(\mathbb{C})$ obtained by the specialization ev_{ld} of z at $\zeta_{ld} = \exp(\frac{2i\pi}{ld})$.

Recall, by Proposition 2.4.0.6, that S is indecomposable if and only if its permutation group $\mathcal{G}$ acts transitively on S. As $\mathcal{G}$ is a quotient of both G and $\overline{G}_l$, indecomposability is also equivalent to a transitive action of the structure group (resp. germ) on S.

Proposition 3.1.0.1. *Let l be a positive integer. Consider the following assertions:*

(i) S is indecomposable

(ii) $\Theta \colon G \to M_S(\mathbb{C}(z))$ is irreducible

(iii) $\overline{\Theta}_l \colon \overline{G}_l \to M_S(\mathbb{C})$ is irreducible.

Then the followings hold:

a) $(ii) \Leftrightarrow (i)$

b) If $l = 1$, then $(iii) \Rightarrow (i)$

c) If $l > 1$, then $(iii) \Leftrightarrow (i)$.

Proof. We begin by showing that (ii) (resp. (iii) for $l \geq 1$) implies (i). By contradiction, suppose that S is decomposable and let K be $\mathbb{C}$ or $\mathbb{C}(z)$, say $S = S_1 \sqcup S_2$ with $S_1, S_2 \notin \{\varnothing, S\}$. This means that for any s in S, $\psi(s)(S_i) = S_i$. Then, the permutation matrix P_s associated to $\psi(s)$ stabilizes both subspaces $\mathbb{C}(z)^{S_1}$ and $\mathbb{C}(z)^{S_2}$ (resp. $\mathbb{C}^{S_1}$ and $\mathbb{C}^{S_2}$). As S generates G (resp. $\overline{G}_l$), any element of G (resp $\overline{G}$) also stabilizes the two subspaces $\mathbb{C}(z)^{S_1}$ and $\mathbb{C}(z)^{S_2}$ (resp. $\mathbb{C}^{S_1}$ and $\mathbb{C}^{S_2}$). Thus, Θ (resp. $\overline{\Theta}_l$) would be reducible, a contradiction.

We now show that (i) (resp. (iii) for $l > 1$) implies (ii). Suppose that S is indecomposable. Let V be a non-trivial subspace of $\mathbb{C}(z)^S$ (resp. $\mathbb{C}^S$) that is G-invariant (resp. $\overline{G}_l$-invariant). Let $v = (v_s)_{s \in S}$ be a non-trivial vector in V, so there exists s such that $v_s \neq 0$. As S is of class d, we have $ds \in \mathrm{Soc}(G)$ (i.e $\Theta(ds)$ is the diagonal matrix D_s^d). Moreover, as $l > 1$, ds is non-trivial in $\overline{G}_l = G/\langle ldS \rangle$. Then, if we denote by $(e_t)_{t \in S}$ the canonical basis of $\mathbb{C}(z)^S$ (resp. $\mathbb{C}^S$), we deduce that $\Theta(ds)v - v = (z^d - 1)v_s e_s$ (resp. $\overline{\Theta}_l(ds)v - v = (\zeta_{ld}^d - 1)v_s e_s$, which is non-zero as $l > 1$). In both cases, we obtain that e_s is in V. As S is indecomposable, for any $t \in S$, there exists $f \in G$ (resp. $f \in \overline{G}_l$) such that $\lambda_f(s) = t$. If $f = \sum_{u \in S} f_u u$, then $f \cdot s = z^{f_t} t$ (resp. $f \cdot s = \zeta_{ld}^{f_t} t$), so $t \in V$. We thus obtain that the canonical basis of the whole space is in V, so the representation is irreducible. □

Remark 3.1.0.2. *For $l = 1$, the indecomposability of S does not necessarily imply the irreducibility of $\Theta \colon \overline{G} \to M_S(\mathbb{C})$.*

Indeed, consider the case of Example 2.2.0.7 with $n = 2$: let $S = \{s, t\}$ with $\psi(s) = \psi(t)$ the permutation that swaps s and t. Then S is of class 2 and $\overline{\Theta}(s) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\overline{\Theta}(t) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -\overline{\Theta}(s)$. These matrices are simultaneously diagonalizable over $\mathbb{C}$ (the eigenvalues are $\pm i$), and so the representation is not irreducible.

3.2 Estimating the size of $\mathcal{G}(X)$

Proposition 3.1.0.1 only gives that the irreducibility of $\overline{\Theta}$ implies the indecomposability of S. In this section, we obtain a sufficient condition for the reciprocal.

Let us assume that S is an indecomposable cycle set of size n and class d.

Proposition 3.2.0.1. *If S is indecomposable and $|\mathcal{G}| < d^{\frac{n}{2}}$, then $\overline{\Theta}$ is irreducible.*

Note that, as $\mathcal{G} = \overline{G}/\mathrm{Soc}(\overline{G})$, we have $|\mathcal{G}| = \frac{|\overline{G}|}{|\mathrm{Soc}(\overline{G})|} = \frac{d^n}{|\mathrm{Soc}(\overline{G})|}$. Thus

$$|\mathcal{G}| < d^{\frac{n}{2}} \iff |\mathrm{Soc}(\overline{G})| > d^{\frac{n}{2}}.$$

Proof. Write $S = \{s_1, \dots, s_n\}$ and let $e_1, \dots, e_n$ be the associated canonical basis of $\mathbb{C}^S$. Let $0 \neq V$ be a $\overline{G}$-invariant subspace of $\mathbb{C}^S$ with. Let $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{C}^S$ be a non-zero vector. We will show by induction on the number of non-zero coordinates of v that $V = \mathbb{C}^S$. If there is only one i such that $v_i \neq 0$, then by rescaling and applying the transitivity of the action of $\overline{G}$ on S, we obtain $V = \mathbb{C}^S$. Indeed, as v_i is the unique non-zero coordinate, $\frac{v}{v_i} = e_i$. Then, by the indecomposability of S, for any $1 \leq j \leq n$, there exists $g \in \overline{G}$ such that $\lambda_g^{-1}(s_i) = s_j$. If $g = \sum_{s_k \in S} g_k s_k$, we have $g \cdot e_i = \zeta_d^{g_j} e_j$, so $e_j \in V$. Thus we obtain that the canonical basis of $\mathbb{C}^S$ is in V, meaning that $V = \mathbb{C}^S$.

Otherwise, assume that v has at least two non-zero coordinates v_i, v_j with $i \neq j$. We will show that there exists $g \in \mathrm{Soc}(\overline{G})$, such that we have $g_i \neq g_j$, when writing $g = \sum_{s_k \in S} g_k s_k$ with $0 \leq g_i < d$. This will imply that $g \cdot v - \zeta_d^{g_i} v$ has i-th coordinate $\zeta_d^{g_i} v_i - \zeta_d^{g_i} v_i = 0$. As $g_i \neq g_j$ and $v_j \neq 0$, $g \cdot v - \zeta_d^{g_i} v$ has j-th coordinate $\zeta_d^{g_j} v_j - \zeta_d^{g_i} v_j = (\zeta_d^{g_j} - \zeta_d^{g_i}) v_j \neq 0$. For the other coordinates, say $k \notin \{i, j\}$, we find that the k-th coordinate of $g \cdot v - \zeta_d^{g_i} v$ is $(\zeta_d^{g_k} - \zeta_d^{g_i}) v_k$, which remains zero when $v_k = 0$. Thus we strictly decreased the number of non-zero coordinates of v, without obtaining a zero vector. Thus, by induction, we conclude that $V = \mathbb{C}^S$.

By contradiction, suppose that for every $g \in \mathrm{Soc}(\overline{G})$, $g_i = g_j$. For any $1 \leq k \leq n$, by the transitivity of the action of $\overline{G}$, there exists $f \in \overline{G}$ such that $\lambda_f(s_k) = s_i$. Let l be such that $\lambda_f(x_l) = x_j$, and as λ_f is a bijection we have $l \neq k$. Then, as $\mathrm{Soc}(\overline{G})$ is an ideal, we have $\lambda_f(g) = \sum_{s_i \in S} g_i \lambda_f(s_i) \in \mathrm{Soc}(\overline{G})$. Thus

$$g_k = (\lambda_f(g))_i = (\lambda_f(g))_j = g_l.$$

This means that for every k, there exists at least one $l \neq k$ such that $g_k = g_l$. So an element of $\mathrm{Soc}(\overline{G})$ (a diagonal matrix) has at most $\frac{n}{2}$ different entries on the diagonal, i.e. $|\mathrm{Soc}(\overline{G})| \leq d^{\frac{n}{2}}$, a contradiction. □

Let p be a prime and $n > 0$. We can always uniquely factorize $n = p^v m$ with $v, m \geq 0$ and $p \nmid m$. Therefore we can define the *p-valuation* $v_p(n)$ as the exponent v in such a factorization. On the other hand, there is a unique base p representation $n = \sum_{i=0}^{\infty} a_i p^i$ with finitely many non-zero $0 < a_i < p$. We define the *p-adic digit sum* as $\mathrm{DS}_p(n) = \sum_{i=0}^{\infty} a_i$.

We denote by $\mathcal{P}$ the set of prime numbers.

We will need the following result about the p-valuation of factorials:

Lemma 3.2.0.2 ([Coh07, Lemma 4.2.8.]). *For all $n \geq 0$, we have $v_p(n!) = \frac{n-\mathrm{DS}_p(n)}{p-1}$.*

Lemma 3.2.0.3. *The following bound holds:*

$$|\mathcal{G}| \leq \prod_{\substack{p \in \mathcal{P} \\ p|d}} p^{\frac{n-1}{p-1}}.$$

Proof. Write $\mathcal{G} = \mathcal{G}(X)$. By Corollary 2.4.0.15, for any $p \in \mathcal{P}$, we know that p divides d if and only if p divides $|\mathcal{G}|$. Therefore, $|\mathcal{G}| = \prod_{p|d} p^{v_p(|\mathcal{G}|)}$. As $\mathcal{G} \leq \mathfrak{S}_X$, we must have that $|\mathcal{G}|$ divides $|\mathfrak{S}_S| = n!$. Therefore, by Lemma 3.2.0.2, for $p \in \mathcal{P}$ we have

$$v_p(|\mathcal{G}|) \leq v_p(n!) = \frac{n - \mathrm{DS}_p(n)}{p-1} \leq \frac{n-1}{p-1}.$$

Thus,

$$|\mathcal{G}| = \prod_{p|d} p^{v_p(|\mathcal{G}|)} \leq \prod_{p|d} p^{\frac{n-1}{p-1}}.$$

□

Definition 3.2.0.4. *A group G is called solvable if there exists a finite series of normal subgroups*

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G,$$

such that G_{i-1} is a normal subgroup of G_i and G_i/G_{i-1} is abelian for all $1 \leq i \leq k$.

Proposition 3.2.0.5 ([CR62, Theorem 5.3]). *If G is a solvable group and $H \lhd G$ is a normal subgroup, then G/H is solvable.*

In [CR23] the following is indirectly obtained, as already mentioned in Proposition 2.4.0.10:

Proposition 3.2.0.6 ([CR23, Proposition 5.10]). *Let S be a cycle set of size n. Then*

$$|\mathcal{G}| \leq 24^{\frac{n-1}{3}}.$$

Proof. By [ESS99, Theorem 2.14], the structure group G is a solvable group. Thus, by Proposition 3.2.0.5, we obtain that $\mathcal{G} = G/\mathrm{Soc}(G)$ is solvable.

Moreover, in [Dix67, Theorem 3], it is shown that a solvable group of $\mathfrak{S}_n$ has cardinal at most $24^{\frac{n-1}{3}}$. Thus, as $\mathcal{G}$ is solvable, $|\mathcal{G}| \leq 24^{\frac{n-1}{3}}$. □

Theorem 3.2.0.7. *Let S be an indecomposable cycle set of size n and class d, such that $d \notin \{2, 6\}$. Then $\overline{\Theta}\colon \overline{G} \to M_S(\mathbb{C})$ is irreducible.*

Proof. We will show that if $d \notin \{2, 6\}$, then $|\mathrm{Soc}(\overline{G})| > d^{\frac{n}{2}}$. We can then apply Proposition 3.2.0.1 to conclude that $\overline{\Theta}$ is irreducible.

