Orbit length generating functions of automorphisms of a rooted regular binary tree

Richard Pink

Department of Mathematics
ETH Zürich
8092 Zürich
Switzerland
pink@math.ethz.ch

March 27, 2014

Abstract

To every automorphism w of an infinite rooted regular binary tree we associate a two variable generating function Φ_w that encodes information on the orbit structure of w. We prove that this is a rational function if w can be described by finitely many recursion relations of a particular form. We show that this condition is satisfied for all elements of the discrete iterated monodromy group Γ associated to a postcritically finite quadratic polynomial over $\mathbb{C}$. For such Γ we also prove that there are only finitely many possibilities for the denominator of Φ_w, and we describe a procedure to determine their lowest common denominator.

MSC classification: 20E08 (37B20, 37D40)

Contents

1 Introduction

Let T be an infinite rooted regular binary tree. To any automorphism w of T we associate the power series

$$\Phi_w \;=\; \sum_{n\geqslant m\geqslant 0} o_{m,n}(w)X^mY^n \;\in\; 1+Y\mathbb{Z}[[X,Y]]$$

where $o_{m,n}(w)$ is the number of orbits of w of length 2^m on the set of vertices of level n of T. This *orbit length generating function* encodes some information, but in general not all, about the conjugacy class of w.

The use of this construction stems from its behavior with respect to recursion relations. Specifically, assume that we are given an isomorphism from T to each half subtree of T obtained after deleting the root. Then for any $u,v\in\mathrm{Aut}(T)$ there is a unique element $(u,v)\in\mathrm{Aut}(T)$ which acts on the two half subtrees by u and v, respectively. Also, let $\sigma\in\mathrm{Aut}(T)$ denote the involution which interchanges the two half subtrees. Then one easily shows that

$$\begin{aligned}\Phi_{(u,v)} &= 1+Y\Phi_u+Y\Phi_v \quad\text{and}\\ \Phi_{(u,v)\,\sigma} &= 1+XY\Phi_{uv}.\end{aligned}\tag{1.1}$$

These relations are particularly useful for automorphisms that are themselves described by recursion relations. Many such automorphisms can be described abstractly, but they arise most notably as elements of iterated monodromy groups of quadratic morphisms.

To apply the recursion relations we say that an element $w\in\mathrm{Aut}(T)$ is Φ-*finite* if repeated application of the rules $(u,v)\rightsquigarrow u,v$ and $(u,v)\,\sigma\rightsquigarrow uv$ beginning with w leads to only finitely many elements of $\mathrm{Aut}(T)$. We say that w is Φ-*irreducible* if, in addition, the rules eventually lead back to w. Using (1.1) it is not hard to prove that for any Φ-finite element w the power series Φ_w is the expansion of a rational function in X and Y, and that new factors in the denominator arise only for Φ-irreducible elements (Theorems 2.7 and 2.8).

Roughly speaking an element w is Φ-finite if and only if it results from finitely many recursion relations of some particular form. This condition is probably quite restrictive. In fact, for the automorphism defined by the relatively easy looking recursion relation $b=(b,b\sigma)\,\sigma$ we explicitly calculate Φ_b and show that it is not a rational function (see Section 3).

By contrast, fix two integers $r>s\geqslant 0$ and consider a tuple $\underline{x}=(x_2,\ldots,x_r)$ with entries in $\{0,1\}$. To this data Bartholdi and Nekrashevych [1] have associated a certain subgroup $\Gamma_{\underline{x}}\subset\mathrm{Aut}(T)$ by explicit recursion relations for r generators. They have shown that the iterated monodromy group of any quadratic polynomial in one variable over $\mathbb{C}$ with a finite postcritical orbit of size r and eventual period $r-s$ is conjugate to $\Gamma_{\underline{x}}$ for some $\underline{x}$.

From the recursion relations of the generators alone we deduce with modest effort that all elements of $\Gamma_{\underline{x}}$ are Φ-finite (Propositions 4.9 and 5.11). More surprisingly, and with much more work, we prove that the rational functions Φ_w for all $w \in \Gamma_{\underline{x}}$ possess a common denominator that depends only on $\Gamma_{\underline{x}}$. We describe a common denominator explicitly and characterize the unique lowest common denominator $D_{\underline{x}}$ in terms of a finite combinatorial problem concerning the data r, s, and $\underline{x}$ (Theorems 4.46 and 5.50).

These results rely on a detailed analysis of the Φ-irreducible elements in $\Gamma_{\underline{x}}$. While there are infinitely many of them, we show that they lie in an explicit finite collection of conjugacy classes of $\mathrm{Aut}(T)$ (Propositions 4.15 and 5.30). As Φ_w is invariant under conjugacy, this implies the existence of some common denominator of Φ_w for all $w \in \Gamma_{\underline{x}}$. The characterization of the lowest common denominator requires additional effort.

The results of this article lead to a number of interesting questions and open problems. Among these are:

- By Nekrashevych [4, Thm. 6.4.4] the iterated monodromy group of any postcritically finite rational function over $\mathbb{C}$ is *contracting* in the sense of [4, Def. 2.11.1]. Our notion of Φ-finiteness is similar, but not equivalent. Are there deeper connections? Also, is there a relation with the notions of *finite state*, *bounded*, and/or *finitary* automorphisms from Bartholdi-Nekrashevych [1, §2.4]?

- When $\Gamma_{\underline{x}}$ is the iterated monodromy group of a postcritically finite quadratic polynomial over $\mathbb{C}$, what do Φ-finiteness and the rationality of Φ_w mean geometrically? What is the geometric meaning of the numerator and denominator of Φ_w, and of the lowest common denominator of all Φ_w?

- Prove Φ-finiteness and rationality and describe the denominators directly for iterated monodromy groups, without using their classification à la Bartholdi-Nekrashevych [1], perhaps in a way similar to how the group theoretic contracting property is deduced from geometric facts.

- Based on the polynomial case, we conjecture that for the iterated monodromy group Γ of any postcritically finite quadratic morphism $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, the Φ_w for all $w \in \Gamma$ are rational and possess a common denominator.

- Define orbit length generating functions for automorphisms of an infinite d-regular rooted tree for an arbitrary, possibly composite, integer $d \geqslant 2$ and extend the present results accordingly.

- As part of our analysis we prove that any Φ-irreducible element of $\Gamma_{\underline{x}}$ is conjugate under $\mathrm{Aut}(T)$ to some Φ-irreducible element of $\Gamma_{(0,\ldots,0)}$ with the same pair (r, s) (Propositions 4.18 and 5.32). Is the analogue true for non-Φ-irreducible elements?

- The role of $\Gamma_{(0,\ldots,0)}$ as a receptacle for conjugacy classes resembles the way that a quasi-split connected reductive group G over a field K possesses K-rational elements corresponding to the conjugacy classes of all K-rational elements of all inner forms of G. Is there a similar sense in which $\Gamma_{(0,\ldots,0)}$ is a 'quasi-split inner form of $\Gamma_{\underline{x}}$'?

- Our results show that the lowest common denominator $D_{\underline{x}}$ varies with $\underline{x}$ and that it is largest when $\underline{x} = (0, \ldots, 0)$ or $(1, \ldots, 1)$. Since $D_{\underline{x}}$ depends only on the $\mathrm{Aut}(T)$-conjugacy class of $\Gamma_{\underline{x}}$, it can help distinguish some of these conjugacy classes, especially from the conjugacy class of $\Gamma_{(0,\ldots,0)}$. However, there are still many different tuples $\underline{x}$ with the same $D_{\underline{x}}$. Can these groups be distinguished using the precise form of Φ_w, or using the conjugacy classes of non-Φ-irreducible elements?

- Do the orbit length generating functions also distinguish the Grigorchuk group from its 'twisted twin' of Bartholdi-Siegenthaler [2]?

- If the iterated monodromy groups associated to two postcritically finite quadratic polynomials over $\mathbb{C}$ are conjugate in $\mathrm{Aut}(T)$, does it follow that the polynomials are equivalent under an affine linear transformation and/or complex conjugation?

- Determine all subsets $J \subset \{1, \ldots, r\}$ satisfying Condition 4.16, respectively Conditions 5.25. Give a direct formula for the lowest common denominator $D_{\underline{x}}$ instead of a finite algorithm.

- Our original motivation was to understand the action of Frobenius elements associated to quadratic morphisms defined over finite or finitely generated fields of characteristic $\neq 2$. However, preliminary sample calculations suggest that their orbit length generating functions behave differently from those of the discrete groups studied in the present article. Nevertheless this question should be studied further, maybe in connection with the approach of Boston-Jones [3].

2 General definitions and results

2.1 Notation

Let T be the infinite tree whose vertices are the finite words over the alphabet $\{0,1\}$ and where each vertex t is connnected by an edge to the vertices $t0$ and $t1$. The empty word is called the *root of* T, making T an infinite rooted regular binary tree.

Let W denote the automorphism group of T. For any elements $u, v \in W$ we let (u,v) denote the element of W defined by $t0 \mapsto u(t)0$ and $t1 \mapsto v(t)1$ for any word t. This defines an isomorphism from $W \times W$ to the subgroup of W that fixes the vertices 0 and 1. We identify $W \times W$ with its image. Let $\sigma \in W$ denote the element of order 2 defined by $t0 \mapsto t1 \mapsto t1$ for any word t, and let $\langle\sigma\rangle$ be the subgroup of W generated by it. Then W is the semidirect product $W = (W \times W) \rtimes \langle\sigma\rangle$.

For any integer $n \geqslant 0$, the *level* n of T is the set of vertices at distance n from the root, i.e., the set of 2^n words of length n. Any element $w \in W$ fixes the root and thus permutes the level n. We let $\mathrm{sgn}_n(w)$ denote the sign of the induced permutation of the level n. Then $\mathrm{sgn}_1(\sigma) = -1$ and $\mathrm{sgn}_n(\sigma) = 1$ for all $n \neq 1$, and for any $u, v \in W$ we have $\mathrm{sgn}_{n+1}((u,v)) = \mathrm{sgn}_n(u) \cdot \mathrm{sgn}_n(v)$.

For any $n \geqslant 0$ let T_n denote the finite subtree obtained by cutting off T at level n. The automorphism group of T_n is a certain iterated wreath product of the group of two elements with itself and therefore a finite 2-group. Thus for any $w \in W$, any orbit of w on level n has length 2^m for some integer $0 \leqslant m \leqslant n$. The root of T is the unique vertex on level 0 and constitutes an orbit of length 1.

2.2 Orbit length generating functions

Definition 2.1 *The* orbit length generating function of $w \in W$ *is the power series*

$$\Phi_w \;=\; \sum_{n \geqslant m \geqslant 0} o_{m,n}(w) X^m Y^n \;\in\; 1 + Y\mathbb{Z}[[X,Y]]$$

where $o_{m,n}(w)$ is the number of orbits of w of length 2^m on level n.

Lemma 2.2 *For any element $w \in W$ we have:*

(a) Φ_w depends only on the W-conjugacy class of w.

(b) $\Phi_{w^k} = \Phi_w$ for any odd integer k.

(c) $\Phi_{w^2}(X,Y) = \Phi_w(0,Y) + 2 \cdot \dfrac{\Phi_w(X,Y) - \Phi_w(0,Y)}{X}$.

Proof. Assertions (a) and (b) follow from the fact that the orbit lengths remain the same. Next, any fixed point of w remains a fixed point of w^2, and any orbit of length $2^{m+1} > 1$ of w splits into two orbits of length 2^m of w^2. Thus $o_{0,n}(w^2) = o_{0,n}(w) + 2o_{1,n}(w)$, and $o_{m,n}(w^2) = 2o_{m+1,n}(w)$ whenever $m > 0$. This implies (c). □

Proposition 2.3 *For any elements $u, v \in W$ we have*

$$\begin{aligned} \Phi_{(u,v)} &= 1 + Y\Phi_u + Y\Phi_v, \\ \Phi_{(u,v)\,\sigma} &= 1 + XY\Phi_{uv}. \end{aligned}$$

Proof. By the definition of (u,v), its orbits on level $n+1$ are obtained from the orbits of u on level n by appending the letter 0 to each word and from the orbits of v on level n by appending the letter 1 each word. Thus $o_{m,n+1}((u,v)) = o_{m,n}(u) + o_{m,n}(v)$, which implies the first formula.

