Dehornoy's class and Sylows for set-theoretical solutions of the Yang-Baxter equation

Edouard Feingesicht

DEHORNOY'S CLASS AND SYLOWS FOR SET-THEORETICAL SOLUTIONS OF THE YANG–BAXTER EQUATION

EDOUARD FEINGESICHT

Abstract. We explain how the germ of the structure group of a cycle set decomposes as a product of its Sylow-subgroups, and how this process can be reversed to construct cycle sets from ones with coprime classes. We study the Dehornoy's class associated to a cycle set, and conjecture a bound that we prove in a specific case. The main tool used is a monomial representation, which allows for intuitive, short and self-contained proofs, in particular to easily re-obtain previously known results (Garsideness, I-structure, Dehornoy's class and germ, non-degeneracy of finite cycle sets).

0. Introduction

In 1992 Drinfeld ([11]) posed the question of classifying set-theoretical solutions of the (quantum) Yang–Baxter equation, 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 [12], 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). Since then, many advances have been made on this question and objects introduced: structure group ([12]), I-structure ([14]), etc. Many equivalent objects are known, but in particular here we are interested in cycle sets, introduced by Rump ([19]). Dehornoy ([7]) then studied the structure group (from cycle sets) seen from a Garside perspective (divisibility, word problem, ...), he then concludes with a faithful representation, which will be the base of this article. Starting from this representation, we retrieve most of Dehornoy's results in simpler, shorter and self-contained proofs, and other well known results (I-structure, non-degeneracy of finite left-non-degenerate involutive solutions of [19]). Then we study finite quotient defined through an integer called the Dehornoy's class of the solution, those quotients are called germs because they come with a natural way to recover the structure monoid and its Garside structure. We state the following conjecture on Dehornoy's class (Conjecture 3.6):

Conjecture. *Let S be a cycle set of size n. The Dehornoy's class d of S is bounded above by the "maximum of different products of partitions of n into distinct parts" and the bound is minimal, i.e.*

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

We then focuses on the germ and its Sylows, with the main result on cycle sets being constructed from the Zappa–Szép product of germs (Theorem 4.12), this product being a sort of generalized semi-direct products where each term acts on the others :

Theorem. *Any cycle set can be obtained as the Zappa–Szép product of cycle sets with class a prime power.*

2020 *Mathematics Subject Classification.* 16T25, 20N02, 20C10.

Key words and phrases. Yang–Baxter equation, Garside monoid, Cycle set, Monomial representation, Sylow, Zappa-Szép.

Taking decomposability ([2]) into account, one can consider that the "basic" cycle sets are of class and size powers of the same prime.

The first two sections are mostly a new approach to well-known theorems which allows simpler and more intuitive proofs, while the last two contain new results obtained by using the new approach developed in the two first sections. More precisely:

Section 1 is a brief introduction to monomial matrices and the main properties that we will use for our proofs. Section 2 consists in recovering most results of [7] with a monomial representation, allowing shorter, simpler and self-contained proofs. Including the study of right-divisibility without Rump's theorem on the non-degeneracy of finite cycle sets (while also easily re-obtaining this theorem). Section 3 focuses on Dehornoy's class and germ, in particular we state a conjecture on the bound of the classes and prove it in a particular case. Section 4 explains how to construct all cycle sets from ones with coprime classes through the Zappa–Szép product of germs, with a precise condition and an explicit algorithm/formula to do so.

Acknowledgements The author wishes to thank Leandro Vendramin for his insightful remarks on the content and readability of this article.

1. Monomial matrices

The basic tool to work on the representation are monomial matrices. We recall the definition and some basic 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 1.1. *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 1.2. *Let m, m' be monomial matrices. Then we have $D_{mm'} = D_m \left({}^{\psi(m)} D_{m'}\right)$ 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 $D_m = \operatorname{diag}(a, b, c)$, $D_{m'} = \operatorname{diag}(x, y, z)$ 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 $mm' = \begin{pmatrix} 0 & ay & 0 \\ bz & 0 & 0 \\ 0 & 0 & cx \end{pmatrix} = \mathrm{diag}(ay,bz,cx)P_{(12)}$.

2. Cycle sets and monomial matrices

In this section, we retrieve the results of [7] using monomial matrices. In particular, our proofs don't rely on Rump's theorem on the bijectivity of finite cycle sets ([19]), and use simpler arguments compared with the technicality of [7]. Moreover, although we don't need it in this section, we provide a short and simple proof of Rump's theorem.

2.1. Cycle sets

Definition 2.1 ([19])**.** *A cycle set is a set S endowed with a binary operation $*$ such that for all s in S the map $\psi(s)\colon t \mapsto s*t$ is bijective and for all s,t,u in S:*

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

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

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

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

Definition 2.2 ([19])**.** *The group G_S associated with S is defined by the presentation:*

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

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

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

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

Example 2.3. Let $S = \{s_1,\dots,s_n\}$, $\sigma = (12\dots n) \in \mathfrak{S}_n$. The operation $s_i * s_j = s_{\sigma(j)}$ makes S into a cycle set, as for all s,t in S we have $(s*t)*(s*s_j) = s_{\sigma^2(j)} = (t*s)*(t*s_j)$.

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

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

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

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

Remark 2.4. By the definition of $\psi\colon S \to \mathfrak{S}_n$ we have that $s_i * s_j = s_{\psi(s_i)(j)}$, which we will also write $\psi(s_i)(s_j)$ for simplicity.

2.2. 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 by directly looking at the representation introduced in the same paper [7], and we use those to retrieve the well-known I-structure of the structure monoid ([14]).

Although all these results are already stated in [7], their provided proofs are very technical, whereas using monomial matrices greatly simplifies proofs and allows for more intuition.

Definition 2.5 ([7]). *For a positive integer k, we define inductively the formal expression Ω_k by $\Omega_1(x_1) = x_1$ and*

$$\Omega_k(x_1, \dots, x_k) = \Omega_{k-1}(x_1, \dots, x_{k-1}) * \Omega_{k-1}(x_1, \dots, x_{k-2}, x_k). \tag{3}$$

We then define another formal expression Π_k by:

$$\Pi_k(x_1, \dots, x_k) = \Omega_1(x_1) \cdot \Omega_2(x_1, x_2) \cdot \ \dots \ \cdot \Omega_k(x_1, \dots, x_k). \tag{4}$$

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.

Lemma 2.6 ([7]). *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):

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

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 doesn't 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)
Which concludes the proof. □

Proposition 2.7. *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 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

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

Clearly, the first $i-1$ terms remain unchanged by σ_i. And by the previous Lemma 2.6, 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 concludes the proof. □

Lemma 2.8. *For 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

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

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

Proposition 2.9. *Let f be in M. Then there exists $(t_1, \ldots, t_k)^k$ in S^k such that $f = \Pi_k(t_1, \ldots, t_k)$.*

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

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

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

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.:

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

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

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

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

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

□

Example 2.10. 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 $f = \Pi_4(s_3, s_1, s_1, s_2)$.

2.3. **The monomial representation**

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 2.11 ([7])**.** *Let q be an indeterminate and consider $\mathfrak{Monom}_n(\mathbb{Q}[q,q^{-1}])$, denote D_{s_i} the matrix $diag(1,\dots,q,\dots,1)$ the $n\times n$ diagonal matrix with a q on the i-th row.*

The map Θ defined on S by

$$\Theta(s_i) \coloneqq D_{s_i}P_{\psi(s_i)} \tag{5}$$

extends to a representation $G\to\mathfrak{Monom}_n(\mathbb{Q}[q,q^{-1}])$ and similarly to a morphism $M\to\mathfrak{Monom}_n(\mathbb{Q}[q])$.

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 1.2 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 1.1. By symmetry and commutativity of diagonal matrices, we deduce $D_g=D_{g'}$.

On the other hand, again by Corollary 1.2, 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 $\Theta(g)=D_gP_g$ to mean $\Theta(g)=D_{\Theta(g)}P_{\Theta(g)}$.

Remark 2.12. The image of G by Θ lies in the subgroup of $\mathfrak{Monom}_n(\mathbb{Q}[q,q^{-1}])$ consisting of matrices such that the non-zero coefficients (i.e. the diagonal part of the decomposition) consists only of powers of q (including $q^0=1$). We denote this subgroup by Σ_n. By Σ_n^+ we denote the submonoid of $\mathfrak{Monom}_n(\mathbb{Q}[q])$ consisting of non-matrices whose non-zero coefficients are non-negative powers of q only, and by D_i the matrix $\mathrm{diag}(1,\dots,q,\dots,1)$ with a q in the i-th place.

Remark 2.13. Let G^+ be the submonoid of M of positive words. As M and G^+ have the same generators, their images in their respective representations Θ coincide. Thus, when working in $\mathfrak{Monom}_n(\mathbb{Q}[q,q^{-1}])$, 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 2.14. Set $S=\{s_1,s_2,s_3\}$ and $\psi(s_i)=(123)$ for all i.