As $|\mathrm{Soc}(\overline{G})| > d^{\frac{n}{2}}$ is equivalent to $|\mathcal{G}| < \frac{d^n}{d^{\frac{n}{2}}} = d^{\frac{n}{2}}$, we need to show that $|\mathcal{G}| < d^{\frac{n}{2}}$ for $d \notin \{2, 6\}$.

First suppose that $d \geq 9$. By Proposition 3.2.0.6, we know that $|\mathcal{G}| \leq 24^{\frac{n-1}{3}} < 27^{\frac{n-1}{3}} = 3^{n-1}$. Moreover, $d^{\frac{n}{2}} \geq 9^{\frac{n}{2}} = 3^n$. Thus,

$$|\mathcal{G}| < 3^{n-1} < 3^n \leq d^{\frac{n}{2}}.$$

Next, consider the cases of $d \in \{3, 5, 7\}$. By Lemma 3.2.0.3, as d is prime, we have

$$|\mathcal{G}| \leq d^{\frac{n-1}{d-1}} \leq d^{\frac{n-1}{2}} < d^{\frac{n}{2}}.$$

We are left with $d \in \{4, 8\}$. As 4 and 8 are powers of 2, by Lemma 3.2.0.3, we have

$$|\mathcal{G}| \leq 2^{n-1} < 2^n < 4^{\frac{n}{2}} \leq d^{\frac{n}{2}}.$$

This finishes the proof. □

Remark 3.2.0.8. *For $d = 2$, we gave a counterexample in Remark 3.1.0.2. For $d = 6$, our proof fails on the bound given by Lemma 3.2.0.3: we find that $|\mathcal{G}| \leq 2^{n-1}3^{\frac{n-1}{2}} = 12^{\frac{n-1}{2}}$, when we need $|\mathcal{G}| < 6^{\frac{n}{2}}$.*

We do not know whether there exists an indecomposable cycle set of class 6 such that the representation $\overline{\Theta}$ is not irreducible.

From the enumeration of [AMV22], one can check that for all indecomposable cycle sets of size $n \leq 10$ and class $d = 6$ the representation $\overline{\Theta}$ is irreducible. To do so, we applied [Ser77, Theorem 5], stating that a representation ρ of a finite group G is irreducible if and only if $\frac{1}{|G|}\sum_{g\in G} |Tr(\rho(g))|^2 = 1$.

From Lemma 2.4.0.16, we know that the prime divisors of the size of a cycle set are divisors of its Dehornoy class. Thus, we know that no indecomposable cycle set of size 11 have class 6. Therefore, a cycle set of class 6 such that $\overline{\Theta}$ is not irreducible should be looked for in size $n = 12$ (then 16, 18, 24, ...).

3.3 Inducing the representations

By [CR62, Corollary 50.4], an irreducible monomial representation is induced by a character of a subgroup. So in this section, we explicitly construct a subgroup of G (resp. $\overline{G}$) and a character that induce the representation Θ (resp. $\overline{\Theta}$).

In this section we fix S an indecomposable cycle set of size n.

For details on representation theory of finite groups, we refer to [Ser77]. We'll need the following from this reference:

Let G be a group, R a commutative ring and V a finite dimensional R-module. A representation $\rho\colon G \to \mathrm{GL}(V)$ is equivalent to a $R[G]$-module structure on V. We'll identify ρ with V endowed with the associated $R[G]$-module structure.

Proposition-Definition 3.3.0.1 ([Ser77, Chapter 7])**.** *If H is a subgroup of G and V is a $R[G]$-module, then the induced representation $Ind_H^G V$ is defined as the $R[G]$-module $R[G] \otimes_{R[H]} V$.*

If we denote by $[G : H]$ the index of H in G, then $rk_R Ind_H^G V = [G : H] \cdot rk_R W$.

Moreover, for any $R[G]$-module W we have the following isomorphism

$$Hom_{R[H]}(V, W) \cong Hom_{R[G]}(Ind_H^G V, W),$$

obtained by sending $f\colon V \to W$ to $f^*\colon R[G]\otimes_{R[H]} \to W$, where $f^*(g \otimes v) = g \cdot f(v)$.

We now chose an element s_0 in S. We define $G_0 = \{g \in G \mid \lambda_g(s_0) = s_0\}$ and $\overline{G}_{l,0} = \{g \in \overline{G}_l \mid \lambda_g(s_0) = s_0\}$. Recall that we can write any element g in the structure brace G as $g = \sum_{s\in S} g_s s$.

Lemma 3.3.0.2. *Suppose S is an indecomposable cycle set. Then, for any s_0 in S, we have the equalities*

$$[G : G_0] = [\overline{G} : \overline{G}_{l,0}] = |S|.$$

Proof. The index $[G : G_0]$ (resp. $[\overline{G} : \overline{G}_{l,0}]$ is the number of equivalence classes of G modulo G_0 (resp. $\overline{G}_l$ modulo $\overline{G}_{l,0}$). So two elements of G (resp. $\overline{G}_l$ are in the same class if they send s_0 to the same element of S. As S is indecomposable, G (resp. $\overline{G}_l$) acts transitively on S by Proposition 2.4.0.6, we conclude that $[G : G_0] = [\overline{G}_l : \overline{G}_{l,0}] = |S|$. □

Proposition 3.3.0.3. *The mapping*

$$c_0 : G \to \mathbb{Z}; \quad g \mapsto g_{s_0}$$

satisfies the following property: for $g \in G_0$, $h \in G$, we have

$$c_0(gh) = c_0(g) + c_0(h).$$

In particular, the restriction $c_0|_{G_0}$ is a morphism of groups.

Proof. By Proposition-Definition 1.6.0.4, we have $gh = g + \lambda_g(h) = \sum_{s\in S} g_s s + \sum_{s\in S} h_s \lambda_g(s)$. As $g \in G_0$, we have $\lambda_g(s_0) = s_0$. Thus, $c_0(gh) = g_{s_0} + h_{s_0} = c_0(g) + c_0(h)$.

This means that, when restricting to G_0, c_0 is a morphism. Which implies that $c_0(gh) = c_0(g) + c_0(h)$. The second statement of the proposition is now immediate. □

By Proposition 3.3.0.3, we can define the character $\chi_0 : G_0 \to \mathbb{C}[z^{\pm 1}] \subset \mathbb{C}(z)$ by $g \mapsto z^{c_0(g)} = z^{g_{s_0}}$.

Lemma 3.3.0.4. *The character $\chi_0 \colon G_0 \to \mathbb{C}(z)$ induces a character $\overline{\chi}_{l,0} \colon \overline{G}_{l,0} \to \mathbb{C}$.*

Proof. With the specialization $\mathrm{ev}_{ld} \colon \mathbb{C}(z) \to \mathbb{C}$ of z at $\zeta_d = \exp(\frac{2i\pi}{ld})$, we obtain a character $\mathrm{ev}_{ld}\chi_0 : G_0 \to \mathbb{C}$ defined by $g \mapsto \zeta_{ld}^{g_{s_0}}$. Moreover, we have $\overline{G}_l = G/\langle lds\rangle$ and $ldS \subseteq \mathrm{Soc}(G) \subseteq G_0$. Thus χ_0 factorizes as $\overline{\chi}_{l,0}$ through $G_0/\langle lds\rangle$. Furthermore, $\mathrm{Ker}(G_0 \to \overline{G}_{l,0}) = G_0 \cap \mathrm{Ker}(G \to \overline{G}_l) = G_0 \cap ldG = ldG$. Thus $G_0/\langle lds\rangle = \overline{G}_{l,0}$ and $\overline{\chi}_{l,0}$ is well-defined. □

We can now show that the monomial representations of indecomposable cycle sets are induced:

Theorem 3.3.0.5. *Let S be an indecomposable cycle set and s_0 be an element of S.*

Let $(A, \Gamma, \Gamma_0, \rho, \alpha_0, \omega)$ be one of the followings:

a) $(\mathbb{C}(z), G, G_0, \Theta, \chi_0, z)$

b) $(\mathbb{C}[z^{\pm 1}], G, G_0, \Theta, \chi_0, z)$

c) $\left(\mathbb{C}, \overline{G}_l, \overline{G}_{l,0}, \overline{\Theta}_l, \overline{\chi}_{l,0}, \zeta_{ld}\right)$, *for $l \geq 1$.*

Then the monomial representation $\rho \colon \Gamma \to M_S(A)$ is isomorphic to the induced representation $Ind_{\Gamma_0}^{\Gamma} A$ seen as a $A[\Gamma]$-module.

Proof. Consider A (resp A^S) as the $A[\Gamma_0]$-module (resp. $A[\Gamma]$-module) with its associated structure coming from α_0 (resp. ρ).

Define $f : A \to A^S$ by $a \mapsto as_0$. We claim that $f \in \mathrm{Hom}_{A[\Gamma_0]}(A, A^S)$. We need to show that, for any $g \in \Gamma_0$ and $a \in A$, $f(g \cdot a) = g \cdot f(a)$. On the one hand, $f(g \cdot a) = f(\omega^{g_{s_0}} a) = \omega^{g_{s_0}} as_0$. On the other hand we have $g \cdot f(a) = g \cdot as_0 = D_g P_g(as_0) = D_g(as_0) = D_{s_0}^{g_{s_0}}(as_0) = \omega^{g_{s_0}} as_0$, where we used that $g \in \Gamma_0$ to have that D_g stabilizes s_0 and then that D_g acts on $s \in S$ by $D_s^{g_s}$.

By Proposition-Definition 3.3.0.1, f induces a morphism $f^* \in \mathrm{Hom}_{A[\Gamma]}(\mathrm{Ind}_{\Gamma_0}^{\Gamma} A, A^S)$. For any $g = \sum_{u \in S} g_u u \in \Gamma$, let $t = \lambda_g^{-1}(s_0)$, so that we have $f^*(g \otimes 1) = g \cdot f(1) = g \cdot s_0 = \omega^{g_t} t$. As S is indecomposable, by Proposition 2.4.0.6, we know that Γ acts transitively on S. So for any $s \in S$, there exists $g \in \Gamma$ such that $f^*(g \otimes 1) = \omega^{g_s} s \in A^S$. As ω is invertible in A, we obtain that f^* is surjective.

Moreover, by Proposition-Definition 3.3.0.1 and Lemma 3.3.0.2, we have:

$$\mathrm{rk}_A \mathrm{Ind}_{\Gamma_0}^{\Gamma} A = [\Gamma : \Gamma_0] \cdot \mathrm{rk}_A A = |S| = \mathrm{rk}_A A^S.$$

As f^* is surjective, it must be an isomorphism, which finishes the proof. □

Example 3.3.0.6. *For $n > 2$, consider the cycle set $S = \{s_1, \dots, s_n\}$ with $\psi(s_i) = \begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix} = \sigma$ (i.e $s_i * s_j = s_{\sigma(j)}$). We have seen in Example 2.2.0.7 that S is of class n. Moreover, S has permutation group $\mathcal{G} = \langle \sigma \rangle$ which acts transitively on S, thus S is indecomposable. So, by Proposition 3.1.0.1, the representation Θ is irreducible. In particular, $|\mathcal{G}| = |\langle \sigma \rangle|$ is equal to the order of σ, so $|\mathcal{G}| = n < n^{\frac{n}{2}}$ because $n > 2$. Thus by Proposition 3.2.0.1, we have that $\overline{\Theta}$ is irreducible. Moreover, by [Ser77, Theorem 5], a representation ρ of a finite group G is irreducible if and only if $\frac{1}{|G|} \sum_{g \in G} |Tr(\rho(g))|^2 = 1$.*

We now apply this formula to the representation $\overline{\Theta}$:

For any $g \in \overline{G}$, by Proposition-Definition 1.6.0.4, we have $\psi(g) = \lambda_g^{-1} = \sigma^{\overline{\ell}(g)}$. Let $g \in \overline{G}$ with $g = \sum_{i=1}^{n} g_i s_i$ with $\sum_{i=1}^{n} g_i = \overline{\ell}(g)$ and where $0 \leq g_i < d$. By Corollary 1.6.0.15, $\overline{\Theta}(g) = D_1^{g_1} \cdots D_n^{g_n} P_g = D_1^{g_1} \cdots D_n^{g_n} P_\sigma^{\overline{\ell}(g)}$ where $D_i = diag(1, \dots, \zeta_n, \dots, 1)$ with ζ_n on the i-th place. So

$$Tr(\overline{\Theta}(g)) = \begin{cases} 0, & \text{if } \overline{\ell}(g) \neq 0 \ mod\ n \\ \sum_{i=1}^{n} \zeta_d^{g_i}, & \text{if } \overline{\ell}(g) = 0 \ mod\ n \end{cases}$$

As $\overline{\Theta}$ is irreducible, by [Ser77, Theorem 5] we have $\frac{1}{|\overline{G}|} \sum_{g \in \overline{G}} |Tr(\overline{\Theta}(g))|^2 = 1$. We conclude that

$$\sum_{\substack{0 \leq a_1, \dots, a_n < n \\ a_1 + \cdots + a_n = 0 \ mod\ n}} |\zeta_d^{a_1} + \cdots + \zeta_d^{a_n}|^2 = n^n.$$

CHAPTER 4

Hecke algebras for set-theoretical solutions to the Yang–Baxter equation

As mentioned in the introduction, the Iwahori-Hecke algebra is a deformation of the group ring of a Coxeter group seen as a quotient of the group ring of the associated Artin–Tits group. The Iwahori-Hecke algebras can then be used to construct all irreducible characters of the Coxeter group ([GP00, Section 4.4, 8, 9]). As structure groups of solutions are Garside groups, the question of defining a deformation of the group ring of the germ of a solution naturally occurs. This is precisely the goal of this section: defining such an object, showing it has property similar to the Coxeter case (natural basis, invertibility of the generators, semi-simplicity), but also highlighting some differences between the two objects. Moreover, when working to find a suitable definition, another object happened to be studied: an Hecke algebra defined from a two-generator presentation of $\mathbb{Z}/n\mathbb{Z}$ which reminds of the ones defined for Complex Reflexion Groups ([RMB98, Proposition 4.22]).

Let $(S, *)$ be a finite cycle set of size n with $S = \{s_1, \dots, s_n\}$, class d and structure monoid (resp. group) M (resp. G). Because we are going to work over group rings, to avoid the confusion when writing ds (it means different things in $R[G]$ or G), we'll use the notation from [Deh15] as $s^{[d]} = ds$ in G. For a positive integer k we define the k-germ of G by $\overline{G}_k = G/\langle s^{[kd]} \rangle_{s \in S}$ which is in bijection with the divisors of the kd-th power of the Garside element Δ. Moroever, for any element g in a group G, we denote by T_g the associated generator in a group ring.

4.1 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 subsections (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;
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);
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

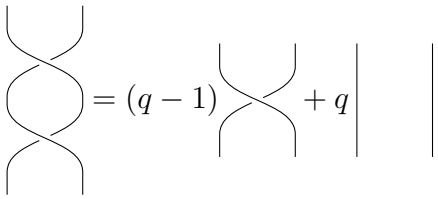
To do this verification for $S = \{s, t, u\}, \psi(s) = \psi(t) = \psi(u) = (stu) = \sigma$, we consider all relations of the form

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

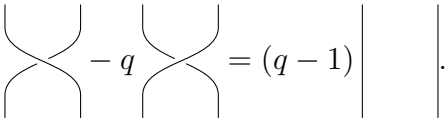
and $T_{t^{[d]}} = \sigma(T_{s^{[d]}}), T_{u^{[d]}} = \sigma^2(T_{s^{[d]}})$ to retain the symmetry. Note that we chose a particular specialization of the coefficients a_i, as we expect the definition of the Hecke algebra to work for all specializations. We then use the *GBNP* package functions to compute 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 Subsection 4.5. 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 [Pou23].

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.

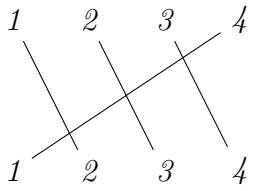
Definition 4.1.0.1. *Let n be a positive integer. Consider the $2n$ points in $\mathbb{R}^2$ with coordinates $(1, 0), \ldots, (n, 0)$, $(1, 1), \ldots (n, 1)$. A family of n curves $(C_i \colon [0, 1] \to \mathbb{R}^2)_{1 \leq i \leq n}$ is called a n-strand permutation diagram if there exists a permutation $\sigma \in \mathfrak{S}_n$ 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.

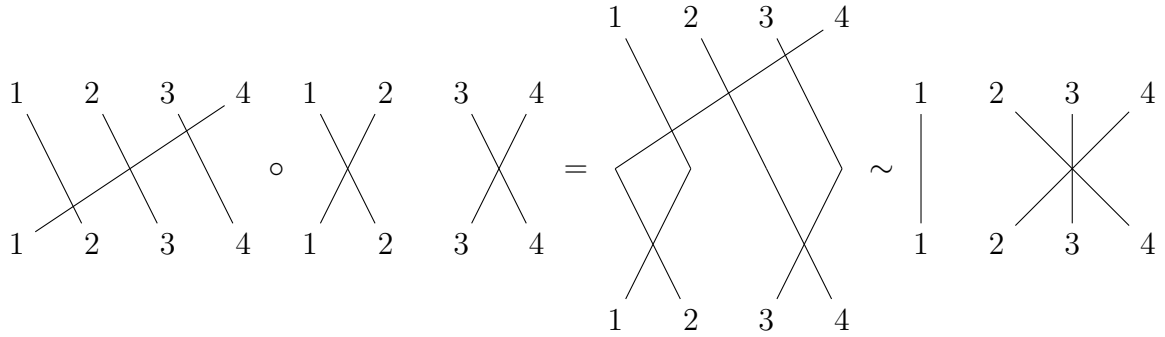
The inverse of σ will be called the permutation associated to the diagram. Equivalently, the associated permutation can be read as the permutation obtained looking at the diagram from bottom to top.

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

Example 4.1.0.2. *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 4.1.0.3. *There is an isomorphism between the group of n-strand permutation diagrams up to equivalence and $\mathfrak{S}_n$.*

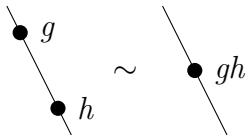
Proof. Consider the stacking of two diagrams with associated permutations respectively σ and τ. The first diagram sends i to $\sigma(i)$, and the second one sends $\sigma(i)$ to $\tau(\sigma(i)$. So we obtain that the permutation of the stacking is the product of the permutation. This implies that, when 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 4.1.0.4. *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:

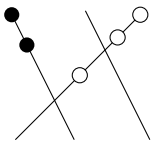


Example 4.1.0.5. *We will later focus on* $\mathbb{Z}$ *and* $\mathbb{Z}/d\mathbb{Z}$ *markings. As those groups are cyclic, we can simplify the markings:*

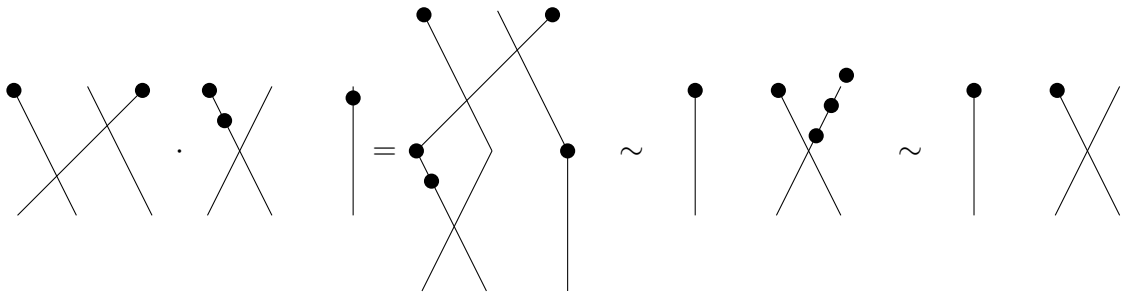
For $\mathbb{Z}$*, associate to* $+1$ *the marking by* $\bullet$ *and to* -1 *the marking by* $\circ$*. A marking by a positive integer* n *then corresponds to* n *markings by* $\bullet$*, and similarly for negative integers with* $\circ$*.*

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 4.1.0.6. *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 4.1.0.7. *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 $f((g_1,\dots,g_n,\sigma)(h_1,\dots,h_n,\tau)) = f(g_1h_{\sigma^{-1}(1)},\dots,g_nh_{\sigma^{-1}(n)},\sigma\tau)$.

On the other hand, when stacking $f((g_1,\dots,g_n,\sigma))$ and $f((h_1,\dots,h_n,\tau))$ from bottom to top. The permutation associated to this diagram is $\sigma\tau$ by Proposition 4.1.0.3. 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 $g_ih_{\sigma^{-1}(i)}$. 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 [ESS99; GV98] and Theorem 1.5.0.19.

Theorem 4.1.0.8. *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 Corollary 1.5.0.22, 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. Proposition 2.2.0.5 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 4.1.0.7 to conclude. □

Remark 4.1.0.9. *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.

4.2 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 Corollary 1.5.0.22 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

$\mathrm{cp}^{-1} = \Pi\colon \mathbb{Z}^n \to G$ which we studied in Section 1.5: we have $\Pi(gh) = \Pi(g)\lambda^{-1}_{\Pi(g)}(\Pi(h))$. In particular, if $\psi(\Pi(g)) = 1$, then $\Pi(gh) = \Pi(g)\Pi(h)$. Moreover, by Proposition 2.2.0.5 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 $\sum\limits_i r_i X_1^{i_1} \dots X_n^{i_n}$ to $\sum\limits_i r_i \Pi(s_1, \dots, s_1, \dots, s_n, \dots, s_n)$ 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 $P(X) = \sum\limits_{k=0}^{l} a_k X^k$.

Remark 4.2.0.1. *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 4.2.0.2. *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 2.3.0.4 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 1.6.0.8, we have for all $g \in G$ that $g s^{[d]} = \lambda_g(s^{[d]})\lambda_{s^{[d]}}(g) = \psi(g)(s^{[d]})g$. Thus, in $R[G]$, we have

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

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 $\Pi^{-1}(f P(s_i^{[d]}) g) = \sum a_k \Pi^{-1}(f s^{[dk]} g) = \sum a_k Y^{dk} \Pi^{-1}(fg) = P(Y^d)\Pi^{-1}(fg)$, which is in I_P by Remark 4.2.0.1. We conclude that $J_P \subseteq \Pi(I_P)$. □

Example 4.2.0.3. *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 $(1+g)(1+s^{[d]}) = 1 + s^{[d]} + g + g s^{[d]} = 1 + s^{[d]} + g + t^{[d]} g = (1 + s^{[d]}) + (1 + t^{[d]}) g = P(s^{[d]}) + P(t^{[d]}) g = \Pi(P(X^d)) + \Pi(Y^d)\Pi(Q) = \Pi(P(X^d) + P(Y^d) Q)$.*

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 4.2.0.4. *Let $(S,*)$ be the cycle set, with $S=\{s,t,u\}$ and $\psi(s)=\psi(t)=\psi(u)=(stu)=\sigma$. Then, from Example 2.2.0.7, we know that 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 $1 \leq i \leq k$,

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

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 4.2.0.2.

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

$$\mathcal{H}(S,P) = R[G]/\left(T_{s^{[ld]}} = \sum_{k=0}^{l-1} \frac{-a_k}{a_l} T_{s^{[kd]}}\right). \tag{4.1}$$

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

Lemma 4.2.0.5. *The following hold:*

(i) We have the isomorphism $R[G] \cong R\langle T_s, s \in S \mid T_sT_{s*t}=T_tT_{t*s}, \forall s,t \in S\rangle$

(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 2.2.0.21 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 2.2.0.22, we have $s^{[ld]} = s \cdot (s * s)^{[ld-1]}$. Thus, Equation (4.1) means that, in $\mathcal{H}(S,P)$ we have

$$T_s T_{s*s}^{[ld-1]} = \sum_{k=0}^{l-1} \frac{-a_k}{a_l} T_{s^{[kd]}}. \tag{4.2}$$

Even though $T_s^{[ld]}$ is not defined in $\mathcal{H}(S,P)$ from Lemma 4.2.0.5, 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 4.2.0.6. *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 2.2.0.17, either sg is reduced and then $T_s T_g = T_{sg}$, 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 2.2.0.21. Thus, if sg is not reduced, by Equation -4.2), we have $T_s T_g = T_s T_{s*s}^{[ld-1]} T_h = \sum_{k=0}^{l-1} \frac{-a_k}{a_l} T_{s^{[kd]}h}$, where $s^{[kd]}h$ is reduced in $\overline{G}_l$ as $k < l$ and $g = s^{[ld-1]}h$ is reduced. □

Lemma 4.2.0.7. *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 $0 \leq j_1, \dots, j_n < ld$.*

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 $0 \leq j_i < ld$.

