

HOW STRUCTURE GROUPS AND MONOIDS GROW

CARSTEN DIETZEL, EDOUARD FEINGESICHT, VICTORIA LEBED

ABSTRACT. The structure groups and monoids of set-theoretic solutions to the Yang–Baxter Equation can be regarded as deformations of free abelian groups resp. monoids. In this work, we obtain explicit formulae for the growth series of the structure groups and monoids of transposition and dihedral quandles, and of the structure groups of permutation quandles. These quandles provide important families of YBE solutions. The intricate nature of our formulae confirms that, while preserving many nice properties of free abelian groups, even the simplest structure groups and monoids are remarkably rich objects. We also establish some structural properties and easily computable normal forms for the monoids considered.

INTRODUCTION

The free abelian group on a set X admits the following standard presentation:

$$\mathrm{FAb}(X) = \langle e_x : x \in X \mid e_x e_y = e_y e_x : x, y \in X \rangle.$$

This presentation suggests the following natural deformation. Consider a map $r : X \times X \rightarrow X \times X$ sending (x, y) to $(\lambda_x(y), \rho_y(x))$, and put

$$(0.1) \quad \mathrm{As}(X, r) = \langle e_x : x \in X \mid e_x e_y = e_{\lambda_x(y)} e_{\rho_y(x)} : x, y \in X \rangle.$$

This defines the *structure group* (alternatively called the *associated*, *enveloping*, or *adjoint group*) of (X, r) . Imposing appropriate conditions on r , one forces $\mathrm{As}(X, r)$ to preserve the desired properties of $\mathrm{FAb}(X)$. For example, if X is finite and r is a solution to the Yang–Baxter Equation

$$(r \times \mathrm{Id}_X)(\mathrm{Id}_X \times r)(r \times \mathrm{Id}_X) = (\mathrm{Id}_X \times r)(r \times \mathrm{Id}_X)(\mathrm{Id}_X \times r),$$

that is involutive, meaning that $r^2 = \mathrm{Id}_{X \times X}$, and non-degenerate, that is, λ_x and ρ_x are bijections for all $x \in X$, then $\mathrm{As}(X, r)$ is Bieberbach [13] and Garside [8]. In particular, this gave the first systematic way of constructing Garside groups going beyond the foundational example of spherical Artin–Tits groups.

In the present work, we go in an orthogonal direction, and show that even for very simple maps r , the group $\mathrm{As}(X, r)$ might significantly differ from $\mathrm{FAb}(X)$. The invariant that we chose to measure this difference is the growth series. Recall that the *growth series* of a group G with respect to a generating set S is the formal power series defined as

$$\mathcal{G}_{G,S}(t) = \sum_{n=0}^{\infty} \# \left(\overline{S}^n \setminus \left(\bigcup_{i=0}^{n-1} \overline{S}^i \right) \right) t^n = \sum_{g \in G} t^{l_S(g)},$$

where $\overline{S} = S \cup \{s^{-1} : s \in S\}$; $\overline{S}^k = \{s_1 s_2 \cdots s_k : s_1, \dots, s_k \in \overline{S}\}$ for $k \geq 1$ and $\overline{S}^0 = \{1_G\}$; and $l_S(g)$ is the minimal number of elements of \overline{S} needed to produce (multiplicatively) g . The growth series measures how fast the words in the letters $s^{\pm 1}$, $s \in S$, cover the entire group G when the word length is allowed to grow. The generating set is omitted in notations when clear from the context. Thus, for $\mathrm{As}(X, r)$, we will always take $S = \{e_x : x \in X\}$. For the free abelian group

Date: September 22, 2025.

2020 Mathematics Subject Classification. 57K12, 16P90, 20B30, 20F05, 16T25.

Key words and phrases. Growth series, structure group, structure monoid, conjugation quandle, symmetric group, dihedral groups, Yang–Baxter Equation.

$\mathbb{Z}^d = \text{FAb}(\{1, \dots, d\})$ which is also the structure group of the solution $r(x, y) = (y, x)$ on the set $X = \{1, \dots, d\}$, we have

$$(0.2) \quad \mathcal{G}_{\mathbb{Z}^d}(t) = \left(\frac{1+t}{1-t} \right)^d.$$

The typical questions on growth series are their rationality and asymptotic behaviour. Explicit computation of the entire series is usually beyond reach, since it requires a fine understanding of how the given group works. Some notable exceptions are [2, 4, 7, 19]. The reader is directed to the introductory book [17] for basics on the growth of groups¹.

The question of determining the growth series of structure groups was first explicitly raised in [21]. To our knowledge, no concrete computations have been carried out so far. According to [16], the structure group of an invertible non-degenerate YBE solution is related to the structure group of its *derived solution* of the “only-left-deformed” form

$$(0.3) \quad r_{\triangleright}(x, y) = (x \triangleright y, x)$$

by a bijective length-preserving group 1-cocycle. Thus, the two structure groups have identical growth series. This explains why solutions of the form (0.3) are particularly important. They can also be regarded as *quandle* solutions, but since we do not use the quandle theory here, we will only mention connections to quandles as remarks for specialists.

In this work, we provide computations for four important families of YBE solutions. Concretely, we take as X :

- (1) the set S_d of all permutations of d elements;
- (2) the set T_d of all transpositions (i, j) in S_d ;
- (3) the set D_d of all symmetries of a regular d -gon;
- (4) the set R_d of all reflections inside D_d .

As r , we take the map r_{\triangleright} , where \triangleright is the conjugation operation:

$$x \triangleright y = xyx^{-1}.$$

For any group, or a union of conjugacy classes thereof, r_{\triangleright} is a bijective non-degenerate YBE solution. Our four solutions, called, respectively, *permutation*, *transposition*, *dihedral* and *reflection solutions* in what follows, correspond to conjugation quandles (and their subquandles) of symmetric and dihedral groups. Note that the name *dihedral quandle* historically refers to (R_d, \triangleright) rather than to the whole (D_d, \triangleright) ; we will not use this name to avoid confusion. The map r_{\triangleright} will be omitted in notations when clear from the context; thus, $\text{As}(X)$ stands for $\text{As}(X, r_{\triangleright})$.

Our first results are the following formulae for the growth series of $\text{As}(T_d)$ and $\text{As}(R_d)$:

$$\begin{aligned} \mathcal{G}_{\text{As}(T_d)}(t) &= \prod_{k=2}^{d-1} (1+kt) \cdot \frac{1+t^2}{1-t} + t \cdot \prod_{k=1}^{d-1} (1+kt) \cdot \left(\sum_{k=1}^{d-1} \frac{k}{1+kt} \right), \\ \mathcal{G}_{\text{As}(R_d)}(t) &= \frac{2dt}{1-t} + 1 + (d-1)t^2 \quad \text{for odd } d. \end{aligned}$$

They are derived from the relation we establish between these growth series $\tilde{\mathcal{G}}$ and the growth series \mathcal{G} for S_d with respect to the generating set T_d (respectively, D_d w.r.t. R_d):

$$(0.4) \quad \tilde{\mathcal{G}}(t) = t \cdot \frac{d}{dt} \mathcal{G}(t) + \frac{1+t^2}{1-t^2} \mathcal{G}(t),$$

and classical formulae for \mathcal{G}_{S_d, T_d} and \mathcal{G}_{D_d, R_d} . Note that Eq. (0.4) actually holds for a large family of groups, including all Coxeter groups of ADE type (Theorem 1.3).

¹Note however a misprint in Example 7 from [17] treating the case $G = \mathbb{Z}^d$. For $d = 3$, the n th coefficient should be $a_3(n) = 4n^2 + 2$ instead of $4n^2 + 4n + 2$.

We further compute the growth series of the structure groups of entire permutation and odd rank dihedral solutions (actually, of a more general type of solutions, see Theorem 2.2):

$$\mathcal{G}_{\text{As}(\text{S}_d \text{ or } \text{D}_d)}(t) = \gamma_d \cdot \left(\frac{1+t}{1-t} \right)^{c_d} - (1+t)^2 \cdot \left(\sum_{\bar{k} \in \mathbb{Z}^{c_d-1}} \left(\gamma_d - \# \left(\prod_{i=1}^{c_d-1} \mathcal{C}_i^{k_i} \right) \right) \cdot t^{|\bar{k}|} \right).$$

Here γ_d is the size of the commutator subgroup and c_d the number of conjugacy classes of S_d or D_d ; the \mathcal{C}_i are the conjugacy classes different from $\{1\}$; \bar{k} stands for a tuple of integers (k_1, \dots, k_{c_d-1}) ; and $|\bar{k}| = \sum_{i=1}^{c_d-1} |k_i|$. For S_d , the cumbersome correction term in the end of the formula is a polynomial except for $d = 4$, and can be explicitly computed starting from the multiplication table for the conjugacy classes of S_d . The products of conjugacy classes of S_d are an interesting subject in itself, see for instance [1] and references therein. In particular, asymptotically the growth behaviour of $\text{As}(\text{S}_d)$ is close to that of a free abelian group, except for $d = 4$. For dihedral groups D_d with odd non-prime d , the correction term is not a polynomial.

In parallel to the structure group, one can define the *structure monoid* $\text{As}^+(X, r)$ of (X, r) using the same recipe as (0.1), but this time regarding it as a monoid presentation. This object tends to better capture the nature of the map r ; see for instance [5, 6] and references therein. We note here that the growth series of $\text{As}^+(X, r)$ coincides with the Hilbert–Poincaré series of the associated *structure algebra* $K(X, r)$ over a field K ; see for instance [12, 14] for a detailed study of the latter object.

In Theorem 3.10, we explicitly compute the growth series of the structure monoids $\text{As}^+(\text{T}_d)$. The result possesses a surprisingly compact yet intricate presentation when these monoids are considered simultaneously for all d :

$$\sum_{d \geq 0} \frac{1}{d!} \mathcal{G}_{\text{As}^+(\text{T}_d)}(t) x^d = \exp \left(\frac{(1-tx)^{-t} - 1 - t^4 x}{t^2(1-t^2)} \right).$$

This should be compared with the much simpler growth series of the free abelian monoid \mathbb{N}_0^d :

$$(0.5) \quad \mathcal{G}_{\mathbb{N}_0^d}(t) = \left(\frac{1}{1-t} \right)^d, \quad \sum_{d \geq 0} \frac{1}{d!} \mathcal{G}_{\mathbb{N}_0^d}(t) x^d = \exp \left(\frac{x}{1-t} \right).$$

The key ingredient of our computation is a structural study of the monoid $\text{As}^+(\text{T}_d)$, interesting per se. We decompose $\text{As}^+(\text{T}_d)$ as a semilattice of subsemigroups, isomorphic to the partition semilattice of rank d . Each subsemigroup is a direct product of what we call the *full transposition semigroups* FTS_k . The latter are then injected into the direct product $\text{S}_k \times \mathbb{N}$, where the second component keeps track of the length. This is a semigroup version of the group injection $\text{As}(\text{T}_d) \hookrightarrow \text{S}_d \times \mathbb{Z}$ from [15], which does not work for the entire monoid $\text{As}^+(\text{T}_d)$.

Finally, Theorem 5.16 settles the case of the structure monoids of R_d both for odd and even d :

$$\mathcal{G}_{\text{As}^+(\text{R}_d)}(t) = 1 + d \cdot \left(t + \left(\sum_{c|d} \frac{\varphi(c)}{c} \right) t^2 + \tau(d) \frac{t^3}{1-t} + \tau \left(\frac{d}{2} \right) \frac{t^4}{2(1-t)^2} \right),$$

where τ is the number-of-divisors function, and φ is Euler’s totient function. At the heart of this computation are once again a semilattice decomposition of $\text{As}^+(\text{R}_d)$, a reduction of necessary computations to the extremal subsemigroups of this semilattice, and the injection of the latter into elementary semi-direct products with easily extractable length. This injection is realised using easily computable numeric invariants and simple normal forms, which surprisingly turn out to be more approachable for the reflections R_∞ inside infinite dihedral groups D_∞ (see Section 4). We then return to the finite case by reducing modulo d .

Acknowledgements. The authors thank Eddy Godelle and Stéphane Launois for their contributions to the working group on the growth of structure groups, which gradually reduced to a working subgroup containing the three current authors.

1. HOW STRUCTURE GROUPS OF TRANSPOSITION- AND REFLECTION-TYPE SOLUTIONS GROW

In this section, we explicitly compute the growth series of the structure group of any transposition solution T_d , and any reflection solution R_d with odd d . Our computations can be adapted to a more general class of solutions, presented below.

Definition 1.1. A $\bar{\mathcal{C}}$ -presentation of a group is a presentation involving relations of two types only:

- *conjugation relations* $a \triangleright b = c$ for certain triples of generators where $a \triangleright b = aba^{-1}$;
- *power relations* of the form $a^p = 1$, for certain generators a and certain integers $p \geq 2$ (at most one relation per conjugacy class).

A group admitting such a presentation is called a $\bar{\mathcal{C}}$ -group.

This definition goes back to [15]; see there for examples of very different nature. The letter \mathcal{C} in the name stands for *conjugation*, and the bar for the quotient by powers of generators, as in the finite quotients of certain structure groups.

We will work here with a particular type of $\bar{\mathcal{C}}$ -groups:

Definition 1.2. A $\bar{\mathcal{C}}$ -presentation of class 2 is a $\bar{\mathcal{C}}$ -presentation whose set of generators C is a single conjugacy class, and which has exactly one power relation, $a^2 = 1$.

Examples include:

- (1) the symmetric group S_d generated by the set of transpositions T_d , and, more generally, Coxeter groups of ADE type;
- (2) the dihedral group D_d for odd d , generated by the set of reflections R_d ;
- (3) finite quotients of the structure groups of finite connected involutory quandles [16].

Endow C with the YBE solution r_\triangleright from (0.3). We will first show how to express the growth series of the structure group $\text{As}(C)$ (with respect to the standard generators e_x) in terms of the growth series of the original group G with respect to the generating set C :

Theorem 1.3. Let G be a group with a $\bar{\mathcal{C}}$ -presentation of class 2, with a set of generators C . Then one has the following relation between two group growth series:

$$(1.1) \quad \mathcal{G}_{\text{As}(C)}(t) = \frac{1+t^2}{1-t^2} \cdot \mathcal{G}_{G,C}(t) + t \cdot \frac{d}{dt} \mathcal{G}_{G,C}(t)$$

Before giving a proof, let us explore the consequences of this relation in our favourite examples. First, take $G = D_d$ and $C = R_d$ for odd d . The reflection lengths of symmetries of a regular d -gon look as follows:

- (1) 0 for the identity;
- (2) 1 for all d reflections;
- (3) 2 for all $d-1$ non-trivial rotations.

Thus

$$\mathcal{G}_{D_d, R_d}(t) = 1 + dt + (d-1)t^2.$$

Plugging this into (1.1), we get

$$\begin{aligned} \mathcal{G}_{\text{As}(R_d)}(t) &= \frac{1+t^2}{1-t^2} \cdot (1 + dt + (d-1)t^2) + t \cdot (d + 2(d-1)t) \\ &= \frac{1+t^2}{1-t} \cdot (1 + (d-1)t) + dt + 2(d-1)t^2 \\ &= \frac{(1+t^2) \cdot (1 + (d-1)t) + (1-t) \cdot (-1 + dt + (d-1)t^2)}{1-t} + 1 + (d-1)t^2 \\ &= \frac{2dt}{1-t} + 1 + (d-1)t^2. \end{aligned}$$

This formula can also be obtained by showing that every element of $\text{As}(R_d)$ can be uniquely presented in the form $e_0^k e_x$. This can be deduced from [9, 11]. Results in [15] can furthermore be

applied to show that for even d there is an explicit isomorphism $\text{As}(\mathbb{R}_d) \cong \mathbb{Z}_2^{\frac{d}{2}} \times_{\mathbb{Z}_2 \times \mathbb{Z}_2} \mathbb{D}_d$ which can be used to show that $\mathcal{G}_{\text{As}(\mathbb{R}_d)}(t) = \frac{d}{2} \left(\frac{1+t}{1-t} \right)^2 + \left(\frac{d}{2} - 1 \right) (t^2 - 1)$, in that case.

Second, take $G = S_d$, $C = T_d$. To improve readability, we will use the notation

$$\mathcal{G}_d = \mathcal{G}_{S_d, T_d}, \quad \tilde{\mathcal{G}}_d = \mathcal{G}_{\text{As}(T_d)}$$

for the growth series considered, which will be referred to as the *small* and the *big* series respectively. We will need the following formula for the small series:

Proposition 1.4. *One has*

$$(1.2) \quad \mathcal{G}_d(t) = \prod_{k=1}^{d-1} (1 + kt).$$

This formula admits many generalisations, and can be deduced from the classical work on finite unitary reflection groups, see [20]. We will present here an elementary inductive proof for completeness.