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

and similarly

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

Proposition 2.15. *For all $s,t\in S$:*

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

In particular, $P_sD_{s*t}=D_tP_s$.

Proof. This is a direct consequence of Lemma 1.1. □

Definition 2.16. *For an element $g\in\Sigma_n$, we define its "coefficient-powers tuple" $cp(g)$ to be the unique n-tuple of integers $(c_1,\dots,c_n)$ such that $D_g=diag(q^{c_1},\dots,q^{c_n})$.*

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

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

Example 2.17. If $g = \begin{pmatrix} q^2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & q^{-1} \\ 0 & q & 0 & 0 \end{pmatrix}$, then $\mathrm{cp}(g) = (2, 0, -1, 1)$ and $\lambda(g) = 2 + 0 + 1 + 1 = 4$.

Proposition 2.18. *For all $g, h \in \Sigma_n$ we have:*

$$cp(gh) = cp(g) + {}^{\psi(g)}cp(h). \tag{6}$$

Moreover $\lambda(gh) = \lambda(g) + \lambda(h)$.

Proof. The first equality is a direct consequence of Corollary 1.2 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 2.2, that is $\Pi'_k(t_1, \dots, t_k) = \Theta(\Pi(t_1, \dots, t_k))$.

Proposition 2.19. *Let $t_1, \dots, t_k$ be in S, then*

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

and

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

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

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 $\Pi(t_1, \dots, t_k) = \Pi_{k-1}(t_1, \dots, t_{k-1}) \cdot \Omega_k(t_1, \dots, t_k)$, so by the induction hypothesis

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

Note that $\Omega'_k(t_1, \dots, t_k) = \Omega'_{k-1}(t_1, \dots, t_{k-1}) * \Omega'_{k-1}(t_1, \dots, t_{k-2}, t_k)$. So by Proposition 2.15 we get

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

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

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

Thus we find

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

As $P_\sigma P_\tau = P_{\tau\sigma}$, we have $\psi(\Pi'_k(t_1, \dots, t_k))(s) = \psi(\Omega'_k(t_1, \dots, t_k)) \circ \dots \circ \psi(\Omega'_1(t_1))(s)$. 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 2.20. *Any tuple of non-negative integers $(c_1 \dots, c_n) \in \mathbb{N}^n$ 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, Π'_l applied to this tuple gives the expected result. □

Example 2.21. As in 2.10 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 we did:

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

Computing $\psi(s_1)^{-1} \circ \psi(s_2)^{-1} \circ \psi(s_3)^{-1}(s_4) = s_2$ precisely retrieves the Example 2.10.

Those reasonings are inverse to one another: to construct an element with given coefficient-powers we use permutations step by step and letter by letter (this is the construction of Π), and to get a Π-expression we use all the inverse of those permutations.

Corollary 2.22. *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.

In particular, this means that the representation is injective on the monoid, as the diagonal part is determined by the entries of a Π-expression, which is invariant by permutations of those entries.

Proof. This follows from the previous proposition and Proposition 2.9. 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 2.9 there exist $t_1, \dots, t_k \in S$ such that $f = \Pi_k(t_1, \dots, t_k)$. By Proposition 2.19, 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 2.7 the orders of the t_i's doesn't 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 $\mathfrak{M}_n$ (resp. $\mathfrak{M}_n^+$). We have an obvious inclusion $\mathfrak{D}_n^+ \hookrightarrow \mathfrak{D}_n$, and a faithful representation $\mathbb{N}^n \xrightarrow{\sim} \mathfrak{D}_n^+$.

Corollary 2.23. *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 is said to be reduced if its length k is minimal among the representative words of g.

Proposition 2.24. *Any element $g \in G$ can be decomposed as a reduced left-fraction in M, that is:*

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

where λ 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 later state a similar result for right-fractions (Proposition 2.71).

Corollary 2.25. *Any element in G can be decomposed as a left-fraction fg^{-1} in M such that D_g commutes with all permutation matrices (more precisely that D_g is a power of $D_{s_1} \dots D_{s_n}$).*

Proof. Take a Π-expression $\Pi_k(t_1, \dots, t_k)$ of g. up to permuting the entries, we can assume that $g = \Pi_k(s_1, \dots, s_1, \dots, s_n, \dots, s_n)$, 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 $\Pi_{k+1}(s_1, \dots, s_1, \dots, s_n, \dots, s_n, s_i) = g \cdot \Omega_{k+1}(s_1, \dots, s_1, \dots, s_n, \dots, s_n, s_i)$, where s_i occurs $a_i + 1$ times and that is obtained from g by right-multiplying by an element in S. Doing so, until all s_i occurs a_j times, provides an element $\overline{g}$ which is obtained from g by right-multiplication by some $g' \in M$ and such that $D_{\overline{g}} = (D_{s_1} \dots D_{s_n})^{a_j}$.

Let P_σ be a permutation matrix, then $P_\sigma D_{\overline{g}} = {}^{\sigma}D_{\overline{g}} P_\sigma = D_{\overline{g}} P_\sigma$ where the last equality is because all the diagonal terms in $D_{\overline{g}}$ are equal so are invariant by σ.

Finally $fg'(\overline{g})^{-1} = fg^{-1}$, so replacing (f, g) by (fg', gg') gives us the result. □

Example 2.26. Take $S = \{s_1, s_2, s_3\}$ and $\psi(s_i) = (123)$ for all i. Consider $h = s_3^{-1}s_2^{-1}s_3$, the relation $s_2s_1 = s_3s_3$ (i.e. $s_1s_3^{-1} = s_2^{-1}s_3$) gives $h = s_3^{-1}s_1s_3^{-1}$; similarly $s_3s_2 = s_1s_1$ (i.e. $s_2s_1^{-1} = s_3^{-1}s_1$) yields $h = s_2s_1^{-1}s_1^{-1}$.

Let $f = s_2$ and $g = s_1s_1$ so that $h = fg^{-1}$, we have $g = s_1(s_1 * s_3) = \Pi_2(s_1, s_3)$, thus $D_g = D_{\Theta(g)} = D_{s_1}D_{s_3}$, which is not stable under permutation (as we have ${}^{(123)}D_g = D_{s_{(123)^{-1}(1)}}D_{s_{(123)^{-1}(2)}} = D_{s_3}D_{s_2} \neq D_g$). To complete g so that it commutes, we must add D_{s_3}, so we take $g' = \Pi_3(s_1, s_2, s_3) = gs_1$ and $f' = fs_1$. Now $D_{g'} = D_{s_1}D_{s_2}D_{s_3}$ commutes with permutation matrices, and $f'g'^{-1} = fs_1s_1^{-1}g^{-1} = fg^{-1} = h$.

Theorem 2.27. *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 2.24 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 2.23, $\Theta(f) = \Theta(h) \iff f = h$, thus Θ is faithful. □

From now on, we assume that S is a finite cycle set with $S = \{s_1, \dots, s_n\}$. 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 2.28. *A subgroup of Σ_n is called permutation-free if the only permutation matrix it contains is the identity.*

Proposition 2.29. *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 2.24, there exists $f, g \in M$ such that $P_\sigma = fg^{-1}$, i.e. $D_f P_f = P_\sigma D_g P_g$. By Corollary 2.25 we can assume that $P_\sigma D_g = D_g P_\sigma$, 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 2.22 $f = g$ and thus $P_\sigma =$Id (and $\sigma =$id). □

Corollary 2.30. *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 a permutation matrix in G, so it must be the identity, so $P_g = P_h$ and thus $g = h$. □

Proposition 2.31. *For any tuple $a = (a_1, \dots, a_k)$ in $\mathbb{Z}^k$, there exists a unique $g \in G$ with $cp(g) = (a_1, \dots, a_k)$.*

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

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

Proof. For the first part, the existence follows from Corollary 2.20 and the unicity from the previous Corollary.

The second statement is just Proposition 2.18 applied to the generators of the monoid, and, similarly, the third is a consequence of considering irreducible left-fractions in Proposition 2.24. □

Remark 2.32. This is precisely a matricial formulation of the I-structure of [14].

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:

Theorem 2.33. *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 $q \mapsto q^p$ provides an injective morphism $\Sigma_n \to \Sigma_n$, so we can assume $p = 1$.

(i) ⇒ (ii): For $1 \leq i, j \leq n$, we have from Proposition 2.15:

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

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) ⇒ (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)⇒ (i): This is Proposition 2.29. □

2.4. **Garsideness**

In a 2017 talk ([8]), Dehornoy addressed the question of whether his results on the construction of the Garside structure and the I-structure can be derived without using Rump's result on the non-degeneracy of finite cycle set ([13]). In this section, we answer his question positively.

Although equivalent to working in the I-structure [14] $\mathbb{Z}^n \rtimes \mathfrak{S}_n$ by decomposing elements $(\underline{c}, \sigma) = (\underline{c}, 1)(1, \sigma) = (1, \sigma)({}^{\sigma}\underline{c}, 1)$, working with monomial matrices and their decomposition has the advantage of giving more intuition, and allows for looking at both left and right structure at the same time. For instance, this is efficient when looking at divisibility, that we study in this section.