By considering the powers of such a monomial, this basis is in bijection with $(\mathbb{Z}/ld\mathbb{Z})^n$. By Proposition 2.2.0.5, $\overline{\Pi}$ gives a bijection $(\mathbb{Z}/ld\mathbb{Z})^n \to \overline{G}_l$, finishing the proof. □

Theorem 4.2.0.8. *$\mathcal{H}(S,P)$ 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 4.2.0.5 we know that $\{T_g \mid g \in \overline{G}_l\}$ generates $\mathcal{H}(S,P)$ as an R-module, so in particular $\dim\mathcal{H}(S,P) \leq (ld)^n$. We just have to show this family is free, but this follows from Lemmas 4.2.0.2 and 4.2.0.7:

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 4.2.0.7 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 4.2.0.9. *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 4.2.0.2 we just need that two elements are in the same orbit to obtain that $\Pi(J) \subseteq I$. If we denote such polynomials by $\underline{P} = (P_i)_{1\leq i\leq n} \in R[X]^n$ 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 $G/\langle s_i^{[l_id]}\rangle_{1\leq i\leq n}$.*

With the same reasoning we can also take a different d for each of those orbits, see for instance [LRV22], but this will not be used in this thesis.

It was chosen to not consider those generalizations (except in Section 4.4) to avoid heavy notation and make the proofs easier to read.

Corollary 4.2.0.10. *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 4.2.0.11. *Take $S = \{s_1, \dots, s_n\}$, $\sigma \in \mathfrak{S}_n$ and $\psi(s_i) = \sigma$ from Example 2.2.0.7. Then S is of class $d = o(\sigma)$ (the order of the permutation), and taking $P(X) = X^2 - X - 1$ we get*

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

Remark 4.2.0.12. *For all $g \in G$, by Proposition-Definition 1.6.0.4, 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 4.2.0.13. *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 [Cox59] 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 2.4.0.21, we denote by S' the retraction of S. Then the class d' of S' divides the class d of S by Lemma 2.4.0.22. We deduce the following:

Proposition 4.2.0.14. *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 Proposition 2.2.0.1, for any $s \in S$ and any positive integer k, we have $(s^{[d]})^k = s^{[kd]}$. Moreover, by Proposition 2.4.0.22 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 4.2.0.15. *If S is of class 4, S' of class 2, and we take $P(X) = X^2 + X + 1$, then we have a morphism $\mathcal{H}(S, X^8 + X^4 + 1) \to \mathcal{H}(S', X^8 + X^4 + 1)$.*

4.3 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. In Section 4.2 we defined the Hecke algebra for cycle sets $\mathcal{H}(S, P)$. In this subsection, 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 [GP00, Exercise 4.8] for instance).

Proposition 4.3.0.1. *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 2.3.0.4 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 (4.2) 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 2.2.0.22, 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 2.3.0.4 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 Proposition 1.5.0.23, 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 4.3.0.2. *One has to be careful that $T_s^{-1} \neq T_{s^{-1}}$. Indeed, by Lemma 2.2.0.22 and Proposition 2.3.0.4, 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 4.3.0.3. *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 4.3.0.1. Then*

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

Corollary 4.3.0.4. *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 [GP00, 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 4.3.0.5. *If P splits over R with (non-necessarily distinct) invertible roots $\alpha_1, \dots, \alpha_l$, 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

$$P(T_s^{[d]}) = 0 \iff a_l \prod_{k=1}^{l} (T_s^{[d]} - \alpha_k) = 0 \tag{4.3}$$

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 (4.3) 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 2.2.0.22 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 4.3.0.1 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 $\tilde{\iota}(T_sT_{s*t}) = (T_sT_{s*t})^{-1} = T_{s*t}^{-1}T_s^{-1} = T_{t*s}^{-1}T_t^{-1} = \tilde{\iota}(T_tT_{t*s})$.

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

Remark 4.3.0.6. *In the above proof, one has to be careful that $T_g^{-1} \neq T_{g^{-1}}$ as mentioned in Remark 4.3.0.2. 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 4.3.0.7. *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 ([GP00]).*

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

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

4.4 Semi-simplicity

This section is based on [CR90a; CR90b; GP00] and inspired from the lecture notes [Dig; Mic98]. For details on character theory we refer to [CR90a]. 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 4.2.0.9, 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 4.2.0.8, 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 4.4.0.1. *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 4.4.0.2 ([Bou22, 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 following holds:

(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 4.4.0.3 ([CR90a])**.** *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 4.4.0.4. *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 4.4.0.3, 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 4.4.0.5 ([CR90a, 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 4.4.0.4.

So it is enough to show that A is semi-simple. As A is finite dimensional, by Proposition 4.4.0.2 A is semi-simple iff $\mathrm{rad}(A)$ is trivial. Also from Proposition 4.4.0.2, $\mathrm{rad}(A)$ 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 4.4.0.6. *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 4.4.0.4:

Proposition 4.4.0.7 ([Bro00, 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 4.4.0.8 ([Dig, 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 $\tau(\sum_{g\in G} r_g T_g) = r_1$ (where T_g is the standard basis of $K[G]$) is a symmetrizing trace and $K[G]$ is separable.*

Proof. We have that $\tau(\sum_{g\in G} r_g T_g)(\sum_{h\in G} r'_h T_h) = \tau(\sum_{g,h\in G} r_g r'_h T_g T_h) = \sum_{g\in G} r_g r'_{g^{-1}} = \sum_{h\in G} r'_h r_{h^{-1}}$, so $\tau(ab) = \tau(ba)$. Moreover, $\tau(T_g T_g^{-1}) = \tau(T_1) = 1$, so $\tau((\sum_{g\in G} r_g T_g)T_h^{-1}) = r_h$ 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 4.4.0.7, $K[G]$ is separable. □

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

Theorem 4.4.0.9 ([CR90b, 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 4.4.0.10. *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 $\underline{q} = (q_{i,k})_{1\leq i\leq n, 0\leq k\leq l_i}$ 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 4.4.0.9 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 $K[\overline{G_{\underline{l}}}] = K[G]/(T_{s_i}^{[l_i d]} - 1)$.

First, by Corollary 4.4.0.8, $K \otimes A = K[G_{\underline{l}}]$ is separable when $\mathrm{char}(K)$ does not divide $\#\overline{G_{\underline{l}}} = \prod_{i=1}^{n} (l_i d)$.

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 4.4.0.7 to have that $F \otimes A$ is separable. By Theorem 4.2.0.8, $(T_g)_{g\in\overline{G}_{\underline{l}}}$ 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 4.4.0.8. We have $\mathrm{Tr}_{F\otimes A/F}((1 \otimes T_g)(1 \otimes T_h)) = \mathrm{Tr}_{F\otimes A/F}(1 \otimes T_g T_h) = 1 \otimes \mathrm{Tr}_{A/K}(T_g T_h)$ by Lemma 4.4.0.3. 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 4.4.0.9 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 4.4.0.11. *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 $Irr(\mathbb{C}[\overline{G}_{\underline{l}}]) \to Irr\left(\overline{\mathbb{C}(\underline{l})} \otimes \mathcal{H}(S, \underline{P})\right)$.

Proof. We apply Theorem 4.4.0.9 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 4.4.0.10 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 4.4.0.9 says that the specialization $\mathcal{H}(S, \underline{P}) \to \mathbb{C}[\overline{G}_{\underline{l}}]$ induces a bijection $\mathrm{Irr}(\mathbb{C}[\overline{G}_{\underline{l}}]) \to \mathrm{Irr}(\overline{\mathbb{C}(\underline{l})} \otimes \mathcal{H}(S, \underline{P}))$. □

4.5 Two-generated Cyclic group

At the beginning of Section 4.1, 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 $R\langle T_a, T_b \mid T_a^2 = T_b^2, T_a T_b = T_b T_a = p(T_a + T_b) + q \rangle$ 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 ([DP99; Gob24; Gob23]). 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 $\mathcal{H}_{n,m}(p, q) = R\langle T_a, T_b \mid T_a^n = T_b^m, T_a T_b = T_b T_a = p(T_a + T_b) + q \rangle$, i.e. that $(T_g)_{g\in\overline{\mathcal{T}_{n,m}}}$ is a basis of $\mathcal{H}_{n,m}(p, q)$.

Proposition 4.5.0.1. *$\mathcal{T}_{n,m}$ is a Garside group with germ $\overline{\mathcal{T}_{n,m}} \cong \mathbb{Z}/(n+m)\mathbb{Z}$.*

Proof. It is shown in [DP99, 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,

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

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 $1 \le i, j \le n$. If $i + j \le n$, 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 $2 \le i \le n$ 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 $i + j \le m$. Thus we can omit $\overline{b}^i$ for $2 \le i \le m$ 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 $1 \le i \le n, 1 \le j \le m$. But $\overline{a} = \overline{b}^{-1}$, so $\overline{\ell}(\overline{a}^i\overline{b}^j) = \begin{cases} \overline{\ell}(\overline{a}^{i-j}) = (i-j)m, \text{ if } i \ge j \\ \overline{\ell}(\overline{b}^{j-i}) = (j-i)n, \text{ if } i < j \end{cases}$. 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 4.5.0.2. *The following 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* $1 \le k \le m$

(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* $1 \le k \le n$

(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 4.5.0.3. *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 [GP00, 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:

- $T_ae_{a^k} = e_{a^{k+1}}$, for $0 \leq k \leq n-1$
- $T_ae_{b^k} = p^{k-1}qe_1 + p^ke_a + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}e_{b^i} + pe_{b^k}$, for $1 \leq k \leq m$
- $T_be_{b^k} = e_{b^{k+1}}$, for $0 \leq k \leq m-1$
- $T_be_{a^k} = p^{k-1}qe_1 + p^ke_b + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}e_{a^i} + pe_{a^k}$, for $1 \leq k \leq n$

In particular, $T_ae_{a^n} = T_ae_{b^m} = p^{m-1}qe_1 + p^me_a + \sum_{i=1}^{m-1}(p^2+q)p^{m-i-1}e_{b^i} + pe_{b^m}$.

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 $T_aT_b = p(T_a+T_b)+q$, we only need to consider the cases of $T_aT_be_{b^k}$ and $T_aT_be_{a^k}$, as the cases of $T_bT_ae_{b^k}$ and $T_bT_ae_{a^k}$ are obtained by symmetry. First assume that $k < m$, then, on one hand, $T_aT_be_{b^k} = T_ae_{b^{k+1}} = p^kqe_1 + p^{k+1}e_a + \sum_{i=1}^{k}(p^2+q)p^{k-i}e_{b^i} + pe_{b^{k+1}}$. On the hand, $(pT_a + pT_b + q)e_{b^k} = pT_ae_{b^k} + qe_{b^k} + pe_{b^{k+1}} = p^kqe_1 + p^{k+1}e_a + \sum_{i=1}^{k-1}(p^2+q)p^{k-i}e_{b^i} + p^2e_{b^k} + qe_{b^k} + pe_{b^{k+1}}$ and those are easily seen to be equal by just noticing $p^2e_{b^k} + qe_{b^k} = (p^2+q)p^{k-k}e_{b^k}$.