The other element $(u,v)\,\sigma$ fixes the root, but changes the last letter of every word of length > 0. Thus its orbits of length 2^{m+1} are in bijection with the orbits of length 2^m of $(u,v)\,\sigma\,(u,v)\,\sigma = (uv, vu)$ on the set of words ending in 0. By the definition of (uv, vu) the latter are obtained from the orbits of uv of length 2^m by appending the letter 0 to each word. Thus $o_{m+1,n+1}((u,v)\,\sigma) = o_{m,n}(uv)$, which implies the second formula. □

The recursion relations in Proposition 2.3 are the main tools for calculating Φ_w. To formalize their use we introduce the following ad hoc terminology.

2.3 Finiteness

Definition 2.4 *The* first descendants of *an element $w \in W$ are the elements u and v if $w = (u,v)$, respectively uv alone if $w = (u,v)\,\sigma$. For any $n \geqslant 1$, the first descendants of all n^{th} descendants of w are the $(n+1)^{\text{st}}$* descendants of w. *The n^{th} descendants of w for all $n \geqslant 1$ are the* descendants of w. *The set of all descendants of w is denoted* $\operatorname{Desc}(w)$.

Thus $\operatorname{Desc}(w)$ is the set of elements of W encountered on repeatedly applying the recursion relations 2.3.

Definition 2.5 *(a) An element $w \in W$ is called* Φ-finite *if* $\operatorname{Desc}(w)$ *is finite.*

(b) An element $w \in W$ is called Φ-irreducible *if* $\operatorname{Desc}(w)$ *is finite and* $w \in \operatorname{Desc}(w)$.

As a direct consequence of the definition we have:

Proposition 2.6 *For any $w' \in \operatorname{Desc}(w)$ we have $\operatorname{Desc}(w') \subset \operatorname{Desc}(w)$. In particular, any descendant of a Φ-finite element is Φ-finite.*

2.4 Rationality

Theorem 2.7 *If $w \in W$ is Φ-finite, then Φ_w is the power series expansion of a rational function in X and Y with denominator in $1 + Y\mathbb{Z}[X,Y]$.*

Proof. Write $\{w\} \cup \mathrm{Desc}(w) = \{w_1, \ldots, w_r\}$. Then Propositions 2.3 and 2.6 imply that for any $1 \leqslant i \leqslant r$ there exist $1 \leqslant j, k \leqslant r$ such that $\Phi_{w_i} = 1 + Y\Phi_{w_j} + Y\Phi_{w_k}$ or $\Phi_{w_i} = 1 + XY\Phi_{w_j}$. In particular we can write $\Phi_{w_i} = 1 + \sum_{j=1}^{r} Y a_{i,j} \Phi_{w_j}$ for certain $a_{i,j} \in \mathbb{Z}[X]$. In terms of the column vectors $f := (\Phi_{w_i})_{i=1}^{r}$ and $e := (1)_{i=1}^{r}$ and the matrix $A := (a_{i,j})_{i,j=1}^{r}$ this means that $f = e + YAf$. This in turn is equivalent to $(I - YA)f = e$, where I denotes the identity matrix. The determinant $D := \det(I - YA)$ lies in $1 + Y\mathbb{Z}[X, Y]$ and is therefore invertible in $\mathbb{Z}[[X, Y]]$, and the coefficients of $(I - YA)^{-1}$ lie in $D^{-1}\mathbb{Z}[X, Y]$. Thus the coefficients of $f = (I - YA)^{-1}e$ lie in $D^{-1}\mathbb{Z}[X, Y]$, and hence so does Φ_w, as desired. □

Theorem 2.8 *If $w \in W$ is Φ-finite, then Φ_w is a $\mathbb{Z}[X, Y]$-linear combination of the $\Phi_{w'}$ for all Φ-irreducible $w' \in \mathrm{Desc}(w)$.*

Proof. By induction on the cardinality of $\{w\} \cup \mathrm{Desc}(w)$ we may assume that the assertion holds for all Φ-finite elements $w' \in W$ with $|\{w'\} \cup \mathrm{Desc}(w')| < |\{w\} \cup \mathrm{Desc}(w)|$. If w is Φ-irreducible, there is nothing to prove. So assume that w is not Φ-irreducible. Then for any $w' \in \mathrm{Desc}(w)$ we have $w \notin \mathrm{Desc}(w') \subset \mathrm{Desc}(w)$. Thus $\{w'\} \cup \mathrm{Desc}(w')$ is a proper subset of $\{w\} \cup \mathrm{Desc}(w)$, and so by the induction hypothesis the assertion already holds for w'. In particular, in the case $w = (u, v)$ the assertion holds for u and v, and in the case $w = (u, v)\,\sigma$ the assertion holds for uv. Thus with the recursion relations from Proposition 2.3 the assertion follows for w, as desired. □

2.5 Examples

Now we do some simple examples. First, the identity element $1 \in W$ is equal to $(1, 1)$ and therefore Φ-irreducible. With Proposition 2.3 we find that $\Phi_1 = 1 + 2Y\Phi_1$ and so

$$\Phi_1 \;=\; \frac{1}{1 - 2Y}. \tag{2.9}$$

Next $\sigma = (1, 1)\,\sigma$ has the unique descendant 1. Thus it is Φ-finite but not Φ-irreducible, and from (2.9) and Proposition 2.3 we deduce that

$$\Phi_\sigma \;=\; 1 + \frac{XY}{1 - 2Y}. \tag{2.10}$$

Next the *standard odometer* is the element $a \in W$ defined by the recursion relation $a = (a, 1)\,\sigma$. Thus it is Φ-irreducible, and from Proposition 2.3 we deduce that $\Phi_a = 1 + XY\Phi_a$ and hence

$$\Phi_a \;=\; \frac{1}{1 - XY}. \tag{2.11}$$

Also, for any odd integer $k = 2\ell + 1$ the element $a^k = (a^{\ell+1}, a^\ell)\sigma$ is again Φ-irreducible and has $\Phi_{a^k} = \Phi_a$ by Lemma 2.2 (b). In fact, one easily shows that any odd power of any Φ-irreducible element is Φ-irreducible.

On the other hand, not all elements of W that are described by finitely many recursion relations have rational orbit length generating functions, as the example in the next section shows. Also, rationality is rare in the following sense. Recall that as a profinite group W has a unique Haar measure with total volume 1.

Proposition 2.12 *The set of elements $w \in W$ with Φ_w rational has measure zero.*

Proof. As there are only countably many rational functions with coefficients in $\mathbb{Z}$, it suffices to prove that for any fixed $\Phi \in 1+Y\mathbb{Z}[[X,Y]]$, the set S of all $w \in W$ with $\Phi_w = \Phi$ has measure zero. But Φ_w determines $\mathrm{sgn}_n(w)$ for all $n \geqslant 1$, and so S is contained in a single coset of the subgroup $\bigcap_{n\geqslant 1} \mathrm{Ker}(\mathrm{sgn}_n)$ of W. This is a closed subgroup of infinite index and therefore of measure zero; hence S has measure zero, as desired. □

2.6 Variant

Some calculations become easier with the following slight variant of Φ_w obtained by 'removing trivial poles and zeros':

Proposition 2.13 *For any $w \in W$ there exists a unique $\Psi_w \in Y\mathbb{Z}[[X,Y]]$ with*

$$\Phi_w \;=\; \frac{1}{1-2Y} + \frac{X-2}{1-2Y}\cdot\Psi_w.$$

Proof. The term $o_{m,n}(w)$ in Definition 2.1 is the number of orbits of w of length 2^m on level n. Since the total number of vertices on level n is 2^n, this implies that

$$\Phi_w(2,Y) \;=\; \sum_{n\geqslant m\geqslant 0} o_{m,n}(w)2^mY^n \;=\; \sum_{n\geqslant 0} 2^nY^n \;=\; \frac{1}{1-2Y}.$$

Thus $\Phi_w - \frac{1}{1-2Y}$ is divisible by $X-2$, and the decomposition follows. □

Proposition 2.14 *For any elements $u, v \in W$ we have*

$$\begin{aligned}\Psi_{(u,v)} &= Y\Psi_u + Y\Psi_v,\\ \Psi_{(u,v)\,\sigma} &= Y + XY\Psi_{uv}.\end{aligned}$$

Proof. Direct consequence of Proposition 2.3. □

For example, the formulas (2.9) and (2.10) and (2.11) correspond to:

(2.15) $$\Psi_1 = 0,$$

(2.16) $$\Psi_\sigma = Y,$$

(2.17) $$\Psi_a = \frac{Y}{1-XY}.$$

3 A non-rational orbit length generating function

In this section we study the element $b \in W$ defined by the recursion relation

$$(3.1) \qquad b \;=\; (b, b\sigma)\sigma.$$

We will explicitly calculate Φ_b and show that it is not a rational function. This implies that the description of elements of W by finitely many recursion relations does not guarantee that their orbit length generating functions are rational.

3.1 Preparations

First note that the power σ^p for $p \in \mathbb{Z}$ depends only on p mod 2 and can therefore be defined for any $p \in \mathbb{F}_2$. Thus to any integer $r \geqslant 1$ and any polynomial $P(T) = \sum p_i T^i \in \mathbb{F}_2[T]$ of degree $< 2^r$ we can associate the element

$$(3.2) \qquad w_{r,P} \;:=\; b\,\sigma^{p_0}\, b\,\sigma^{p_1} \cdots b\,\sigma^{p_{2^r-1}} \;\in\; W.$$

To any such r and P we also associate

$$\begin{aligned} Q(T) \;&:=\; \frac{P(T)\cdot T - P(1)\cdot T^{2^r}}{T-1} + T\cdot (T-1)^{2^r-2}, \\ R(T) \;&:=\; Q(T) + (T-1)^{2^r-1}, \qquad \text{and} \\ S(T) \;&:=\; Q(T) + T^{2^r}\cdot R(T), \end{aligned}$$

which are again polynomials in $\mathbb{F}_2[T]$ of respective degrees $< 2^r$, $< 2^r$, and $< 2^{r+1}$.

Lemma 3.3 *In this situation $w_{r,P} = (w_{r,Q}, w_{r,R})\,\sigma^{P(1)}$ and $w_{r,Q}w_{r,R} = w_{r+1,S}$.*

Proof. Set $q_i = \sum_{j=0}^{i-1}(p_j - 1) \in \mathbb{F}_2$ for all $0 \leqslant i \leqslant 2^r$. Then $q_0 = 0$ and $p_i = 1 - q_i + q_{i+1}$ for all $0 \leqslant i < 2^r$, and hence

$$w_{r,P} \;=\; (\sigma^{q_0}\, b\,\sigma^{1-q_0})\cdot(\sigma^{q_1}\, b\,\sigma^{1-q_1})\cdots(\sigma^{q_{2^r-1}}\, b\,\sigma^{1-q_{2^r-1}})\cdot\sigma^{q_{2^r}}.$$

Here $q_{2^r} = \sum_{j=0}^{2^r-1}(p_j-1) = \sum_{j=0}^{2^r-1} p_j - 2^r = P(1)$ because $r \geqslant 1$. Also, for any $q \in \mathbb{F}_2$ we have

$$\sigma^q\, b\,\sigma^{1-q} \;=\; \sigma^q\,(b, b\sigma)\,\sigma^{-q} \;=\; \left\{\begin{array}{ll} (b, b\sigma) & \text{if } q = 0 \\ (b\sigma, b) & \text{if } q = 1 \end{array}\right\} \;=\; (b\,\sigma^q, b\,\sigma^{q+1}).$$

Therefore

$$\begin{aligned} w_{r,P} \;&=\; (b\,\sigma^{q_0}, b\,\sigma^{q_0+1})\cdots(b\,\sigma^{q_{2^r-1}}, b\,\sigma^{q_{2^r-1}+1})\cdot\sigma^{P(1)} \\ &=\; \big(b\,\sigma^{q_0}\cdots b\,\sigma^{q_{2^r-1}}, b\,\sigma^{q_0+1}\cdots b\,\sigma^{q_{2^r-1}+1}\big)\cdot\sigma^{P(1)}. \end{aligned}$$

Thus with $Q(T) := \sum_{i=0}^{2^r-1} q_i T^i$ and $R(T) := \sum_{i=0}^{2^r-1}(q_i+1)T^i$ we deduce that $w_{r,P} = (w_{r,Q}, w_{r,R})\,\sigma^{P(1)}$. A direct calculation which we leave to the reader shows that $Q(T)$ and $R(T)$ are given by the indicated formulas. Finally, the formula $w_{r,Q}w_{r,R} = w_{r+1,S}$ follows directly on expanding both sides. □

As usual, for any polynomial $f \in \mathbb{F}_2[T]$ we let $\mathrm{ord}_{T-1}(f)$ denote the supremum of the set of integers d such that $(T-1)^d$ divides f.