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

Definition 2.34. *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 $\lambda(g_2) = \lambda(g_1) + \lambda(h)$.*

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

We equip $\mathbb{Z}^n$ with the partial ordering given by $(a_1, \dots, a_n) \leq (b_1, \dots, b_n)$ iff $a_i \leq b_i$ for all $1 \leq i \leq n$. In particular, this means that given $g_1, g_2 \in G$, $\mathrm{cp}(g_1) \leq \mathrm{cp}(g_2)$ iff the power of q on the i-th row of g_1 is less than the one of g_2 for $1 \leq i \leq n$. Moreover, note that, as $g_1 = P_{g_1}\, {}^{g_1}D_{g_1}$ and $g_1^t = P_{g_1}^t D_{g_1} = P_{g_1}^{-1} D_{g_1} = {}^{g_1}D_{g_1} P_{g_1}^{-1}$, the coefficient on the i-th column of g_1 is the coefficient on the i-th row of g_1^t.

Proposition 2.35. *g_1 left-divides g_2 if and only if $cp(g_1) \leq cp(g_2)$,*

Similarly, g_1 right-divides g_2 if and only if $cp(g_1^t) \leq cp(g_2^t)$.

This means that, to check if g_1 is a left- (resp. right-) divisor of g_2, we only have to check if the power of q is smaller on each row (resp. column).

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 $h = g_1^{-1} g_2 = P_{g_1}^{-1} D_{g_1}^{-1} D_{g_2} P_{g_2}$. By Proposition 2.31 $h \in M$ iff $D_{g_1}^{-1} D_{g_2})$ contains only non-negative powers of q, 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 q, which is the same criterion on the columns. □

Example 2.36. Taking $S = \{s_1, s_2\}$ with $\psi(s_1) = \psi(s_2) = (12)$, we can see that:

$\begin{pmatrix} 0 & q^3 \\ 1 & 0 \end{pmatrix}$ left-divides $\begin{pmatrix} q^4 & 0 \\ 0 & 1 \end{pmatrix}$ (as $3 \leq 4$ on the first line and $0 \leq 0$ on the second since $1 = q^0$), but doesn't right divide it (as $3 > 0$ on the second column)

Corollary 2.37. *Let $g = \Pi_k(t_1, \dots, t_k)$, then the left-divisors of g are precisely the Π's of subtuples of $(t_1, \dots, t_k)$.*

Reciprocally, the right multiples of g are the elements h such that, when writing $h = \Pi_l(u_1, \dots, u_l)$, the tuple $(u_1, \dots, u_l)$ contains the tuple $(t_1, \dots, t_k)$.

Corollary 2.38. *Let g_1, g_2 be in M. The left-gcd (resp. left-lcm) of g_1 and g_2, 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 maximum (resp. minimum) of those of g_1 and g_2.*

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

Explicitly, if $\mathrm{cp}(g_1) = (a_1, \dots, a_n)$ and $\mathrm{cp}(g_2) = (b_1, \dots, b_n)$, then $\mathrm{cp}(g_1 \wedge g_2) = (\max(a_1, b_1), \dots, \max(a_n, b_n))$ and $\mathrm{cp}(g_1 \vee g_2) = (\min(a_1, b_1), \dots, \min(a_n, b_n))$.

Example 2.39. As in 2.10 take $S = \{s_1, s_2, s_3, s_4\}$ with

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

We have

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

Which can be understood in two ways:

- $\gcd(\Pi_2(s_1, s_3), \Pi_2(s_1, s_2)) = \Pi_1(s_1)$ as s_1 the only term appearing in both Π_2.
- The gcd of the two given matrices must have cp-tuple $(1, 0, 0, 0)$ (taking the minimal coefficient-power row by row), which uniquely exists by the I-structure.

Similarly:

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

can be understood as both:

- $\mathrm{lcm}(\Pi_2(s_1, s_3), \Pi_2(s_2, s_4)) = \Pi_4(s_1, s_2, s_3, s_4)$ (we took the maximum number of each occurences of each s_i, here always 1)
- The lcm of the two given matrices must have cp-tuple $(1, 1, 1, 1)$ (taking the maximal coefficient-power row by row), which uniquely exists by the I-structure.

The second description however does not provide an explicit description of the element, as we don't have the permutation part.

For the right gcd and lcm, we do the same on the columns, which has the disadvantage and not having something as explicit as the first-description of the left versions (see the $\tilde{\Pi}$ of [7] for a more detailled approach).

Corollary 2.40. *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 2.41. *An element of M is called a Garside element if it is balanced, $Div(g)$ is finite and generates M.*

Proposition 2.42 ([7])**.** *The unique element Δ such that $D_\Delta = diag(q, \dots, q)$ is a Garside element of M.*

Equivalently, $\Delta = \Pi_n(s_1, \dots, s_n)$ or $\mathrm{cp}(\Delta) = (1, \dots, 1)$.

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

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

Remark 2.43. The powers of Δ, which are the unique elements with cp-tuple $(k, \dots, k)$ for $k \geq 1$, are also Garside elements by the same reasoning.

More generally, Garside elements are precisely the balanced elements with no 1's.

Definition 2.44 ([9])**.** *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, $hg_1k = hg_2k \Rightarrow f = g$.

(ii) There exists a map Λ *to the integers such that* $\lambda(g_1g_2) \geq \lambda(g_1)+\lambda(g_2)$ *and* $\lambda(g) = 0 \Rightarrow g = 1$.
(iii) Any two elements have a gcd and lcm relative to both $\preceq$ *and* $\preceq_r$.
(iv) It possesses a Garside element Δ.

Proposition 2.45 ([7])**.** *M is a Garside monoid.*

Proof. The map λ previously defined satisfies point (ii) (and in fact as an equality).

For (iii) we have Corollary 2.38 and for (iv) Proposition 2.42.

We are left to prove (i), which is a direct consequence of Corollary 2.23 (alternatively, we can see this is that our elements are monomial matrices, such inject into the linear group $\mathrm{GL}_n(\mathbb{Q}[q,q^{-1}])$ from which we deduce the cancellative property). □

2.5. **Germs**

In [7] Dehornoy associates a germ to structure groups of cycle sets, in the construction he uses the non-degeneracy of finite cycle sets. Here we provide proofs that do not rely on this property. In particular the direct existence of Dehornoy's class is obtained along with a better bound (again improved in the next section). Moreover, we state an exchange lemma and a solution to the word problem, as is known in the context of Coxeter groups.

Recall that we fix $(S,*)$ a finite cycle set of size n with structure monoid (resp. group) M (resp. G). For $s \in S$ and $k \in \mathbb{N}$ denote by $s^{[k]}$ the unique element in M such that $D_{s^{[k]}} = D_s^k$, i.e. $s^{[k]} = \Pi_k(s,\dots,s) = sT(s)\dots T^{k-1}(s)$ where T is the diagonal map $s \mapsto s * s$.

Proposition 2.46. *There exists a positive integer* d *such that for all* $s_i \in S$, $s_i^{[d]}$ *is diagonal, i.e.* $P_{s_i^{[d]}} = Id$.

The smallest 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 most would work for any multiples.

Proof. First fix $s \in S$. The map sending $s^{[k]}$ to $\psi(s^{[k]})$ is a map from an infinite (countable) set to a finite one ($\mathfrak{S}_n$), therefore it is not injective. So there exists $k_1, k_2 \in \mathbb{N}$ such that $P_{s^{[k_1]}} = P_{s^{[k_2]}}$. We can assume $k_1 > k_2$ without loss of generality. We have $s^{[k_1]}(s^{[k_2]})^{-1} = D_s^{k_1-k_2}$ which is in G, and as $k_1 - k_2 > 0$ is also in M (it is $\Pi_{k_1-k_2}(s,\dots,s)$), so it is necessarily equal to $s^{[k_1-k_2]}$ which is thus diagonal.

Doing this for all $s_i \in S$, we get the existence of $d_i \in \mathbb{N}$ such that $s_i^{[d_i]}$ is diagonal. Notice that again, by the same argument, we must have for all $k \in \mathbb{N}$ $(s_i^{[d_i]})^k = D_{s_i}^{kd_i} = s_i^{[kd_i]}$. Taking $d = \mathrm{lcm}(d_1,\dots,d_n)$ we have for all i the existence of $d_i' > 0$ such that $d = d_i d_i'$, we find that for all i, $s_i^{[d]} = (s_i^{[d_i]})^{d_i'}$ is diagonal. □

Remark 2.47. In [7], the author gives 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 $d = \mathrm{lcm}(d_1,\dots,d_n)$ with $d_i \leq n!$). This bound will be improved in Propositions 3.10 and 3.11.

Proposition 2.48. *Let* d *be the class of* S *and denote by* $G^{[d]}$ *the subgroup of* G *generated by all the* $s^{[d]}$. *Then* $G^{[d]}$ *is a normal subgroup of* G.