Then, for $k < n$, we have $T_a T_b e_{a^k} = T_a(p^{k-1}qe_1 + p^k e_b + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}e_{a^i} + pe_{a^k}) = p^{k-1}qe_a + p^k T_a e_b + \sum_{i=1}^{k-1}(p^2+q)p^{k-i-1}e_{a^{i+1}} + pe_{a^{k+1}}$ 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 $T_a T_b e_{b^m} = T_a T_b e_{a^n} = T_a(p^{n-1}qe_1 + p^n e_b + \sum_{i=1}^{n-1}(p^2+q)p^{n-i-1}e_{a^i} + pe_{a^n})$, so

$$T_a T_b e_{b^m} = p^{n-1}qe_a + p^n T_a e_b + \sum_{i=1}^{n-1}(p^2+q)p^{n-i-1}e_{a^{i+1}} + pT_a e_{a^n}. \tag{4.4}$$

On the other hand,

$$(pT_a + pT_b + q)e_{b^m} = pT_a e_{b^m} + pT_b e_{b^m} + qe_{b^m}. \tag{4.5}$$

The last term of Equation (4.4) and the first term of Equation (4.5) match, as $a^n = b^m$. So we have to show

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

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

$$p^n qe_1 + p^{n+1}e_b + \sum_{i=1}^{n}(p^2+q)p^{(n+1)-i-1}e_{a^i}$$

and

$$p^n qe_1 + p^{n+1}e_b + \sum_{i=1}^{n-1}(p^2+q)p^{(n+1)-i-1}e_{a^i} + p^2 e_{a^n} + qe_{a^n}$$

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 [RMB98]:

Definition 4.5.0.4. *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 [ST54], 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 [RMB98], 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 [RMB98] for the case $G(k, 1, 1) \cong \mathbb{Z}/k\mathbb{Z}$:

Theorem 4.5.0.5 ([RMB98, Propositions 4.22-4.24])**.** *For the Hecke algebra of $C_k := \mathbb{Z}/k\mathbb{Z}$ we have*

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

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 4.5.0.6. *It was remarked by Loïc Poulain-d'Andecy ([Pou]) that, if $R = \mathbb{Z}$, then $\mathcal{H}_{n,m}(p, q)$ is a specialization of $\mathcal{H}(C_{n+m})$. Indeed, by Proposition 4.5.0.1 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

Histograms for Dehornoy's class

Note that the following histograms values are log-scaled. Each histogram is for a fixed size n, and shows the number of solutions with a given class (in log scale).

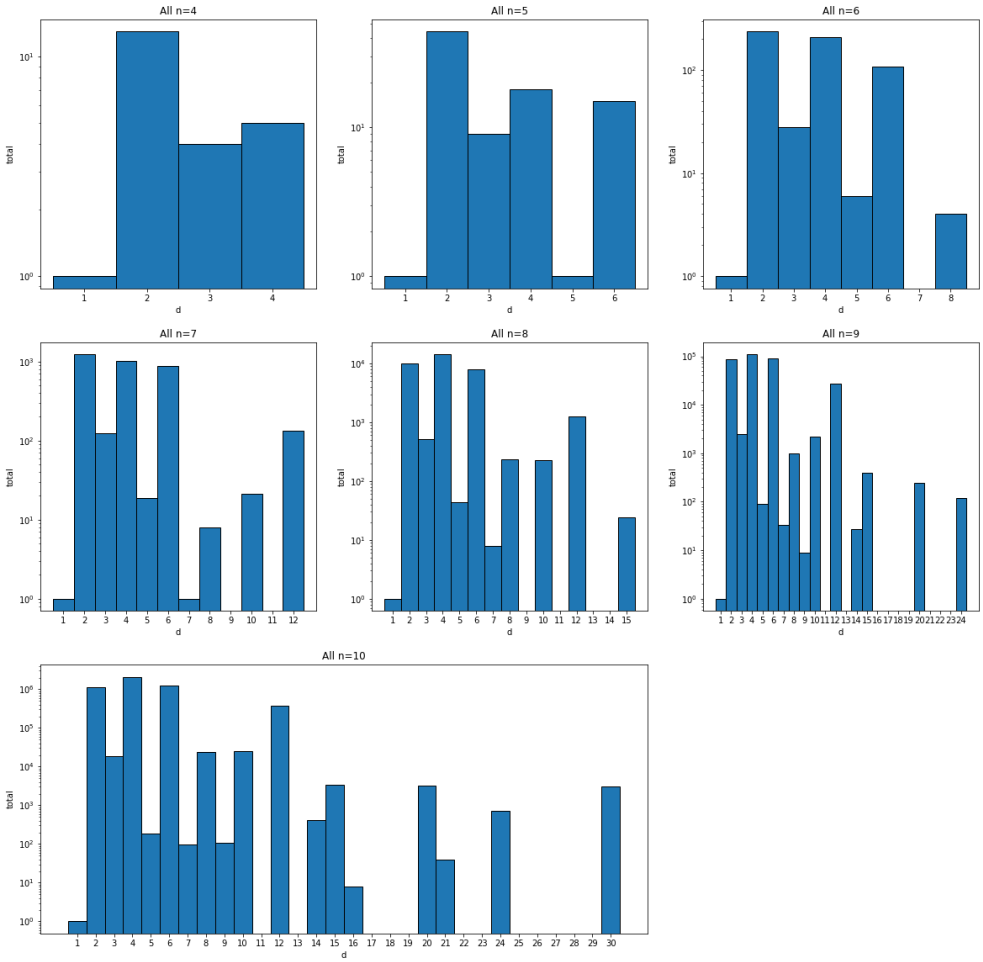


Figure A.1: All solutions

Figure A.1 is the basis for Figure 2.2 that leads to Conjecture 2.4.0.8.

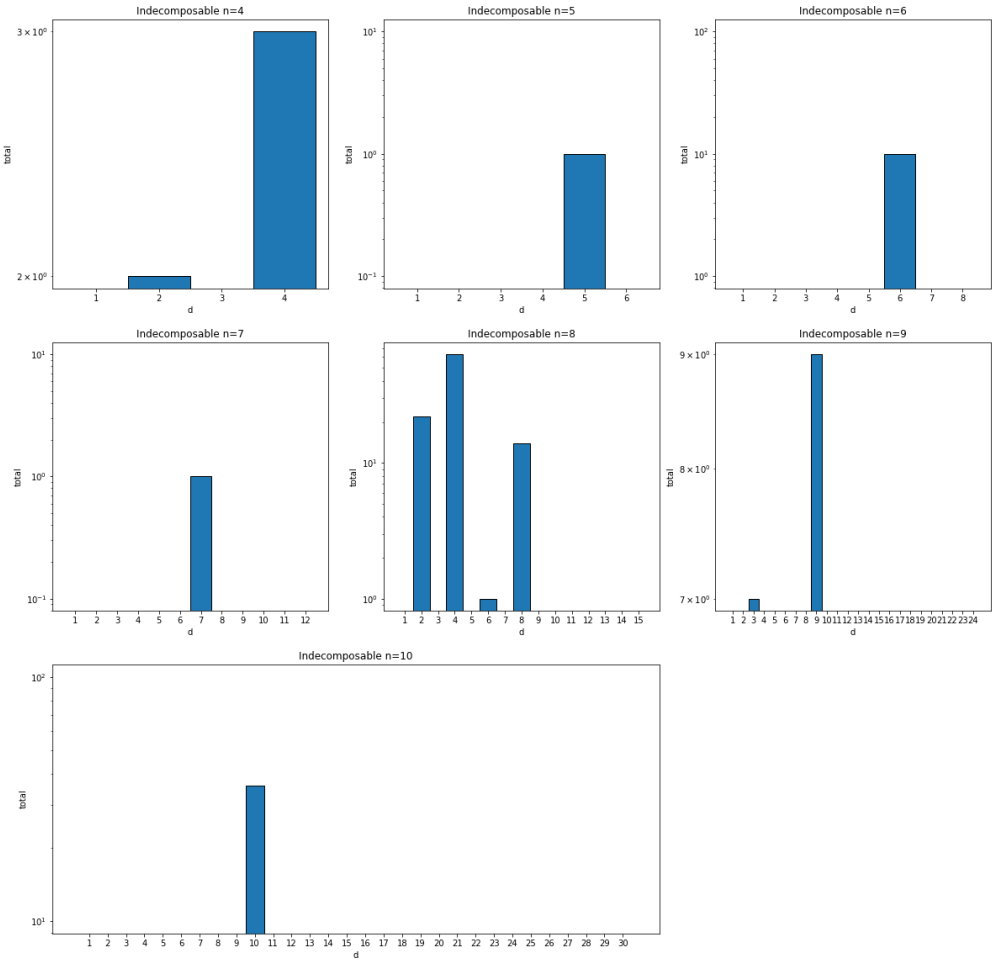


Figure A.2: Indecomposable solutions

Figure A.2 is the basis of Conjecture 2.4.0.11. In particular, one should note that the possible classes are divisible by any prime divisors of n, as indicated by Lemma 2.4.0.16.