Proof. Since in our case all generators are involutive, in the formula

$$\mathcal{G}_{G,C}(t) = \sum_{g \in G} t^{l_C(g)}$$

one can take as $l_C(g)$ is the minimal number of generators from C needed to write g as a product. The shortest expressions of a permutation in terms of transpositions correspond to cycle decompositions. Now, the $d+1$ st element can be inserted into a permutation $\sigma \in S_d$ either as a fixed point, which preserves the length of the permutation (in terms of transpositions), or after any of the d elements in the cycle decomposition of σ , which increases the length of the permutation by 1 and thus adds a factor t . Hence the recursion relation

$$(1.3) \quad \mathcal{G}_{d+1}(t) = (1 + dt) \cdot \mathcal{G}_d(t).$$

Together with $\mathcal{G}_1(t) = 1$, it yields (1.2). □

Inserting this formula into (1.1), one gets

Corollary 1.5. *For any integer $d \geq 2$, one has*

$$\tilde{\mathcal{G}}_d(t) = \prod_{k=2}^{d-1} (1 + kt) \cdot \frac{1+t^2}{1-t} + t \cdot \prod_{k=1}^{d-1} (1 + kt) \cdot \left(\sum_{k=1}^{d-1} \frac{k}{1+kt} \right).$$

For small values of d , this becomes

$$\begin{aligned} \tilde{\mathcal{G}}_2(t) &= \frac{1+t}{1-t}, \\ \tilde{\mathcal{G}}_3(t) &= \frac{1+t}{1-t} \cdot (-2t^2 + 4t + 1), \\ \tilde{\mathcal{G}}_4(t) &= \frac{1+t}{1-t} \cdot (-12t^3 + 13t^2 + 10t + 1), \end{aligned}$$

which for $d > 2$ differs significantly from the free abelian case (0.2).

To see how the big series $\tilde{\mathcal{G}}_d$ changes with d , we establish a recursive formula, very much resembling the formula (1.3) for the small series:

Corollary 1.6. *For any integer $d \geq 2$, one has*

$$(1.4) \quad \tilde{\mathcal{G}}_{d+1}(t) = (1 + dt) \cdot \tilde{\mathcal{G}}_d(t) + dt \cdot \mathcal{G}_d(t).$$

Proof. Deriving the recursive formula (1.3) for \mathcal{G}_d , one gets

$$\frac{d}{dt}\mathcal{G}_{d+1}(t) = (1 + dt) \cdot \frac{d}{dt}\mathcal{G}_d(t) + d \cdot \mathcal{G}_d(t).$$

Thus

$$\begin{aligned} \tilde{\mathcal{G}}_{d+1}(t) &= t \cdot \frac{d}{dt}\mathcal{G}_{d+1}(t) + \frac{1+t^2}{1-t^2} \cdot \mathcal{G}_{d+1}(t) \\ &= t \cdot \left((1 + dt) \cdot \frac{d}{dt}\mathcal{G}_d(t) + d \cdot \mathcal{G}_d(t) \right) + \frac{1+t^2}{1-t^2} \cdot (1 + dt) \cdot \mathcal{G}_d(t) \\ &= (1 + dt) \cdot \left(t \cdot \frac{d}{dt}\mathcal{G}_d(t) + \frac{1+t^2}{1-t^2} \cdot \mathcal{G}_d(t) \right) + dt \cdot \mathcal{G}_d(t) \\ &= (1 + dt) \cdot \tilde{\mathcal{G}}_d(t) + dt \cdot \mathcal{G}_d(t). \end{aligned} \quad \square$$

Proof of Theorem 1.3. As was shown in [15], the assignment

$$(1.5) \quad \begin{aligned} \text{As}(C) &\rightarrow G \times \mathbb{Z}, \\ e_x &\mapsto (x, 1) \end{aligned}$$

uniquely extends to an injective group morphism, whose image is

$$G \times_{\mathbb{Z}_2} \mathbb{Z} = \{ (g, m) \in G \times \mathbb{Z} : l_C(g) \equiv m \pmod{2} \}.$$

Identifying elements of $\text{As}(C)$ with their images in $G \times \mathbb{Z}$, one can interpret the desired growth series as follows:

$$(1.6) \quad \mathcal{G}_{\text{As}(C)}(t) = \sum_{(g,m) \in G \times_{\mathbb{Z}_2} \mathbb{Z}} t^{l(g,m)},$$

where $l(g, m)$ denotes the length with respect to the generators e_x , $x \in C$. Let us show that this length reduces to the following elementary formula:

$$l(g, m) = \max(l_C(g), |m|).$$

Indeed, to construct (g, m) from the generators $(x, 1)$, $x \in C$, one needs on the one hand at least $l_C(g)$ of them (to obtain g as the first factor), and on the other hand at least $|m|$ of them (to obtain m as the second factor). So, $l(g, m) \geq \max(l_C(g), |m|)$. To prove the \leq inequality, let $g = c_1 \cdots c_i$ be a minimal length representation of g with respect to the generating set C . In the product $e_{c_1}^{\pm 1} \cdots e_{c_i}^{\pm 1}$, one can choose the signs ± 1 to get as total degree any integer between $-i$ and i having the same parity as i . If $l_C(g) \geq |m|$, this yields a representation of (g, m) of length $l_C(g)$. In the opposite case $l_C(g) \leq |m|$, to get a representation of (g, m) of length $|m|$, all signs ± 1 should be the same as the sign of m , and several copies of the element $e_{c_1}^{\pm 2}$ (contributing only to the second factor of $G \times \mathbb{Z}$ since $c_1^{\pm 2} = 1$ in G) should be added. Let us now split (1.6) into two parts, according to

which component yields the above max. We will abbreviate $l_C(g)$ as $l(g)$ here.

$$\begin{aligned}
\mathcal{G}_{\text{As}(C)}(t) &= \sum_{g \in G} \sum_{\substack{m \in \mathbb{Z}, \\ l(g) \geq |m|, \\ m-l(g) \text{ even}}} t^{l(g)} + \sum_{g \in G} \sum_{\substack{m \in \mathbb{Z}, \\ l(g) < |m|, \\ m-l(g) \text{ even}}} t^{|m|} \\
&= \sum_{g \in G} (l(g) + 1) t^{l(g)} + \sum_{g \in G} \sum_{\substack{m \in \mathbb{Z}, \\ |m|-l(g) > 0, \\ |m|-l(g) \text{ even}}} t^{|m|-l(g)} t^{l(g)} \\
&= \sum_{g \in G} l(g) t^{l(g)} + \sum_{g \in G} t^{l(g)} + \sum_{g \in G} \sum_{i \in \mathbb{N}} 2t^{2i} t^{l(g)} \\
&= t \cdot \frac{d}{dt} \mathcal{G}_{G,C}(t) + \sum_{g \in G} (1 + \sum_{i \in \mathbb{N}} 2t^{2i}) t^{l(g)} \\
&= t \cdot \frac{d}{dt} \mathcal{G}_{G,C}(t) + \frac{1+t^2}{1-t^2} \cdot \mathcal{G}_{G,C}(t). \quad \square
\end{aligned}$$

Remark 1.7. Note that for a finite group G , in the analysis detailed in the proof, only the case $l(g) \leq |m|$ is possible for $|m|$ large enough. Thus

$$\begin{aligned}
\mathcal{G}_{\text{As}(C)}(t) &= \sum_{m \in \mathbb{Z}} \frac{\#G}{2} t^{|m|} + \text{some polynomial} \\
&= \sum_{m \in \mathbb{N}} 2 \frac{\#G}{2} t^m + \text{some polynomial} \\
&= \frac{\#G}{1-t} + \text{some polynomial}.
\end{aligned}$$

Thus all coefficients in the series, except for a finite number, equal $\#G$.

2. HOW STRUCTURE GROUPS OF PERMUTATION- AND DIHEDRAL-TYPE SOLUTIONS GROW

In this section, we explain how to compute the growth series of the structure group of the entire permutation solution S_d and dihedral solution D_d . Again, we will work in a more general context, that of a finite \bar{C} -group G with commutator length 1. That is, each element in the commutator subgroup $[G, G]$ is a simple commutator $[a, b] = aba^{-1}b^{-1} = (a \triangleright b)b^{-1}$. Typical examples are symmetric groups (see [18, Theorem 1]) and odd-order dihedral groups (for which the commutator subgroup is the subgroup of all rotations, which are always products of two reflections).

We will need the following notations. Given a group G , denote by c the number of its conjugacy classes, and by $\mathbf{C} = \{\mathcal{C}_i : 0 \leq i \leq c-1\}$ the set of its conjugacy classes. We impose $\mathcal{C}_0 = \{1\}$. Given a sequence of conjugacy classes \mathcal{C}_{i_j} ($1 \leq j \leq n$), we define

$$\prod_{j=1}^n \mathcal{C}_{i_j} = \{g_1 g_2 \dots g_j : g_j \in \mathcal{C}_{i_j} (1 \leq j \leq n)\}.$$

An empty product, meaning that $n = 0$, is furthermore to be understood as $\{1\}$. As each factor is invariant under conjugation, this product is independent of the specific order of factors. Furthermore, for some conjugacy class $\mathcal{C} = \mathcal{C}_i$ and an integer k , we define

$$\mathcal{C}^k = \begin{cases} \prod_{j=1}^k \mathcal{C} & k \geq 0 \\ \prod_{j=1}^{-k} \mathcal{C}^{-1} & k < 0, \end{cases}$$

where $\mathcal{C}^{-1} = \{g^{-1} : g \in \mathcal{C}\}$.

Definition 2.1. The *defect measure* of a finite group G with a fixed order on its conjugacy classes is the map

$$\delta_G: \mathbb{Z}^{c-1} \longrightarrow \mathbb{Z}_{\geq 0},$$

$$\bar{k} \longmapsto \#[G, G] - \# \left(\prod_{i=1}^{c-1} \mathcal{C}_i^{k_i} \right).$$

Note that \mathcal{C}_0 is excluded from the above product. Furthermore, the *defect series* of G is defined as

$$\Delta_G(t) = \sum_{\bar{k} \in \mathbb{Z}^{c-1}} \delta_G(\bar{k}) \cdot t^{|\bar{k}|},$$

where $|\bar{k}| = \sum_{i=1}^{c-1} |k_i|$.

Contrary to defect measures, the defect series is independent of the order on conjugacy classes of G . We remark here that δ_G takes only non-negative values as under the canonical homomorphism $\text{Ab}: G \rightarrow G^{\text{ab}}$, any product of conjugacy classes in G is mapped to a singleton; therefore, the size of such a product cannot exceed $\#[G, G]$.

We now state the main result of this section:

Theorem 2.2. *Let G be a finite $\bar{\mathcal{C}}$ -group with commutator length 1, and with c conjugacy classes. Then the growth series of the structure group of (G, r_{\triangleright}) can be computed as follows:*

$$(2.1) \quad \mathcal{G}_{\text{As}(G)}(t) = \#[G, G] \cdot \left(\frac{1+t}{1-t} \right)^c - (1+t)^2 \cdot \Delta_G(t).$$

In particular, the computation of the growth series of $\text{As}(G)$ boils down to the computation of the defect series of G .

Proof. Since the element e_1 generates a central subgroup of $\text{As}(G)$ that is isomorphic to \mathbb{Z} , we can factor it out, and get

$$\mathcal{G}_{\text{As}(G)}(t) = \mathcal{G}_{(\mathbb{Z}, 1)}(t) \cdot \mathcal{G}_{\text{As}(G_0)}(t) = \frac{1+t}{1-t} \cdot \mathcal{G}_{\text{As}(G_0)}(t),$$

where $G_0 = G \setminus \{1\}$. We will thus concentrate on G_0 in what follows.

As was shown in [15], the assignment

$$(2.2) \quad \begin{aligned} \text{As}(G_0) &\rightarrow G \times \mathbb{Z}^{c-1}, \\ e_x &\mapsto (x, 1_i), \end{aligned}$$

where 1_i generates the component in \mathbb{Z}^{c-1} corresponding to the conjugacy class \mathcal{C}_i of x , uniquely extends to an injective group morphism. Its image is the pullback of the homomorphisms

$$\mathbb{Z}^{c-1} \longrightarrow G^{\text{ab}} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{c-1}} \xleftarrow{\text{Ab}} G_0.$$

Here p_i is the power in the unique power relation $a^{p_i} = 1$ with $a \in \mathcal{C}_i$ if there is one, and $p_i = +\infty$ otherwise. The map on the left is the canonical projection for each of the $c-1$ factors. It will be convenient for us to identify $\text{As}(G_0)$ with its image in $G \times \mathbb{Z}^{c-1}$.

Now, the abelianisation map $\text{Ab}: \text{As}(G_0) \rightarrow \mathbb{Z}^{c-1}$ is surjective. Its kernel is

$$(2.3) \quad \text{Ab}^{-1}(0) = [G, G] \times \{0\} \subset G \times \mathbb{Z}^{c-1}.$$

We need to compute

$$\mathcal{G}_{\text{As}(G_0)}(t) = \sum_{(g, \bar{k}) \in \text{As}(G_0)} t^{l(g, \bar{k})},$$

where $l(g, \bar{k})$ denotes the length with respect to the generators e_x , $x \in G_0$. Let us show that this length is never too far from $|\bar{k}|$:

$$l(g, \bar{k}) \in \{|\bar{k}|, |\bar{k}| + 2\}.$$

Since each e_x contributes at most 1 to exactly one factor in \mathbb{Z}^{c-1} , at least $|\bar{k}|$ such generators are needed to produce (g, \bar{k}) , hence $l(g, \bar{k}) \geq |\bar{k}|$. For the same reason, $l(g, \bar{k})$ has the same parity as $|\bar{k}|$. If $l(g, \bar{k})$ turns out to exceed $|\bar{k}|$, then pick any $h \in G$ with $l(h, \bar{k}) = |\bar{k}|$. As

$$(gh^{-1}, 0) = (g, \bar{k})(h, \bar{k})^{-1} \in \text{Ab}^{-1}(0) = [G, G] \times \{0\},$$

we have $gh^{-1} \in [G, G]$. Our assumption on the commutator length implies that gh^{-1} can be presented as $[a, b] = (a \triangleright b)b^{-1}$. Since $a \triangleright b$ and b lie in the same conjugacy class, say \mathcal{C}_j (with $j \neq 0$), one can write

$$(gh^{-1}, 0) = (a \triangleright b, 1_j)(b, 1_j)^{-1} = e_{a \triangleright b} e_b^{-1}.$$

Therefore,

$$(g, \bar{k}) = (gh^{-1}, 0)(h, \bar{k}) = (a \triangleright b, 1_j)(b, 1_j)^{-1}(h, \bar{k})$$

can be written as a product of $|\bar{k}| + 2$ generators and their inverses. Together with the parity remark above, this yields $l(g, \bar{k}) = |\bar{k}| + 2$, as announced.

Now, the above analysis shows that the option $l(g, \bar{k}) = |\bar{k}|$ actually means that g is realisable as a product of $|k_i|$ elements from each conjugacy class \mathcal{C}_i (if $k_i > 0$) or of inverses thereof (if $k_i < 0$). This can be translated as $g \in \prod_{i=1}^{c-1} \mathcal{C}_i^{k_i}$. Thus, for a fixed $\bar{k} \in \mathbb{Z}^{c-1}$, the number of elements (g, \bar{k}) realising this generic option is $\# \left(\prod_{i=1}^{c-1} \mathcal{C}_i^{k_i} \right)$. Then the number of elements (g, \bar{k}) realising the defect option $l(g, \bar{k}) = |\bar{k}| + 2$ is

$$\# \text{Ab}^{-1}(\bar{k}) - \# \left(\prod_{i=1}^{c-1} \mathcal{C}_i^{k_i} \right) = \#[G, G] - \# \left(\prod_{i=1}^{c-1} \mathcal{C}_i^{k_i} \right) = \delta_G(\bar{k}).$$

Indeed, Eq. (2.3) together with the surjectivity of Ab implies that all fibers of Ab have the same cardinality, $\#[G, G]$.