Proof. The generators of $G^{[d]}$ are diagonal, thus this subgroup consists of diagonal matrices only. Conjugating a diagonal matrix D by a permutation matrix is diagonal, thus for all g in G, $(D_gP_g)D(P_g^{-1}D_g^{-1}) = {}^{\psi(g)}D$. Because the subgroup contains all possible diagonal matrix with coefficients powers of q^d, it is stable by the action of $\mathfrak{S}_n$ by permutation, so $\forall h \in G^{[d]}$, $ghg^{-1} \in G^{[d]}$. □

We define the quotient group $\overline{G}$ by $\overline{G} = G/G^{[d]}$.

Proposition 2.49 ([7])**.** *The projection $\pi\colon G \to \overline{G}$ amounts to adding to the presentation of G the relations $s^{[d]} = 1$, more precisely quotienting is the same as specializing at $q = \exp(\frac{2i\pi}{d})$ noted ev_q.*

Moreover, the map $\pi \circ \Pi\colon \mathbb{Z}^S \to \overline{G}$ induces a (set) bijection $\overline{\Pi}\colon (\mathbb{Z}/d\mathbb{Z})^S \to \overline{G}$.

Proof. The first part comes from the fact that $G^{[d]}$ is generated by the $s^{[d]}$ which are diagonal, and as each element containing a coefficient-power greater than d is a multiple of some $s_i^{[d]}$ by Proposition 2.35, we see that quotienting is just specializing at $q = \exp(\frac{2i\pi}{d})$.

The second part then follows as (canonical representative of) elements of $\overline{G}$ have non-zero coefficients in $\{1, q, \dots, q^{d-1}\}$. □

Remark 2.50. If $d = 1$ then $G^{[d]} = G$ 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. So we will assume $d \geq 2$, but this unique trivial case can still be included as all our results work for any multiples of the class (thus any positive integer for the trivial cycle set).

From now on, assume $d \geq 2$.

Example 2.51. Let $S = \{s_1, \dots, s_n\}$ with $\psi(s_i) = (12 \dots n) = \sigma$ for all i. Then for any $s \in S$, $k \in \mathbb{Z}$: $s_i^{[k]} = D_s^k P_{\sigma^k}$. 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 $\overline{s_i} = \mathrm{diag}(1, \dots, \zeta_n, \dots, 1)P_\sigma$.

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:

Lemma 2.52. *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 $s^{[kd]} = (s^{[d]})^k$ is diagonal, thus we could also consider the germ $G/\langle s^{[kd]} \rangle_{s \in S} \rangle$. The embedding $\iota_d^{dk}(\overline{G})$ can then be seen as embedding the germ $\overline{G}$ is this bigger quotient group.

Definition 2.53. *[7] If (M, Δ) be a Garside monoid and G 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 2.54 ([7])**.** *The specialization ev_q that imposes $q = \exp(\frac{2i\pi}{d})$ 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 $q^k \in \mathbb{Q}[q]$ for $1 \leq k < d$. It trivially satisfies $\mathrm{ev}_q \circ \chi = \mathrm{Id}_{\overline{G}}$. Its image is the elements of M such that each coefficient-power (the power of q) is strictly less than d, and thus identifies with $\mathrm{Div}(\Delta^{d-1})$ by the characterization of divisibility. And the presentation amounts to forgetting that q 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 2.55. *The projection $ev_q\colon M \to \overline{G}$ is surjective.*

Proof. G is generated by the s_i (positive generators) and their inverses s_i^{-1} (negative generators), so the same holds for $\overline{G}$. Moreover, as $\overline{G}$ is finite, inverses can be obtained from only positive generators. Finally, because $M \hookrightarrow G$ as the submonoid generated by positive generators, we obtain the statement. □

Example 2.56. Let $S = \{s_1, \dots, s_n\}$ with $\psi(s_i) = (12 \dots n) = \sigma$ for all i. Then for any $s \in S$, $k \in \mathbb{Z}$: $s_i^{[k]} = D_s^k P_{\sigma^k}$. The Dehornoy's class of S is n and $\overline{G}$ is generated by the $\overline{s_i} = \mathrm{diag}(1, \dots, \zeta_n, \dots, 1) P_\sigma$ 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 q is a root of unity in the following sense: when computing the product of two elements and finding a coefficient q^a with $a > d$, we do not use that $q^d = 1$ and just consider it as a new element. So for instance in $\langle \chi(\overline{G}) \rangle$ with $n = 4$:

$$\chi\left(\overline{s_1^{[3]}}\right)\chi\left(\overline{s_4^{[2]}}\right) = \chi(\overline{s_1}^{[3]})\chi(\overline{s_4}^{[2]}) = \begin{pmatrix} 0 & 0 & 0 & q^3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & q^2 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & q^5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = s_1^{[5]}.$$

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

The quotient group $\overline{G}$ defined above is called a Coxeter-like group, it was first studied by Chouraqui and Godelle in [6] for $d = 2$ and generalized by Dehornoy in [7].

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).

Proposition 2.57. *$\overline{G}$ is permutation-free.*

Proof. From Proposition 2.29, we know that G is permutation-free. As $\overline{G}$ is the image of G by the evaluation at $q = \zeta_d$, a matrix $\overline{g} \in \overline{G}$ is a permutation matrix if it comes from an equivalence class of $g \in M$ such that $\mathrm{cp}(g) = (da_1, \dots, da_n)$ (with $a_1, \dots, a_n \in \mathbb{N}$), i.e. $g = (s_1^{[d]})^{a_1} \dots (s_n^{[d]})^{a_n} = D_{s_1}^{da_1} \dots D_{s_n}^{da_n}$ which is diagonal, thus $\overline{g}$ is diagonal. □

Definition 2.58. *For $c = (\overline{c_1}, \dots, \overline{c_n}) \in (\mathbb{Z}/d\mathbb{Z})^n$, define $\overline{cp}(diag(q^{\overline{c_1}}, \dots, q^{\overline{c_n}}))$ to be the unique representative of c as $(c_1, \dots, c_n) \in \{0, \dots, d-1\}^n$. If $g \in \overline{G}$, we define $\overline{cp}(g)) = \overline{cp}(D_g)$.*

We define a function l_d by:

$$\forall k \in \{0, 1, \dots, d-1\}, l_d(k) = \begin{cases} k, & \text{if } k \leq \frac{d}{2} \\ k - d, & \text{if } k > \frac{d}{2}. \end{cases} \tag{7}$$

And we define $\overline{\lambda}(c) = \sum_{i=1}^{n} |l_d(c_i)|$.

Note that $\overline{\mathrm{cp}}$ corresponds to cp with the projection $\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$) and taking representatives in the interval $[0, d-1[\cap \mathbb{Z}$, while $\overline{\lambda}$ corresponds to λ with the same projection but with representatives in $]-\frac{d}{2}, \frac{d}{2}] \cap \mathbb{Z}$. The latter is chosen because, if we have $q^6 = 1$, the shortest way to write q^2 is $q \cdot q$ but to write q^4 we should use $q^{-1} \cdot q^{-1}$.

Proposition 2.59. *The followings hold:*

(i) For any $c = (\overline{c_1}, \dots, \overline{c_n}) \in (\mathbb{Z}/d\mathbb{Z})^n$, there exists a unique element $g \in \overline{G}$ such that $\overline{cp}(g) = c$.

(ii) The length of an element $g \in \overline{G}$ over $\overline{S} = \pi(S)$ is given by $\overline{\lambda}$

Proof. (i) follows from Proposition 2.57.

Point (ii) is obtained by realizing that the shortest way to write q^k for $k \in \{0, \dots, d-1\}$ is using $q \cdot \dots \cdot q$ is $k \leq \frac{d}{2}$ and otherwise we use the fact that $q^d = 1$ to write it as $q^{-1} \cdot \dots \cdot q^{-1}$. □

Corollary 2.60. *Because $\overline{G}$ is finite, the generators have finite order, so any element has a decomposition as a product of generators (we don't have to include inverses). Thus, any element in $\overline{G}$ has a $\overline{\Pi}$-expression (in the same sense as in M).*

Corollary 2.61. *Defining similarly to Σ_n the group $\overline{\Sigma_n}$ with non-zero coefficients powers of $\exp(\frac{2i\pi}{d})$, we get that a subgroup of $\overline{\Sigma_n}$ respecting the conditions of Proposition 2.33 is a Coxeter-like group.*

Remark 2.62. We say that a word in $\overline{S} = \pi(S)$ is reduced in $\overline{G}$ if it has length $\overline{\lambda}(w)$ when seen as an element of $\overline{G}$.

For instance, if $d > 2$ then $w = s(s * s)$ is reduced as it represents $\overline{\Pi_2}(s, s)$ which has $\lambda = 2$ but the word corresponding to $\overline{\Pi_d}(s, \dots, s)$ is not as it has $\overline{\lambda} = 0$. More generally, the word associated to $\overline{\Pi_r}((t_1), \dots, (t_r))$ is reduced in $\overline{G}$ if each $\overline{s}_i$ occurs strictly less than d times in the family (t_i).