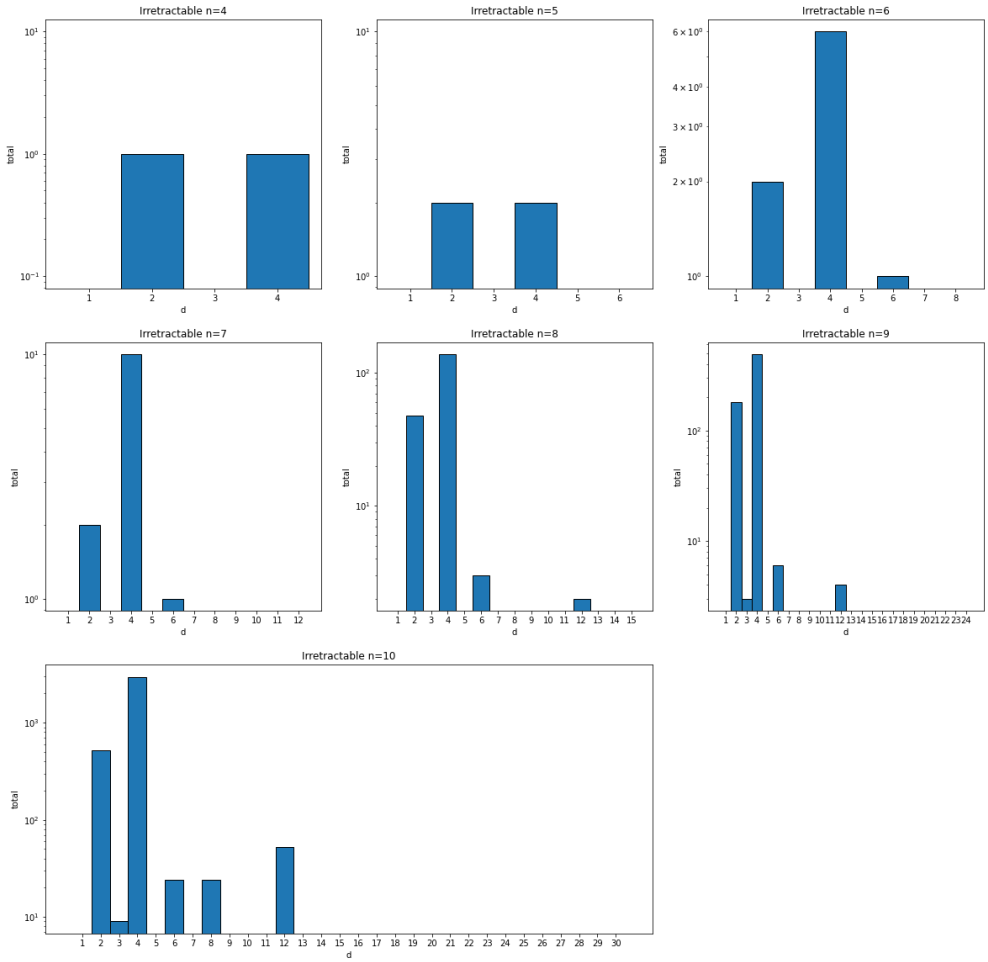


Figure A.3: Irretractable solutions

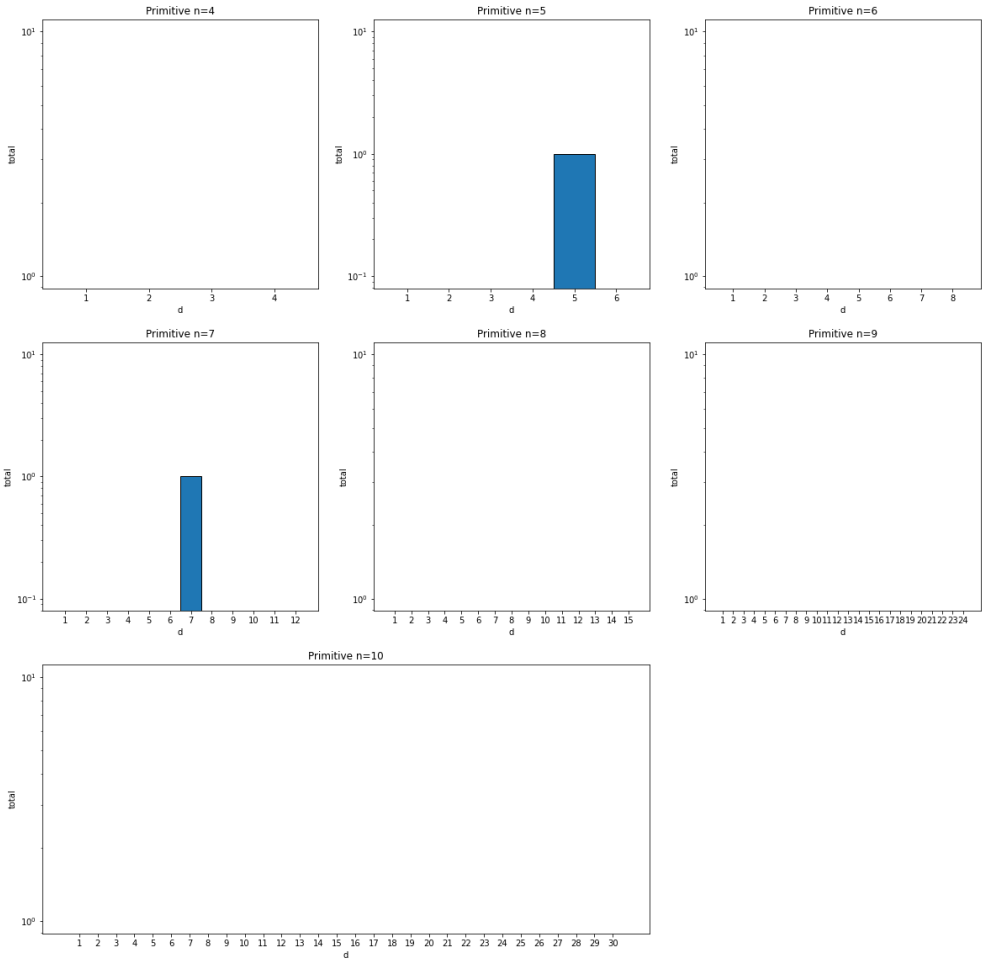


Figure A.4: Primitive solutions

Figure A.4 highlights the main result of [CJO22]:

A cycle set $(S, *)$ is said to be primitive if its permutation group $\mathcal{G}$ acts primitively on X, i.e. the action is transitive and does not preserve non-trivial partition of S.

By [CJO22, Theorem 3.1], a cycle set is primitive if and only if it isomorphic to the solution of prime size p given by $S = \{s_1, \ldots, s_p\}$ with $\psi(s) = \begin{pmatrix} 1 & 2 & \ldots & p \end{pmatrix}$ for all s in S.

Moreover, such a solution is of class p as shown in Example 2.2.0.7.