Lemma 3.4 *If* $0 < \mathrm{ord}_{T-1}(P) < 2^r - 1$, *then* $\mathrm{ord}_{T-1}(Q) = \mathrm{ord}_{T-1}(R) = \mathrm{ord}_{T-1}(P) - 1$. *Moreover, we always have* $\mathrm{ord}_{T-1}(S) = 2^r - 1$.

Proof. If $\mathrm{ord}_{T-1}(P) > 0$, then $P(0) = 0$ and so by construction

$$Q(T) \;=\; \frac{P(T)}{T-1} \cdot T + T \cdot (T-1)^{2^r-2}.$$

If in addition $\mathrm{ord}_{T-1}(P) < 2^r - 1$, then $\mathrm{ord}_{T-1}\bigl(\frac{P(T)}{T-1} \cdot T\bigr) = \mathrm{ord}_{T-1}(P) - 1 < 2^r - 2$ and therefore $\mathrm{ord}_{T-1}(Q) = \mathrm{ord}_{T-1}(P) - 1$. By the definition of $R(T)$ this is then also equal to $\mathrm{ord}_{T-1}(R)$, proving the first assertion. On the other hand, the construction of S directly implies that

$$S(T) \;=\; Q(T) + T^{2^r} \cdot \bigl(Q(T) + (T-1)^{2^r-1}\bigr) \;=\; (T-1)^{2^r} \cdot Q(T) + T^{2^r} \cdot (T-1)^{2^r-1},$$

whence the second assertion. □

3.2 The orbit length generating function

For any integer $r \geqslant 0$ consider the power series

$$\Omega_r \;:=\; \sum_{m \geqslant 0} \bigl(\tfrac{X}{2}\bigr)^m \cdot (2Y)^{2^{m+r}-2^r} \;\in\; \mathbb{Z}[[X,Y]].$$

For any $w \in W$ let Ψ_w denote the power series from Proposition 2.13.

Lemma 3.5 *For any polynomial* P *in* $\mathbb{F}_2[T]$ *of degree* $< 2^r$ *with* $d := \mathrm{ord}_{T-1}(P) < 2^r - 1$ *we have*

$$\Psi_{w_{r,P}} \;=\; 2^d Y^{d+1} \Omega_r.$$

Proof. It suffices to show the equation modulo Y^N for all $N \geqslant 0$, which we will achieve by induction on N. The case $N = 0$ is trivial, so assume that $N > 0$ and that the equation holds universally modulo Y^{N-1}.

If $d > 0$, then $P(1) = 0$, and so $w_{r,P} = (w_{r,Q}, w_{r,R})$ by Lemma 3.3. By Proposition 2.14 we therefore have $\Psi_{w_{r,P}} = Y\Psi_{w_{r,Q}} + Y\Psi_{w_{r,R}}$. On the other hand we have $\mathrm{ord}_{T-1}(Q) = \mathrm{ord}_{T-1}(R) = d - 1$ by Lemma 3.4 and so by the induction hypothesis $\Psi_{w_{r,Q}} \equiv \Psi_{w_{r,R}} \equiv 2^{d-1} Y^d \Omega_r$ modulo Y^{N-1}. Together this implies that $\Psi_{w_{r,P}} \equiv 2^d Y^{d+1} \Omega_r$ modulo Y^N, as desired.

If $d = 0$, then $P(1) = 1$, and so $w_{r,P} = (w_{r,Q}, w_{r,R})\,\sigma$ with $w_{r,Q} w_{r,R} = w_{r+1,S}$ by Lemma 3.3. By Proposition 2.14 we therefore have $\Psi_{w_{r,P}} = Y + XY\Psi_{w_{r+1,S}}$. Since $\mathrm{ord}_{T-1}(S) = 2^r - 1$ by Lemma 3.4 and $2^r - 1 < 2^{r+1} - 1$, the induction hypothesis implies that $\Psi_{w_{r+1,S}} \equiv 2^{2^r-1} Y^{2^r} \Omega_{r+1}$ modulo Y^{N-1}. Together this shows that

$$\Psi_{w_{r,P}} \;\equiv\; Y + XY 2^{2^r-1} Y^{2^r} \Omega_{r+1} \quad \text{modulo} \quad Y^N.$$

A short calculation shows that the right hand side is equal to $Y\Omega_r$; hence $\Psi_{w_{r,P}} \equiv Y\Omega_r$ modulo Y^N, as desired. □

Proposition 3.6 *We have*

$$\Phi_b \;=\; 1 \;+\; \sum_{m\geqslant 1}\;\sum_{2^{m-1}\leqslant n<2^m} 2^{n-m}X^mY^n.$$

Proof. For $r := 1$ the polynomial $P := T$ has degree $1 < 2^r$ and $d := \mathrm{ord}_{T-1}(P) = 0 < 2^r - 1$, which satisfies the assumptions of Lemma 3.5. Since in this case $w_{r,P} = bb\sigma$ by (3.2), we find that $\Psi_{bb\sigma} = Y\Omega_1$. But by definition $b = (b, b\sigma)\sigma$, so with Proposition 2.14 we deduce that $\Psi_b = Y + XY\Psi_{bb\sigma} = Y + XY^2\Omega_1$. A direct calculation now shows that

$$\Psi_b \;=\; \tfrac{1}{2}\cdot\sum_{m\geqslant 0}\left(\tfrac{X}{2}\right)^m\cdot(2Y)^{2^m}, \tag{3.7}$$

and another yields the indicated formula for Φ_b. □

Corollary 3.8 *(a) The length of any orbit of b on any level $n \geqslant 0$ is the smallest power of 2 which is greater than n.*

(b) For any $m \geqslant 0$, the power b^{2^m} fixes all vertices on level $2^m - 1$, but none on level 2^m.

Proof. By the definition of Φ_b both assertions are equivalent to Proposition 3.6. □

3.3 Irrationality

Proposition 3.9 *The power series Φ_b is not a rational function of (X, Y).*

Proof. By construction Φ_b is rational if and only if Ψ_b is rational. If so, there exist non-zero polynomials $f, g \in \mathbb{Q}[X, Y]$ with $f = g \cdot \Psi_b$. By (3.7) this means that

$$f(X,Y) \;=\; \tfrac{1}{2}\cdot\sum_{m\geqslant 0} g(X,Y)\cdot\left(\tfrac{X}{2}\right)^m\cdot(2Y)^{2^m}.$$

But for degree reasons, the summands for all m with $2^m > \max\{\deg_Y(f), \deg_Y(g)\}$ cannot cancel with any other terms, yielding a contradiction. Thus Ψ_b and hence Φ_b is not rational, as desired. □

4 Iterated monodromy groups of quadratic polynomials: Periodic case

4.1 The iterated monodromy group

Throughout this section we fix an integer $r > 0$ and a tuple $\underline{x} = (x_2, \ldots, x_r)$ of elements of $\{0, 1\}$. Consider the elements $b_1, \ldots, b_r \in W$ defined by the recursion relations

$$(4.1) \qquad \begin{cases} b_1 = (1, b_r)\,\sigma, \\ b_i = (b_{i-1}, 1) \quad \text{for all } 2 \leqslant i \leqslant r \text{ with } x_i = 0, \\ b_i = (1, b_{i-1}) \quad \text{for all } 2 \leqslant i \leqslant r \text{ with } x_i = 1, \end{cases}$$

and let $\Gamma_{\underline{x}} \subset W$ be the subgroup generated by them. Up to a change in notation, these are the generators and the subgroup studied by Bartholdi and Nekrashevych in [1, §3]. Thus by [1, Thm. 5.1] we have:

Theorem 4.2 *Let f be any quadratic polynomial over $\mathbb{C}$ and $\eta \in \mathbb{C}$ be its unique critical point. Assume that $\eta, f(\eta), \ldots, f^{r-1}(\eta)$ are all distinct and that $f^r(\eta) = \eta$. Then the iterated monodromy group of f is W-conjugate to $\Gamma_{\underline{x}}$ for a certain choice of $\underline{x}$.*

Note that the inverses of the generators in (4.1) satisfy

$$\begin{cases} b_1^{-1} = (b_r^{-1}, 1)\,\sigma, \\ b_i^{-1} = (b_{i-1}^{-1}, 1) \quad \text{for all } 2 \leqslant i \leqslant r \text{ with } x_i = 0, \\ b_i^{-1} = (1, b_{i-1}^{-1}) \quad \text{for all } 2 \leqslant i \leqslant r \text{ with } x_i = 1. \end{cases}$$

Thus all the following results on $\Gamma_{\underline{x}}$ also hold if the first relation in (4.1) is replaced by the relation $b_1 = (b_r, 1)\,\sigma$ (see [1, p. 316]). In particular, the results in the case $\underline{x} = (0, \ldots, 0)$ apply to the subgroup generated by the elements $a_1, \ldots, a_r$ studied in [5, §2], which were defined by

$$(4.3) \qquad \begin{cases} a_1 = (a_r, 1)\,\sigma, \\ a_i = (a_{i-1}, 1) \quad \text{for all } 2 \leqslant i \leqslant r. \end{cases}$$

Also observe:

Proposition 4.4 *The group $\Gamma_{(x_2,\ldots,x_r)}$ is conjugate to the group $\Gamma_{(1-x_2,\ldots,1-x_r)}$ under W.*

Proof. Consider the element $w \in W$ that is defined by the recursion relation $w = (w, w)\,\sigma$. Then a direct calculation shows that

$$\begin{cases} wb_1^{-1}w^{-1} = (1, wb_r^{-1}w^{-1})\,\sigma, \\ wb_i^{-1}w^{-1} = (1, wb_{i-1}^{-1}w^{-1}) \quad \text{for all } 2 \leqslant i \leqslant r \text{ with } x_i = 0, \\ wb_i^{-1}w^{-1} = (wb_{i-1}^{-1}w^{-1}, 1) \quad \text{for all } 2 \leqslant i \leqslant r \text{ with } x_i = 1. \end{cases}$$

Thus the elements $wb_i^{-1}w^{-1}$ satisfy the relations (4.1) with $1-x_i$ in place of x_i, and so $w\Gamma_{(x_2,\ldots,x_r)}w^{-1} = \Gamma_{(1-x_2,\ldots,1-x_r)}$. □

The aim of this section is to show that the orbit length generating functions of all elements of $\Gamma_{\underline{x}}$ are rational and possess an explicit common denominator.

4.2 Finiteness

We begin with some preparations. Let π denote the cyclic permutation of the set $\{1,\ldots,r\}$ defined by

$$\pi(i) \;:=\; \begin{cases} r & \text{if } i=1, \\ i-1 & \text{if } i>1. \end{cases} \tag{4.5}$$

Then the recursion relations (4.1) express each b_i in terms of $b_{\pi(i)}$.

Definition 4.6 *The* length $|w|$ *of an element* $w \in \Gamma_{\underline{x}}$ *is the minimal length of a word over the alphabet* $\{b_1^{\pm 1},\ldots,b_r^{\pm 1}\}$ *that represents* w*. Any word of minimal length representing* w *is called a* minimal word for w.

Lemma 4.7 *For any element* $w = (u,v)\,\sigma^\mu \in \Gamma_{\underline{x}}$ *we have* $u,v \in \Gamma_{\underline{x}}$ *and*

$$|uv| \leqslant |u| + |v| \leqslant |w|.$$

Proof. By the recursion relations (4.1), any letter $b_i^{\pm 1}$ in a minimal word for w contributes precisely one letter $b_{\pi(i)}^{\pm 1}$ to a word representing u or v. This implies the second inequality, and the first one follows directly from the definition of length. □

Lemma 4.8 *For all* $w \in \Gamma_{\underline{x}}$ *and all* $w' \in \mathrm{Desc}(w)$ *we have* $w' \in \Gamma_{\underline{x}}$ *with* $|w'| \leqslant |w|$.