For Coxeter groups, we have the so-called exchanging lemma (see [18]). We provide a similar result for Coxeter-like groups:

Lemma 2.63 (Exchange Lemma)**.** *Let $g \in \overline{G}$ be written as a reduced expression given by $\overline{\Pi_k}(t_1, \dots, t_k)$. For $s \in S$, if $\overline{\Pi_{k+1}}(s, t_1, \dots, t_k)$ is not reduced, then there exists some i such that $g = \overline{\Pi_k}(s, t_1, \dots, \hat{t_i}, \dots, t_k)$, where $\hat{t_i}$ means we omit t_i.*

Proof. As $\overline{\Pi_k}(t_1, \dots, t_k)$ is reduced, s occurs strictly less than d times in $(t_j)_{1 \leq j \leq k}$.

Thus, if $\overline{\Pi_{k+1}}(s, t_1, \dots, t_k)$ is not reduced as word, then s must occur exactly d times in $s \cup (t_j)_{1 \leq j \leq k}$, in particular as $d > 1$, s occurs at least once in $(t_j)_{1 \leq j \leq k}$, say $t_i = s$. Because $\overline{\Pi}$ is invariant by permutation of the entries (as Π is), we can move this t_i at the beginning and thus $g = \overline{\Pi_k}(s, t_1, \dots, \hat{t_i}, \dots, t_k)$. □

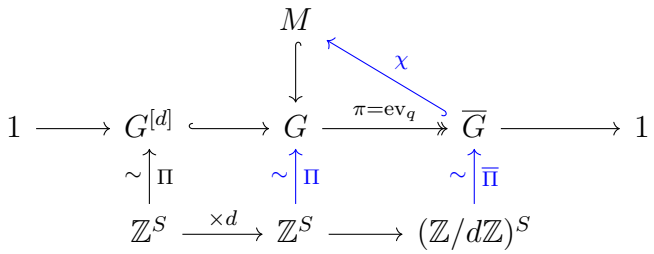
Another part of interest of the study of Garside groups is that they provide a solution to the word problem:

Proposition 2.64. *Two words $t = t_1 \dots t_k$ and $u = u_1 \dots u_l \in S^*$ represent the same element in M (resp. $\overline{G}$) if, when taking a Π-expression (resp. $\overline{\Pi}$-expression) of both, they have the same number of occurrences of each s_i, $1 \leq i \leq n$ (resp. modulo d).*

Proof. • In M, the elements corresponding to t and u have respectively a Π-expression of length k and l, and because Π is a bijection from $\mathbb{N}^n$ to M, they represent the same element iff they have the same number of occurrences of each of the atoms in $\mathbb{N}^n$. In particular, $k = l$.

• In $\overline{G}$, the same reasoning applies: take a $\overline{\Pi}$-expression of both elements, they represent the same equivalence class iff the number of occurrences of each atom is the same modulo d in $\mathbb{N}^n$, as the map $\overline{\Pi}\colon (\mathbb{Z}/d\mathbb{Z})^n \to \overline{G}$ is a bijection. □

We summarize all the previous results in the following diagram, where black arrows are morphism and blue arrows are just maps of sets, and the middle line is a short exact sequence.



Note that the left Π is a group morphism because all elements of $G^{[d]}$ have trivial permutation, so this group is abelian and thus Π is the morphism sending $(a_1, \dots, a_n)$ to $\mathrm{diag}(q^{da_1}, \dots, q^{da_n})$.

2.6. **Non-degeneracy**

Here we give a new proof of Rump's result on the non-degeneracy of finite cycle sets [19], that is the fact that $s \mapsto s*s$ is bijective; in Dehornoy's paper it is used to obtain the bijectivity of $(s,t) \mapsto (s*t, t*s)$. Here we prove both of those results using the previous section, the first proof has the advantage of being a simple direct consequence of the I-structure compared to the proof in [19] which involves several steps and constructions.

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

Lemma 2.65 ([19])**.** $\forall s, s' \in S, s*s = s'*s' \iff s = s'$.

Proof. If $s = s'*s'$ then trivially $s*s = s'*s'$. Suppose $s*s = s'*s'$, and consider $g = ss'^{-1}$, we want to show $g = 1$.

We have $g = ss'^{-1} = D_s P_s P_{s'}^{-1} D_{s'}^{-1}$, using that $P_\sigma D = {}^\sigma D P_\sigma$ and $P_\sigma^{-1} = P_{\sigma^{-1}}$ twice we find

$$g = D_s P_s D_{s'*s'}^{-1} P_{s'}^{-1} = D_s D_{\psi^{-1}(s)(s'*s')}^{-1} P_s P_{s'}^{-1}.$$

By assumption $s*s = s'*s'$ thus $g = D_s D_{\psi^{-1}(s)(s*s)}^{-1} P_s P_{s'}^{-1} = D_s D_s^{-1} P_s P_{s'}^{-1} = P_s P_{s'}^{-1}$. As G_S is permutation-free, we deduce $g = 1$. □

Proposition 2.66. *(i) The diagonal map $T : s \mapsto s*s$ is a bijection of S.*

(ii) The order o of T divides d. In particular, for any integer k, we have $s^{[kd]} = (sT(s)\dots T^{o-1}(s))^k$.

(iii) More generally $s^{[k]} = sT(s)\dots T^{o-1}(s)sT(s)\dots$ with exactly k terms

Proof. As S is finite and T is injective by the previous lemma, it is bijective and so has finite order. The third point follows directly from the equalities $s^{[k]} = \Pi_k(s, \dots, s) = sT(s)\dots T^{k-1}(s)$ and, as $T^o(s) = s$, we regroup as many words $sT(s)\dots T^{o-1}(s)$ as possible. For the second point, if $s^{[k]}$ is diagonal, then $s^{[k]}s = D_s^k D_s P_s$ which has diagonal part D_s^{k+1} so must be $s^{[k+1]}$. As $s^{[d+1]} = s^{[d]}T^d(s)$, we deduce $T^d(s) = s$, thus $o = o(T)$ divides d. □

Corollary 2.67. *Let G^t be the set of transposes of the elements of G. Then G^t is the structure group of a cycle set structure on S^t.*

Proof. First note that, because G is generated by S, G^t is generated by S^t. As T is a bijection, for each i the set S^t contains exactly one element s^t such that $D_{s^t} = D_i$, that is $s = T^{-1}(s_i)$. Moreover, as G is permutation-free, so is G^t. So by Theorem 2.33 it is the structure group of the cycle set S^t. □

In particular, this can be used to work on the columns in G: if we want an element of G with coefficient powers tuple $(a_1, \dots, a_n)$ on the columns, we can work in G^t, use the Π of Dehornoy's calculus to obtain an elements g^t in G^t with $\mathrm{cp}(g^t) = (a_1, \dots, a_n)$ and transpose it to get g in G with q^{a_i} on the i-th column.

Proposition 2.68. *For any $k \in \mathbb{N}$, $\psi(s^{[k]})(s) = T^k(s)$. In particular, the map $s \mapsto \psi(s^{[k]})(s)$ is a bijection of S.*

Proof. For $k = 0$, $s^{[0]} = 1$ so both sides of the equality are s. For $k = 1$, this is just the definitions $\psi(s)(s) = s * s = T(s)$. Now proceed by induction:

Recall that, by Proposition 2.19,

$$\psi(s^{[k+1]})(s) = \left(\psi(T^k(s)) \circ \psi(T^{k-1}(s)) \circ \cdots \circ \psi(s)\right)(s) = \psi(T^k(s))(\psi(s^{[k]})(s)).$$

So by the induction hypothesis $\psi(s^{[k+1]})(s) = \psi(T^k(s))(T^k(s)) = T^k(s) * T^k(s) = T^{k+1}(s)$.

As T is a bijection, so is T^k. □

Corollary 2.69. *For k in $\mathbb{N}$ and s in S, let $t = (T^k)^{-1}(s)$ then $s^{[-k]} = \Pi_k(t, \dots, t)^{-1}$.*

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

$$(t^{[k]})^{-1} = (D_t^k P_{t^{[k]}})^{-1} = P_{t^{[k]}}^{-1} D_t^{-k} = {}^{\psi(t^{[k]})^{-1}}D_t^{-k} P_{t^{[k]}}^{-1} = D^{-k}_{\psi(t^{[k]})(t)} P_{t^{[k]}}^{-1} = D^{-k}_{T^k(t)} P_{t^{[k]}}^{-1}.$$

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

Proposition 2.70 ([7])**.** *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, i.e. assume $s*t = s'*t'$ and $t * s = t' * s'$ for some $s, t, s', t' \in S$.

Since $\Pi_2(s, t) = s(s * t) = t(t * s) = \Pi_2(t, s)$, we get $\Pi_2(s, t)\Pi_2(s', t')^{-1} = s(s * t)(s' * t')^{-1} s'^{-1} = ss'^{-1}$ by hypothesis and then as previously $ss'^{-1} = D_s D^{-1}_{\psi^{-1}(s)(s'*s')} P_s P_{s'}^{-1}$.