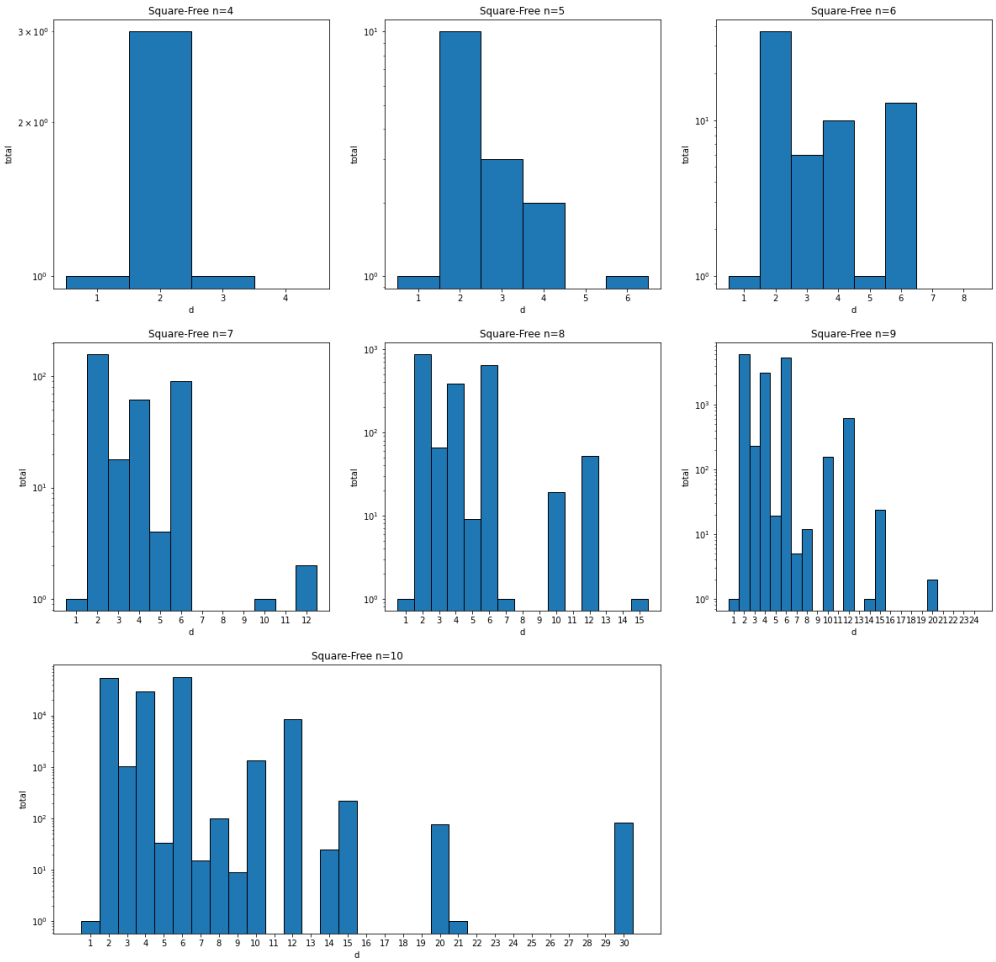


Figure A.5: Square-free solutions

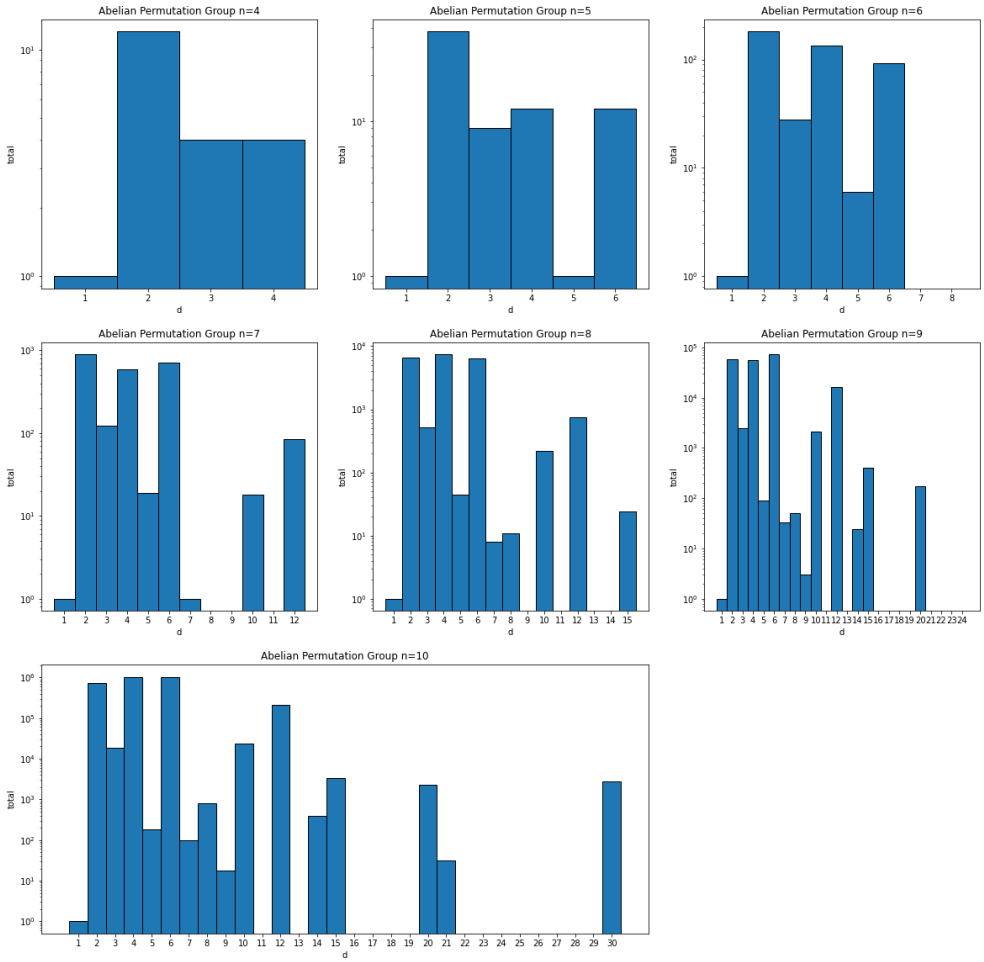


Figure A.6: Solutions with abelian permutation group

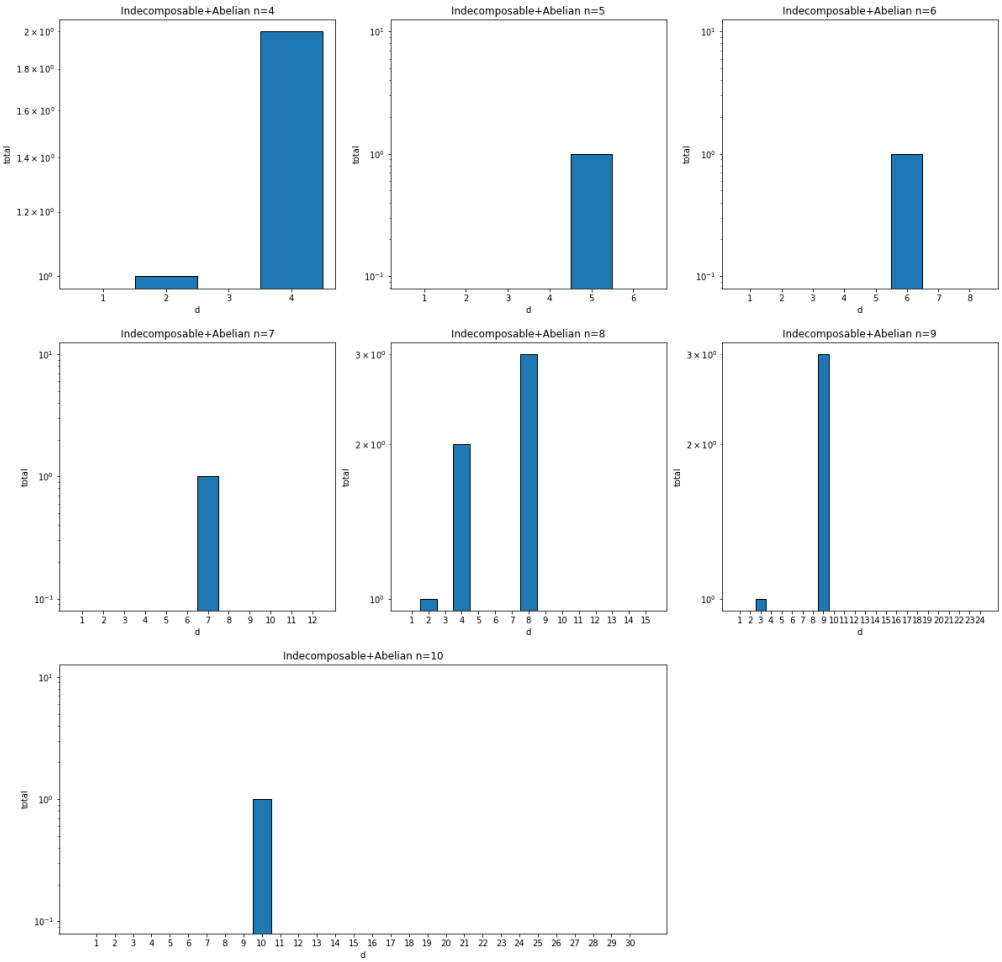


Figure A.7: Indecomposable solutions with abelian permutation group

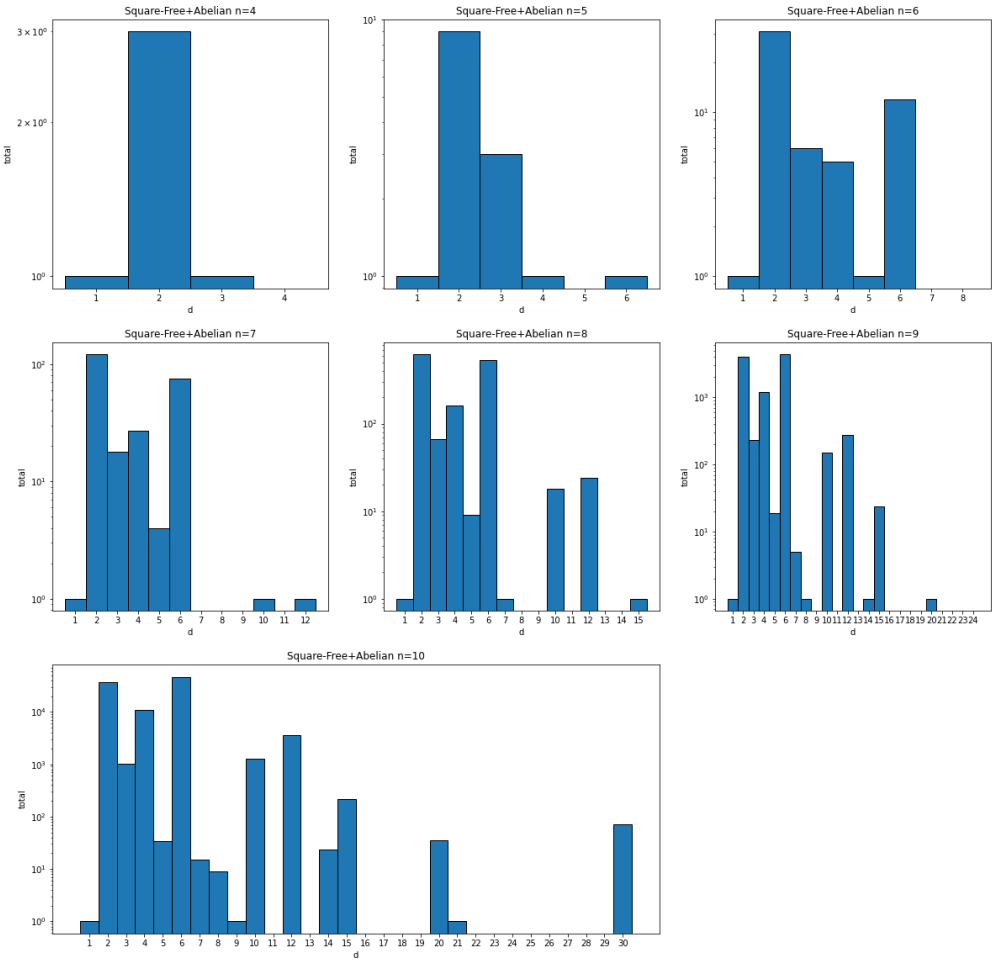


Figure A.8: Square-free with abelian permutation group

Figure A.8 corresponds to the cases covered by Proposition 2.4.0.9. We can see that such solutions are approximately 1% of all solutions (see Figure A.1.

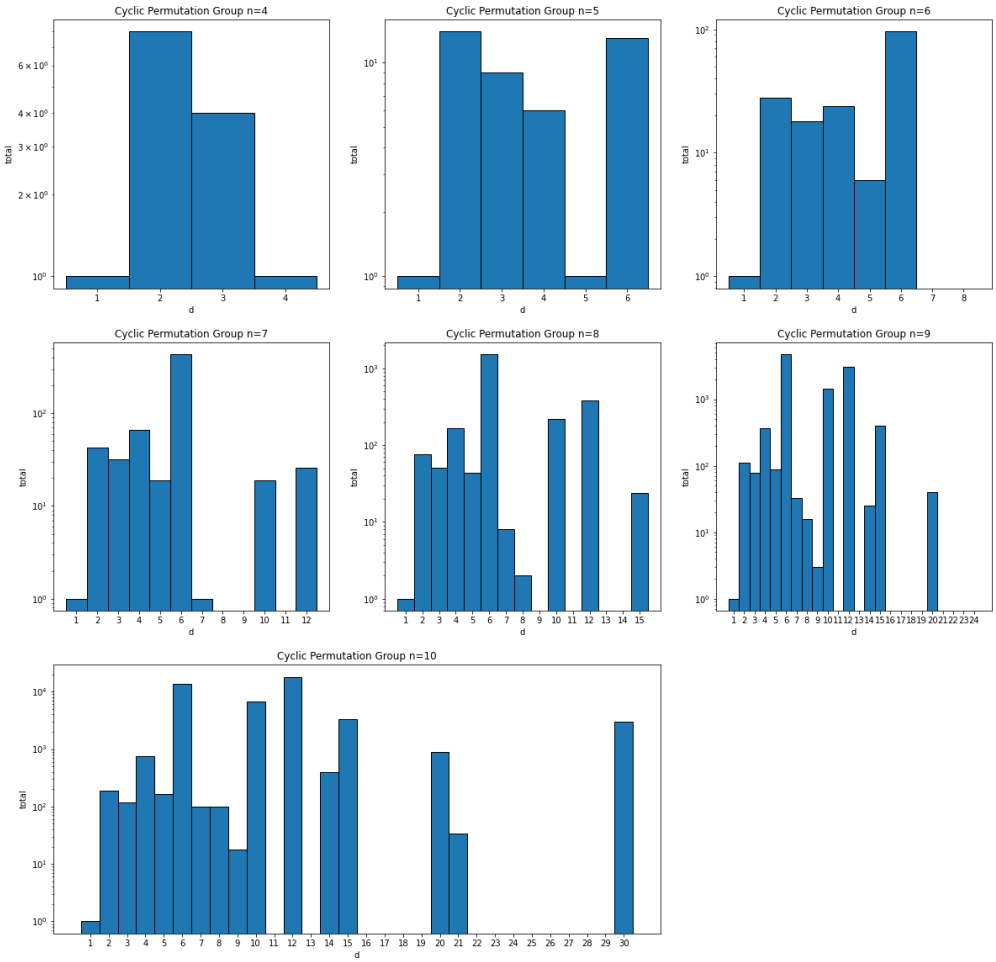


Figure A.9: Solutions with cyclic permutation group

Figure 1.3 corresponds to the case obtained in [[CR23, Proposition 5.9]], as mentionned in Proposition 2.4.0.10.

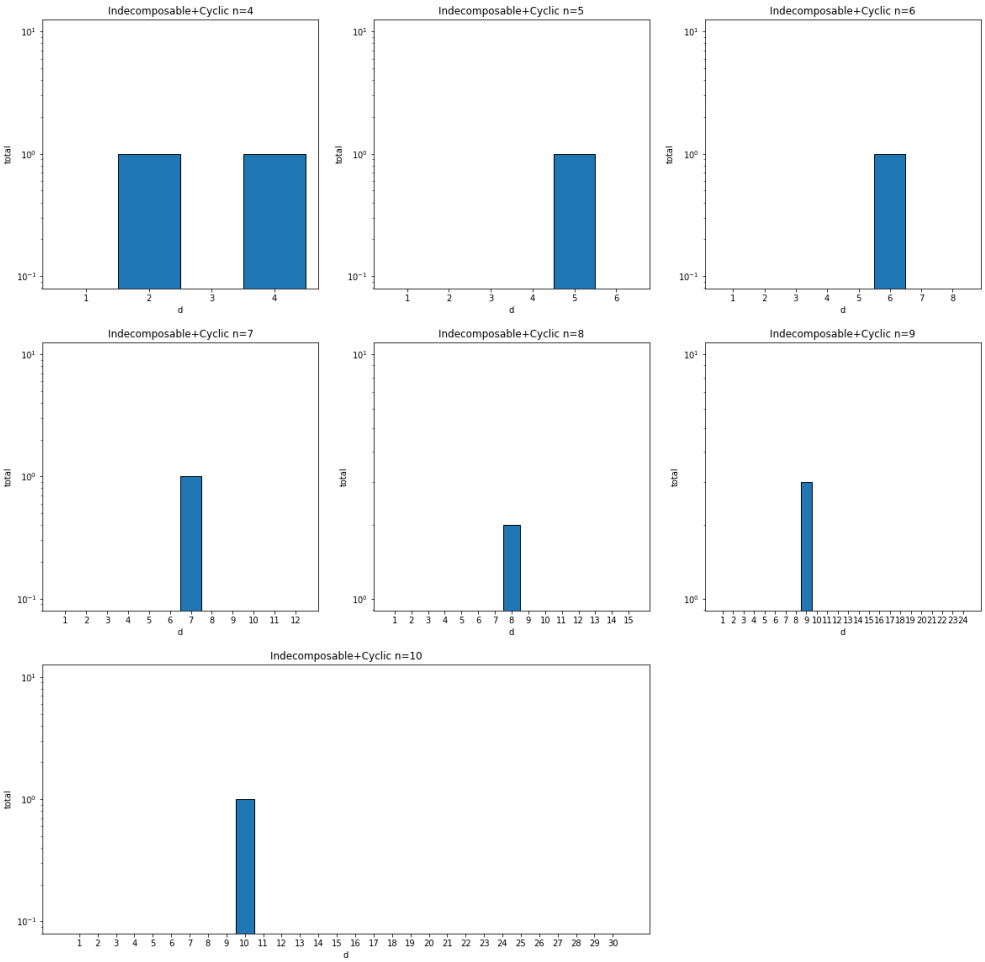


Figure A.10: Indecomposable solutions with cyclic permutation group

Index

Algebra, 90
  Radical, 90
  Semi-simple, 90
  Separable, 90
  Simple, 90
  Split, 90
  Trace, 90

Brace, 38
  λ-map, 39
  Ideal, 40
  Left ideal, 40
  Subbrace, 40

Complex reflection group, 95
Coxeter group, 8
Cycle set, 24
  Diagonal map, 53
  Indecomposable, 56
  Morphism of, 24
  Permutation group, 55
  Retraction, 60
  Square-free, 24
  Structure group, 24
  Structure monoid, 24

Dehornoy's class, 47

Garside
  Element, 45
  Germ, 49
  Group, 46

Induced representation, 73
Iwahori-Hecke algebra, 11

Monomial Representation
  Structure monoid, 31
Monomial representation
  Germ, 48
  Structure group, 31

Reduced word, 51
Rump's theorem, 53

Set-theoretical solution of the YBE, 21
  Involutive, 23
  Morphism of, 22
  Non-degenerate, 23
  Structure group, 23

Zappa–Szép product, 61

Bibliography

[Ale23] J. W. Alexander. "A Lemma on Systems of Knotted Curves". *Proceedings of the National Academy of Sciences* 9.3 (Mar. 1923), 93–95.

[AMV22] Ö. Akgün, M. Mereb, and L. Vendramin. "Enumeration of Set-Theoretic Solutions to the Yang–Baxter Equation". *Math. Comp.* 91.335 (2022), 1469–1481.

[Art25] E. Artin. "Theorie der Zöpfe". *Abh.Math.Semin.Univ.Hambg.* 4.1 (Dec. 1925), 47–72.

[Art47] E. Artin. "Theory of Braids". *Annals of Mathematics* 48.1 (1947), 101–126. JSTOR: 1969218.

[Bac18] D. Bachiller. "Extensions, Matched Products, and Simple Braces". *Journal of Pure and Applied Algebra* 222 (2018), 1670–1691.

[Bax72] R. J. Baxter. "Partition Function of the Eight-Vertex Lattice Model". *Annals of Physics* 70.1 (Mar. 1972), 193–228.