Proof. By Definition 2.4 and iteration this follows from Lemma 4.6. □

Proposition 4.9 *Every element of* $\Gamma_{\underline{x}}$ *is* Φ*-finite.*

Proof. Since $\Gamma_{\underline{x}}$ contains only finitely many elements of any given length, Lemma 4.8 implies that $\mathrm{Desc}(w)$ is finite for any $w \in \Gamma_{\underline{x}}$, as desired. □

Combining Proposition 4.9 with Theorem 2.7 we find that the orbit length generating functions of all elements of $\Gamma_{\underline{x}}$ are rational. By Theorem 2.8 the study of their denominators reduces to the case of Φ-irreducible elements.

4.3 Properties of Φ-irreducible elements

Lemma 4.10 *Any Φ-irreducible element $w \in \Gamma_{\underline{x}}$ has a unique first descendant w' which is Φ-irreducible with $|w'| = |w|$. Moreover w is either W-conjugate to $(w',1)\,\sigma$, or equal to $(w',1)$ or $(1,w')$.*

Proof. Suppose first that $w = (u,v)\,\sigma$. Then w is W-conjugate to $(uv,1)\,\sigma$, and uv is the unique first descendant of w. Thus the assumption $w \in \mathrm{Desc}(w)$ means that w is equal to or a descendant of uv. On the one hand this implies that uv is a descendant of itself; hence uv is Φ-irreducible. On the other hand it implies by Lemma 4.8 that $|w| \leqslant |uv| \leqslant |w|$ and hence $|uv| = |w|$, and we are done with $w' := uv$.

Suppose now that $w = (u,v)$, so that u and v are the first descendants of w. Then the assumption $w \in \mathrm{Desc}(w)$ means that w is equal to, or a descendant of, one of u, v; let us call it w'. On the one hand this implies that w' is a descendant of itself; hence w' is Φ-irreducible. On the other hand it implies by Lemma 4.8 that $|w| \leqslant |w'| \leqslant |w|$ and hence $|w'| = |w|$. Plugging this into the inequality $|u| + |v| \leqslant |w|$ from Lemma 4.7, we now deduce that the other entry of (u,v) has length 0 and is therefore the identity element. Thus $w = (w',1)$ or $w = (1,w')$. This makes w' unique (though for $w' = 1$ we can write w in both ways). Since $(1,w')$ is W-conjugate to $(w',1)$, in either case we are done. □

Next we look at signs. The same proof as that of [5, Prop. 2.1.1] shows:

Lemma 4.11 *For all $n \geqslant 1$ and all $1 \leqslant i \leqslant r$ we have*

$$\mathrm{sgn}_n(b_i) \;=\; \begin{cases} -1 & \text{if } n \equiv i \bmod r, \\ 1 & \text{if } n \not\equiv i \bmod r. \end{cases}$$

Thus for any fixed $w \in \Gamma_{\underline{x}}$, the value $\mathrm{sgn}_n(w)$ for $n \geqslant 1$ depends only on $n \bmod r$.

To any element $w \in \Gamma_{\underline{x}}$ we associate the subset

$$J_w \;:=\; \{1 \leqslant i \leqslant r \mid \mathrm{sgn}_i(w) = -1\}. \tag{4.12}$$

Lemma 4.13 *For any w and w' as in Lemma 4.10 we have $J_{w'} = \pi(J_w)$.*

Proof. The recursion relations for signs and their invariance under conjugation implies that $\mathrm{sgn}_i(w) = \mathrm{sgn}_{i-1}(w')$ for all $i \geqslant 2$. Using the periodicity from Lemma 4.11 we also find that $\mathrm{sgn}_1(w) = \mathrm{sgn}_{r+1}(w) = \mathrm{sgn}_r(w')$. By (4.5) we therefore have $\mathrm{sgn}_i(w) = \mathrm{sgn}_{\pi(i)}(w')$ for all $1 \leqslant i \leqslant r$, or equivalently $J_{w'} = \pi(J_w)$. □

4.4 Conjugacy classes of Φ-irreducible elements

Lemma 4.14 *Consider any distinct indices $i_1, \ldots, i_k \in \{1, \ldots, r\}$, in any order. Set $\mu := 1$ if 1 appears among them, and $\mu := 0$ otherwise. Then $a_{i_1} \cdots a_{i_k}$ is conjugate to $(a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1)\, \sigma^\mu$ under W.*

Proof. If 1 does not appear among $i_1, \ldots, i_k$, the recursion relations (4.3) imply that

$$a_{i_1} \cdots a_{i_k} \;=\; (a_{i_1-1}, 1) \cdots (a_{i_k-1}, 1) \;=\; (a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1)\, \sigma^\mu,$$

and the assertion follows. Otherwise let j be the unique index with $i_j = 1$. Then the recursion relations (4.3) imply that

$$\begin{aligned} a_{i_1} \cdots a_{i_k} &= (a_{i_1-1}, 1) \cdots (a_{i_{j-1}-1}, 1) \cdot (a_r, 1)\, \sigma \cdot (a_{i_{j+1}-1}, 1) \cdots (a_{i_k-1}, 1) \\ &= (a_{\pi(i_1)} \cdots a_{\pi(i_j)}, a_{\pi(i_{j+1})} \cdots a_{\pi(i_k)})\, \sigma^\mu. \end{aligned}$$

This is W-conjugate to $(a_{\pi(i_1)} \cdot \cdots \cdot a_{\pi(i_k)}, 1)\, \sigma^\mu$, as desired. □

Proposition 4.15 *Consider any Φ-irreducible element $w \in \Gamma_{\underline{x}}$. Let $i_1, \ldots, i_k$ be the distinct elements of J_w, in any order. Then w is conjugate to $a_{i_1} \cdots a_{i_k}$ under W.*

Proof. By [5, Lemma 1.3.3] it suffices to prove that the restrictions $w|_{T_n}$ and $a_{i_1} \cdots a_{i_k}|_{T_n}$ are conjugate in the automorphism group of T_n for every $n \geqslant 0$. We will achieve this by induction on n. For $n = 0$ the assertion is trivially true, so assume that $n > 0$ and that the assertion is universally true for the restrictions to T_{n-1}.

Let $w' \in \Gamma_{\underline{x}}$ be the unique Φ-irreducible descendant of w from Lemma 4.10. Then w is conjugate to $(w', 1)\, \sigma^\mu$ for some $\mu \in \{0, 1\}$. Thus $\mathrm{sgn}_1(w) = (-1)^\mu$, and hence $\mu = 1$ if and only if $1 \in J_w$. Also, Lemma 4.13 shows that $\pi(i_1), \ldots, \pi(i_k)$ are the distinct elements of $J_{w'}$. By the induction hypothesis $w'|_{T_{n-1}}$ is therefore conjugate to $a_{\pi(i_1)} \cdots a_{\pi(i_k)}|_{T_{n-1}}$ under the automorphism group of T_{n-1}. Thus $w|T_n$ is conjugate to $(a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1)\, \sigma^\mu|_{T_n}$ under the automorphism group of T_n. From Lemma 4.14 it now follows that $w|T_n$ is conjugate to $a_{i_1} \cdots a_{i_k}|_{T_n}$ under the automorphism group of T_n, as desired. □

The next result concerns the following condition on a subset $J \subset \{1, \ldots, r\}$.

Condition 4.16 *For any $n \geqslant 0$ with $1 \notin \pi^n(J)$, the values x_i for all $i \in \pi^n(J)$ are equal.*

Proposition 4.17 *For any subset $J \subset \{1, \ldots, r\}$ satisfying Condition 4.16 there exists a Φ-irreducible element $w \in \Gamma_{\underline{x}}$ with $J_w = J$.*

Proof. Consider any integer $n \geqslant 0$. For the purpose of this proof we call any element of $\Gamma_{\underline{x}}$ of the form $b_{i_1} \cdots b_{i_k}$, where $i_1, \ldots, i_k$ are the distinct elements of $\pi^n(J)$ in any order, *strongly of type* $\pi^n(J)$. We claim that any element that is strongly of type $\pi^n(J)$ possesses a first descendant which is strongly of type $\pi^{n+1}(J)$.

Granting this, by induction on n it follows that for any $n \geqslant 1$, any element that is strongly of type J possesses a descendant which is strongly of type $\pi^n(J)$. Since π is a permutation of finite order, we deduce that any element that is strongly of type J possesses a descendant which is again strongly of type J. As there are only finitely many elements that are strongly of type J, and being a descendant is a transitive relation, it follows that some element w_0 that is strongly of type J must be its own descendant. This element is therefore Φ-irreducible. Finally, writing $w_0 = b_{i_1} \cdots b_{i_k}$ where $i_1, \ldots, i_k$ are the distinct elements of J, Lemma 4.11 implies that $J_w = J$, as desired.

To prove the claim consider $w := b_{i_1} \cdots b_{i_k}$ where $i_1, \ldots, i_k$ are the distinct elements of $\pi^n(J)$. Suppose first that $1 \notin \pi^n(J)$. Then by Condition 4.16 the values x_i are equal for all $i \in \pi^n(J)$. Thus the recursion relations (4.1) imply that $b_{i_1} \cdots b_{i_k} = (b_{\pi(i_1)} \cdots b_{\pi(i_k)}, 1)$ or $(1, b_{\pi(i_1)} \cdots b_{\pi(i_k)})$. In both cases w has the first descendant $b_{\pi(i_1)} \cdots b_{\pi(i_k)}$, which is strongly of type $\pi^{n+1}(J)$.

Suppose now that $1 \in \pi^n(J)$. Then $\mathrm{sgn}_1(w) = -1$ by Lemma 5.14 (a); hence w has the form $w = (u, v)\,\sigma$. By the recursion relations (4.1), any factor b_{i_j} of $w = b_{i_1} \cdots b_{i_k}$ contributes precisely one factor $b_{\pi(i_j)}$ to the product uv. Thus uv is a product of the elements $b_{\pi(i_1)}, \ldots, b_{\pi(i_k)}$ in some order. It is therefore strongly of type $\pi^{n+1}(J)$, as desired. □

Proposition 4.18 *Any Φ-irreducible element w of $\Gamma_{\underline{x}}$ is W-conjugate to a Φ-irreducible element of $\Gamma_{(0,\ldots,0)}$.*

Proof. By Proposition 4.15 it is conjugate to $a_{i_1} \cdots a_{i_k} \in \Gamma_{(0,\ldots,0)}$, where $i_1, \ldots, i_k$ are the distinct elements of J_w in any order. But the same argument as in the proof of Proposition 4.17 shows that for some order, the element $a_{i_1} \cdots a_{i_k}$ is Φ-irreducible. □

4.5 Some combinatorics

The content of this subsection and the next is needed only to determine the precise lowest common denominator in Theorem 4.46 below, and can be skipped if one is happy with some common denominator.