We also have $\Pi_2(s, t)\Pi_2(s', t')^{-1} = \Pi_2(t, s)\Pi_2(t', s')^{-1} = tt'^{-1} = D_t D^{-1}_{\psi^{-1}(t)(t'*t')} P_t P_{t'}^{-1}$.

By unicity of the diagonal part, we must have $D_s D^{-1}_{\psi^{-1}(s)(s'*s')} = D_t D^{-1}_{\psi^{-1}(t)(t'*t')}$, i.e. $D_s D_{\psi^{-1}(t)(t'*t')} = D_t D_{\psi^{-1}(s)(s'*s')}$. Because each term on each side corresponds to a diagonal matrix with only one q, we have either $D_s = D_t$ and so $t' = s'$ by the previous lemma, or $s = \psi^{-1}(s)(s' * s')$, thus $s * s = s' * s'$ and again by the previous lemma $s = s'$, so $ss'^{-1} = 1 = tt'^{-1}$ and finally $t = t'$. In both cases, we are done. □

Proposition 2.71. *Any element $g \in G$ can be decomposed as a reduced right-fraction in M, that is:*

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

Proof. The proof is essentially the same as in Proposition 2.24. Take a reduced decomposition of g as product of elements in $S \cup S^{-1}$, the defining relations of G give

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

From the previous proposition, for any couple $(s', t') \in S^2$ there exists (s, t) such that $(s*t, t*s) = (s', t')$, thus we can inductively use the relations $s't'^{-1} = (s*t)(t*s)^{-1} = s^{-1}t$ to "move" all inverses of the generators to the left in a decomposition of g, which gives the desired form. □

From Propositions 2.24 and 2.71 we deduce:

Corollary 2.72 ([7])**.** *G is the group of fractions of M.*

This also implies that G is a Garside group.

3. Bounding of the Dehornoy's class

We fix a finite cycle set $(S, *)$ of size n with structure monoid (resp. group) M (resp. G), of Dehornoy's class $d > 1$ and associated germ $\overline{G}$.

Definition 3.1. *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 $\psi(gh) = \psi(h)\psi(h)$, thus an antimorphism. This won't pose problem here, as we'll only use $\psi(s^n) = \psi(s)^n$.

Definition 3.2 ([2])**.** *A subset X of S is said to be $\mathcal{G}$-invariant if for every $s \in S$, $\psi(s)(X) \subset X$. S is called decomposable if there exists a proper partition $S = X \sqcup Y$ such that X, Y are $\mathcal{G}_S$-invariant.*

In this case $(X, *_{|_X})$ and $(Y, *_{|_Y})$ are also cycle sets.

A cycle set that is not decomposable is called indecomposable.

Example 3.3. For $S = \{s_1, s_2, s_3, s_4\}$ and $\psi(s_1) = \psi(s_2) = (2143)$, $\psi(s_3) = \psi(s_4) = (2134)$, we have $\mathcal{G} = \langle (2143), (2134) \rangle < \mathfrak{S}_n$. 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 $\psi_Y(s_3) = \psi_Y(s_4) = (34)$.

In personal communications [20], the following conjecture was mentionned:

Conjecture 3.4 ([20])**.** *If S is indecomposable then $d \leq n$.*

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

Using a python program based on the proof of Proposition 2.46, we find the following maximum values of the class of cycle sets of size n:

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

This corresponds to the OEIS sequence A034893 *"Maximum of different products of partitions of n into distinct parts"*, studied in [10] where the following is proved:

Lemma 3.5 ([10])**.** *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 3.6. *The class d of S is bounded above by a_n and the bound is minimal.*

Note that the set map $\Pi \colon \mathbb{Z}^n \to G$ allows us to transport the abelian group structure of $\mathbb{Z}^n$ to G as follows:

Proposition 3.7. *There exists a commutative group structure on G denoted $(G, +)$ such that for all g, h in G, $g + h$ is the unique element such that $D_{g+h} = D_g D_h$.*

Proof. This is a direct consequence of Theorem 2.29. □

This structure corresponds to the structure of left braces, see for instance [5].

Proposition 3.8. *There exist g', h' in G such that $g + h = gh' = hg'$ with $D_{h'} = {}^{g^{-1}}D_h$ and $D_{g'} = {}^{h^{-1}}D_g$.*

Moreover, if g, h are in M with $g = \Pi_k(t_1, \dots, t_k)$ and $h = \Pi_l(u_1, \dots, u_l)$ then $g + h = \Pi_{k+l}(t_1, \dots, t_k, u_1, \dots, u_l)$, and g', h' are in M.

Proof. By definition $g + h = D_g D_h P_{g+h}$. Let $h' = g^{-1}(g + h)$ then $h' = P_g^{-1} D_h P_{g+h} = {}^{g^{-1}}D_h P_g^{-1} P_{g+h}$, thus $D_{h'} = {}^{g^{-1}}D_h$ by the unicity of monomial left-decomposition. And similarly for g' using $g + h = h + g$.

For the second part, the Π-expression is a consequence of Proposition 2.9. Then, by the first statement g' (resp. h') only has non-negative coefficient-powers iff g (resp. h) does, which is equivalent to being in M. □

Proposition 3.9. *The additive commutative structure $(M, +)$ induces an abelian group structure on $\mathcal{G}$ compatible with the map $\psi : M \to \mathcal{G}$.*

Proof. Let σ, τ be in $\mathcal{G}$ and g, h in M such that $\psi(g) = \sigma$ and $\psi(h) = \tau$ (i.e. $P_g = P_\sigma$, $P_h = P_\tau$). We will show that P_{g+h} does not depend on g and h but only on σ and τ, so that $\sigma + \tau$ is well-defined as $\psi(g + h)$.

By the commutativity of $(M, +)$, it suffices to show that $\sigma + \tau$ does not depend on the choice of the representative g of σ. From Proposition 3.8 we have the existence of h' in M such that $g + h = gh'$ and $D_{h'} = {}^{g^{-1}}D_h$ which only depends on h and $P_g = P_\sigma$. As h' is uniquely determined by $D_{h'}$, it does not depend on the choice of g, so neither does $P_{h'}$. Finally, we have that $P_{g+h} = P_g P_{h'}$ is the product of terms only depending on $\sigma = \psi(g)$. □

As a consequence we obtain the following result:

Proposition 3.10 ([5])**.** *The class d divides the order of $\mathcal{G}$. In particular d divides $n!$.*

Proof. For $s \in S$, the set $\{s^{[k]} \mid k \in \mathbb{Z}\}$ is a subgroup of $(G, +)$, and the smallest integer d_s such that $s^{[d_s]}$ is diagonal corresponds to the order of $\psi(s)$ in $(\mathcal{G}, +)$, which thus divides $|\mathcal{G}|$.

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

The landau function $g\colon \mathbb{N}^* \to \mathbb{N}^*$ ([15]) is defined as the largest order of a permutation in $\mathfrak{S}_n$.

Proposition 3.11. *If S is square-free and $\mathcal{G}$ abelian then $d \leq a_n$*

That is, under these conditions the bound part of Conjecture 3.6 holds.

Proof. If S is square-free, then for all $s \in S$ we have by definition $T(s) = s$, so for any $k \in \mathbb{Z}$, $s^{[k]} = sT(s) \dots T^{k-1}(s) = s^k$ so $\{s^{[k]} \mid k \in \mathbb{Z}\}$ is a subgroup of $(G, \cdot)$ and the smallest integer d_s such that $s^{[d_s]}$ is diagonal corresponds to the order of $\psi(s)$ in $(\mathcal{G}, \cdot)$, which thus divides $e(\mathcal{G})$ 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 in disjoint cycles, $g(n)$ is equal to the maximum of the lcm of partitions of n:

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

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 set is bounded above by the product of the elements, we have $g(n) \leq a_n$. Thus $d \leq g(n) \leq a_n$. □

Proposition 3.12. *The followings hold:*

(i) $\psi\colon G \to \mathcal{G}$ *factorizes through the projection* $G \to \overline{G}$

(ii) We have the following divisibilities:

- $o(T) \mid d$
- $d \mid \#\mathcal{G}$
- $\#\mathcal{G} \mid d^n$

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).*

Proof. (i) follows from the definition of d as $\psi(s^{[d]}) = \mathrm{id}$.

For (ii), the first divisibility is Proposition 2.66, the second is Proposition 3.10 and the third is (i). □

For a positive integer k, denote by $\pi(k)$ the set of divisors of k.

Corollary 3.13. *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 divide $\#\mathcal{G}$ 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 3.14. *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 [12] 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 3.15. *If* S *is indecomposable and* $\mathcal{G}$ *is abelian, then* $n = |\mathcal{G}|$

Proof. [a] Again by [12] 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. □

• Let $k \geq 1$ and $G^{[k]}$ be the subgroup of G generated by $S^{[k]} = \{s^{[k]} \mid s \in S\}$. The following result was simultaneously introduced in [16]:

Proposition 3.16. *For* ≥ 1, $G^{[k]}$ *induces a cycle set structure on* $S^{[k]}$.