Summarising, we get

$$\begin{aligned} \mathcal{G}_{\text{As}(G_0)}(t) &= \sum_{\bar{k} \in \mathbb{Z}^{c-1}} (\#[G, G] - \delta_G(\bar{k}))t^{|\bar{k}|} + \delta_G(\bar{k})t^{|\bar{k}|+2} \\ &= \#[G, G] \cdot \sum_{\bar{k} \in \mathbb{Z}^{c-1}} t^{|\bar{k}|} + (t^2 - 1) \cdot \sum_{\bar{k} \in \mathbb{Z}^{c-1}} \delta_G(\bar{k})t^{|\bar{k}|} \\ &= \#[G, G] \cdot \left(\frac{1+t}{1-t} \right)^{c-1} + (t^2 - 1)\Delta_G(t). \end{aligned}$$

Multiplying by the missing factor $\mathcal{G}_{(\mathbb{Z}, 1)}(t) = \frac{1+t}{1-t}$, one recovers the desired formula for the entire growth series $\mathcal{G}_{\text{As}(G)}(t)$. \square

To apply Theorem 2.2 to our favourite groups $G = S_d$, we need a thorough study of their defects. First, in this case each conjugacy class \mathcal{C} satisfies $\mathcal{C}^{-1} = \mathcal{C}$, hence

$$(2.4) \quad \delta_{S_d}(k_1, k_2, \dots, k_{c-1}) = \delta_{S_d}(|k_1|, |k_2|, \dots, |k_{c-1}|),$$

i.e. the defect measure is independent of the signs of its arguments. This simplifies the computation of the defect series:

$$(2.5) \quad \Delta_{S_d}(t) = \sum_{\bar{k} \in \mathbb{Z}_{\geq 0}^{c-1}} 2^{\#\{i \in \{1, \dots, c-1\} : k_i \neq 0\}} \cdot \delta_{S_d}(\bar{k})t^{|\bar{k}|}.$$

We now demonstrate how to use this to compute $\mathcal{G}_{\text{As}(S_d)}(t)$ for $d = 3$ and $d = 4$.

First, let us list the conjugacy classes of S_3 :

i	0	1	2
\mathcal{C}_i	{1}	$S_3(1\ 2)$	$S_3(1\ 2\ 3)$
$\#\mathcal{C}_i$	1	3	2

Here $c = 3$, and $[S_3, S_3] = A_3 = \mathcal{C}_0 \cup \mathcal{C}_2$ is of size 3. We need to determine all non-zero defects $\delta_{S_3}(\bar{k})$ for $k_i \geq 0$. To do this, it is essential to understand the products of all pairs of conjugacy classes, which are necessarily unions of conjugacy classes. We therefore build a multiplication table whose i, j -entry contains the indices of the conjugacy classes contained in $\mathcal{C}_i \cdot \mathcal{C}_j$:

\cdot	0	1	2
0	0	1	2
1	1	0, 2	1
2	2	1	0, 2

From this table, one reads that $\# \left(\prod_{i=1}^2 \mathcal{C}_i^{k_i} \right) = 3 = \#[S_3, S_3]$ whenever $|\bar{k}| = k_1 + k_2 \geq 2$. That is, the defect measure $\delta_{S_3}(\bar{k})$ vanishes for such \bar{k} . For the remaining entries, we compute δ_{S_3} as follows:

$$\begin{aligned} \delta_{S_3}(0, 0) &= 3 - 1 = 2, \\ \delta_{S_3}(1, 0) &= 3 - \#\mathcal{C}_1 = 3 - 3 = 0, \\ \delta_{S_3}(0, 1) &= 3 - \#\mathcal{C}_2 = 3 - 2 = 1. \end{aligned}$$

Thus

$$\Delta_{S_3}(t) = 2^0 \cdot \delta_{S_3}(0, 0)t^{0+0} + 2^1 \cdot \delta_{S_3}(1, 0)t^{1+0} + 2^1 \cdot \delta_{S_3}(0, 1)t^{0+1} = 2 + 2t,$$

and

$$\begin{aligned} \mathcal{G}_{\text{As}(S_3)}(t) &= 3 \cdot \left(\frac{1+t}{1-t} \right)^3 - (1+t)^2 \cdot (2+2t) = 3 \cdot \left(\frac{1+t}{1-t} \right)^3 - 2 \cdot (1+t)^3 \\ &= (1+t)^3 \cdot \left(\frac{3}{(1-t)^3} - 2 \right). \end{aligned}$$

For $d = 4$, the $c = 5$ conjugacy classes are as follows:

i	0	1	2	3	4
\mathcal{C}_i	$\{1\}$	$S_4(1\ 2)$	$S_4(1\ 2)(3\ 4)$	$S_4(1\ 2\ 3)$	$S_4(1\ 2\ 3\ 4)$
$\#\mathcal{C}_i$	1	6	3	8	6

The commutator subgroup $[S_4, S_4] = A_4 = \mathcal{C}_0 \cup \mathcal{C}_2 \cup \mathcal{C}_3$ is of size 12. The multiplication table for its conjugacy classes is

\cdot	0	1	2	3	4
0	0	1	2	3	4
1	1	0, 2, 3	1, 4	1, 4	2, 3
2	2	1, 4	0, 2	3	1, 4
3	3	1, 4	3	0, 2, 3	1, 4
4	4	2, 3	1, 4	1, 4	0, 2, 3

In this table appears a phenomenon which makes S_4 special among symmetric groups. We have $\mathcal{C}_2^m = \mathcal{C}_2 \cup \mathcal{C}_0$ (of size $4 < 12$) for all $m \geq 2$, and $\mathcal{C}_2^m \cdot \mathcal{C}_3 = \mathcal{C}_3$ (of size $8 < 12$) for all $m \geq 1$. In particular, the defect series Δ_{S_4} is not a polynomial. Also, $\mathcal{C}_1 \cdot \mathcal{C}_4 = \mathcal{C}_2 \cup \mathcal{C}_3$ is of size 11. Other multiple products of conjugacy classes yield either $\mathcal{C}_0 \cup \mathcal{C}_2 \cup \mathcal{C}_3$ or $\mathcal{C}_1 \cup \mathcal{C}_4$, and are of size $12 = \#[S_4, S_4]$. We summarise non-trivial defects in the following table:

\bar{k}	$\delta_{S_4}(\bar{k})$
(0, 0, 0, 0)	11
(1, 0, 0, 0)	6
(0, 1, 0, 0)	9
(0, 0, 1, 0)	4
(0, 0, 0, 1)	6
(1, 0, 0, 1)	1
(0, m , 0, 0), $m \geq 2$	8
(0, m , 1, 0), $m \geq 1$	4

Using Eq. (2.5), we can now compute:

$$\Delta_{S_4}(t) = 11 + 2^1 \cdot (6 + 9 + 4 + 6)t + 2^2 \cdot t^2 + (2^1 \cdot 8 + 2^2 \cdot 4) \cdot \sum_{m=2}^{\infty} t^m = 11 + 50t + 4t^2 + \frac{32t^2}{1-t},$$

hence

$$\mathcal{G}_{\text{As}(S_4)}(t) = 12 \cdot \left(\frac{1+t}{1-t} \right)^5 - (1+t)^2 \cdot \left(11 + 50t + 4t^2 + \frac{32t^2}{1-t} \right).$$

Note that for $d \geq 3$ with $d \neq 4$, the simplicity of $A_d = [S_d, S_d]$ guarantees that for any nontrivial conjugacy class $\{1\} \neq \mathcal{C}$ of S_d , we have $\mathcal{C}^{2m} = A_d$ for m large enough, hence $\delta_{S_d}(\bar{k}) = 0$ for sufficiently large $|k|$. In particular, $\Delta_{S_d}(t)$ is a *polynomial* that can be computed explicitly.

The table below contains the numerators of $\mathcal{G}_{\text{As}(S_d)}(t)$ (the denominators being $(1-t)^c$), obtained using a computer program²:

d	numerator of $\mathcal{G}_{\text{As}(S_d)}(t)$
5	$4t^{12} + 92t^{11} - 46t^{10} - 1455t^9 + 3505t^8 - 980t^7 - 4760t^6 + 7150t^5 + 2050t^4 - 1200t^3 + 3086t^2 + 233t + 1$
6	$8t^{17} + 640t^{16} + 1836t^{15} - 42306t^{14} + 172997t^{13} - 294051t^{12} + 93174t^{11} + 467324t^{10} - 728893t^9 + 339031t^8 + 530288t^7 - 368178t^6 + 339579t^5 + 214699t^4 - 41778t^3 + 51480t^2 + 1429t + 1$
7	$4t^{22} + 1500t^{21} - 9052t^{20} + 59768t^{19} - 604186t^{18} + 3616477t^{17} - 12219475t^{16} + 23927860t^{15} - 22726364t^{14} - 7980432t^{13} + 55843840t^{12} - 65892060t^{11} + 35195992t^{10} + 44917674t^9 - 38168278t^8 + 47903548t^7 + 11652920t^6 - 3556516t^5 + 11546372t^4 - 1720204t^3 + 775906t^2 + 10065t + 1$
8	$-4t^{30} - 10144t^{29} + 134812t^{28} - 972046t^{27} + 5044568t^{26} - 14288042t^{25} - 34866279t^{24} + 606830872t^{23} - 3360342688t^{22} + 11590895976t^{21} - 27738090666t^{20} + 46699079226t^{19} - 50843972868t^{18} + 21390854702t^{17} + 43714754431t^{16} - 99390934656t^{15} + 121989261436t^{14} - 58116641248t^{13} + 8695013472t^{12} + 67561029126t^{11} - 46119135216t^{10} + 47606045586t^9 - 7722313273t^8 + 5034722152t^7 + 3123671976t^6 - 634489832t^5 + 555116750t^4 - 53617970t^3 + 14307868t^2 + 80618t + 1$

Let us next turn to the dihedral group $G = D_d$ for odd d . It is of size $2d$. Its conjugacy classes are $\mathcal{C}_0 = \{1\}$, $\mathcal{C}_1 = R_d$ (the set of d reflections), and $\mathcal{C}_i = \{\rho^{i-1}, \rho^{1-i}\}$ for $i = 2, \dots, \frac{d+1}{2}$. Here ρ is the rotation by the angle $\frac{2\pi}{d}$. This yields $\frac{d+3}{2}$ classes in total. Omitting the reflection class \mathcal{C}_1 , we get the subgroup Rot_d of all the d rotation in D_d , which is isomorphic to the cyclic group \mathbb{Z}_d . It turns out to be the derived subgroup of D_d : $[D_d, D_d] = \text{Rot}_d$. Relation $\mathcal{C}^{-1} = \mathcal{C}$ for all conjugacy classes allows us to compute the defect measures for positive entries only, and to use the relations (2.4) and (2.5).

We are now ready to compute $\mathcal{G}_{\text{As}(D_5)}(t)$. (The case $d = 3$ is of no interest since $D_3 = S_3$.) The multiplication table for the conjugacy classes of D_5 looks as follows:

\cdot	0	1	2	3
0	0	1	2	3
1	1	0, 2, 3	1	1
2	2	1	0, 3	2, 3
3	3	1	2, 3	0, 2

²A link to the GAP-file is available under <https://sites.google.com/view/carstendietzel/> in the respective entry in the list of publications

We thus have $\# \left(\prod_{i=1}^3 \mathcal{C}_i^{k_i} \right) = 5 = \#[\mathbf{D}_5, \mathbf{D}_5]$ whenever $k_1 \geq 1$, or $k_2 \geq 4$, or $k_3 \geq 4$, or $k_2 + k_3 \geq 3$ and $k_2 k_3 \neq 0$. For the remaining entries, we compute $\delta_{\mathbf{S}_3}$ as follows:

$$\begin{aligned} \delta_{\mathbf{D}_5}(0, 0, 0) &= 5 - 1 = 4, \\ \delta_{\mathbf{D}_5}(0, 1, 0) &= 5 - \#\mathcal{C}_2 = 5 - 2 = 3, \\ \delta_{\mathbf{D}_5}(0, 0, 1) &= 5 - \#\mathcal{C}_3 = 5 - 2 = 3, \\ \delta_{\mathbf{D}_5}(0, 1, 1) &= 5 - \#(\mathcal{C}_2 \times \mathcal{C}_3) = 5 - 4 = 1, \\ \delta_{\mathbf{D}_5}(0, 2, 0) &= \delta_{\mathbf{D}_5}(0, 0, 2) = 5 - 3 = 2, \\ \delta_{\mathbf{D}_5}(0, 3, 0) &= \delta_{\mathbf{D}_5}(0, 0, 3) = 5 - 4 = 1. \end{aligned}$$

Thus

$$\Delta_{\mathbf{D}_5}(t) = 4 + 2^1 \cdot (3 + 3)t + 2^2 \cdot t^2 + 2^1 \cdot (2 + 2)t^2 + 2^1 \cdot (1 + 1)t^3 = 4 + 12t + 12t^2 + 4t^3,$$

and

$$\mathcal{G}_{\text{As}(\mathbf{D}_5)}(t) = 5 \cdot \left(\frac{1+t}{1-t} \right)^4 - (1+t)^2 \cdot (4 + 12t + 12t^2 + 4t^3) = 5 \cdot \left(\frac{1+t}{1-t} \right)^4 - 4(1+t)^5.$$

For $d = 7$, we get

$$\mathcal{G}_{\text{As}(\mathbf{D}_7)}(t) = 7 \cdot \left(\frac{1+t}{1-t} \right)^5 - 6(1+t)^7 + 6t^3(1+t)^3.$$

For $d = 9$

$$\Delta_{\mathbf{D}_9}(t) = 8(1 + 7t + 21t^2 + 35t^3) - 10t^3 + \text{higher terms}.$$

Our last observation is that the defect series $\Delta_{\mathbf{D}_d}(t)$ does not need to be a polynomial in general. For instance for $d = 9$, the classes $\mathcal{C}_0 = \{1\}$ and $\mathcal{C}_4 = \{\rho^3, \rho^{-3}\}$ generate a subgroup of 3 rotations inside \mathbf{D}_9 (a copy of \mathbb{Z}_3 inside $\text{Rot}_9 \cong \mathbb{Z}_9$), hence $\delta_{\mathbf{D}_9}(0, 0, 0, k, 0) = 9 - 3 = 6 \neq 0$ for all $k \geq 2$.

3. HOW STRUCTURE MONOIDS OF TRANSPOSITION SOLUTIONS GROW

Let us now turn to the growth series of the structure monoid $\text{As}^+(\mathbf{T}_d)$ of the transposition solution. The basic ingredient of our computations in the group case was the injection (1.5) of $\text{As}(\mathbf{T}_d)$ into a more accessible group, the direct product $\mathbf{S}_d \times \mathbb{Z}$. The corresponding map is no longer injective for the monoid. Indeed, the elements e_x^2 , $x \in \mathbf{T}_d$, are all *frozen* in the monoid $\text{As}^+(\mathbf{T}_d)$ (since no non-trivial braiding moves apply to them) and thus pairwise distinct, whereas the map (1.5) sends them all to $(\text{Id}, 2) \in \mathbf{S}_d \times \mathbb{Z}$. However, the situation changes in the presence of other generators. Concretely, for all $x, y \in \mathbf{T}_d$ we have

$$(3.1) \quad e_x^2 e_y = e_x e_{x \triangleright y} e_x = e_{x \triangleright (x \triangleright y)} e_x e_x = e_{x^2 \triangleright y} e_x^2 = e_y e_x^2,$$

hence the squares of all generators are central in $\text{As}^+(\mathbf{T}_d)$. On the other hand,

$$(3.2) \quad e_y e_x^2 = e_{y \triangleright x} e_y e_x = e_{y \triangleright x} e_{y \triangleright x} e_y = e_{y \triangleright x}^2 e_y.$$

Since \mathbf{T}_d is a single conjugacy class in \mathbf{S}_d , relations (3.1)-(3.2) imply that the squares e_x^2 are all equal in the group $\text{As}(\mathbf{T}_d)$, whereas in the monoid $\text{As}^+(\mathbf{T}_d)$ they are equal only in the presence of appropriate generators. To make this statement precise, we need the following definition.

Definition 3.1. Let w be a word in the letters e_x , $x \in \mathbf{T}_d$. The (undirected) *graph* Γ_w of w is constructed on the vertices $1, 2, \dots, d$ by connecting i and j whenever the letter $e_{(i,j)}$ appears in w at least once. Here, for each transposition we allow two notations, (i, j) and (j, i) . The connected components of Γ_w yield a partition of the set $\{1, 2, \dots, d\}$, called the *partition* of w . A component is considered to be *trivial* if it is a singleton.

Lemma 3.2. *Two words in the letters e_x , $x \in \mathbf{T}_d$, representing the same element of the monoid $\text{As}^+(\mathbf{T}_d)$, have the same partition.*

Proof. Indeed, the defining relations $e_{(i,j)}e_{(k,l)} = e_{(k,l)}e_{(i,j)}$ and $e_{(i,j)}e_{(k,j)} = e_{(k,i)}e_{(i,j)}$ do not change the connected components of the graph from the above definition. Here the indices i, j, k, l are all distinct. \square

Thus, one can talk about the partition $\mathbf{p}(a) \in \mathcal{P}_d$ (the set of all partitions of the set $\{1, 2, \dots, d\}$) of an element $a \in \text{As}^+(\text{T}_d)$. This yields a map

$$\mathbf{p}: \text{As}^+(\text{T}_d) \rightarrow \mathcal{P}_d.$$

Recall that the *join* $\pi \vee \rho$ of two partitions π and ρ is obtained by gluing together all intersecting parts from π and ρ . Note that $\pi \vee \rho$ is the finest partition that is coarser than π and ρ , therefore the join describes the semilattice structure of \mathcal{P}_d with respect to the refinement relation. It is called the *partition semilattice of rank d* .