For all $x \in \{0, 1\}$ we set

$$S^x := \{2 \leqslant i \leqslant r \mid x_i = x\} \quad \text{and} \tag{4.19}$$

$$I_r^x := \pi(S^x). \tag{4.20}$$

For all $x \in \{0, 1\}$ and $1 < i \leqslant r$ we define by descending induction

$$I_{i-1}^x := \begin{cases} \pi(I_i^x \cap S^{x_i}) & \text{if } 1 \notin I_i^x, \\ \pi(I_i^x \cup S^{1-x_i}) & \text{if } 1 \in I_i^x. \end{cases} \tag{4.21}$$

Lemma 4.22 *For all $1 \leqslant i \leqslant r$ we have a decomposition into disjoint subsets*

$$\{1, \ldots, r\} = \{i\} \sqcup I_i^0 \sqcup I_i^1.$$

Proof. From (4.19) we deduce that $\{1,\ldots,r\} = \{1\} \sqcup S^0 \sqcup S^1$. By (4.20) this implies the desired assertion for $i = r$. Suppose that the assertion holds for $1 < i \leqslant r$. Then there is a unique index $x \in \{0,1\}$ with $1 \in I_i^x$ and $1 \notin I_i^{1-x}$. By (4.21) we thus have

$$\begin{aligned} I_{i-1}^{1-x} &= \pi(I_i^{1-x} \cap S^{x_i}) \quad \text{and} \\ I_{i-1}^{x} &= \pi(I_i^{x} \cup S^{1-x_i}). \end{aligned}$$

The fact that $1 \notin I_i^{1-x}$ also implies that

$$I_i^{1-x} \;=\; (I_i^{1-x} \cap S^{1-x_i}) \sqcup (I_i^{1-x} \cap S^{x_i}).$$

The induction hypothesis and the fact that $i \notin S^{1-x_i}$ imply that

$$I_i^x \cup (I_i^{1-x} \cap S^{1-x_i}) \;=\; I_i^x \cup S^{1-x_i}.$$

Together it follows that

$$\begin{aligned} \{1,\ldots,r\} &= \pi\big(\{i\} \sqcup I_i^x \sqcup I_i^{1-x}\big) \\ &= \pi\big(\{i\} \sqcup I_i^x \sqcup (I_i^{1-x} \cap S^{1-x_i}) \sqcup (I_i^{1-x} \cap S^{x_i})\big) \\ &= \pi\big(\{i\} \sqcup (I_i^x \cup S^{1-x_i}) \sqcup (I_i^{1-x} \cap S^{x_i})\big) \\ &= \{i-1\} \sqcup I_{i-1}^x \sqcup I_{i-1}^{1-x}, \end{aligned}$$

and the desired assertion holds for $i-1$. By downward induction it follows for all i. □

Lemma 4.23 *For any distinct $1 \leqslant i, j \leqslant r$ there exist $x, y \in \{0,1\}$ such that*

$$I_i^x \cup I_j^y \;=\; \{1,\ldots,r\}.$$

Proof. Suppose first that one of i, j is equal to r. By symmetry we may assume that $i < j = r$. By Lemma 4.22 there is a unique $x \in \{0,1\}$ such that $1 \in I_{i+1}^x$. With $y := x_{i+1}$ the constructions (4.20) and (4.21) then imply that

$$I_i^x \cup I_r^y \;=\; \pi\big(I_{i+1}^x \cup S^{1-y} \cup S^y\big).$$

Since $1 \in I_{i+1}^x$ and $\{1\} \cup S^{1-y} \cup S^y = \{1,\ldots,r\}$, the right hand side is equal to $\{1,\ldots,r\}$, as desired.

Suppose now that the assertion holds for given $i, j > 1$. We then prove it for $i-1$ and $j-1$. By Lemma 4.22 there are unique $x, y \in \{0,1\}$ such that $1 \in I_i^x \cap I_j^y$. The construction (4.21) then implies that

$$I_{i-1}^x \cup I_{j-1}^y \;=\; \pi\big(I_i^x \cup S^{1-x_i} \cup I_j^y \cup S^{1-x_j}\big). \tag{4.24}$$

If $x_i \neq x_j$, the right hand side of (4.24) contains $\pi\big(\{1\} \cup S^0 \cup S^1\big) = \{1,\ldots,r\}$, and we are done. Otherwise abbreviate $z := x_i = x_j$. Using the induction hypothesis choose

$x', y' \in \{0,1\}$ such that $I_i^{x'} \cup I_j^{y'} = \{1,\ldots,r\}$. Then in particular $1 \in I_i^{x'} \cup I_j^{y'}$, and so either $x' = x$ or $y' = y$ or both. If $(x', y') = (x, y)$, the right hand side of (4.24) contains $\pi\big(I_i^x \cup I_j^y\big) = \{1,\ldots,r\}$, and we are done. Otherwise by symmetry we may without loss of generality assume that $(x', y') = (x, 1-y)$. Instead of $I_{i-1}^x \cup I_{j-1}^y$ we then look at $I_{i-1}^x \cup I_{j-1}^{1-y}$. Since $1 \in I_i^x \smallsetminus I_j^{1-y}$, the construction (4.21) implies that

$$I_{i-1}^x \cup I_{j-1}^{1-y} \;=\; \pi\big(I_i^x \cup S^{1-z} \cup (I_j^{1-y} \cap S^z)\big).$$

Since $1 \in I_i^x$ and $\{1\} \cup S^{1-z} \cup S^z = \{1,\ldots,r\}$, we deduce that

$$I_{i-1}^x \cup I_{j-1}^{1-y} \;\supset\; \pi\big(I_i^x \cup I_j^{1-y}\big) \;=\; \{1,\ldots,r\},$$

and again we are done. The lemma thus follows by descending induction. □

Lemma 4.25 *There exist* $1 \leqslant i \leqslant r$ *and* $x \in \{0,1\}$ *such that* $I_i^x = \varnothing$.

Proof. Choose i and x such that $|I_i^x|$ is minimal. If $|I_i^x| > 0$, pick any $j \in I_i^x$. Then Lemma 4.22 implies that $j \neq i$. Using Lemma 4.23 choose $x', y \in \{0,1\}$ such that $I_i^{x'} \cup I_j^y = \{1,\ldots,r\}$. Then by Lemma 4.22 for j in place of i we have $j \notin I_j^y$, and therefore $j \in I_i^{x'}$. Thus $j \in I_i^{x'} \cap I_i^x$, which by Lemma 4.22 implies that $x' = x$. Therefore $I_i^x \cup I_j^y = \{1,\ldots,r\}$. Counting elements, and using Lemma 4.22 for j in place of i again, we deduce that

$$|I_i^x| + |I_j^y| \;\geqslant\; r \;=\; 1 + |I_j^{1-y}| + |I_j^y|.$$

Therefore $|I_i^x| \geqslant 1 + |I_j^{1-y}| > |I_j^{1-y}|$, contradicting the minimality of $|I_i^x|$. Thus after all we have $|I_i^x| = 0$, and hence $I_i^x = \varnothing$, as desired. □

Lemma 4.26 *There exists* $x \in \{0,1\}$ *such that* $I_1^x = \varnothing$.

Proof. By Lemma 4.25 there exists a smallest index $1 \leqslant i \leqslant r$ such that $I_i^x = \varnothing$ for some $x \in \{0,1\}$. If that index is > 1, we in particular have $1 \notin I_i^x$; hence the construction (4.21) implies that $I_{i-1}^x = \pi(I_i^x \cap S^{x_i}) = \varnothing$, contradicting the minimality of i. □

4.6 Minimal words for Φ-irreducible elements

In this subsection we study the minimal words for Φ-irreducible elements in more detail.

Here and only here we use the following abbreviations: For any subset $I \subset \{1,\ldots,r\}$ we let $\langle I \rangle$ denote any (possibly empty) word over the alphabet $\{b_i^{\pm 1} \mid i \in I\}$. A concatenation of expressions $\langle I \rangle$ for subsets I and/or of individual letters $b_i^{\pm 1}$ represents the concatenation of any words or letters of the indicated form. An overline $\overline{}$ over such a confounded expression means that the template is repeated an arbitrary non-negative number of times. One should keep in mind that this notation refers to words and not to the group elements represented by them.

Lemma 4.27 *If $w \in \Gamma_{\underline{x}}$ is represented by a word of the form $\langle I \rangle$, then $J_w \subset I$.*

Proof. Lemma 4.11 implies that $\mathrm{sgn}_i(b_i) = -1$ and $\mathrm{sgn}_i(b_j) = 1$ whenever $i \neq j$. $\square$

Let S^x and I_i^x be as in the preceding subsection.

Lemma 4.28 *Consider any Φ-irreducible element $w \in \Gamma_{\underline{x}}$ with $1 \notin J_w$. Then any minimal word for w has one of the forms*

$$\begin{aligned} &\langle S^0 \rangle \; \overline{b_1^{-1} \langle S^1 \rangle \, b_1 \langle S^0 \rangle}, \\ &\langle S^1 \rangle \; \overline{b_1 \langle S^0 \rangle \, b_1^{-1} \langle S^1 \rangle}. \end{aligned}$$

Proof. The assumption $1 \notin J_w$ means that $\mathrm{sgn}_1(w) = 1$. Thus $w = (u, v)$ for certain $u, v \in \Gamma_{\underline{x}}$. By the recursion relations (4.1), any letter $b_k^{\pm 1}$ in the minimal word for w contributes precisely one letter $b_{\pi(k)}^{\pm 1}$ to a word representing u or v. Since one of u, v has the same length as w by Lemma 4.10, this letter must always land in the same one of u, v. Now suppose that the minimal word in question contains a subword of one of the forms

$b_1 b_1$	$b_1^{-1} b_i^{\pm 1}$	$b_1 b_j^{\pm 1}$	$b_i^{\pm 1} b_j^{\pm 1}$
$b_1^{-1} b_1^{-1}$	$b_i^{\pm 1} b_1$	$b_j^{\pm 1} b_1^{-1}$	$b_j^{\pm 1} b_i^{\pm 1}$

for some $i \in S^0$ and $j \in S^1$ and independent exponents ± 1. By (4.1) the recursive expansion of this subword is, respectively:

(b_r, b_r)	$(b_r^{-1}, b_{i-1}^{\pm 1})\, \sigma$	$(b_{j-1}^{\pm 1}, b_r)\, \sigma$	$(b_{i-1}^{\pm 1}, b_{j-1}^{\pm 1})$
(b_r^{-1}, b_r^{-1})	$(b_{i-1}^{\pm 1}, b_r)\, \sigma$	$(b_r^{-1}, b_{j-1}^{\pm 1})\, \sigma$	$(b_{i-1}^{\pm 1}, b_{j-1}^{\pm 1})$

Thus the two letters of this subword bequeath one letter to each of u and v, yielding a contradiction. Therefore the minimal word does not contain a subword of the above form. This means that the minimal word is a subword of a word of the form

$$\ldots b_1 \langle S^0 \rangle \, b_1^{-1} \langle S^1 \rangle \, b_1 \langle S^0 \rangle \, b_1^{-1} \langle S^1 \rangle \, b_1 \ldots .$$

Finally, since $\mathrm{sgn}_1(w) = 1$, and $\mathrm{sgn}_1(b_i) = -1$ only for $i = 1$, the total number of letters $b_1^{\pm 1}$ is even. Depending on the first letter the minimal word therefore has the indicated form. $\square$

For the following argument we fix a Φ-irreducible element $w_0 \in \Gamma_{\underline{x}}$ with $1 \notin J_w$. We construct a sequence of Φ-irreducible elements $w_n \in \Gamma_{\underline{x}}$ by defining each w_{n+1} as the first descendant of w_n furnished by Lemma 4.10. We also fix any minimal word $\widetilde{w}_0$ for w_0. By repeated recursive expansion using the relations (4.1) this yields a minimal word $\widetilde{w}_n$ for w_n for every $n \geqslant 0$.

Lemma 4.29 *For every $n \geqslant 0$ we have $J_{w_n} = \pi^n(J_{w_0})$.*

Proof. This follows by induction from Lemma 4.13. $\square$

Lemma 4.30 *For any $1 \leqslant i \leqslant r$ the word $\widetilde{w}_{r+1-i}$ has one of the forms*

$$\begin{aligned}&\langle I_i^0\rangle\ \overline{b_i^{-1}\langle I_i^1\rangle\, b_i\langle I_i^0\rangle},\\ &\langle I_i^1\rangle\ \overline{b_i\langle I_i^0\rangle\, b_i^{-1}\langle I_i^1\rangle}.\end{aligned}$$

Proof. Recall from (4.20) that $\pi(S^x) = I_r^x$ for each $x = 0, 1$. Thus the recursion relations (4.1) show that any word of the form $\langle S^0\rangle\ \overline{b_1^{-1}\langle S^1\rangle\, b_1\langle S^0\rangle}$ expands to one of the form $\big(\langle I_r^0\rangle\ \overline{b_r^{-1}\langle I_r^1\rangle\, b_r\langle I_r^0\rangle},\ 1\big)$, and any word of the form $\langle S^1\rangle\ \overline{b_1\langle S^0\rangle\, b_1^{-1}\langle S^1\rangle}$ expands to one of the form $\big(1,\ \langle I_r^1\rangle\ \overline{b_r\langle I_r^0\rangle\, b_r^{-1}\langle I_r^1\rangle}\,\big)$. Lemma 4.28 therefore implies the desired assertion in the case $i = r$ for the word $\widetilde{w}_{r+1-i} = \widetilde{w}_1$.