Proof. Recall that $\psi(s^{[k]})(t) = \Omega_{k+1}(s, \ldots, s, t)$ for all $s, t \in S$, and note that

$$s^{[k]}t^{[k]} = D_s^k P_{s^{[k]}} D_t^k P_{t^{[k]}} = D_s^k \left({}^{s^{[k]}}D_t^k \right) P_{s^{[k]}} P_{t^{[k]}} = D_s^k D^k_{\psi(s^{[k]})^{-1}(t)} P_{s^{[k]}} P_{t^{[k]}}.$$

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

For all $s^{[k]}, t^{[k]} \in S^{[k]}$, define $s^{[k]} \star t^{[k]}$ as $\Omega_{k+1}(s, \dots, s, t)^{[k]}$. Then we have

$$s^{[k]}(s^{[k]} \star t^{[k]}) = D_s^k D^k_{\psi(s^{[k]})^{-1}(s^{[k]} \star t^{[k]})} P_{s^{[k]}} P_{t^{[k]}} = D_s^k D_t^k P_{s^{[k]}} P_{t^{[k]}}.$$

By symmetry, we have that $D_{s^{[k]}(s^{[k]} \star t^{[k]})} = D_{t^{[k]}(t^{[k]} \star s^{[k]})}$. Thus as G is permutation-free we conclude that $s^{[k]}(s^{[k]} \star t^{[k]}) = t^{[k]}(t^{[k]} \star s^{[k]})$.

All generators satisfy the conditions of Theorem 2.33 with $D_{s_i} = D_i^k$ so $(S^{[k]}, \star)$ is a cycle set. □

Remark 3.17. Alternatively, one can directly show that $\star$ satisfies Equation (1): let $s, t, u \in S$, then we have
$(s^{[k]} \star t^{[k]}) \star (s^{[k]} \star u^{[k]}) = \Omega_{k+1}(s, \dots, s, t)^{[k]} \star \Omega_{k+1}(s, \dots, s, u)^{[k]}$
$= \Omega_{k+1}(\Omega_{k+1}(s, \dots, s, t), \dots, \Omega_{k+1}(s, \dots, s, t), \Omega_{k+1}(s, \dots, s, u))^{[k]}$.

By definition of Ω (see [7] eq 4.8), the two expressions $\Omega_{p+q}(x_1, \dots, x_p, y_1, \dots, y_q)$ and $\Omega_q(\Omega_{p+1}(x_1, \dots, x_p, y_1), \dots, \Omega_{p+1}(x_1, \dots, x_p, y_q))$ coincide. Thus $(s^{[k]} \star t^{[k]}) \star (s^{[k]} \star u^{[k]}) = \Omega_{2k+1}(s, \dots, s, t \dots, t, u)$. As Ω is invariant by permutation all but the last coordinate, we have $\Omega_{2k+1}(s, \dots, s, t, \dots, t, u) = \Omega_{2k+1}(t, \dots, t, s, \dots, s, u)$. Thus, we conclude that: $s^{[k]} \star t^{[k]}) \star (s^{[k]} \star u^{[k]}) = (t^{[k]} \star s^{[k]}) \star (t^{[k]} \star u^{[k]})$.

Proposition 3.18. *Let k be a positive integer smaller than d, then $(S^{[k]}, \star)$ is of class $\frac{d}{gcd(d,k)}$.*

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

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

Proof. Recall that $(s^{[k]})^{[j]} = s^{[kj]}$. Thus $(s^{[k]})^{[a]}$ is diagonal when ka is a multiple of d, so we deduce that $S^{[k]}$ is of class $\frac{\mathrm{lcm}(d,k)}{k} = \frac{d}{\gcd(d,k)}$.

By definition of d, we have that $(S^{[d]}, \star)$ is the trivial cycle set ($\psi(s) = \mathrm{id}$), thus $\psi(s^{[d+1]}) = \psi(s)$. □

4. Sylow subgroups and decomposition

Recall that for $k > 1$, Σ_n^k denotes the group of monomial matrices with non-zero coefficients powers of ζ_k, and 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 cycle set can be obtained as a Zappa–Szép product of cycle sets with coprime classes.

Definition 4.1. *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 ([17]) 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 $gh = h'g'$.

Remark 4.2. 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 ([17], 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 4.3. *S_1 and S_2 are said to be $\bowtie$-compatible if $\overline{G}$ is the structure group of some cycle set $S_1 \bowtie S_2$, called the Zappa–Szép product of S_1 and S_2.*

We now 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 $s^{[k]_2}$ will denote an element of M_2.

Algorithm 1 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: Set a
3: **for** $i = 1$ to n **do**
4: Compute $g_1 = s_i^{[u]_1} \in \overline{G}_1$
5: Let $\sigma = \psi_1(s_i^{[u]})$
6: Compute $g_2 = s_{\sigma(i)}^{[v]_2} \in \overline{G}_2$
7: Let $\psi(s_i)$ be the permutation part of $\iota_{d_1}^d(g_1)\iota_{d_2}^d(g_2)$
8: **return** $S_1 \bowtie_d S_2 = (S, *)$ with $s_i * s_j = s_{\psi(s_i)(j)}$.

Remark 4.4. The heart of the algorithm is lign 6 which relies on the following

$$D_i^k P_\sigma D_j^l P_\tau = D_i^k D_{\sigma^{-1}(j)}^l P_{\tau\sigma}.$$

To obtain an element with coefficient-powers 1 on the i-th coordinate and zero elsewhere, we have to take $j = \sigma(i)$ with here $\sigma = \psi(s_i^{[k]_1})$ and as we apply ι^d on the elements (in S_1 this does $q \mapsto q^{d_2}$ and in S_2 $q \mapsto q^{d_1}$), we obtain $D_{s_i} = D_i^{d_2 u + d_1 v} = D_i$ from lign 1.

Example 4.5. Take two cycle sets of size $n = 5$ and class respectively 2 and 3, and apply Algorithm 1 providing a candidate for a cycle set of class 6:

Let $S_1 = \{s_1', \ldots, s_5'\}$ and $S_2 = \{s_1'', \ldots, s_5''\}$, with $(S_1, \psi_1), (S_2, \psi_2)$ given by:

$$\psi_1(s_1') = \psi_1(s_3') = (1234) \qquad \psi_1(s_2') = \psi_1(s_4') = (1432) \qquad \psi(s_5') = \mathrm{id}$$
$$\psi_2(s_1'') = \psi_2(s_2'') = (354) \qquad \psi_2(s_3'') = \psi_2(s_4'') = \psi_2(s_5'') = (345)$$

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 define $\overline{G} = \overline{G}_1 \bowtie_6 \overline{G}_2$ over the basis $S = \{s_1, \ldots, s_5\}$. For instance:

$$\iota_2^6(s_1') = \iota_2^6\left(\begin{pmatrix} 0 & \zeta_2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\right) = \begin{pmatrix} 0 & \zeta_6^3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\iota_3^6(s_1'') = \iota_3^6\left(\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&\zeta_3\\0&0&1&0&0\\0&0&0&1&0\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&\zeta_6^2\\0&0&1&0&0\\0&0&0&1&0\end{pmatrix}$$

To construct an element $g \in \overline{G}$ with $\overline{\mathrm{cp}}(g) = (0,0,1,0,0)$ 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 $\iota_2^6(s_i'^{[1]})$ and $\iota_2^6(s_j''^{[2]})$ so that their product has coefficient-powers $(0,0,3*1+2*2,0,0) = (0,0,1,0,0)[6]$. Recall that:

$$D_i^k P_\sigma D_j^l P_\tau = D_i^k D_{\sigma^{-1}(j)}^l P_{\tau\sigma}.$$

Here we want $i = \sigma^{-1}(j) = 3$, $k = 3u$ and $l = 2v$, so we take $i = 3$. As $\sigma = \psi(s_3'^{[1]}) = \psi(s_3') = (1234)$, we have $j = \sigma(3) = 4$, and note that $s_4''^{[2]} = s_4''s_5''$. Finally:

$$\iota_2^6(s_3')\iota_3^6(s_4''^{[2]}) = \begin{pmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&\zeta_6^{3\cdot 1}&0\\1&0&0&0&0\\0&0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&\zeta_6^{2\cdot 2}&0&0\\0&0&0&1&0\end{pmatrix}$$

$$= \begin{pmatrix}0&1&0&0&0\\0&0&0&0&1\\0&0&\zeta_6^{3+4}&0&0\\1&0&0&0&0\\0&0&0&1&0\end{pmatrix} = \begin{pmatrix}0&1&0&0&0\\0&0&0&0&1\\0&0&\zeta_6&0&0\\1&0&0&0&0\\0&0&0&1&0\end{pmatrix}$$

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 permutation-free or in Dehornoy's Calculus terms: with our candidates s_1, s_2 we have that $\Pi_2(s_1, s_2)$ and $\Pi_2(s_2, s_1)$ both have coefficient-powers $(1,1,0,0,0)$ but different permutations.