Proposition 3.3. *The monoid $\text{As}^+(\text{T}_d)$ splits as a disjoint union of its subsemigroups $\mathbf{p}^{-1}(\pi)$, $\pi \in \mathcal{P}_d$. Moreover, for any elements $a \in \mathbf{p}^{-1}(\pi)$ and $b \in \mathbf{p}^{-1}(\rho)$, their product ab lies in $\mathbf{p}^{-1}(\pi \vee \rho)$.*

Proof. By definition, to construct the graph of ab on the vertices $1, 2, \dots, d$, one takes as edges precisely the edges corresponding to the letters $e_{(i,j)}$ from a word w representing a (hence present in the graph of w), and the letters $e_{(i,j)}$ from a word v representing b (hence present in the graph of v). Hence the connected components of the word wv representing ab are obtained by gluing together all intersecting components of the graphs of w and v . \square

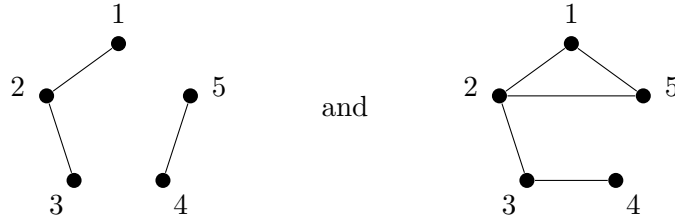
The monoid $\text{As}^+(\text{T}_d)$ thus splits as a semilattice of semigroups $\mathbf{p}^{-1}(\pi)$. To understand the latter, it suffices to study only the semigroups of the following particular type.

Definition 3.4. An element $a \in \text{As}^+(\text{T}_d)$ is called *full* if the induced partition $\mathbf{p}(a)$ has only one part, the whole set $\{1, 2, \dots, d\}$. The subsemigroup of elements of $\text{As}^+(\text{T}_d)$ is called the *full transposition semigroup* on d elements, denoted by FTS_d .

Example 3.5. In $\text{As}^+(\text{T}_5)$, consider the elements

$$a = e_{(1,2)}e_{(2,3)}e_{(4,5)}e_{(1,2)} \quad \text{and} \quad b = e_{(2,3)}e_{(1,5)}e_{(2,5)}e_{(3,4)}e_{(1,2)}.$$

Their respective graphs are



Their respective partitions are $\mathbf{p}(a) = \{\{1, 2, 3\}, \{4, 5\}\}$ and $\mathbf{p}(b) = \{\{1, 2, 3, 4, 5\}\}$. So b is full whereas a is not.

Lemma 3.6. *Let $\pi \in \mathcal{P}_d$ be a partition with parts of size i_1, \dots, i_k . Then the semigroup $\mathbf{p}^{-1}(\pi)$ is isomorphic to the direct product of the following full transposition semigroups:*

$$\mathbf{p}^{-1}(\pi) \cong \text{FTS}_{i_1} \times \dots \times \text{FTS}_{i_k}.$$

Note that a part of size 1 gives rise to a trivial factor isomorphic to $\text{FTS}_1 = \{1\}$.

Proof. The defining relations of $\text{As}^+(\text{T}_d)$ guarantee that two elements commute if their non-trivial components are mutually disjoint. This yields a surjection $\text{FTS}_{i_1} \times \dots \times \text{FTS}_{i_k} \twoheadrightarrow \mathbf{p}^{-1}(\pi)$. It is injective since the defining relations of $\text{As}^+(\text{T}_d)$ applicable to a word representing an element from $\mathbf{p}^{-1}(\pi)$ are either commutation relations for letters coming from different components FTS_{i_j} , or commutation or commutation-conjugation relations between letters from the same component of size i , which are valid in FTS_i . \square

For small values of d , we have:

- (1) $\text{As}^+(\text{T}_1) = \text{FTS}_1 = \{1\}$, the trivial monoid. Note that $\text{T}_1 = \{\}$.

- (2) $\text{As}^+(\text{T}_2) = \{1\} \sqcup \text{FTS}_2$, where $\text{FTS}_2 \cong \mathbb{N}$ is generated by $e_{(1,2)}$.
- (3) $\text{As}^+(\text{T}_3)$ contains a copy of $\{1\}$; three copies of FTS_2 , generated by the three elements $e_{(i,j)}$, respectively, and one copy of FTS_3 . The product of two elements from different copies of FTS_2 lands in FTS_3 .

The computation of the growth series of $\text{As}^+(\text{T}_d)$ is thus reduced to that for all full components. The nice thing about the semigroup FTS_d is that it does inject into $\text{S}_d \times \mathbb{N}$, as suggested by the computations at the beginning of this section. This opens the way to the techniques used in Section 1.

Theorem 3.7. *For $d \geq 2$, the assignment*

$$\begin{aligned} \text{As}^+(\text{T}_d) &\rightarrow \text{S}_d \times \mathbb{N}, \\ e_x &\mapsto (x, 1) \end{aligned}$$

uniquely extends to a semigroup morphism. Its restriction to FTS_d , denoted by

$$\iota_d: \text{FTS}_d \rightarrow \text{S}_d \times \mathbb{N}$$

is injective, and its image is

$$\text{Im}(\iota_d) = \{ (g, 2(d-1) - l(g) + 2k) \in \text{S}_d \times \mathbb{N} : k \in \mathbb{Z}, k \geq 0 \}.$$

As usual, $l(g)$ is the minimal number of transpositions from T_d whose product yields g .

In the first non-trivial case $d = 3$, the theorem identifies FTS_3 with the subsemigroup of $\text{S}_3 \times \mathbb{N}_{\mathbb{Z}_2}$ obtained by discarding the elements $(\text{Id}, 2)$ and $((i, j), 1)$.

Proof. The computation

$$(x \triangleright y, 1)(x, 1) = ((x \triangleright y) \cdot x, 2) = (xy, 2) = (x, 1)(y, 1)$$

guarantees that we indeed have a well-defined semigroup morphism.

Our proof of injectivity is based on the following classical properties of the symmetric group S_d [3, Proposition 1.6.1]:

- (1) The minimal number $l(g)$ of transpositions $(i, j) \in \text{T}_d$ needed to write a permutation $g \in \text{S}_d$ equals $d - c(g)$, where $c(g)$ is the number of cycles in g .
- (2) Two minimal length representations of a $g \in \text{S}_d$ can be related by a finite series of rewriting rules

$$(3.3) \quad (i, j) \cdot (k, l) \longleftrightarrow ((i, j) \triangleright (k, l)) \cdot (i, j)$$

(going in any direction).

- (3) Any representation of a $g \in \text{S}_d$ can be turned into one of minimal length using the rewriting rules (3.3) and

$$(3.4) \quad (i, j)^2 \longrightarrow 1.$$

Now, take $a, b \in \text{FTS}_d$ represented by words w and v (in the generators $e_{(i,j)}$) respectively, and assume that $\iota_d(a) = \iota_d(b) = (g, m)$. Replacing each $e_{(i,j)}$ with (i, j) , one gets two representations of the same permutation $g \in \text{S}_d$. Rewrite them to get minimal length representations, as explained in item 3 above. These rewriting procedures can be mimicked for the words w and v . Indeed, the rewriting steps (3.3) become $e_{(i,j)}e_{(k,l)} \leftrightarrow e_{(i,j) \triangleright (k,l)}e_{(i,j)}$, while (3.4) can be replaced with pushing the central element $e_{(i,j)}^2$ to the left of the word. For the two minimal length representations of g obtained this way, mimic the rewriting procedure from item 2 in the same manner. This yields two words $w' = e_{(i_1, j_1)}^2 \cdots e_{(i_k, j_k)}^2 u$ and $v' = e_{(s_1, t_1)}^2 \cdots e_{(s_k, t_k)}^2 u$ in the generators $e_{(i,j)}$ representing a and b respectively. Here the common subword u lifts one of the minimal length representatives of g . Note that the two words w' and v' have the same number k of square factors $e_{(\bullet, \bullet)}^2$ since they have the same length m . Now, choose arbitrary representatives r_1, \dots, r_q of the parts of the partition π of u . Eq. (3.1) allows one to move any factor $e_{(i,j)}^2$ in any of the two words towards any letter $e_{(s,t)}$ in u ; then, with Eq. (3.2) one can make the transposition (s, t) act on (i, j) by conjugation;

finally, the modified square can be returned to its initial position using (3.1) again. This sequence of operations will be called a *contamination* of $e_{(i,j)}^2$ in this proof. Repeating contamination for all the squares $e_{(i,j)}^2$ in the subwords of w' and v' , one can replace i and j with our selected indices r_1, \dots, r_q , whenever i and j come from distinct parts of π . Then, for the squares $e_{(i,j)}^2$ with i and j from the same part, i can be first contaminated into the index r_x from the same part, then, if there are at least two parts, to another r_y using the remaining squares $e_{(s,t)}^2$ (recall that a and b are full), after which j can be contaminated into r_x . Thus all the indices in the squares can be forced to be of the form r_x . To relate the words w'' and v'' obtained this way, one can use

Lemma 3.8. *Consider a full element $a \in \text{FTS}_d$ which can be represented as a product of squares of generators, $a = e_{(i_1,j_1)}^2 \cdots e_{(i_k,j_k)}^2$. Then it can be rewritten in the following canonical way:*

$$a = e_{(1,2)}^2 e_{(2,3)}^2 \cdots e_{(d-2,d-1)}^2 e_{(d-1,d)}^{2p},$$

for $p = k - (d - 2)$.

Proof. We will use induction on k . An element $e_{(i_1,j_1)}^2$ can be full only if $d = 2$, in which case the statement is tautological.

Next, assume the statement established for a certain k , and consider a full element

$$a = e_{(i_1,j_1)}^2 \cdots e_{(i_k,j_k)}^2 e_{(i_{k+1},j_{k+1})}^2.$$

Case 1. The word remains full after omitting some square, say $e_{(i_{k+1},j_{k+1})}^2$ (commuting squares can always be rearranged in this way). The induction hypothesis then applies to the prefix $e_{(i_1,j_1)}^2 \cdots e_{(i_k,j_k)}^2$, allowing us to rewrite a as

$$a = e_{(1,2)}^2 e_{(2,3)}^2 \cdots e_{(d-2,d-1)}^2 e_{(d-1,d)}^{2p} e_{(i_{k+1},j_{k+1})}^2.$$

The last square $e_{(i_{k+1},j_{k+1})}^2$ can then be contaminated into $e_{(d-1,d)}^2$.

Case 2. If on the contrary the removal of any edge disconnects the graph of a , then this graph is necessarily a tree. Pick any square $e_{(c,d)}^2$ where one of the indices is d . Using contamination by $e_{(c,d)}$, replace all other occurrences of the index d with c . Finally, contaminate $e_{(c,d)}^2$ into $e_{(d-1,d)}^2$ (recall that the graph is connected, since a is full). Then one can rewrite $a = b e_{(d-1,d)}^2$, where $b \in \text{FTS}_{d-1}$ is a full product of $d - 2$ squares on $d - 1$ letters. The induction hypothesis allows us to rewrite it as $b = e_{(1,2)}^2 e_{(2,3)}^2 \cdots e_{(d-2,d-1)}^2$, and we are done. \square

The one-partition case is not covered by the above arguments. In this situation, all squares can be contaminated into the same square, say $e_{(1,2)}^2$, and the numbers of such squares in the two words are equal because of the second component of the map ι_d .

To compute the image of ι_d , we need to find the minimal length $l^f(g)$ of a full representation of a permutation $g \in S_d$ in terms of the transpositions $(i, j) \in T_d$. Here *full representations* are defined in the same way as the full elements of $\text{As}^+(T_d)$. Indeed, since in the image $\iota_d(a) = (g, m)$ the permutation g and the integer m are of the same parity, and since m can be increased by 2 by multiplying a by $e_{(1,2)}^2$, we have

$$\text{Im}(\iota_d) = \{ (g, l^f(g) + 2k) \in S_d \times \mathbb{N} : k \in \mathbb{Z}, k \geq 0 \}.$$

Starting with a representation of g as a product of $l(g)$ transpositions, whose graph has $c(g)$ connected components, one can make it full by adding $c(g) - 1$ squares $(i, j)^2$. Thus,

$$l^f(g) \leq l(g) + 2(c(g) - 1).$$

On the other hand, any full representation of $g \in S_d$ yields a full element $a \in \text{FTS}_d$ with $\iota_d(a) = (g, m)$. As explained before Lemma 3.8, a can be rewritten as $e_{(i_1,j_1)}^2 \cdots e_{(i_k,j_k)}^2 u$, where u lifts a minimal length representation of g . Then u is of length $l(g)$, and its graph has $c(g)$ connected components. To connect the graph, one needs at least $c(g) - 1$ edges, hence $k \geq c(g) - 1$. Thus,

$$l^f(g) \geq l(g) + 2(c(g) - 1).$$

Hence the announced equality

$$l^f(g) = l(g) + 2(c(g) - 1) = l(g) + 2(d - l(g) - 1) = 2(d - 1) - l(g). \quad \square$$

Note that the proof actually works for any group with a $\bar{\mathcal{C}}$ -presentation of class 2 satisfying the rewriting conditions 2-3.

The theorem gives for free the following useful property:

Corollary 3.9. *The tautological map*

$$\begin{aligned} \text{FTS}_d &\rightarrow \text{As}(\mathbb{T}_d), \\ e_{a_1} \dots e_{a_k} &\mapsto e_{a_1} \dots e_{a_k} \end{aligned}$$

is an injective morphism of semigroups.

Proof. Realising FTS_d inside $S_d \times \mathbb{N}$ using the map ι_d , and $\text{As}(\mathbb{T}_d)$ inside $S_d \times \mathbb{Z}$ using (1.5), one interprets the map from the statement as the standard inclusion $S_d \times \mathbb{N} \hookrightarrow S_d \times \mathbb{Z}$. \square

We have prepared all ingredients needed to compute the growth series of the structure monoids $\text{As}^+(\mathbb{T}_d)$, which we organise into a single two-variable series.

Theorem 3.10. *The growth series $\tilde{\mathcal{G}}_d^+(t)$ of $\text{As}^+(\mathbb{T}_d)$ can be computed by the following formula:*

$$\sum_{d \geq 0} \frac{1}{d!} \tilde{\mathcal{G}}_d^+(t) x^d = \exp \left(\frac{(1 - tx)^{-t} - 1 - t^4 x}{t^2(1 - t^2)} \right).$$

Here we use the exponential \exp defined for formal series $f = \sum_{k,l=0}^{\infty} r_{k,l} t^k x^l \in \mathbb{Q}[[t, x]]$ with $r_{0,0} = 0$ by

$$\exp(f) = \sum_{n=0}^{\infty} \frac{f^n}{n!}.$$

Note that, as usual, $\exp(f + g) = \exp(f) \exp(g)$.

Also, the expression $(1 - tx)^{-t}$ should be understood as the formal binomial series

$$(1 + y)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} y^n = 1 + \alpha y + \frac{\alpha(\alpha - 1)}{2!} y^2 + \frac{\alpha(\alpha - 1)(\alpha - 2)}{3!} y^3 + \dots$$

with $\alpha = -t$ and $y = -tx$.

Proof. Let us first compute the restricted growth series $\tilde{\mathcal{G}}_d^{+,f}(t) = \sum_{g \in \text{FTS}_d} t^{l(g)}$ for $d \geq 2$. Theorem 3.7 identifies the elements of FTS_d with the couples $(g, 2(d - 1) - l(g) + 2k) \in S_d \times \mathbb{N}$, with $k \in \mathbb{Z}$, $k \geq 0$. The argument at the end of the proof of that theorem guarantees that the length of such an element, in terms of the generators $e_{(i,j)}$, is simply the second component $2(d - 1) - l(g) + 2k$. Thus

$$\begin{aligned} \tilde{\mathcal{G}}_d^{+,f}(t) &= \sum_{g \in S_d} \sum_{k \geq 0} t^{2(d-1)-l(g)+2k} = \frac{t^{2(d-1)}}{1 - t^2} \sum_{g \in S_d} t^{-l(g)} \\ &= \frac{t^{2(d-1)}}{1 - t^2} \mathcal{G}_d(t^{-1}) = \frac{t^{2(d-1)}}{1 - t^2} \prod_{k=1}^{d-1} (1 + kt^{-1}) \\ &= \frac{t^{d-2}}{1 - t^2} \prod_{k=0}^{d-1} (t + k) = \frac{(-t)^d}{t^2(1 - t^2)} \prod_{k=0}^{d-1} (-t - k) \\ &= d! \frac{(-t)^d}{t^2(1 - t^2)} \binom{-t}{d}. \end{aligned}$$

We used the formula (1.2) for the growth series $\mathcal{G}_d = \mathcal{G}_{S_d, T_d}$. For $d = 1$, the above formula fails. For future computations, we need its corrected version:

$$\tilde{\mathcal{G}}_1^{+,f}(t) = 1 = 1! \frac{(-t)^1}{t^2(1-t^2)} \binom{-t}{1} \cdot (1-t^2).$$

So, the correction factor is $(1-t^2)$.