Suppose now that the assertion holds for some $1 < i \leqslant r$. We then prove it for $i-1$. We first look at the individual pieces of $\widetilde{w}_{r+1-i}$. Using Lemma 4.22 let $x \in \{0,1\}$ be the unique index with $1 \in I_i^{1-x}$ and $1 \notin I_i^x$.

Sublemma 4.31 *The recursive expansion of the letter b_i is*

$$\begin{aligned}&(b_{i-1}, 1) \quad \text{if } x_i = 0,\\ &(1, b_{i-1}) \quad \text{if } x_i = 1.\end{aligned}$$

The recursive expansion of any word of the form $\langle I_i^x\rangle$ has the form

$$\begin{aligned}&\big(\langle I_{i-1}^x\rangle, \langle I_{i-1}^{1-x}\rangle\big) \quad \text{if } x_i = 0,\\ &\big(\langle I_{i-1}^{1-x}\rangle, \langle I_{i-1}^x\rangle\big) \quad \text{if } x_i = 1.\end{aligned}$$

The recursive expansion of any word of the form $\langle I_i^{1-x}\rangle$ has one of the forms

$$\begin{aligned}&\big(\langle I_{i-1}^{1-x}\rangle, \langle I_{i-1}^{1-x}\rangle\big),\\ &\big(\langle I_{i-1}^{1-x}\rangle, \langle I_{i-1}^{1-x}\rangle\big)\,\sigma.\end{aligned}$$

Proof. The first statement is a special case of the recursion relations (4.1). Since $1 \notin I_i^x$, the relations also imply that the recursive expansion of any word of the form $\langle I_i^x\rangle$ has the form $\big(\langle\pi(I_i^x \cap S^0)\rangle, \langle\pi(I_i^x \cap S^1)\rangle\big)$. But by (4.21) we have $\pi(I_i^x \cap S^{x_i}) = I_{i-1}^x$ and $\pi(I_i^x \cap S^{1-x_i}) \subset I_{i-1}^{1-x}$, so the second statement follows. Likewise the recursive expansion of any word of the form $\langle I_i^{1-x}\rangle$ involves only letters $b_{\pi(j)}^{\pm 1}$ for $j \in I_i^{1-x}$ and (possibly) some factors σ. It is therefore of the form $\big(\langle\pi(I_i^{1-x})\rangle, \langle\pi(I_i^{1-x})\rangle\big)$ or $\big(\langle\pi(I_i^{1-x})\rangle, \langle\pi(I_i^{1-x})\rangle\big)\,\sigma$. Since $1 \in I_i^{1-x}$, by (4.21) we have $\pi(I_i^{1-x}) \subset I_{i-1}^{1-x}$, and the third statement follows. $\square$

Returning to the proof of Lemma 4.30, we now set $\mu := 1-2x$. Then by the induction hypothesis $\widetilde{w}_{r+1-i}$ has one of the forms

$$\langle I_i^{1-x}\rangle\, \overline{b_i^{\mu}\langle I_i^{x}\rangle\, b_i^{-\mu}\cdot\langle I_i^{1-x}\rangle}, \tag{4.32}$$

$$\langle I_i^{x}\rangle\, \overline{b_i^{-\mu}\langle I_i^{1-x}\rangle\, b_i^{\mu}\cdot\langle I_i^{x}\rangle}, \tag{4.33}$$

and we must prove the same for $\widetilde{w}_{r+2-i}$ with $i-1$ in place of i.

In the case (4.32) Sublemma 4.31 implies that the recursive expansion of $\widetilde{w}_{r+1-i}$ is a product of terms of the form $\big(b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}, \langle I_{i-1}^{1-x}\rangle\big)$ or $\big(\langle I_{i-1}^{1-x}\rangle, b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\big)$ and/or $\big(\langle I_{i-1}^{1-x}\rangle, \langle I_{i-1}^{1-x}\rangle\big)$ and/or σ. It is thus equal to $(\tilde{u},\tilde{v})$ or $(\tilde{u},\tilde{v})\,\sigma$, where both $\tilde{u}$ and $\tilde{v}$ are products of terms of the form $b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}$ and/or $\langle I_{i-1}^{1-x}\rangle$. The next descendant $\widetilde{w}_{r+2-i}$ is equal to $\tilde{u}$ or $\tilde{v}$ or $\tilde{u}\tilde{v}$ and therefore also such a product. Thus the lemma follows for $i-1$.

In the case (4.33) suppose first that $\widetilde{w}_{r+1-i}$ does not contain the letter $b_i^{\pm1}$. Then it has the form $\langle I_i^{x}\rangle$. By Sublemma 4.31 it thus has the recursive expansion $(\tilde{u},\tilde{v})$ with one entry of the form $\langle I_{i-1}^{x}\rangle$ and the other of the form $\langle I_{i-1}^{1-x}\rangle$. Since in this case the next descendant $\widetilde{w}_{r+2-i}$ is equal to one of $\tilde{u}$, $\tilde{v}$, the lemma again follows for $i-1$.

Now suppose that $\widetilde{w}_{r+1-i}$ has the form (4.33) and contains the letter $b_i^{\pm1}$. We then regroup its factors in the form

$$\underbrace{\langle I_i^{x}\rangle\, b_i^{-\mu}}\cdot\underbrace{\langle I_i^{1-x}\rangle\, \overline{b_i^{\mu}\langle I_i^{x}\rangle\, b_i^{-\mu}\cdot\langle I_i^{1-x}\rangle}}\cdot\underbrace{b_i^{\mu}\langle I_i^{x}\rangle}. \tag{4.34}$$

As in the case (4.32) the whole shebang in the middle expands to $(\tilde{u},\tilde{v})$ or $(\tilde{u},\tilde{v})\,\sigma$, where $\tilde{u}$ and $\tilde{v}$ are products of terms of the form $b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}$ and/or $\langle I_{i-1}^{1-x}\rangle$. Assume first that it expands to $(\tilde{u},\tilde{v})$. Sublemma 4.31 then implies that $\widetilde{w}_{r+1-i}$ expands to

$$\begin{aligned}
&\big(\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{u}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle,\ \langle I_{i-1}^{1-x}\rangle\cdot\tilde{v}\cdot\langle I_{i-1}^{1-x}\rangle\big) && \text{if } x_i=0,\\
&\big(\langle I_{i-1}^{1-x}\rangle\cdot\tilde{u}\cdot\langle I_{i-1}^{1-x}\rangle,\ \langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{v}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\big) && \text{if } x_i=1.
\end{aligned}$$

By construction with Lemma 4.10 the next descendant $\widetilde{w}_{r+2-i}$ is the unique non-empty entry of this pair; hence it is the one containing $b_{i-1}^{\pm1}$. Since $\tilde{u}$ and $\tilde{v}$ are products of terms of the form $b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}$ and/or $\langle I_{i-1}^{1-x}\rangle$, both $\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{u}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle$ and $\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{v}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle$ are products of terms of the form $\langle I_{i-1}^{x}\rangle$ and/or $b_{i-1}^{-\mu}\langle I_{i-1}^{1-x}\rangle\, b_{i-1}^{\mu}$. Thus $\widetilde{w}_{r+2-i}$ is such a product, and so the lemma holds for $i-1$.

Assume now that the middle of (4.34) expands to $(\tilde{u},\tilde{v})\,\sigma$. Sublemma 4.31 then implies that $\widetilde{w}_{r+1-i}$ expands to

$$\begin{aligned}
&\big(\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{u}\cdot\langle I_{i-1}^{1-x}\rangle,\ \langle I_{i-1}^{1-x}\rangle\cdot\tilde{v}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\big)\,\sigma && \text{if } x_i=0,\\
&\big(\langle I_{i-1}^{1-x}\rangle\cdot\tilde{u}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle,\ \langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{v}\cdot\langle I_{i-1}^{1-x}\rangle\big)\,\sigma && \text{if } x_i=1.
\end{aligned}$$

The next descendant $\widetilde{w}_{r+2-i}$ is now the concatenation of these entries and thus of the form

$$\begin{aligned}
&\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{u}\cdot\langle I_{i-1}^{1-x}\rangle\cdot\tilde{v}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle && \text{if } x_i=0,\\
&\langle I_{i-1}^{1-x}\rangle\cdot\tilde{u}\cdot b_{i-1}^{\mu}\langle I_{i-1}^{x}\rangle\, b_{i-1}^{-\mu}\cdot\tilde{v}\cdot\langle I_{i-1}^{1-x}\rangle && \text{if } x_i=1.
\end{aligned}$$

In the case $x_i = 0$ it follows that $\widetilde{w}_{r+2-i}$ is a product of terms of the form $\langle I^x_{i-1}\rangle$ and/or $b^{-\mu}_{i-1}\langle I^{1-x}_{i-1}\rangle\, b^{\mu}_{i-1}$. In the case $x_i = 1$ it is a product of terms of the form $\langle I^{1-x}_{i-1}\rangle$ and/or $b^{\mu}_{i-1}\langle I^{x}_{i-1}\rangle\, b^{-\mu}_{i-1}$. In either case the lemma holds for $i-1$.

This finishes the proof of the induction step, and so the lemma follows for all $1 \leqslant i \leqslant r$ by descending induction on i. □

Lemma 4.35 *The word $\widetilde{w}_r$ has the form $\langle I\rangle$ or $b_1^{-1}\langle I\rangle\, b_1$ or $b_1\langle I\rangle\, b_1^{-1}$ for $I := \{2,\ldots,r\}$.*

Proof. By Lemma 4.26 there exists $x \in \{0,1\}$ such that $I^x_1 = \varnothing$. By Lemma 4.22 we then have $I^{1-x}_1 = \{2,\ldots,r\} = I$. If $x = 0$, Lemma 4.30 implies that $\widetilde{w}_r$ has the form $\overline{b_1^{-1}\langle I\rangle\, b_1}$ or the form $\langle I\rangle\ \overline{b_1 b_1^{-1}\langle I\rangle}$. But since $\widetilde{w}_r$ is minimal, it does not contain the subword $b_1 b_1^{-1}$. Therefore $\widetilde{w}_r$ has the form $b_1^{-1}\langle I\rangle\, b_1$ or $\langle I\rangle$, as desired. If $x = 1$, Lemma 4.30 implies that $\widetilde{w}_r$ has the form $\langle I\rangle\ \overline{b_1^{-1} b_1\langle I\rangle}$ or the form $\overline{b_1\langle I\rangle\, b_1^{-1}}$. Again by minimality $\widetilde{w}_r$ does not contain the subword $b_1^{-1}b_1$. It therefore has the form $\langle I\rangle$ or $b_1\langle I\rangle\, b_1^{-1}$, as desired. □

Lemma 4.36 *The word $\widetilde{w}_r$ has the form $\langle S^0\rangle$ or $b_1\langle S^0\rangle\, b_1^{-1}$ or $\langle S^1\rangle$ or $b_1^{-1}\langle S^1\rangle\, b_1$.*

Proof. By Lemma 4.29 we have $J_{w_r} = \pi^r(J_{w_0}) = J_{w_0}$ and hence $1 \notin J_{w_r}$. Since $\widetilde{w}_r$ is a minimal word for the Φ-irreducible element w_r, it therefore satisfies the conditions of Lemma 4.28. Moreover, Lemma 4.35 means that $\widetilde{w}_r$ contains the letters $b_1^{\pm 1}$ at most in the first and last positions. With Lemma 4.28 it follows that $\widetilde{w}_r$ has the indicated form. □

Lemma 4.37 *The word $\widetilde{w}_0$ has the form $\langle \{1\} \cup S^0\rangle$ or the form $\langle \{1\} \cup S^1\rangle$.*

Proof. For any $n \geqslant 0$, each letter $b_i^{\pm 1}$ of the word $\widetilde{w}_n$ bequeathes a letter $b^{\pm 1}_{\pi(i)}$ to the word $\widetilde{w}_{n+1}$. By induction it follows that each letter $b_i^{\pm 1}$ of the word $\widetilde{w}_0$ bequeathes a letter $b^{\pm 1}_{\pi^r(i)} = b_i^{\pm 1}$ to the word $\widetilde{w}_r$. Thus $\widetilde{w}_0$ and $\widetilde{w}_r$ consist of the same letters, possibly rearranged. By Lemma 4.36 these letters $b_i^{\pm 1}$ either all satisfy $i \in \{1\} \cup S^0$ or all satisfy $i \in \{1\} \cup S^1$. Thus $\widetilde{w}_r$ and $\widetilde{w}_0$ have the indicated form. □