[Bax85] R. J. Baxter. "Exactly Solved Models in Statistical Mechanics". *Integrable Systems in Statistical Mechanics*. Vol. Volume 1. Series on Advances in Statistical Mechanics. World Scientific, May 1985, 5–63.

[BCJ16] D. Bachiller, F. Cedó, and E. Jespers. "Solutions of the Yang–Baxter Equation Associated with a Left Brace". *Journal of Algebra* 463 (Oct. 2016), 80–102.

[Bha+21] P. Bhandari, M. Córdoba, J. Henderson, and S. Warrander. *On the Extraordinary Construction of Cycle Sets by Wolfgang Rump*. 2021. arXiv: 2106.05149 [math].

[Bou07] N. Bourbaki. *Groupes et algébras de Lie (Tome 4,5 et 6)*. Berlin, Heidelberg: Springer, 2007.

[Bou22] N. Bourbaki. "Chapter VIII Semisimple Modules and Rings". *Algebra: Chapter 8*. Ed. by N. Bourbaki. Cham: Springer International Publishing, 2022, 1–467.

[Bri05] M. G. Brin. "On the Zappa-Szép Product". *Communications in Algebra* 33.2 (Feb. 2005), 393–424.

[Bro00] M. Broué. "Reflection Groups, Braid Groups, Hecke Algebras, Finite Reduction Groups". *Curr. Dev. in Math.* 2000.1 (2000), 1–107.

[BS72] E. Brieskorn and K. Saito. “Artin-Gruppen und Coxeter-Gruppen”. *Invent Math* 17.4 (Dec. 1972), 245–271.

[CCS20] F. Catino, I. Colazzo, and P. Stefanelli. “The Matched Product of Set-Theoretical Solutions of the Yang-Baxter Equation”. *Journal of Pure and Applied Algebra* 224 (2020), 1173–1194.

[Ced18] F. Cedó. “Left Braces: Solutions of the Yang-Baxter Equation”. *Advances in Group Theory and Applications* 5 (2018), 33–90.

[CG12] F. Chouraqui and E. Godelle. “Folding of Set-Theoretical Solutions of the Yang-Baxter Equation”. *Algebras and Representation Theory* 15 (2012), 1277–1290.

[CG14] F. Chouraqui and E. Godelle. “Finite Quotients of Groups of I-type”. *Advances in Mathematics* 258 (June 2014), 46–68.

[Cho10] F. Chouraqui. “Garside Groups and Yang–Baxter Equation”. *Communications in Algebra* 38.12 (2010), 4441–4460.

[Cho23] F. Chouraqui. “On Some Garsideness Properties of Structure Groups of Set-Theoretic Solutions of the Yang-Baxter Equation”. *Communications in Algebra* 51.8 (Aug. 2023), 3221–3231.

[CJO14] F. Cedó, E. Jespers, and J. Okniński. “Braces and the Yang–Baxter Equation”. *Commun. Math. Phys.* 327.1 (2014), 101–116.

[CJO22] F. Cedó, E. Jespers, and J. Okniński. “Primitive Set-Theoretic Solutions of the Yang–Baxter Equation”. *Communications in Contemporary Mathematics* 24 (2022), 2150105.

[Coh07] Cohen. *Number Theory, Volume I: Tools and Diophantine Equations*. Vol. 239. Graduate Texts in Mathematics. New York, NY: Springer, 2007.

[Cox35] H. S. M. Coxeter. “The Complete Enumeration of Finite Groups of the Form Ri2=(RiRj)Kij=1”. *Journal of the London Mathematical Society* s1-10.1 (1935), 21–25.

[Cox59] H. S. M. Coxeter. “Factor Groups of the Braid Group,” *Proceedings of the Fourth Cananadian Mathematical Congress* (1959), 95–122.

[CPR20] M. Castelli, G. Pinto, and W. Rump. “On the Indecomposable Involutive Set-Theoretic Solutions of the Yang-Baxter Equation of Prime-Power Size”. *Communications in Algebra* 48.5 (May 2020), 1941–1955.

[CR23] M. Castelli and S. Ramirez. *On Uniconnected Solutions of the Yang-Baxter Equation and Dehornoy’s Class*. June 2023.

[CR62] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. AMS Chelsea Publishing, 1962.

[CR90a] C. W. Curtis and I. Reiner. *Methods of Representation Theory, Volume I*. New York: Wiley, 1990.

[CR90b] C. W. Curtis and I. Reiner. *Methods of Representation Theory, Volume II*. New York: Wiley, 1990.

[Deh+15] P. Dehornoy, F. Digne, E. Godelle, D. Krammer, and J. Michel. *Foundations of Garside Theory*. Vol. 22. EMS Tracts in Mathematics. 2015.

[Deh15] P. Dehornoy. "Set-Theoretic Solutions of the Yang–Baxter Equation, RC-calculus, and Garside Germs". *Advances in Mathematics* 282 (2015), 93–127.

[Deh17] P. Dehornoy. "Garside Germs for YBE Structure Groups, and an Extension of Ore's Theorem". *Groups, Rings and the Yang-Baxter Equation*. Spa, Belgium, 2017.

[Del72] P. Deligne. "Les immeubles des groupes de tresses généralisés". *Invent Math* 17.4 (Dec. 1972), 273–302.

[Dig] F. Digne. *Algèbres de Hecke*. www.lamfa.u-picardie.fr/digne/hecke.pdf.

[Dix67] J. D. Dixon. "The Fitting Subgroup of a Linear Solvable Group". *Journal of the Australian Mathematical Society* 7.4 (Nov. 1967), 417–424.

[Došl05] T. Došlić. "Maximum Product over Partitions into Distinct Parts". *Journal of Integer Sequences* 8 (2005), Article 05.5.8.

[DP99] 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.

[DPT24] C. Dietzel, S. Properzi, and S. Trappeniers. *Indecomposable Set-Theoretical Solutions to the Yang-Baxter Equation of Size p^2*. Mar. 2024. arXiv: 2403.18653 [math].

[Dri92] V. G. Drinfeld. "On Some Unsolved Problems in Quantum Group Theory". Vol. 1510. Lecture Notes in Mathematics. 1992, 1–8.

[Eck19] H.-P. Eckle. *Models of Quantum Matter: A First Course on Integrability and the Bethe Ansatz*. Oxford University Press, July 2019.

[ESG01] P. Etingof, A. Soloviev, and R. Guralnick. "Indecomposable Set-Theoretical Solutions to the Quantum Yang–Baxter Equation on a Set with a Prime Number of Elements". *Journal of Algebra* 242 (2001), 709–719.

[ESS99] P. Etingof, T. Schedler, and A. Soloviev. "Set-Theoretical Solutions to the Quantum Yang-Baxter Equation". *Duke Mathematical Journal* 100 (1999), 169–209.

[Fei24] E. Feingesicht. "Dehornoy's Class and Sylows for Set-Theoretical Solutions of the Yang–Baxter Equation". *Int. J. Algebra Comput.* 34 (2024), 147–173.

[Fre+85] P. Freyd, D. Yetter, J. Hoste, W. B. R. Lickorish, K. Millett, and A. Ocneanu. "A New Polynomial Invariant of Knots and Links". *Bull. Amer. Math. Soc.* 12.2 (1985), 239–246.

[Gar69] F. A. Garside. "The Braid Group and Other Groups". *The Quarterly Journal of Mathematics* 20.1 (Jan. 1969), 235–254.

[Gob23] T. Gobet. "A New Garside Structure on Torus Knot Groups and Some Complex Braid Groups". *J. Knot Theory Ramifications* 32.13 (Nov. 2023), 2350094.

[Gob24] T. Gobet. "Toric Reflection Groups". *Journal of the Australian Mathematical Society* 116.2 (Apr. 2024), 171–199.

[GP00] M. Geck and G. Pfeiffer. *Characters of Finite Coxeter Groups and Iwahori-Hecke Algebras*. Clarendon Press, 2000.

[GV17] L. Guarnieri and L. Vendramin. "Skew Braces and the Yang–Baxter Equation". *Math. Comp.* 86.307 (Sept. 2017), 2519–2534.

[GV98] T. Gateva-Ivanova and M. Van den Bergh. "Semigroups of I-Type". *Journal of Algebra* 206 (1998), 97–112.

[Iwa64] N. Iwahori. "On the Structure of a Hecke Ring of a Chevalley Group over a Finite Field". Mar. 1964.

[Jes+21] E. Jespers, Ł. Kubat, A. Van Antwerpen, and L. Vendramin. "Radical and Weight of Skew Braces and Their Applications to Structure Groups of Solutions of the Yang–Baxter Equation". *Advances in Mathematics* 385 (July 2021), 107767.

[Jim89] M. Jimbo. "Introduction to the Yang-Baxter Equation". *Int. J. Mod. Phys. A* 04.15 (Sept. 1989), 3759–3777.

[Jon87] V. F. R. Jones. "Hecke Algebra Representations of Braid Groups and Link Polynomials". *Annals of Mathematics* 126.2 (1987), 335–388. JSTOR: 1971403.

[Lan03] E. Landau. "Über Die Maximalordnung Der Permutationen Gegebenen Grades". *Archiv der Mathematik und Physik* 5 (1903), 92–103.

[Led73] W. Ledermann. *Introduction to Group Theory*. Oliver and Boyd, 1973.

[LRV22] V. Lebed, S. Ramírez, and L. Vendramin. *Involutive Yang-Baxter: Cabling, Decomposability, Dehornoy Class*. 2022. arXiv: 2209.02041 [math].

[Lus16] G. Lusztig. *Characters of Reductive Groups over a Finite Field. (AM-107), Volume 107*. Princeton University Press, Mar. 2016.

[Mic14] J. Michel. "Lectures on Coxeter Groups". Beijing, 2014.

[Mic98] J. Michel. "Groupes de tresses, Groupes réductifs et algèbres de Hecke". Lecture Notes. 1998.

[PA06] J. H. H. Perk and H. Au-Yang. "Yang–Baxter Equations". *Encyclopedia of Mathematical Physics*. Ed. by J.-P. Françoise, G. L. Naber, and T. S. Tsun. Oxford: Academic Press, Jan. 2006, 465–473.

[Pou] L. Poulain d'Andecy. "Personnal Communications".

[Pou23] L. Poulain d'Andecy. "Algèbres de Hecke Fusionnées et Dualité de Schur–Weyl". *Séminaire d'Algèbre et de Géométrie*. Caen, May 2023.

[RMB98] R. Rouquier, G. Malle, and M. Broué. "Complex Reflection Groups, Braid Groups, Hecke Algebras". *Crelles Journal* 1998.500 (July 1998), 127–190.

[Rum05] W. Rump. "A Decomposition Theorem for Square-Free Unitary Solutions of the Quantum Yang-Baxter Equation". *Advances in Mathematics* 193 (2005), 40–55.

[Rum07] W. Rump. "Braces, Radical Rings, and the Quantum Yang–Baxter Equation". *Journal of Algebra* 307.1 (Jan. 2007), 153–170.

[Rum15] W. Rump. “Right L-Groups, Geometric Garside Groups, and Solutions of the Quantum Yang–Baxter Equation”. *Journal of Algebra* 439 (2015), 470–510.

[Sas] R. Sastriques-Guardiola. “Personnal Communications”.

[Ser77] J.-P. Serre. *Linear Representations of Finite Groups*. Vol. 42. Graduate Texts in Mathematics. New York, NY: Springer, 1977.

[ST54] G. C. Shephard and J. A. Todd. “Finite Unitary Reflection Groups”. *Canadian Journal of Mathematics* 6 (Jan. 1954), 274–304.

[Tit66] J. Tits. “Normalisateurs de Tores I. Groupes de Coxeter Étendus”. *Journal of Algebra* 4.1 (July 1966), 96–116.

[Tit74] J. Tits. *Buildings of Spherical Type and Finite BN-Pairs*. Vol. 386. Lecture Notes in Mathematics. Berlin, Heidelberg: Springer, 1974.

[Yan67] C. N. Yang. “Some Exact Results for the Many-Body Problem in One Dimension with Repulsive Delta-Function Interaction”. *Phys. Rev. Lett.* 19.23 (Dec. 1967), 1312–1315.