To compute the growth series $\tilde{\mathcal{G}}_d^+(t)$ of the entire monoid $\text{As}^+(T_d)$, according to Proposition 3.3, one needs to sum over all partitions $\pi \in \mathcal{P}_d$ of the set $\{1, 2, \dots, d\}$ the restricted growth series of the subsemigroups $\mathbf{p}^{-1}(\pi)$. According to Lemma 3.6, for a partition with parts of size i_1, \dots, i_k , the latter restricted growth series is the product of the restricted growth series of the corresponding full transposition semigroups:

$$\mathcal{G}_{\mathbf{p}^{-1}(\pi)}(t) = \sum_{g \in \mathbf{p}^{-1}(\pi)} t^{l(g)} = \tilde{\mathcal{G}}_{i_1}^{+,f}(t) \cdots \tilde{\mathcal{G}}_{i_k}^{+,f}(t).$$

In particular, it depends only on the part sizes i_1, \dots, i_k of π . Now, take a partition

$$\lambda = (n_1 \leq n_2 \leq \dots \leq n_k) \vdash d$$

of an integer d . Denote by $\mu_i(\lambda)$ the number of its parts of size i . One has $\sum_i \mu_i(\lambda) = k$, and $\sum_i i \mu_i(\lambda) = \sum_j n_j = d$. In our computations, we will need the number of set partitions $\pi \in \mathcal{P}_d$ whose part sizes form the integer partition λ . It is given by the formula

$$\binom{d}{n_1, \dots, n_k} \prod_i \frac{1}{\mu_i(\lambda)!}.$$

The preceding argument then yields:

$$\begin{aligned} \tilde{\mathcal{G}}_d^+(t) &= \sum_{\lambda=(n_1, \dots, n_k) \vdash d} \binom{d}{n_1, \dots, n_k} \prod_i \frac{1}{\mu_i(\lambda)!} \prod_i \left(\tilde{\mathcal{G}}_i^{+,f}(t) \right)^{\mu_i(\lambda)} \\ &= \sum_{\lambda=(n_1, \dots, n_k) \vdash d} \frac{d!}{\prod_i (i!)^{\mu_i(\lambda)}} \prod_i \frac{1}{\mu_i(\lambda)!} \left(i! \frac{(-t)^i}{t^2(1-t^2)} \binom{-t}{i} \right)^{\mu_i(\lambda)} \cdot (1-t^2)^{\mu_1(\lambda)} \\ &= d! \sum_{\lambda=(n_1, \dots, n_k) \vdash d} \prod_i \frac{1}{\mu_i(\lambda)!} \left(\frac{(-t)^i}{t^2(1-t^2)} \binom{-t}{i} \right)^{\mu_i(\lambda)} \cdot (1-t^2)^{\mu_1(\lambda)}. \end{aligned}$$

The result is the factorial $d!$ times a sum of products of terms, each of which depends only on the integers i and $\mu_i(\lambda)$, in the exponential-looking way. $\tilde{\mathcal{G}}_d^+(t)$ is expressed as a sum over partitions of d in a way that is similar to the coefficients in certain exponential generating series. A comparison with the exponential formula from enumerative combinatorics [22, Theorem 3.11] suggests using

the exponential generating series for the sequence of formal series $\tilde{\mathcal{G}}_d^+$:

$$\begin{aligned}
\sum_{d \geq 0} \frac{1}{d!} \tilde{\mathcal{G}}_d^+(t) x^d &= \sum_{d \geq 0} \sum_{\lambda = (n_1, \dots, n_k) \vdash d} \prod_i \frac{1}{\mu_i(\lambda)!} \left(\frac{(-t)^i}{t^2(1-t^2)} \binom{-t}{i} \right)^{\mu_i(\lambda)} \cdot (1-t^2)^{\mu_1(\lambda)} \cdot x^{\sum_i i \mu_i(\lambda)} \\
&= \sum_{d \geq 0} \sum_{\lambda = (n_1, \dots, n_k) \vdash d} \prod_i \frac{1}{\mu_i(\lambda)!} \left(\frac{(-tx)^i}{t^2(1-t^2)} \binom{-t}{i} \right)^{\mu_i(\lambda)} \cdot (1-t^2)^{\mu_1(\lambda)} \\
&= \sum_{m_1, m_2, \dots \in \mathbb{N}_0} \prod_i \frac{1}{m_i!} \left(\frac{(-tx)^i}{t^2(1-t^2)} \binom{-t}{i} \right)^{m_i} \cdot (1-t^2)^{m_1} \\
&= \prod_{i \geq 2} \sum_{m_i \in \mathbb{N}_0} \frac{1}{m_i!} \left(\frac{(-tx)^i}{t^2(1-t^2)} \binom{-t}{i} \right)^{m_i} \cdot \sum_{m_1 \in \mathbb{N}_0} \frac{1}{m_1!} x^{m_1} \\
&= \prod_{i \geq 2} \exp \left(\frac{(-tx)^i}{t^2(1-t^2)} \binom{-t}{i} \right) \cdot \exp(x) \\
&= \exp \left(x + \sum_{i \geq 2} \frac{(-tx)^i}{t^2(1-t^2)} \binom{-t}{i} \right) \\
&= \exp \left(x + \frac{1}{t^2(1-t^2)} \left(\sum_{i \geq 0} (-tx)^i \binom{-t}{i} - 1 - tx \right) \right) \\
&= \exp \left(\frac{1}{t^2(1-t^2)} ((1-tx)^{-t} - 1 - tx) \right),
\end{aligned}$$

as announced. □

Let us resume our computations for small values of d . For the full part, the formula from the proof yields

$$\tilde{\mathcal{G}}_2^{+,f}(t) = 2! \frac{(-t)^2}{t^2(1-t^2)} \frac{(-t)(-t-1)}{2!} = \frac{t}{1-t},$$

hence

$$\tilde{\mathcal{G}}_2^+(t) = 1 + \tilde{\mathcal{G}}_2^{+,f}(t) = \frac{1}{1-t} = \mathcal{G}_{\mathbb{N}_0}(t),$$

as expected. Next,

$$\tilde{\mathcal{G}}_3^{+,f}(t) = 3! \frac{(-t)^3}{t^2(1-t^2)} \frac{(-t)(-t-1)(-t-2)}{3!} = \frac{t^2(t+2)}{1-t} = 2t^2 + 3 \sum_{n \geq 3} t^n.$$

Note that, due to the semigroup injection from Theorem 3.7, we always have

$$\tilde{\mathcal{G}}_d^{+,f}(t) = \frac{d!}{2} \cdot \frac{1}{1-t} + \text{a polynomial of degree } (2d-4).$$

Next, from our structural analysis of $\text{As}^+(\text{T}_3)$ it follows that

$$\begin{aligned}
\tilde{\mathcal{G}}_3^+(t) &= 1 + 3\tilde{\mathcal{G}}_2^{+,f}(t) + \tilde{\mathcal{G}}_3^{+,f}(t) = 1 + 3 \frac{t}{1-t} + \frac{t^2(t+2)}{1-t} = \frac{(t+1)(t^2+t+1)}{1-t} \\
&= 1 + 3t + 5t^2 + 6 \sum_{n \geq 3} t^n.
\end{aligned}$$

Similarly,

$$\tilde{\mathcal{G}}_4^{+,f}(t) = \frac{t^3(t+2)(t+3)}{1-t} = 6t^3 + 11t^4 + 12 \sum_{n \geq 5} t^n,$$

and

$$\begin{aligned}\tilde{\mathcal{G}}_4^+(t) &= 1 + 6\tilde{\mathcal{G}}_2^{+,f}(t) + 4\tilde{\mathcal{G}}_3^{+,f}(t) + \tilde{\mathcal{G}}_4^{+,f}(t) + 3\tilde{\mathcal{G}}_2^{+,f}(t)^2 \\ &= 1 + 6\frac{t}{1-t} + 4\frac{t^2(t+2)}{1-t} + \frac{t^3(t+2)(t+3)}{1-t} + 3\left(\frac{t}{1-t}\right)^2.\end{aligned}$$

Observe that, because of the last summand, this series does not longer stabilise for the degree n large enough.

4. NORMAL FORMS IN THE STRUCTURE MONOID OF THE INFINITE REFLECTION SOLUTION

In this section, we prepare the soil for investigating the growth of the structure monoids of reflection solutions (R_d, r_\triangleright) . An important ingredient for this will be a normal form in these monoids. This form will be convenient to establish first in a common lift of these solutions (for all d), which we will now describe.

Definition 4.1. The *infinite reflection solution*, denoted by R_∞ , is the set \mathbb{Z} endowed with the following map on $\mathbb{Z} \times \mathbb{Z}$:

$$(4.1) \quad r(x, y) = (x \triangleright y = -y + 2x, x).$$

One easily checks that it is an invertible non-degenerate YBE solution. Readers familiar with quandles will readily recognise the infinite dihedral quandle.

Taking a quotient modulo d , one obtains a solution isomorphic to (R_d, r_\triangleright) . Indeed, one just needs to order cyclically the vertices of a regular d -gon, and identify the reflection with respect to the vertex i with $i \in \mathbb{Z}_d$.

To compare words in $\text{As}^+(R_\infty)$, we will need several natural invariants.

Lemma 4.2. *The assignment*

$$\begin{aligned}l_0 \times l_1: \text{As}^+(R_\infty) &\rightarrow \mathbb{N}_0 \times \mathbb{N}_0, \\ e_a &\mapsto \begin{cases} (1, 0) & \text{if } a \text{ is even,} \\ (0, 1) & \text{if } a \text{ is odd} \end{cases}\end{aligned}$$

uniquely extends to a well-defined monoid morphism.

The components l_0 and l_1 simply count the generators with even and odd indices respectively. More conceptually, $l_0 \times l_1$ is the monoid surjection $\text{As}^+(R_\infty) \rightarrow \text{As}^+(R_2) \cong \mathbb{N}_0 \times \mathbb{N}_0$ induced by the above mentioned solution surjection $R_\infty \rightarrow R_2$.

Proof. The compatibility with the defining relations in $\text{As}^+(R_\infty)$ follows from the fact that y and $-y + 2x$ are always of the same parity. \square

Definition 4.3. In what follows, an application of a defining relation in $\text{As}^+(R_\infty)$ or its inverse in a rewriting sequence will be called a *braiding move*.

Definition 4.4. The numbers $l_0(w)$ and $l_1(w)$ are called the *even* and the *odd length* of $w \in \text{As}^+(R_\infty)$ respectively.

Their sum is the familiar length $l(w)$ with respect to the generators e_a .

Lemma 4.5. *The map*

$$\begin{aligned}\omega: \text{As}^+(R_\infty) &\rightarrow \mathbb{Z}, \\ e_{a_1}e_{a_2}\cdots e_{a_n} &\mapsto a_1 - a_2 + \cdots + (-1)^{n+1}a_n, \\ 1 &\mapsto 0\end{aligned}$$

is well defined.

Proof. This definition is compatible with the braiding moves, since

$$x - y = (-y + 2x) - x. \quad \square$$

Definition 4.6. The number $\omega(w)$ is called the *weight* of $w \in \text{As}^+(\mathbb{R}_\infty)$.

This weight function is extended to general Alexander quandles in [10]. Note that ω is not a morphism of monoids, but rather a monoid 1-cocycle. The weight function is useful for computations in $\text{As}^+(\mathbb{R}_\infty)$:

Lemma 4.7. For any $w \in \text{As}^+(\mathbb{R}_\infty)$ and $a \in \mathbb{Z}$, we have

$$(4.2) \quad we_a = e_{(-1)^{l(w)a+2\omega(w)}}w.$$

Proof. An easy induction on the length $l(w)$ of w . □

A direct consequence of the above formula is the centrality of squares in $\text{As}^+(\mathbb{R}_\infty)$:

Lemma 4.8. For any $a, b \in \mathbb{Z}$, we have

$$(4.3) \quad e_a^2 e_b = e_b e_a^2.$$

Lemma 4.9. The map

$$\begin{aligned} \delta: \text{As}_{\geq 1}^+(\mathbb{R}_\infty) &\rightarrow \mathbb{N}_0, \\ e_{a_1} e_{a_2} \cdots e_{a_n} &\mapsto \gcd(a_1 - a_2, a_2 - a_3, \dots, a_{n-1} - a_n), \quad n \geq 2, \\ e_a &\mapsto 0, \end{aligned}$$

is well defined.

Here $\text{As}_{\geq 1}^+(\mathbb{R}_\infty)$ is the set of elements in $\text{As}^+(\mathbb{R}_\infty)$ of length ≥ 1 .

Proof. The gcd from the above definition can be replaced with the gcd of all the differences $a_i - a_j$, where $1 \leq i < j \leq n$. To show its stability under braiding moves, use $x - y = (-y + 2x) - x$ and $a - (-y + 2x) = (a - y) - 2(x - y)$. □

Definition 4.10. The number $\delta(w)$ is called the *density* of $w \in \text{As}_{\geq 1}^+(\mathbb{R}_\infty)$.

The density vanishes if and only if we have $a_1 = a_2 = \dots = a_n$. This happens precisely for the powers e_a^n . They are called *frozen* since they cannot be rewritten in another way: no non-trivial braiding moves apply to them. In what follows, we will mainly consider the interesting case $\delta(w) > 0$.

Lemma 4.11. For $w \in \text{As}_{\geq 2}^+(\mathbb{R}_\infty)$ with $\delta(w) > 0$, let $\alpha(w) \in \mathbb{N}_0$ be the minimal representative of the index a of any of its letters e_a modulo $\delta(w)$. For $w = e_a^n \in \text{As}_{\geq 1}^+(\mathbb{R}_\infty)$ with $\delta(w) = 0$, put $\alpha(w) = a$. This yields a well-defined map

$$\alpha: \text{As}_{\geq 1}^+(\mathbb{R}_\infty) \rightarrow \mathbb{Z}.$$

Proof. By the definition of $\delta(w)$, all letters from any word representing w give the same residue modulo d . □

Definition 4.12. The number $\alpha(w)$ is called the *anchor* of $w \in \text{As}_{\geq 1}^+(\mathbb{R}_\infty)$.

Note that for any word $1 \neq w = e_{a_1} \dots e_{a_n}$, the coset $\alpha(w) + \delta(w) \cdot \mathbb{Z}$ is minimal amongst all cosets in \mathbb{Z} that contain the integers a_1, \dots, a_n .

To better understand how these multiple invariants work, the reader might look at their values for different elements:

w	$l_0(w)$	$l_1(w)$	$\omega(w)$	$\delta(w)$	$\alpha(w)$
$e_1 e_1$	0	2	0	0	1
$e_0 e_{-1}$	1	1	1	1	0
$e_1 e_{-1}$	0	2	2	2	1
$e_1 e_{-1} e_1$	0	3	3	2	1
$e_{-6} e_{-2} e_{-2}$	3	0	-6	4	2

To get a complete family of invariants, we need to replace l_0 and l_1 with something finer.

For integers d, a , we denote by $\text{As}_{d,a}^+(\mathbb{R}_\infty)$ the set of all $w \in \text{As}^+(\mathbb{R}_\infty)$ such that $\delta(w) = d$ and $\alpha(w) = a$.

Lemma 4.13. For $w \in \text{As}_{d,a}^+(R_\infty)$ where $d > 0$ and $0 \leq a < d$, take any of its representatives, and replace each of its letters e_x with $e_{(x-a)/d}$. This yields a well-defined element \bar{w} with $\delta(\bar{w}) = 1$.

Note that the index $(x-a)/d$ can alternatively be expressed as $\lfloor \frac{x}{d} \rfloor$, using the floor function.

Proof. The numbers $(x-a)/d$ are integers due to the definition of $d = \delta(w)$ and $a = \alpha(w)$. The operation is well-defined since the map $f: x \mapsto (x-a)/d$ intertwines the solution r from Eq. (4.1), in the sense of $r \circ (f \times f) = (f \times f) \circ r$. Finally, $\delta(\bar{w}) = \delta(w)/d = 1$. \square

Definition 4.14. The element \bar{w} is called the *essentialisation* of $w \in \text{As}_{\geq 2}^+(R_\infty)$. The numbers $\bar{l}_0(w) = l_0(\bar{w})$ and $\bar{l}_1(w) = l_1(\bar{w})$ are called the *essential even* and the *odd length* of w respectively.