Lemma 4.38 *For any Φ-irreducible element $w \in \Gamma_{\underline{x}}$ with $1 \notin J_w$, the values x_i for all $i \in J_w$ are equal.*

Proof. Apply the above constructions to $w_0 := w$. Then by Lemma 4.37 the word $\widetilde{w}_0$ has the form $\langle \{1\} \cup S^x\rangle$ for some $x \in \{0,1\}$. By Lemma 4.27 we therefore have $J_w \subset \{1\} \cup S^x$ and hence $J_w \subset S^x$, as desired. □

Proposition 4.39 *For any Φ-irreducible $w \in \Gamma_{\underline{x}}$ the subset J_w satisfies Condition 4.16.*

Proof. Apply the above constructions to $w_0 := w$. Then by Lemma 4.29 for any $n \geqslant 0$ we have $J_{w_n} = \pi^n(J_w)$. Thus if $1 \notin \pi^n(J_w)$, applying Lemma 4.38 to w_n implies that the values x_i for all $i \in \pi^n(J_w)$ are equal. Therefore J_w satisfies Condition 4.16. □

4.7 Some rational functions and their denominators

To any subset $J \subset \{1,\ldots,r\}$ we now associate the following rational functions. Write the distinct elements of J in ascending order $i_1 < \ldots < i_k$ and set

$$(4.40) \qquad \Psi_J := \frac{1}{1-X^kY^r}\cdot\sum_{1\leqslant j\leqslant k} X^{j-1}Y^{i_j} \qquad \text{and}$$

$$(4.41) \qquad \Phi_J := \frac{1}{1-2Y} + \frac{X-2}{1-2Y}\cdot\Psi_J.$$

For any $1 \leqslant k \leqslant r$ we define

$$(4.42) \qquad D_k := \text{lowest common denominator of the } \Psi_J \text{ for all } J \text{ with } k = |J|.$$

Proposition 4.43 *For any $1 \leqslant k \leqslant r$ we have*

$$D_k = \begin{cases} (1-X^kY^r) & \text{if } k<r, \\ (1-XY) & \text{if } k=r. \end{cases}$$

Proof. By construction D_k divides $1-X^kY^r$. Conversely, for $J := \{1,\ldots,k\}$ we have

$$(1-X^kY^r)\cdot\Psi_J = \sum_{1\leqslant j\leqslant k} X^{j-1}Y^j = Y\cdot\frac{1-X^kY^k}{1-XY}.$$

In the case $k<r$ the polynomials $1-X^kY^r$ and $Y(1-X^kY^k)$ are coprime, and hence $D_k = 1-X^kY^r$, as desired. In the case $k=r$ the only possible subset is $J=\{1,\ldots,r\}$, and then the above calculation shows that $\Psi_J = \frac{Y}{1-XY}$. □

4.8 Denominators of orbit length generating functions

Proposition 4.44 *For any Φ-irreducible element $w \in \Gamma_{\underline{x}}$ we have $\Phi_w = \Phi_{J_w}$.*

Proof. Let $i_1,\ldots,i_k$ be the distinct elements of J_w, in any order. For all $n \geqslant 0$ set $w_n = a_{\pi^n(i_1)}\cdots a_{\pi^n(i_k)}$. Then w is W-conjugate to w_0 by Proposition 4.15. Also, by Lemma 4.14 each w_n is W-conjugate to $(w_{n+1},1)\,\sigma^{\mu_n}$, where $\mu_n = 1$ if $1 \in \pi^n(J_w)$ and $\mu_n = 0$ otherwise. Since orbit length generating functions are invariant under conjugation, we have $\Psi_w = \Psi_{w_0}$, and with Proposition 2.14 we deduce that

$$\Psi_{w_n} = \begin{cases} Y\Psi_1 + Y\Psi_{w_{n+1}} & \text{if } 1 \notin \pi^n(J_w), \\ Y + XY\Psi_{w_{n+1}} & \text{if } 1 \in \pi^n(J_w). \end{cases}$$

As $\Psi_1 = 0$ by (2.15), the first of these formulas simplifies to $\Psi_{w_n} = Y\Psi_{w_{n+1}}$. By induction on n it follows that

$$\Psi_{w_0} = \sum_{\substack{0\leqslant m<n \\ 1\in\pi^m(J_w)}} X^{k_m}Y^{m+1} + X^{k_n}Y^n\Psi_{w_n},$$

where k_m denotes the number of integers $0 \leqslant \ell < m$ such that $1 \in \pi^\ell(J_w)$. Taking the limit in $\mathbb{Z}[[X,Y]]$ we obtain

$$\Psi_w \;=\; \Psi_{w_0} \;=\; \sum_{\substack{m\geqslant 0\\ 1\in\pi^m(J_w)}} X^{k_m}Y^{m+1}.$$

Since π permutes the letters $1,\ldots,r$ transitively, and J_w has cardinality k, we have $k_{m+r} = k_m + k$ for all $m \geqslant 0$. The last equality therefore implies that

$$\Psi_w \;=\; \frac{1}{1-X^kY^r}\cdot \sum_{\substack{0\leqslant m<r\\ 1\in\pi^m(J_w)}} X^{k_m}Y^{m+1}.$$

Moreover, for all $0 \leqslant m < r$ we have $1 \in \pi^m(J_w)$ if and only if $m+1 = \pi^{-m}(1) \in J_w$, and so

$$\Psi_w \;=\; \frac{1}{1-X^kY^r}\cdot \sum_{i\in J_w} X^{k_{i-1}}Y^i.$$

Also for all $i \in J_w$ we have $k_{i-1} = \bigl|\{m \in J_w \mid m < i\}\bigr|$. Finally, since the last formula is independent of the order of $i_1,\ldots,i_k$, we may without loss of generality assume that $i_1 < \ldots < i_k$. Then for all $1 \leqslant j \leqslant k$ we have $k_{i_j-1} = \bigl|\{m \in J_w \mid m < i_j\}\bigr| = j-1$. Therefore $\Psi_w = \Psi_{J_w}$. By Proposition 2.13 this implies that $\Phi_w = \Phi_{J_w}$, as desired. □

For any $1 \leqslant k \leqslant r$ we now define

$$(4.45)\qquad D_{\underline{x},k} \;:=\; \left[\begin{array}{l}\text{lowest common denominator of the } \Psi_J \text{ for all } J\\ \text{with } k = |J| \text{ satisfying Condition 4.16.}\end{array}\right]$$

By construction this is a divisor of the polynomial D_k from (4.42) and Proposition 4.43.

Theorem 4.46 *The power series $\Phi_w \in 1+Y\mathbb{Z}[[X,Y]]$ for all $w \in \Gamma_{\underline{x}}$ are rational functions with the lowest common denominator*

$$D_{\underline{x}} \;:=\; (1-2Y)\cdot \prod_{1\leqslant k\leqslant r} D_{\underline{x},k} \;\in\; 1+Y\mathbb{Z}[X,Y].$$

Proof. By Proposition 4.9 and Theorem 2.8 the Φ_w for all $w \in \Gamma_{\underline{x}}$ are $\mathbb{Z}[X,Y]$-linear combinations of the Φ_w for all Φ-irreducible elements. By Propositions 4.17 and 4.39 and 4.44 the latter are precisely the Φ_J for all subsets $J \subset \{1,\ldots,r\}$ which satisfy Condition 4.16. They are therefore rational functions, and in view of (4.41) and (4.45) their lowest common denominator is the least common multiple of the polynomials $(1-2Y)D_{\underline{x},k}$ for all k.

The definition (4.40) of Ψ_J implies that each $D_{\underline{x},k}$ divides $1-X^kY^r$. Thus $D_{\underline{x},k}$ can be chosen congruent to $1 \bmod Y$, and then $D_{\underline{x}}$ has the same property. Moreover, the polynomials $1-2Y$ and $1-X^kY^r$ for all $1 \leqslant k \leqslant r$ are pairwise coprime, for instance because, viewed as polynomials in Y, their zeros in an algebraic closure of $\mathbb{Q}(X)$ are mutually distinct. Thus the least common multiple of all $(1-2Y)D_{\underline{x},k}$ is $D_{\underline{x}}$, and we are done. □

Proposition 4.47 *(a) For all $\underline{x}$ we have $D_{\underline{x},1} = D_1 = 1-XY^r$ and $D_{\underline{x},r} = D_r = 1-XY$.*

(b) For $\underline{x} = (0,\dots,0)$ or $(1,\dots,1)$ we have $D_{\underline{x},k} = D_k$ for all k.

Proof. Assertion (a) follows from the fact that any subset J of cardinality 1 or r satisfies Condition 4.16. Assertion (b) follows from the fact that for these $\underline{x}$, Condition 4.16 is satisfied for all J. □

In principle, the determination of the lowest common denominator $D_{\underline{x}}$ in Theorem 4.46 is a finite combinatorial problem concerning the tuple $\underline{x}$. The author does not (yet) know a simple direct description in general. However, we determined $D_{\underline{x}}$ in small cases using the computer algebra system Maple: see [6]. The outcome was that whenever $r \leqslant 10$ and $x_2,\dots,x_r$ are not all equal, then $\prod_{2\leqslant k<r} D_{\underline{x},k} = 1$ except in the following cases:

r	$\prod_{2\leqslant k<r} D_{\underline{x},k}$	Conditions on $\underline{x} = (x_2,\dots,x_r)$
4	$(1-XY^2)$	$x_2 = x_4 \neq x_3$
6	$(1-X^2Y^6)(1-XY^2)$	$x_2 = x_4 = x_6 \neq x_3 = x_5$
6	$(1-XY^3)(1-X^2Y^3)$	$x_2 = x_3 = x_5 = x_6 \neq x_4$
6	$(1-XY^3)$	$x_2 = x_5 \neq x_3 = x_6$
6	$(1-XY^2)$	$x_2 = x_4 = x_6 \ \wedge\ x_3 \neq x_5$
8	$(1-X^2Y^8)(1-X^3Y^8)(1-XY^2)$	$x_2 = x_4 = x_6 = x_8 \neq x_3 = x_5 = x_7$
8	$(1-XY^4)(1-X^2Y^4)(1-X^3Y^4)$	$x_2 = x_3 = x_4 = x_6 = x_7 = x_8 \neq x_5$
8	$(1-XY^4)(1-XY^2)$	$x_2 = x_4 = x_5 = x_6 = x_8 \neq x_3 = x_7$
8	$(1-XY^4)$	$x_2 = x_6 \neq x_4 = x_8 \ \wedge\ x_3 = x_7$
8	$(1-XY^2)$	$x_2 = x_4 = x_6 = x_8 \ \wedge\ x_3 \neq x_7$
9	$(1-X^2Y^9)(1-XY^3)(1-X^2Y^3)$	$x_2 = x_3 = x_5 = x_6 = x_8 = x_9 \neq x_4 = x_7$
9	$(1-XY^3)(1-X^2Y^3)$	$x_2 = x_3 = x_5 = x_6 = x_8 = x_9 \ \wedge\ x_4 \neq x_7$
9	$(1-X^2Y^9)(1-XY^3)$	$x_2 = x_5 = x_8 \neq x_3 = x_6 = x_9 \ \wedge\ x_4 = x_7$
9	$(1-XY^3)$	$x_2 = x_5 = x_8 \neq x_3 = x_6 = x_9 \ \wedge\ x_4 \neq x_7$
10	$(1-X^2Y^{10})(1-X^3Y^{10})(1-X^4Y^{10})(1-XY^2)$	$x_2 = x_4 = x_6 = x_8 = x_{10} \neq x_3 = x_5 = x_7 = x_9$
10	$(1-XY^5)(1-X^2Y^5)(1-X^3Y^5)(1-X^4Y^5)$	$x_2 = x_3 = x_4 = x_5 = x_7 = x_8 = x_9 = x_{10} \neq x_6$
10	$(1-XY^5)$	$x_2 = x_7 \ \wedge\ x_3 = x_8 \ \wedge\ x_4 = x_9 \ \wedge\ x_5 = x_{10}$ but x_2, x_3, x_4, x_5 not all equal
10	$(1-XY^2)$	$x_2 = x_4 = x_6 = x_8 = x_{10}$ but x_3, x_5, x_7, x_9 not all equal