Proposition 4.6. *If $\overline{G}_1$ and $\overline{G}_2$ commute, then S_1 and S_2 are $\bowtie$-compatible.*

In this case, $G = \overline{G}_1 \bowtie_d \overline{G}_2$ is the Zappa–Szép product of $\overline{G}_1$ and $\overline{G}_2$.

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

By ([17], 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. $\overline{G} = \overline{G}_1 \bowtie_d \overline{G}_2 = \overline{G}_2 \bowtie_d \overline{G}_1$. As $\overline{G}_1$ and $\overline{G}_2$ have different (non-zero) coefficient-powers, a product g_1g_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 1, we know that $\overline{G}$ respects condition (ii) for Theorem 2.33, and we've seen it also satisfies condition (i), finishing the proof. □

Remark 4.7. To check whether $\overline{G}_1$ and $\overline{G}_2$ commute, we can restrict to the generators and check that:

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

Proposition 4.8. *If S_1 and S_2 satisfy the following "mixed" cycle set equation*

$$\forall s,t,u \in S, (s *_1 t) *_2 (s *_1 u) = (t *_2 s) *_2 (t *_2 u) \tag{8}$$

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

Explicitly, from Algorithm 1, we have $\psi(s_i) = \psi_2\left(s''^{[v]_2}_{\psi_1(s_i'^{[u]})(i)}\right) \circ \psi_1\left(s_i'^{[u]_1}\right)$ with u, v such that $d_2u + d_1v = 1[d_1d_2]$.

Proof. We will use the previous proposition and show how Equation 8 naturally arises from considering the commutativity of the germs.For clarity, although our two cycle sets have the same underlying set $S = \{s_1, \dots, s_n\}$, 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:

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

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 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 $P_\sigma P_\tau = P_{\tau\sigma}$, the last condition 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, so all this becomes equivalent to:

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

□

Remark 4.9. 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 $\iota_{d_2}^d$ is the identity and $\iota_{d_1}^d$ 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 [4] 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 3.16, given $k > 0$ diving d, the subgroup $\overline{G}^{[k]}$ generated by $S^{[k]} = \{s^{[k]} \mid s \in S\}$ is the germ of a structure group, and has for elements the matrices whose coefficient-powers are multiples of k.

Lemma 4.10. *Let $\beta_i = \frac{d}{\alpha_i}$ then*

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

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

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

Proof. Fix $1 \leq i \leq r$, as β divides d, the group $\overline{G}^{[\beta_i]}$ corresponds to the subgroup of $\overline{G}$ of matrices with coefficient-powers in $\{0, \beta_i, 2\beta_i, \dots, \beta_i(\alpha_i - 1)\}$ and thus has cardinal $\alpha_i^n = p_i^{a_i n}$, so it is a p_i-Sylow subgroup of $\overline{G}$.

For $s, t \in S$ we have that $s^{[\beta_i]}t^{[\beta_j]}$ has a q^{β_j} on some row, thus is left-divisible by $t'^{[\beta_j]}$ for some $t \in S$, i.e. $s^{[\beta_i]}t^{[\beta_j]} = t'^{[\beta_j]}s'^{[\beta_i]}$ for some $s' \in S$.

We've seen that the $\overline{G}^{[\beta_i]}$ are p_i-Sylow subgroups of the abelian group $(\overline{G}, +)$, so by cardinality it is the direct sum of those subgroups. By Proposition 3.8 for any $g, h \in G$, there exists $h' \in G$ such that $g + h = gh'$, where $D_{h'} = {}^{g^{-1}}D_h$, so if h is in some $G^{[k]}$, so is h'. Projecting onto $\overline{G}$, we have that any element g can be expressed as a sum of $g_i \in \overline{G}^{[\beta_i]}$ and thus a product of $g_i' \in \overline{G}^{[\beta_i]}$. □

Example 4.11. 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 $\overline{G}^{[3]} \bowtie_6 \overline{G}^{[2]}$ of its 2- and 3- Sylow. If we denote by (S_2, ψ_2) and (S_3, ψ_3) their respective cycle set structure 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

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

Lemma 4.10 can be rephrased as $\overline{G} = \overline{G}^{[\beta_1]} \bowtie_d \dots \bowtie_d \overline{G}^{[\beta_r]}$. 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 constructing all solutions of a given size.

Theorem 4.12. *Any cycle set can be obtained as the Zappa–Szép product of cycle sets of class a prime power.*

Proof. Any cycle set is determined by its structure monoid, which can be recovered from the germ. By Lemma 4.10 and the above construction, the germ can be decomposed and reconstructed from its Sylows, which also determine cycle set by Proposition 3.16. □

Remark 4.13. The class of the cycle set constructed will Algorithm 1 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 $s^{[d_1 d_2]}$ is diagonal, but it is not necessarily minimal.

Remark 4.14. This construction is similar to the matched product of braces $B_1 \bowtie B_2$ appearing in [1, 3]. Key differences are that we directly construct a cycle set with

permutation group $B_1 \bowtie B_2$ (whereas the authors of [3] construct one over the set $B_1 \bowtie B_2$) and that our construction doesn't rely on groups of automorphisms thanks to the natural embedding ι_k^{kl}. Moreover, instead of classifying all braces, the existence of the germs suggests it is enough to classify braces with abelian group $(\mathbb{Z}/d\mathbb{Z})^n$ for all d and n to recover all cycle-sets.

Corollary 4.15. *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.*

Proof. Let S be obtained from the 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, so with class dividing the class $p_i^{a_i}$ of S_i, thus also a power of p_i. By Lemma 3.14, 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 4.16. 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 $S^{[2]}$ and $S^{[3]}$ 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 4.17. In Example 4.11, 3 does not divide 8 so S_3 has to be decomposable, and indeed it decomposes as $S_3 = \{s_1'', s_3'', s_5''\} \sqcup \{s_2'', s_4'', s_6''\} \sqcup \{s_7'', s_8''\}$.

Corollary 4.18. *Let $N(n, d)$ be the number of cycle sets of size n and of class a divisor of $d = p_1^{a_1} \dots p_r^{a_r}$. Then we have: $N(n, d) \leq \prod_i N(n, p_i^{a_i})$.*

For $n = 10$, we find that there is approximately 67% of cycle sets that have class a prime-power (~ 3.3 out of ~ 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 (Conjecture 3.6).

References

[1] D. Bachiller. "Extensions, Matched Products, and Simple Braces". *Journal of Pure and Applied Algebra* 222 (2018), 1670–1691.

[2] P. Bhandari, M. Córdoba, J. Henderson, and S. Warrander. *On the Extraordinary Construction of Cycle Sets by Wolfgang Rump*. 2021. arXiv: 2106.05149 [math].

[3] 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.

[4] F. Cedó, E. Jespers, and J. Okniński. "Primitive Set-Theoretic Solutions of the Yang–Baxter Equation". *Communications in Contemporary Mathematics* 24 (2022), 2150105.

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

[6] F. Chouraqui and E. Godelle. "Folding of Set-Theoretical Solutions of the Yang-Baxter Equation". *Algebras and Representation Theory* 15 (2012), 1277–1290.
[7] P. Dehornoy. "Set-Theoretic Solutions of the Yang–Baxter Equation, RC-calculus, and Garside Germs". *Advances in Mathematics* 282 (2015), 93–127.
[8] 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.
[9] P. Dehornoy, F. Digne, E. Godelle, D. Krammer, and J. Michel. *Foundations of Garside Theory*. Vol. 22. EMS Tracts in Mathematics. 2015.
[10] T. Došlić. "Maximum Product over Partitions into Distinct Parts". *Journal of Integer Sequences* 8 (2005), Article 05.5.8.
[11] V. G. Drinfeld. "On Some Unsolved Problems in Quantum Group Theory". Vol. 1510. Lecture Notes in Mathematics. 1992, 1–8.
[12] P. Etingof, T. Schedler, and A. Soloviev. "Set-Theoretical Solutions to the Quantum Yang-Baxter Equation". *Duke Mathematical Journal* 100 (1999), 169–209.
[13] 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.
[14] T. Gateva-Ivanova and M. Van den Bergh. "Semigroups of I-Type". *Journal of Algebra* 206 (1998), 97–112.
[15] E. Landau. "Über Die Maximalordnung Der Permutationen Gegebenen Grades". *Archiv der Mathematik und Physik* 5 (1903), 92–103.
[16] V. Lebed, S. Ramírez, and L. Vendramin. *Involutive Yang-Baxter: Cabling, Decomposability, Dehornoy Class*. 2022. arXiv: 2209.02041 [math].
[17] W. Ledermann. *Introduction to Group Theory*. Oliver and Boyd, 1973.
[18] J. Michel. "Lectures on Coxeter Groups". Beijing, 2014.
[19] W. Rump. "A Decomposition Theorem for Square-Free Unitary Solutions of the Quantum Yang-Baxter Equation". *Advances in Mathematics* 193 (2005), 40–55.
[20] R. Sastriques-Guardiola. "Personnal Communications".

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