Here is what this looks like in our examples:

w	\bar{w}	$\bar{l}_0(w)$	$\bar{l}_1(w)$
$e_1 e_{-1}$	$e_0 e_{-1}$	1	1
$e_1 e_{-1} e_1$	$e_0 e_{-1} e_0$	2	1
$e_{-6} e_{-2} e_{-2}$	$e_{-2} e_{-1} e_{-1}$	1	2

Given $d = \delta(w) > 0$, $a = \alpha(w)$, and \bar{w} , one can reconstruct w . We will thus restrict our attention to the case $\delta(w) = 1$ (corresponding to the essentialisations) in the major part of what follows.

Definition 4.15. The elements $w \in \text{As}_{\geq 2}^+(R_\infty)$ with $\delta(w) = 1$ are called *full*. The set of all such elements is called the *full reflection semigroup*, denoted by FRS.

This object plays a role analogous to the full transposition monoids FTS_d in Section 3. It is indeed a semigroup, because of the following property.

Lemma 4.16. The product of any full element $w \in \text{FRS}$ with any $v \in \text{As}^+(R_\infty)$ is full. That is, both wv and vw lie in FRS.

Proof. The differences in the gcd used to compute $\delta(wv)$ or $\delta(vw)$ include those used to compute $\delta(w)$. \square

The purpose of the remainder of this section is to prove that the 5 invariants above completely determine an element from $\text{As}^+(R_\infty)$:

Theorem 4.17. Two elements coincide in $\text{As}_{\geq 1}^+(R_\infty)$ if and only if they have the same values of the invariants δ , α , ω , \bar{l}_0 , and \bar{l}_1 .

This will also allow us to construct a normal form in this monoid, and to completely determine the algebraic structure of the full part FRS.

Let us start with considering short elements in $\text{As}^+(R_\infty)$.

In length 1, every element admits a unique presentation, e_a , and the index a is exactly the weight of the element: $a = \omega(e_a)$.

In length 2, a braiding move can be written as

$$w = e_a e_b = e_{-b+2a} e_a = e_{a+\omega(w)} e_a,$$

hence the set of all the words representing w is

$$(4.4) \quad \{e_{a+k\omega(w)} e_{a+(k-1)\omega(w)} : k \in \mathbb{Z}\}.$$

Such a set is uniquely determined by $\omega(w)$ and $\alpha(w)$ (which is a modulo $\omega(w)$). Note that in degree 2 the density $\delta(w)$ is just the absolute value of the weight.

In the first interesting case, that of length 3, the weight and the density provide a complete invariant:

Lemma 4.18. Any length 3 element $w \in \text{As}^+(D_\infty)$ can be presented as $g = e_{\omega(w)+\delta(w)}^2 e_{\omega(w)}$.

In particular, this presentation tells us that the anchor $\alpha(w)$ is precisely $\omega(w)$ modulo $\delta(w)$.

Proof. To a length 3 word $e_a e_b e_c$ representing w , assign the difference vector $(d_1, d_2) = (a - b, b - c)$. A rewriting step $e_a e_b e_c \sim e_{-b+2a} e_a e_c$ or $e_a e_b e_c \sim e_a e_{-c+2b} e_b$ changes the difference vector to $(d_1, d_2 + d_1)$ or $(d_1 - d_2, d_2)$ respectively. Performing the Euclidean algorithm on the couple (d_1, d_2) , we obtain an expression $e_{a'} e_{b'} e_{c'} \sim e_a e_b e_c$ with difference vector $(0, d)$, where $d = \gcd(d_1, d_2) = \delta(w)$. It follows that $w = e_{a'}^2 e_{a'-d}$. Finally, $\omega(w) = a' - a' + (a' - d) = a' - d$, yielding $a' = \omega(w) + \delta(w)$. \square

The length 2 and length 3 cases exhibit fundamentally different behaviour. Starting from length 4, we at last get a uniform normal form:

Theorem 4.19. *Any full element $w \in \text{As}_{\geq 4}^+(\mathbb{R}_\infty)$ can be written as*

$$(4.5) \quad w = e_0^k e_1^l e_c, \quad \text{where } k, l > 0, c \in \mathbb{Z}.$$

We emphasize that we allow $c \in \{0, 1\}$ here. This presentation is unique for w with $l_0(w)$ or $l_1(w)$ equal to 1. Other w admit exactly two such presentations.

Our proof begins with several lemmata, interesting per se.

First, we will frequently work with the squares e_a^2 as if they were simple generators e_a . Let us explain why this is legitimate.

Lemma 4.20. *Let $e_{a_1} \cdots e_{a_m}$ and $e_{b_1} \cdots e_{b_m}$ be two words representing the same element $w \in \text{As}^+(\mathbb{D}_\infty)$. Let $k_1, \dots, k_m \in \mathbb{N}$ be m positive integers of the same parity. Then the word $e_{a_1}^{k_1} \cdots e_{a_m}^{k_m}$ can be rewritten in $\text{As}^+(\mathbb{D}_\infty)$ as $e_{b_1}^{k_{\sigma(1)}} \cdots e_{b_m}^{k_{\sigma(m)}}$. Here $\sigma \in S_m$ is some permutation.*

This lemma remains valid for all involutive quandles.

Proof. The rewriting procedure for w consists in applying the braiding moves $e_x e_y = e_{x \triangleright y} e_x$. But we have an analogous relation for powers, $e_x^p e_y^q = e_{x \triangleright y}^q e_x^p$, in two situations:

(1) for odd p , since

$$e_x^p e_y = e_x e_y e_x^{p-1} = e_{x \triangleright y} e_x^p;$$

we used that for odd p , e_x^{p-1} is a product of squares, hence central by (4.3);

(2) for even p and q , since

$$e_x^p e_y^q = e_x^{p-1} e_y^q e_x = e_{x \triangleright y}^q e_x^p;$$

we first used the centrality of e_y^q for even q , then the previous calculation for odd $p-1$. \square

We also need the following arithmetic lemma:

Lemma 4.21. *Let $a, b, c \in \mathbb{Z}$, with $a \neq b$. Then there exists an $n \in \mathbb{N}$ such that*

$$\gcd(a + nc, b + nc) = \gcd(a, b, c).$$

Moreover, if a and b are of different parity, then there are both even and odd n satisfying this condition.

Proof. The division by $\gcd(a, b, c)$ reduces the lemma to the case $\gcd(a, b, c) = 1$. We will present $\gcd(a + nc, b + nc)$ in the equivalent form $\gcd(a + nc, b - a)$. A prime divisor p of $b - a$ cannot divide a and c simultaneously, as otherwise it would be also a divisor of b and hence of $\gcd(a, b, c) = 1$. Then there exists an $n_p \in \mathbb{Z}$ such that p does not divide $a + n_p c$. Indeed, one can take $n_p = 0$ if $p \nmid a$ and $n_p = 1$ otherwise. By the Chinese remainder theorem, there exists an $n \in \mathbb{N}$ congruent to n_p for all prime divisors p of $b - a \neq 0$. Then no prime divisor of $b - a$ divides $a + nc$, and $\gcd(a + nc, b - a) = 1$.

Now, if $a - b$ is odd, the above argument concerns only odd primes p . Therefore, when using the Chinese remainder theorem, one can impose any value of $n \pmod 2$. \square

Proof of Theorem 4.19. Take any presentation of a $w \in \text{As}_{\geq 4}^+(\mathbb{D}_\infty)$ with $\delta(w) = 1$, and start simplifying it. A repeated application of Lemma 4.18 to three-letter segments of w yields a presentation

$$w = e_{b_1}^2 \cdots e_{b_m}^2 h, \quad b_j \in \mathbb{Z}, h \in \text{As}^+(\mathbb{D}_\infty) \text{ of length } \leq 2.$$

Lemmata 4.20 and 4.18 allow us to transform this presentation into

$$(4.6) \quad w = e_a^{2k} e_b^{2l} h, \quad a, b \in \mathbb{Z}, \quad k, l \in \mathbb{N}_0, \quad h \in \text{As}^+(\text{D}_\infty) \text{ of length } \leq 2.$$

Case 1: a long tail $h = e_c e_d$.

Lemma 4.22. *Any $g = e_a^2 e_b e_c \in \text{FRS}$ can be rewritten in at least one of the following forms:*

$$g = e_0^2 e_1 e_{1-\omega(g)}, \text{ or } g = e_0 e_1^2 e_{-\omega(g)}.$$

Proof. The element $e_a e_b e_c$ is still full. By Lemma 4.18, we can rewrite g as

$$g = e_a \cdot e_a e_b e_c \sim e_a e_d^2 e_{d-1} \sim e_d^2 e_a e_{d-1}.$$

Since rewriting leaves the weight unchanged, we have $\omega(g) = a - (d - 1)$, so $d = a - \omega(g) + 1$, and the above rewriting sequence becomes

$$(4.7) \quad g \sim e_{a-\omega(g)+1}^2 e_a e_{a-\omega(g)}.$$

Observe that the last word depends only on the first letter e_a and the weight $\omega(g)$ of the original word. By Eq. (4.3) and Eq. (4.2), it can be rewritten as

$$e_{a-\omega(g)+1}^2 e_a e_{a-\omega(g)} \sim e_a e_{a-\omega(g)} e_{a-\omega(g)+1}^2 \sim e_{a-\omega(g)+1+2(a-(a-\omega(g)))}^2 e_a e_{a-\omega(g)} = e_{a+\omega(g)+1}^2 e_a e_{a-\omega(g)}.$$

Now, applying Eq. (4.7) with the first letter $a + \omega(g) + 1$ instead of a and the same weight $\omega(g)$, we obtain

$$g \sim e_{a+2}^2 e_{a+\omega(g)+1} e_{a+1}.$$

A repetition of this procedure or its inverse leaves us either with an expression of the form

$$e_{2\omega(g)+1}^2 e_1 \sim e_2^2 e_1 e_{1-\omega(g)} \sim e_1 e_0^2 e_{1-\omega(g)} \sim e_0^2 e_1 e_{1-\omega(g)},$$

or with an expression of the form

$$e_1^2 e_{\omega(g)} e_0 \sim e_1^2 e_0 e_{-\omega(g)} \sim e_0 e_1^2 e_{-\omega(g)}. \quad \square$$

We will now apply a similar reduction to elements of the form $g = e_a^{2k} e_b^{2l} e_c e_d$.

First assume $k, l > 0$ and $a \neq b$. Lemma 4.20 allows us to apply to $e_a^{2k} e_b^{2l}$ the arguments used for the length 2 case, and rewrite it as $e_{a+n(a-b)}^{2k'} e_{a+(n-1)(a-b)}^{2l'} = e_{a+n(a-b)}^{2k'} e_{b+n(a-b)}^{2l'}$ for any $n \in \mathbb{Z}$ (cf. Eq. (4.4)), with $\{k', l'\} = \{k, l\}$. Putting $a' = a + n(a - b)$ and $b' = b + n(a - b)$, we get

$$(4.8) \quad w = e_{a'}^{2k'} e_{b'}^{2(l'-1)} e_{b'}^2 e_c e_d.$$

We would like to apply Lemma 4.22 to the part $e_{b'}^2 e_c e_d$ of this word. For this we have to ensure that it is full. We have

$$\delta(e_{b'}^2 e_c e_d) = \gcd(b' - c, c - d) = \gcd(b' - c, b' - d) = \gcd(b + n(a - b) - c, b + n(a - b) - d).$$

By Lemma 4.21, for some n the latter expression equals

$$\gcd(b - c, b - d, a - b) = \gcd(a - b, b - c, c - d) = \delta(e_a^{2k} e_b^{2l} e_c e_d) = 1.$$

We will work with such an n , and write again a, b, k, l instead of a', b', k', l' for simplicity. Lemma 4.22 now yields

$$(4.9) \quad w = e_a^{2k} e_b^{2(l-1)} e_0^2 e_1 e_{c'} \text{ or } e_a^{2k} e_b^{2(l-1)} e_0 e_1^2 e_{d'},$$

with $c' = 1 - \omega(w)$ or $d' = -\omega(w)$.

Lemma 4.23. *For any $u \in \text{As}^+(\text{D}_\infty)$ and $t \in \mathbb{Z}$, we have the equality*

$$e_t^2 u e_0 e_1 = e_\tau^2 u e_0 e_1,$$

where $\tau = 0$ for even t and $\tau = 1$ for odd t .

Proof. Using the centrality of the square e_t^2 and the quasi-commutativity relation (4.2), we get

$$e_t^2 u e_0 e_1 \sim u e_0 e_1 e_t^2 \sim u e_{t+2(0-1)}^2 e_0 e_1 = e_{t-2}^2 u e_0 e_1.$$

Iterating this procedure or its inverse, one replaces t with τ . \square

This lemma allows us to replace a and b in Eq. (4.9) with α and $\beta \in \{0, 1\}$. Moving the central elements e_β^2 and e_α^2 inside this word, one gets the desired form (4.5).

If, say, $k = 0$ and $l > 0$, then in $w = e_b^{2(l-1)} e_b^2 e_c e_d$ we directly have $\delta(e_b^2 e_c e_d) = \delta(e_b^{2l} e_c e_d) = 1$, and the above arguments apply.

The case $k = l = 0$ is impossible since we are in length ≥ 4 .

If $a = b$, then $e_a^{2k} e_b^{2l} = e_b^{2(k+l)}$, and we are in the previous situation.

Case 2: an empty tail $h = 1$. If, say, $l > 0$, then the presentation $w = e_a^{2k} e_b^{2(l-1)} e_b e_b$ brings us to the previous case. Alternatively, this case can be dealt with using Lemma 4.20.

Case 3: a 1-letter tail $h = e_c$. In length 5, we have

$$w = e_a^2 e_b^2 e_c = e_a \cdot e_a e_b^2 e_c,$$

with possibly equal a and b . The element $e_a e_b^2 e_c$ is still full, thus Lemma 4.22 yields

$$w \sim e_a e_0^2 e_1 e_{c'} \text{ or } e_a e_0 e_1^2 e_d.$$

In the first case, we once again apply Lemma 4.22, together with the representation (4.6), to the underlined subword to get

$$w \sim e_0 e_{-a} e_0 e_1 e_{c'} \sim e_0 e_0^k e_1^l e_{c''} = e_0^{k+1} e_1^l e_{c''}, \quad k, l > 0.$$

Note that the element $e_{-a} e_0 e_1 e_{c'}$ is indeed full because of the index difference $0 - 1 = -1$.

The second case is similar:

$$w \sim e_a e_0 e_1 e_1 e_d \sim e_a e_0 e_1 e_{-d+2} e_1 \sim e_0^k e_1^l e_{d'} e_1 \sim e_0^k e_1^{l+1} e_{2-d'}, \quad k, l > 0.$$

In greater length, we have

$$w = e_a^{2k} e_b^{2l} e_c \sim e_a^{2(k-1)} e_b^{2(l-1)} e_a^2 e_b^2 e_c \sim e_a^{2(k-1)} e_b^{2(l-1)} e_0^{k'} e_1^{l'} e_{c'}, \quad k', l' > 0.$$

We assumed $k, l > 0$ (otherwise a single power, say e_a^{2k} , should be split into two powers), and used the fullness of the element $e_a^2 e_b^2 e_c$. Lemma 4.23 allows one to replace a and b with α and $\beta \in \{0, 1\}$, and the centrality of squares to rearrange the result into the desired form.

It remains to discuss whether the presentation (4.5) is unique. For a given parity of c , the powers k and l are uniquely determined from $l_0(w)$ and $l_1(w)$; the value of c can then be computed from the weight $\omega(w)$. Thus w admits at most 2 desired presentations, one for each parity of c . The assumption $l_0(w) = 1$ forces k to be 1 and c to be odd; thus w admits only 1 desired presentation. The case $l_1(w) = 1$ is analogous.

We will now show that elements w with $l_0(w) > 1$ and $l_1(w) > 1$ admit 2 desired presentations. In length 4, these two constraints imply $l_0(w) = l_1(w) = 2$. Then $\omega(w)$ is even, and in the proof of 4.22, Eq. (4.7) allows us to change the parity of the first letter. Then the algorithm from the proof can present g both as $e_0^2 e_1 e_{1-\omega(g)}$ and $e_0 e_1^2 e_{-\omega(g)}$.

In general even length, let us go back to the presentation $w = e_a^{2k} e_b^{2l} e_c e_d$ that we have obtained before. If c and d are of the same parity, then for the element $e_b^2 e_c e_d$ in Eq. (4.8) to be full, b' needs to be of the opposite parity. Hence $l_0(e_b^2 e_c e_d) = l_1(e_b^2 e_c e_d) = 2$, and the length 4 case yields for w two presentations of the form (4.5), with last letters of different parity. If c and d are of different parity, then so are a and b (otherwise $l_0(w)$ or $l_1(w) = 1$). Then Lemma 4.21 produces an odd and an even n satisfying $\gcd(b + n(a - b) - c, b + n(a - b) - d) = \gcd(b - c, b - d, a - b)$. Since $a - b$ is odd, one can thus force any desired parity of $b' = b + n(a - b)$. Our rewriting algorithm will then produce two presentations of the form (4.5), with the last letters of different parity.

In the odd length, the indices a and b in the presentation $w = e_a^{2k} e_b^{2l} e_c$ are of different parity (otherwise $l_0(w)$ or $l_1(w) \leq 1$). Since the central elements e_a^{2k} and e_b^{2l} can be interchanged in this expression, one may assume that a and c are of the same parity. But then $l_0(e_a e_b^2 e_c) = l_1(e_a e_b^2 e_c) = 2$, and once again the length 4 case yields for w two presentations of the form (4.5), with the last letters of different parity. \square

Theorem 4.17 now follows easily:

Proof of Theorem 4.17. Since the length ≤ 3 case was settled in Lemma 4.18 and preceding paragraphs, it remains to show how to reconstruct $w \in \text{As}_{\geq 4}^+(\mathbb{R}_\infty)$ from the evaluations of the five invariants δ , α , ω , \bar{l}_0 , and \bar{l}_1 . First, for the essentialisation \bar{w} , we know the values $l_0(\bar{w}) = \bar{l}_0(w)$, $l_1(\bar{w}) = \bar{l}_1(w)$, and

$$\omega(\bar{w}) = \begin{cases} (\omega(w) - \alpha(w)) / \delta(w) & \text{in odd length,} \\ \omega(w) / \delta(w) & \text{in even length.} \end{cases}$$

Theorem 4.19 then allows one to reconstruct \bar{w} , which, together with the values $\omega(w)$ and $\alpha(w)$, gives back w . \square

For full elements, these numeric invariants are sufficient not only to distinguish the elements of FRS, but also to describe the algebraic structure of this semigroup:

Theorem 4.24. *The following map is an injective morphism of semigroups:*

$$\begin{aligned} \iota: \text{FRS} &\rightarrow \mathbb{Z} \rtimes (\mathbb{N} \times \mathbb{N}), \\ w &\mapsto (\omega(w), l_0(w), l_1(w)). \end{aligned}$$

Here $\mathbb{N} \times \mathbb{N}$ acts on \mathbb{Z} via $(k, l) \cdot m = (-1)^{k+l}m$. The image of this inclusion is

$$\text{Im}(\iota) = \{(m, k, l) : k, l \in \mathbb{N}, m \in \mathbb{Z}, l \equiv m \pmod{2}\}.$$

Proof. The map ι preserves products, since

$$\begin{aligned} \iota(v) \cdot \iota(w) &= (\omega(v), l_0(v), l_1(v)) \cdot (\omega(w), l_0(w), l_1(w)) \\ &= (\omega(v) + (-1)^{l_0(v)+l_1(v)}\omega(w), l_0(v) + l_0(w), l_1(v) + l_1(w)) \\ &= (\omega(v) + (-1)^{l(v)}\omega(w), l_0(vw), l_1(vw)) = (\omega(vw), l_0(vw), l_1(vw)) = \iota(vw). \end{aligned}$$

Theorem 4.17 guarantees its injectivity (recall that for a full w , the evaluations $\delta(w) = 1$ and $\alpha(w) = 0$ are irrelevant). Further, $\omega(w)$ and $l_1(w)$ are of the same parity, since the $l_0(w)$ even-indexed letters in w do not change the parity of the weight $\omega(w)$, whereas the $l_1(w)$ odd-indexed letters do. Finally, take $k, l \in \mathbb{N}$ and $m \in \mathbb{Z}$ with $l \equiv m \pmod{2}$. If $l > 1$, then

$$(m, k, l) = \iota(e_0^k e_1^{l-1} e_c), \quad \text{where } c = \begin{cases} 1 - m & k, l \text{ even,} \\ 1 + m & l \text{ even, } k \text{ odd,} \\ m & k \text{ even, } l \text{ odd,} \\ -m & k, l \text{ odd.} \end{cases}$$

Indeed, in all four cases c is odd, implying the desired values of l_0 and l_1 , and the weight of $e_0^k e_1^{l-1} e_c$ is m . In the same way,

$$(m, k, 1) = \iota(e_0^{k-1} e_1 e_{1+(-1)^k m}). \quad \square$$

As a consequence, the full part of the structure **monoid** of the infinite reflection solution injects into the structure **group** of this solution, exactly as it happened for transposition solutions:

Corollary 4.25. *The tautological map*

$$\begin{aligned} \text{FRS} &\rightarrow \text{As}(\mathbb{R}_\infty), \\ e_{a_1} \dots e_{a_k} &\mapsto e_{a_1} \dots e_{a_k} \end{aligned}$$

is an injective morphism of semigroups.

Proof. It suffices to show that the invariants ω , l_0 and l_1 extend to the group $\text{As}(\mathbb{R}_\infty)$. To do this, one easily checks that the assignment

$$\begin{aligned} \text{As}(\mathbb{R}_\infty) &\rightarrow \mathbb{Z} \rtimes (\mathbb{Z} \times \mathbb{Z}), \\ e_a &\mapsto (a, 1, 0) \text{ for even } a, \\ e_a &\mapsto (a, 0, 1) \text{ for odd } a, \end{aligned}$$

extends to the entire group $\text{As}(\mathbb{R}_\infty)$, and that for a product of generators (without any inverses) this map is precisely $\omega \times l_0 \times l_1$. \square

The algebraic structure of the entire monoid $\text{As}^+(\mathbb{R}_\infty)$ is much more subtle. For instance, the density of a product depends not only on the density of each component, but also on their anchors:

Lemma 4.26. *The density of the product of two elements $v, w \in \text{As}_{\geq 1}^+(\mathbb{R}_\infty)$ can be computed as follows:*

$$(4.10) \quad \delta(vw) = \gcd(\delta(v), \delta(w), \alpha(v) - \alpha(w)).$$

Proof. Putting $v = e_{a_1}e_{a_2} \cdots e_{a_n}$ and $w = e_{b_1}e_{b_2} \cdots e_{b_m}$, we get

$$\begin{aligned} \delta(vw) &= \gcd(a_1 - a_2, a_2 - a_3, \dots, a_{n-1} - a_n, a_n - b_1, b_1 - b_2, \dots, b_{m-1} - b_m) \\ &= \gcd(\delta(v), a_n - b_1, \delta(w)) = \gcd(\delta(v), \alpha(v) - \alpha(w), \delta(w)). \end{aligned}$$

Indeed, since $a_n = \alpha(v) + \delta(v)a'$ and $b_1 = \alpha(w) + \delta(w)b'$ for some $a', b' \in \mathbb{Z}$, we have

$$a_n - b_1 \equiv \alpha(v) - \alpha(w) \pmod{\gcd(\delta(v), \delta(w))}. \quad \square$$

5. HOW STRUCTURE MONOIDS OF REFLECTION SOLUTIONS GROW

In this section, we will present a normal form for the structure monoids of all finite reflection solutions $(\mathbb{R}_d, r_\triangleright)$, inherited from the normal form for the infinite reflection solution (\mathbb{R}_∞, r) (Theorem 4.19). This will allow us to compute the growth series of these monoids. Recall that we identify the set \mathbb{R}_d with \mathbb{Z}_d ; the solution r_\triangleright then takes the form (4.1).

We will start by adapting the five invariants for $\text{As}_{\geq 1}^+(\mathbb{R}_\infty)$ to the finite setting. The proofs of the following results repeat verbatim those of the analogous statements from Section 4; one simply turns all equalities into congruences modulo d .

Lemma 5.1. *The map*

$$\begin{aligned} \delta: \text{As}_{\geq 1}^+(\mathbb{R}_d) &\rightarrow \mathbb{Z}, \\ e_{a_1}e_{a_2} \cdots e_{a_n} &\mapsto \gcd(d, a_1 - a_2, a_2 - a_3, \dots, a_{n-1} - a_n), \quad n \geq 2, \\ e_a &\mapsto d, \end{aligned}$$

is well defined.

Note that here it is convenient to impose $\delta(e_a) = d$ rather than 0, which was our choice in the infinite case.

Definition 5.2. The number $\delta(w) \in \mathbb{Z}$ is called the *density* of $w \in \text{As}_{\geq 1}^+(\mathbb{R}_d)$. The elements w with $\delta(w) = 1$ are called *full*. The set of all such elements is called the *full reflection semigroup of level d* , denoted by FRS_d .

We will soon see that FRS_d is indeed a sub-semigroup of $\text{As}_{\geq 1}^+(\mathbb{R}_d)$.

Lemma 5.3. *For $w \in \text{As}_{\geq 1}^+(\mathbb{R}_d)$, let $\alpha(w) \in \mathbb{N}_0$ be the minimal representative of the index a of any of its letters e_a modulo $\delta(w)$. This yields a well-defined map*

$$\alpha: \text{As}_{\geq 1}^+(\mathbb{R}_d) \rightarrow \mathbb{N}_0.$$

Definition 5.4. The number $\alpha(w)$ is called the *anchor* of $w \in \text{As}_{\geq 1}^+(\mathbb{R}_d)$.

Notation 5.5. The (possibly empty) set of all $w \in \text{As}_{\geq 1}^+(\mathbb{R}_d)$ with the same density c and the same anchor a is denoted by $\text{As}_{c,a}^+(\mathbb{R}_d)$.

This set is non-empty if and only if c is a divisor of d and a lies in $\{0, 1, \dots, c-1\}$.

Proposition 5.6. *For any $c \mid d$ and $a \in \{0, 1, \dots, c-1\}$, the set $\text{As}_{c,a}^+(\mathbb{R}_d)$ is a sub-semigroup of $\text{As}_{\geq 1}^+(\mathbb{R}_d)$ isomorphic to the full reflection semigroup $\text{FRS}_{\frac{d}{c}}$:*

$$\text{As}_{c,a}^+(\mathbb{R}_d) \cong \text{FRS}_{\frac{d}{c}}.$$

Proof. Relation (4.10) for densities is still valid in $\text{As}_{\geq 1}^+(\mathbb{R}_d)$. For v and w sharing the same density c and the same anchor a , it yields

$$\delta(vw) = \gcd(c, c, a - a) = c.$$

Also, the indices of all letters in any expression for vw are congruent to $a \pmod{c}$. Hence $vw \in \text{As}_{c,a}^+(\mathbb{R}_d)$, and the latter is a sub-semigroup.

Next, consider the arithmetic bijection

$$\begin{aligned} f: \{x \in \mathbb{Z}_d : x \equiv a \pmod{c}\} &\xrightarrow{\sim} \mathbb{Z}_{\frac{d}{c}}, \\ x &\mapsto \frac{x - a}{c}. \end{aligned}$$

Like any affine function, it intertwines the solution r from Eq. (4.1), and thus induces a semigroup injection $\bar{f}: \text{As}_{c,a}^+(\mathbb{R}_d) \hookrightarrow \text{As}_{\geq 1}^+(\mathbb{R}_{\frac{d}{c}})$. Moreover, the condition $\delta(w) = c$ implies $\delta(\bar{f}(w)) = 1$, thus \bar{f} actually injects $\text{As}_{c,a}^+(\mathbb{R}_d)$ into $\text{FRS}_{\frac{d}{c}}$. To see the surjectivity, for any $u = e_{a_1} \cdots e_{a_n} \in \text{FRS}_{\frac{d}{c}}$, consider the well-defined element $u' = e_{a_1 c + a} \cdots e_{a_n c + a} \in \text{As}^+(\mathbb{R}_d)$. Its degree is $c \cdot \delta(u) = c$, and its anchor is a ; hence $u' \in \text{As}_{c,a}^+(\mathbb{R}_d)$. By construction, $\bar{f}(u') = u$, thus u' is a preimage of u . Hence \bar{f} yields the desired semigroup isomorphism. \square

Thus the semigroup $\text{As}_{\geq 1}^+(\mathbb{R}_d)$ splits into a disjoint union of sub-semigroups. For each divisor c of d , there are exactly c sub-semigroups isomorphic to $\text{FRS}_{\frac{d}{c}}$. The computation of the growth series of the structure monoids $\text{As}^+(\mathbb{R}_d)$ is thus reduced to that of its full components. Note that as an abuse of notation, we write

$$\mathcal{G}_{\text{FRS}_d}(t) = \sum_{g \in \text{FRS}_d} t^{l(g)},$$

which is not a growth series but a restricted growth series.

Corollary 5.7. *For any integer $d \geq 2$, the growth series of the monoids $\text{As}^+(\mathbb{R}_d)$ and FRS_c are related as follows:*

$$(5.1) \quad \mathcal{G}_{\text{As}^+(\mathbb{R}_d)}(t) = 1 + \sum_{c|d} \frac{d}{c} \cdot \mathcal{G}_{\text{FRS}_c}(t).$$

Note that we exchanged the roles of c and $\frac{d}{c}$ from the preceding arguments.

We will thus focus on the full semigroups FRS_d . Their structure will be entirely captured by the weight and the length functions, the latter being split into the odd and the even parts for even d .

Lemma 5.8. *For any integer $d \geq 2$, the assignment*

$$\begin{aligned} l: \text{As}^+(\mathbb{R}_d) &\rightarrow \mathbb{N}_0, \\ e_a &\mapsto 1 \end{aligned}$$

uniquely extends to a well-defined semigroup morphism. For even d , it can be refined into another semigroup morphism by imposing

$$\begin{aligned} l_0 \times l_1: \text{As}^+(\mathbb{R}_d) &\rightarrow \mathbb{N}_0 \times \mathbb{N}_0, \\ e_a &\mapsto \begin{cases} (1, 0) & \text{if } a \text{ is even,} \\ (0, 1) & \text{if } a \text{ is odd.} \end{cases} \end{aligned}$$

For even d , we consider an element in \mathbb{Z}_d to be even resp. odd if any of its representatives in \mathbb{Z} is even resp. odd.

Definition 5.9. The numbers $l(w)$, $l_0(w)$, and $l_1(w)$ are called the *length*, the *even length*, and the *odd length* of w respectively.

Lemma 5.10. *The map*

$$\begin{aligned}\omega: \text{As}^+(\mathbb{R}_d) &\rightarrow \mathbb{Z}_d, \\ e_{a_1}e_{a_2}\cdots e_{a_n} &\mapsto a_1 - a_2 + \cdots + (-1)^{n+1}a_n, \\ 1 &\mapsto 0\end{aligned}$$

is well defined.

Definition 5.11. The element $\omega(w) \in \mathbb{Z}_d$ is called the *weight* of w .

Now, we are ready to adapt the normal form from Theorem 4.19 to the finite setting:

Theorem 5.12. *Any full element $w \in \text{As}_{\geq 4}^+(\mathbb{R}_d)$ can be written as*

$$(5.2) \quad w = e_0^k e_1^l e_c, \quad \text{where } k, l > 0, \quad c \in \mathbb{Z}_d.$$

For even d , this presentation is unique for w with $l_0(w)$ or $l_1(w)$ equal to 1, whereas other w admit exactly two such presentations.

For odd d and any w , there is exactly one such presentation with $l = 1$.

Before presenting the proof, we need a generalisation of Lemma 4.21:

Lemma 5.13. *Take $k \geq 2$ integers a_1, \dots, a_k , and some $d \in \mathbb{Z}$. Then there are integers m_1, \dots, m_k such that*

$$\gcd(a_1 + m_1d, \dots, a_k + m_kd) = \gcd(d, a_1, a_2, \dots, a_k).$$

If d is odd, then these integers can be chosen such that $a_i + m_id$ is odd for all $1 \leq i \leq k$.

Proof. Without loss of generality, we may assume $a_1 \neq 0$. Indeed, for this one should permute the a_i if necessary; this does not work only when all $a_i = 0$, in which case the statement is trivial.

We first prove that for all $a_1, a_2, d \in \mathbb{Z}$, there is an m such that $\gcd(a_1, a_2 + md) = \gcd(d, a_1, a_2)$. Dividing by $\gcd(d, a_1, a_2)$, we may assume that $\gcd(d, a_1, a_2) = 1$. For any prime divisor $p|a_1$, there exists an integer $m_{(p)} \in \mathbb{Z}$ such that p does not divide $a_2 + md$ for any $m \equiv m_{(p)} \pmod{p}$. Applying the Chinese remainder theorem, we obtain an $m \in \mathbb{Z}$ such that $a_2 + md$ and a_1 have no common prime divisors, providing $\gcd(a_1, a_2 + md) = 1$.

Now for the general case, let $d, a_1, \dots, a_k \in \mathbb{Z}$. The previous paragraph provides us with $m_2, \dots, m_k \in \mathbb{Z}$ such that $\gcd(a_1, a_i + m_id) = \gcd(d, a_1, a_i)$ for $1 \leq i \leq k$. Then with $m_1 = 0$, we have

$$\begin{aligned}\gcd(d, a_1, \dots, a_k) &= \gcd(\gcd(d, a_1, a_2), \gcd(d, a_1, a_3), \dots, \gcd(d, a_1, a_k)) \\ &= \gcd(\gcd(a_1, a_2 + m_2d), \gcd(a_1, a_3 + m_3d), \dots, \gcd(a_1, a_k + m_kd)) \\ &= \gcd(a_1, a_2 + m_2d, \dots, a_k + m_kd) = \gcd(a_1 + m_1d, \dots, a_k + m_kd).\end{aligned}$$

If d is odd, then replace a_i with $a'_i = a_i + m'_id$ in a way such that a'_i is odd for all $1 \leq i \leq k$. Then

$$\gcd(d, a_1, \dots, a_k) = \gcd(d, a'_1, \dots, a'_k) = \gcd(2d, a'_1, \dots, a'_k).$$

Now the first statement of the lemma shows the existence of m''_1, \dots, m''_k such that

$$\begin{aligned}\gcd(2d, a'_1, \dots, a'_k) &= \gcd(a'_1 + m''_1 \cdot 2d, \dots, a'_k + m''_k \cdot 2d) \\ &= \gcd(a_1 + (m'_1 + 2m''_1)d, \dots, a_k + (m'_k + 2m''_k)d) \\ &= \gcd(a'_1 + 2m''_1d, \dots, a'_k + 2m''_kd).\end{aligned}$$

It follows that $\gcd(d, a_1, \dots, a_k) = \gcd(a'_1 + 2m''_1d, \dots, a'_k + 2m''_kd)$. Since the a'_i are odd, so are the $a'_i + 2m''_id$. \square

Proof of Theorem 5.12. Take an element

$$u = e_{a_1} \cdots e_{a_k} \in \text{FRS}_d.$$

Its fullness can be expressed by the condition

$$\gcd(d, a_1 - a_2, a_1 - a_3, \dots, a_1 - a_k) = 1.$$

By Lemma 5.13, there are some $m_i \in \mathbb{Z}$ with

$$\gcd(a_1 - a_2 + m_1 d, a_1 - a_3 + m_2 d, \dots, a_1 - a_k + m_{k-1} d) = 1.$$

This allows us to lift u to a full element

$$u' = e_{a_1} e_{a_2 - m_1 d} \cdots e_{a_k - m_{k-1} d} \in \text{FRS}.$$

By Theorem 4.19, it can be presented as

$$u' = e_0^k e_1^l e_{c'} \quad \text{for some } k, l > 0, c' \in \mathbb{Z}.$$

Taking a quotient modulo d yields a new presentation of u :

$$u = e_0^k e_1^l e_c \quad \text{for some } k, l > 0, c \in \mathbb{Z}_d.$$

For even d , the parameters k , l and c are determined by $\omega(u)$, $l_0(u)$, $l_1(u)$ and the parity of c . The number of such presentations is then determined in the same way as in the infinite case (Theorem 4.19).

For odd d , we assume a_1 odd; otherwise replace each a_i with $a_i + d$. Lemma 5.13 guarantees that all elements $a_1 - a_i + m_{i-1} d$ above can be assumed odd, implying that all the $a_i - m_{i-1} d$ are even. This is translated by $l_1(u') = 1$. Then the presentation from Theorem 4.19, takes the particular form

$$u' = e_0^k e_1 e_{c'},$$

inducing an analogous presentation for u . Here $k = l(u) - 2$, and the parameter c for u is then uniquely determined by $\omega(u)$. Such a presentation is thus unique. \square

In a similar way, one adapts Theorem 4.24:

Theorem 5.14. *For even d , the following map is an injective morphism of semigroups:*

$$\begin{aligned} \iota_d: \text{FRS}_d &\rightarrow \mathbb{Z}_d \rtimes (\mathbb{N} \times \mathbb{N}), \\ w &\mapsto (\omega(w), l_0(w), l_1(w)). \end{aligned}$$

The image of this inclusion is

$$\text{Im}(\iota_d) = (\{(m, k, l) : k, l \in \mathbb{N}, k + l > 2, m \in \mathbb{Z}_d, l \equiv m \pmod{2}\}) \sqcup (\mathbb{Z}_d^* \times \{(1, 1)\}).$$

where $\mathbb{Z}_d^* = \{a \in \mathbb{Z}_d : \langle a \rangle = \mathbb{Z}_d\}$.

For odd $d > 1$, the following map is an injective morphism of semigroups:

$$\begin{aligned} \iota_d: \text{FRS}_d &\rightarrow \mathbb{Z}_d \rtimes \mathbb{N}_{\geq 2}, \\ w &\mapsto (\omega(w), l(w)). \end{aligned}$$

The image of this inclusion is

$$\text{Im}(\iota_d) = (\mathbb{Z}_d \times \mathbb{N}_{\geq 3}) \sqcup (\mathbb{Z}_d^* \times \{2\}).$$

For $d = 1$, the length function l realises a semigroup isomorphism $\text{FRS}_1 \cong \mathbb{N}$.

Here $\mathbb{N} \times \mathbb{N}$ and \mathbb{N} act on \mathbb{Z}_d via $(k, l) \cdot m = (-1)^{k+l} m$ and $k \cdot m = (-1)^k m$ respectively.

Note that the injectivity statements from the theorem, together with Proposition 5.6, allow one to exhibit a complete list of numerical invariants for the monoid $\text{As}^+(\text{R}_d)$ (5 for even d and 4 for odd d), in the spirit of Theorem 4.17. This theorem also implies that the full part of the structure **monoids** of all finite reflection solutions inject into the corresponding structure **groups**, as it was established in the infinite case in Corollary 4.25.

Proof. The $d = 1$ case is straightforward. In the remainder of the proof we assume $d > 1$. In particular, all full elements are of length ≥ 2 .

The well-definedness of the maps ι_d is checked in the same way as for the infinite reflection solution R_∞ . Their injectivity in length ≥ 4 is proved using the normal forms from Theorem 5.12.

In length 3, the arguments from the proof of Theorem 5.12 together with Lemma 4.22 yield presentations of the form

$$w = e_{\omega(w)+1}^2 e_{\omega(w)}.$$

Note that an element of this form is necessarily full because of the index difference $(\omega(w) + 1) - \omega(w) = 1$. In length 2, the fullness of w is equivalent to the invertibility of its weight, $\omega(w) \in \mathbb{Z}_d^*$. Then the discussion before Lemma 4.22 yields presentations of the form

$$w = e_0 e_{-\omega(w)}.$$

In both cases, the weight $\omega(w)$ determines w uniquely. Moreover, taking elements of the two particular forms above, one realises any weight in \mathbb{Z}_d and \mathbb{Z}_d^* respectively. This describes the corresponding components of $\text{Im}(\iota_d)$.

From now on, we work in length ≥ 4 .

Let us prove the surjectivity of ι_d for odd $d > 1$. Given some $m \in \mathbb{Z}_d$ and $k \in \mathbb{N}_{\geq 4}$, the element

$$w = e_0^{k-2} e_1 e_c \in \text{As}^+(\mathbb{R}_d), \quad \text{where } c = \begin{cases} 1 + m & \text{for odd } k, \\ 1 - m & \text{for even } k \end{cases}$$

is full because of the index difference $0 - 1$, and satisfies $l(w) = k$ and $\omega(w) = m$. This completes the description of $\text{Im}(\iota_d)$ in this case.

For even d , the proof of the suggested description of $\text{Im}(\iota_d)$ in length ≥ 4 repeats verbatim the proof of Theorem 4.24. \square

The realisation of the monoids FRS_d inside simpler monoids with easily extractable length allows us to easily count the number of their elements of given length, and hence compute the growth series:

Corollary 5.15. *For any integer $d \in \mathbb{N}$, we have*

$$\mathcal{G}_{\text{FRS}_d}(t) = \begin{cases} \frac{t}{1-t}, & d = 1; \\ \varphi(d)t^2 + d \frac{t^3}{1-t}, & d \text{ odd}, d > 1; \\ \varphi(d)t^2 + \frac{d}{2} \frac{t^3(2-t)}{(1-t)^2}, & d \text{ even}. \end{cases}$$

Notation $\varphi(n)$ stands here for *Euler's totient function*, which counts the number of integers between 1 and n coprime with n .

Proof. For $d = 1$, Theorem 5.14 provides exactly one element in each length ≥ 1 .

For odd $d > 1$, it gives $\varphi(d) = \#\mathbb{Z}_d^*$ elements in length 2, and d elements in each length ≥ 3 .

For even d , it gives again $\varphi(d) = \#\mathbb{Z}_d^*$ elements in length 2, and, in each length $n \geq 3$, the number of elements is

$$\frac{d}{2} \cdot \#\{k, l \in \mathbb{N} : k + l = n\} = \frac{d}{2} \cdot (n - 1).$$

We thus need to compute

$$\sum_{n \geq 3} (n - 1)t^n = \left(\sum_{n \geq 4} t^n \right)' - 2 \sum_{n \geq 3} t^n = \frac{t^3(2-t)}{(1-t)^2}. \quad \square$$

To compute the growth series of the entire structure monoids $\text{As}^+(\mathbb{R}_d)$, it remains to plug our formulas for the full parts into Eq. (5.1).

Theorem 5.16. *For any $d \in \mathbb{N}$, the growth series of the structure monoid of the size d reflection solution has the following form:*

$$\mathcal{G}_{\text{As}^+(\mathbb{R}_d)}(t) = 1 + d \cdot \left(t + \left(\sum_{c|d} \frac{\varphi(c)}{c} \right) t^2 + \tau(d) \frac{t^3}{1-t} + \tau\left(\frac{d}{2}\right) \frac{t^4}{2(1-t)^2} \right).$$

Here τ is the number-of-divisors function:

$$\tau(a) = \begin{cases} \#\{c \in \mathbb{N} : c|a\}, & a \in \mathbb{N}, \\ 0, & a \notin \mathbb{N}. \end{cases}$$

Note that the expression $d \cdot \sum_{c|d} \frac{\varphi(c)}{c}$ can be seen as the convolution of φ and Id.

The result depends heavily on the arithmetic properties of d . This is not surprising, given that the algebraic structure of dihedral groups depends heavily on the arithmetic properties of their size.

Proof. Let us split the sum in Eq. (5.1) into three parts, according to the three cases in our computation of $\mathcal{G}_{\text{FRS}_c}(t)$:

$$\begin{aligned}
\mathcal{G}_{\text{As}^+(\mathbb{R}_d)}(t) &= 1 + d \cdot \mathcal{G}_{\text{FRS}_1}(t) + \sum_{\substack{1 < c|d \\ c \text{ odd}}} \frac{d}{c} \cdot \mathcal{G}_{\text{FRS}_c}(t) + \sum_{\substack{c|d \\ c \text{ even}}} \frac{d}{c} \cdot \mathcal{G}_{\text{FRS}_c}(t) \\
&= 1 + d \cdot \frac{t}{1-t} + d \cdot \sum_{\substack{1 < c|d \\ c \text{ odd}}} \left(\frac{\varphi(c)}{c} t^2 + \frac{t^3}{1-t} \right) + d \cdot \sum_{\substack{c|d \\ c \text{ even}}} \left(\frac{\varphi(c)}{c} t^2 + \frac{t^3(2-t)}{2(1-t)^2} \right) \\
&= 1 + d \cdot \left(\frac{t}{1-t} + \left(\sum_{1 < c|d} \frac{\varphi(c)}{c} \right) t^2 + \sum_{1 < c|d} \frac{t^3}{1-t} + \sum_{\substack{c|d \\ c \text{ even}}} \frac{t^4}{2(1-t)^2} \right) \\
&= 1 + d \cdot \left(t + \left(\sum_{c|d} \frac{\varphi(c)}{c} \right) t^2 + \sum_{c|d} \frac{t^3}{1-t} + \sum_{\substack{c|d \\ c \text{ even}}} \frac{t^4}{2(1-t)^2} \right) \\
&= 1 + d \cdot \left(t + \left(\sum_{c|d} \frac{\varphi(c)}{c} \right) t^2 + \tau(d) \frac{t^3}{1-t} + \tau\left(\frac{d}{2}\right) \frac{t^4}{2(1-t)^2} \right). \quad \square
\end{aligned}$$

REFERENCES

- [1] E. Adan-Bante and H. Verrill. Symmetric groups and conjugacy classes. *J. Group Theory*, 11(3):371–379, 2008.
- [2] R. Bacher, P. de la Harpe, and B. Venkov. Séries de croissance et polynômes d'Ehrhart associés aux réseaux de racines. *Ann. Inst. Fourier (Grenoble)*, 49(3):727–762, 1999. Symposium à la Mémoire de François Jaeger (Grenoble, 1998).
- [3] D. Bessis. The dual braid monoid. *Annales Scientifiques de l'École Normale Supérieure*, 36(5):647–683, 2003.
- [4] J. W. Cannon and P. Wagreich. Growth functions of surface groups. *Math. Ann.*, 293(2):239–257, 1992.
- [5] F. Cedó, E. Jespers, L. Kubat, A. Van Antwerpen, and C. Verwimp. On various types of nilpotency of the structure monoid and group of a set-theoretic solution of the Yang-Baxter equation. *J. Pure Appl. Algebra*, 227(2):Paper No. 107194, 38, 2023.
- [6] F. Cedó, E. Jespers, and C. Verwimp. Structure monoids of set-theoretic solutions of the Yang-Baxter equation. *Publ. Mat.*, 65(2):499–528, 2021.
- [7] I. M. Chiswell. The growth series of a graph product. *Bull. London Math. Soc.*, 26(3):268–272, 1994.
- [8] F. Chouraqui. Garside groups and Yang-Baxter equation. *Comm. Algebra*, 38(12):4441–4460, 2010.
- [9] F. J. B. J. Clauwens. The adjoint group of an Alexander quandle, 2010.
- [10] A. Clément. Structure groups and second homology groups of linear Alexander quandles, 2025.
- [11] A. García Iglesias and L. Vendramin. An explicit description of the second cohomology group of a quandle. *Math. Z.*, 286(3-4):1041–1063, 2017.
- [12] T. Gateva-Ivanova, E. Jespers, and J. Okniński. Quadratic algebras of skew type and the underlying monoids. *J. Algebra*, 270(2):635–659, 2003.
- [13] T. Gateva-Ivanova and M. Van den Bergh. Semigroups of I -type. *J. Algebra*, 206(1):97–112, 1998.
- [14] E. Jespers, L. u. Kubat, and A. Van Antwerpen. The structure monoid and algebra of a non-degenerate set-theoretic solution of the Yang-Baxter equation. *Trans. Amer. Math. Soc.*, 372(10):7191–7223, 2019.
- [15] V. Lebed. Conjugation groups and structure groups of quandles, 2024.
- [16] V. Lebed and L. Vendramin. On structure groups of set-theoretic solutions to the Yang-Baxter equation. *Proc. Edinb. Math. Soc. (2)*, 62(3):683–717, 2019.
- [17] A. Mann. *How groups grow*, volume 395 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2012.
- [18] O. Ore. Some remarks on commutators. *Proceedings of the American Mathematical Society*, 2(2):307–314, 1951.
- [19] L. Paris and O. Varghese. The spherical growth series of Dyer groups. *Proc. Edinb. Math. Soc. (2)*, 67(1):168–187, 2024.
- [20] G. C. Shephard and J. A. Todd. Finite unitary reflection groups. *Canad. J. Math.*, 6:274–304, 1954.

- [21] L. Vendramin. Skew braces: a brief survey. In *Geometric methods in physics XL*, Trends Math., pages 153–175. Birkhäuser/Springer, Cham, [2024] ©2024.
- [22] H. Wilf. *Generatingfunctionology: Third Edition*. Ak Peters Series. Taylor & Francis, 2006.

(Carsten Dietzel) NORMANDIE UNIV, UNICAEN, CNRS, LMNO, 14000 CAEN, FRANCE
Email address: `carsten.dietzel@unicaen.fr`

(Edouard Feingésicht) NORMANDIE UNIV, UNICAEN, CNRS, LMNO, 14000 CAEN, FRANCE
Email address: `edouard.feingésicht@unicaen.fr`

(Victoria Lebed) NORMANDIE UNIV, UNICAEN, CNRS, LMNO, 14000 CAEN, FRANCE
Email address: `victoria.lebed@unicaen.fr`