5 Iterated monodromy groups of quadratic polynomials: Pre-periodic case

5.1 The iterated monodromy group

Throughout this section we fix integers $r > s > 0$ and a tuple $\underline{x} = (x_2, \ldots, x_r)$ of elements of $\{0, 1\}$. Consider the elements $b_1, \ldots, b_r \in W$ defined by the recursion relations

$$\text{(5.1)} \qquad \begin{cases} b_1 &= \sigma, \\ b_{s+1} &= (b_r, b_s) \quad \text{if } x_{s+1} = 0, \\ b_{s+1} &= (b_s, b_r) \quad \text{if } x_{s+1} = 1, \\ b_i &= (b_{i-1}, 1) \quad \text{for all } i \neq 1, s+1 \text{ with } x_i = 0, \\ b_i &= (1, b_{i-1}) \quad \text{for all } i \neq 1, s+1 \text{ with } x_i = 1, \end{cases}$$

and let $\Gamma_{\underline{x}} \subset W$ be the subgroup generated by them. Up to a change in notation, these are the generators and the subgroup studied by Bartholdi and Nekrashevych in [1, §4]. Thus by [1, Thm. 5.1] we have:

Theorem 5.2 *Let f be any quadratic polynomial over $\mathbb{C}$ and $\eta \in \mathbb{C}$ be its unique critical point. Assume that $\eta, f(\eta), \ldots, f^r(\eta)$ are all distinct and that $f^{r+1}(\eta) = f^{s+1}(\eta)$. Then the iterated monodromy group of f is W-conjugate to $\Gamma_{\underline{x}}$ for a certain choice of the x_i.*

In the special case where $x_{s+1} = 1$ and all other $x_i = 0$ the above generators coincide with those studied in [5, §3], but we do not care about them here. Instead, we will pay attention to the case where $\underline{x} = (0, \ldots, 0)$, that is, to the elements $a_1, \ldots, a_r$ defined by

$$\text{(5.3)} \qquad \begin{cases} a_1 &= \sigma, \\ a_{s+1} &= (a_r, a_s), \\ a_i &= (a_{i-1}, 1) \quad \text{for all } i \neq 1, s+1. \end{cases}$$

Also observe:

Proposition 5.4 *The group $\Gamma_{(x_2,\ldots,x_r)}$ is conjugate to the group $\Gamma_{(1-x_2,\ldots,1-x_r)}$ under W.*

Proof. Same as that of Proposition 4.4, again with $w = (w, w)\,\sigma$. □

The aim of this section is to show that the orbit length generating functions of all elements of $\Gamma_{\underline{x}}$ are rational and possess an explicit common denominator.

5.2 Finiteness

We begin with some preparations. Let π denote the permutation of the set $\{1,\ldots,r\}$ defined by

$$\pi(i) := \begin{cases} s & \text{if } i=1, \\ r & \text{if } i=s+1, \\ i-1 & \text{otherwise.} \end{cases} \tag{5.5}$$

This induces a cyclic permutation of $\{1,\ldots,s\}$ and a cyclic permutation of $\{s+1,\ldots,r\}$. The recursion relations (5.1) express each b_i in terms of $b_{\pi(i)}$, with b_s thrown in for $i=s+1$ and taken out for $i=1$.

Let Δ denote the subgroup of $\Gamma_{\underline{x}}$ that is generated by $b_1,\ldots,b_s$. The recursive description of these elements implies that Δ acts on the vertices of T by changing only the last s letters of a word, leaving the rest unchanged. Thus Δ is finite and acts faithfully on the subtree T_s. In fact, one can easily show by induction that Δ maps isomorphically to the automorphism group of T_s and is therefore independent of $\underline{x}$ (although the individual generators $b_1,\ldots,b_s$ depend on it). This characterization of Δ also implies:

Lemma 5.6 *The only Φ-irreducible element of Δ is the identity element.*

By contrast, repeated application of the recursion relations to b_i for any $s < i \leqslant r$ eventually leads back to b_i. The two types of generators therefore play different roles in the arguments below. For instance, the letters $b_1,\ldots,b_s$ are not counted in the definition of the length below.

Lemma 5.7 *Every generator b_i has order* 2.

Proof. Same as that of [5, Prop. 3.1.4]. □

Definition 5.8 *The* length $|w|$ *of an element $w \in \Gamma_{\underline{x}}$ is the minimal number of letters from $\{b_{s+1},\ldots,b_r\}$ in a word over the alphabet $\{b_1,\ldots,b_r\}$ that represents w. Any word representing w with the minimal number of letters from $\{b_{s+1},\ldots,b_r\}$ is called a* minimal word *for w.*

Thus the elements of length 0 of $\Gamma_{\underline{x}}$ are precisely those in Δ.

Lemma 5.9 *For any element $w=(u,v)\,\sigma^\mu \in \Gamma_{\underline{x}}$ we have $u,v \in \Gamma_{\underline{x}}$ and*

$$|uv| \leqslant |u|+|v| \leqslant |w|.$$

Proof. By the recursion relations (5.1), any letter b_i for $s < i \leqslant r$ in a minimal word for w contributes precisely one letter $b_{\pi(i)}$ to a word representing precisely one of u, v, and sometimes a letter b_s which does not count towards the length. This implies the second inequality, and the first one follows directly from the definition of length. □

Lemma 5.10 *For all $w \in \Gamma_{\underline{x}}$ and all $w' \in \mathrm{Desc}(w)$ we have $w' \in \Gamma_{\underline{x}}$ with $|w'| \leqslant |w|$.*

Proof. By Definition 2.4 and iteration this follows from Lemma 5.8. □

Proposition 5.11 *Every element of $\Gamma_{\underline{x}}$ is Φ-finite.*

Proof. Any element of $\Gamma_{\underline{x}}$ of length ℓ can be written in the form $\delta_0 b_{i_1} \delta_1 \cdots b_{i_\ell} \delta_\ell$ with ℓ indices $s < i_j \leqslant r$ and elements $\delta_j \in \Delta$. Since Δ is finite, it follows that $\Gamma_{\underline{x}}$ contains only finitely many elements of any given length. With Lemma 5.10 this implies that $\mathrm{Desc}(w)$ is finite for any $w \in \Gamma_{\underline{x}}$, as desired. □

Combining Proposition 5.11 with Theorem 2.7 we find that the orbit length generating functions of all elements of $\Gamma_{\underline{x}}$ are rational. By Theorem 2.8 the study of their denominators reduces to the case of Φ-irreducible elements. This case requires more preparations.

5.3 Types and signs

Definition 5.12 *An element $w \in \Gamma_{\underline{x}}$ is called* of type $I \subset \{1, \ldots, r\}$ *if there exists a minimal word for w which consists only of letters b_i for $i \in I$.*

Note that this concerns a minimal word for w, though in principle a minimal word might require a letter which some non-minimal word can do without. But this is intentional, because we use the notion of type as a secondary measure of complexity after the length.

To any element $w \in \Gamma_{\underline{x}}$ we also associate the subset

$$J_w \;:=\; \{1 \leqslant i \leqslant r \mid \mathrm{sgn}_i(w) = -1\}. \tag{5.13}$$

To determine its relation with types we first observe:

Lemma 5.14 *For all $1 \leqslant i \leqslant r$ and $n \geqslant 1$ we have*

$$\mathrm{sgn}_n(b_i) \;=\; \begin{cases} -1 & \text{if } n = i \leqslant s, \\ -1 & \text{if } n \geqslant i > s \text{ and } n \equiv i \bmod (r-s), \\ 1 & \text{otherwise.} \end{cases}$$

Thus for any fixed $w \in \Gamma_{\underline{x}}$, the value $\mathrm{sgn}_n(w)$ for $n > s$ depends only on $n \bmod (r-s)$.

Proof. Same as that of [5, Prop. 3.1.1]. □

Lemma 5.15 *If $w \in \Gamma_{\underline{x}}$ is of type I, then $J_w \subset I$.*

Proof. Lemma 5.14 implies that $\mathrm{sgn}_i(b_i) = -1$ and $\mathrm{sgn}_i(b_j) = 1$ whenever $i \neq j$. □

5.4 Properties of Φ-irreducible elements

Lemma 5.16 *Any Φ-irreducible element $w \in \Gamma_{\underline{x}}$ has a unique first descendant w' which is Φ-irreducible with $|w'| = |w|$. Moreover w is either W-conjugate to $(w',1)\,\sigma$, or equal to (w',δ) or (δ,w') with $\delta \in \Delta$ where w' and δ are the first descendants of w.*

Proof. Suppose first that $w = (u,v)\,\sigma$. Then w is W-conjugate to $(uv,1)\,\sigma$, and uv is the unique first descendant of w. Thus the assumption $w \in \mathrm{Desc}(w)$ means that w is equal to or a descendant of uv. On the one hand this implies that uv is a descendant of itself; hence uv is Φ-irreducible. On the other hand it implies by Lemma 5.10 that $|w| \leqslant |uv| \leqslant |w|$ and hence $|uv| = |w|$, and we are done with $w' := uv$.

Suppose now that $w = (u,v)$, so that u and v are the first descendants of w. Then the assumption $w \in \mathrm{Desc}(w)$ means that w is equal to, or a descendant of, one of u, v; let us call it w'. On the one hand this implies that w' is a descendant of itself; hence w' is Φ-irreducible. On the other hand it implies by Lemma 5.10 that $|w| \leqslant |w'| \leqslant |w|$ and hence $|w'| = |w|$. Plugging this into the inequality $|u| + |v| \leqslant |w|$ from Lemma 5.9, we now deduce that the other entry of (u,v) has length 0 and therefore lies in Δ. Calling it δ, we then have $w = (w',\delta)$ or $w = (\delta,w')$. Finally this makes w' unique unless $|w| = 0$. But in that case $w = 1 = (1,1)$ by Lemma 5.6 and hence $w' = \delta = 1$ is again unique, and we are done. □

For the following arguments we fix a Φ-irreducible element $w_0 \in \Gamma_{\underline{x}}$ and construct a sequence of Φ-irreducible elements $w_n \in \Gamma_{\underline{x}}$ by defining each w_{n+1} as the first descendant of w_n furnished by Lemma 5.16.

Lemma 5.17 *The sequence $w_0, w_1, \ldots$ is periodic.*

Proof. Repeated application of Lemma 5.16 shows that the descendants of w_0 are precisely the elements w_n for $n \geqslant 1$ and perhaps some elements of Δ. Since by assumption w_0 is a descendant of itself, we must have $w_{n_0} = w_0$ for some $n_0 \geqslant 1$. Then the construction implies that $w_{n+n_0} = w_n$ for all $n \geqslant 0$. □

Lemma 5.18 *Consider any $n \geqslant 0$, and suppose that w_n is of type I. Then w_{n+1} is of type $\pi(I)$. If moreover $s+1 \notin I$ or $1 \notin J_{w_n}$, then w_{n+1} is of type $\pi(I) \smallsetminus \{s\}$.*

Proof. Set $\ell := |w_n|$ and write w_n as a minimal word $w_n = b_{i_1} \cdots b_{i_k}$ with all $i_j \in I$. Then precisely ℓ of these letters lie in $\{b_{s+1}, \ldots, b_r\}$. Write $w_n = (u,v)\sigma^\mu$ and use the recursion relations (5.1), but no other relations, to obtain words representing u and v. Then precisely ℓ of the letters of both words lie in $\{b_{s+1}, \ldots, b_r\}$. Since w_{n+1} is equal to u, v, or uv, and itself of length ℓ by Lemma 5.16, this results in a minimal word representing w_{n+1}.

By construction, any letter $b_{i_j} \neq b_1, b_{s+1}$ contributes at most one letter b_{i_j-1} to the word representing w_{n+1}. Any letter $b_{i_j} = b_{s+1}$ contributes at most the letters b_r and b_s, and any letter $b_{i_j} = b_1$ contributes nothing. This shows that w_{n+1} is of type

$$I' := \begin{cases} \{i-1 \mid 1, s+1 \neq i \in I\} & \text{if } s+1 \notin I, \\ \{i-1 \mid 1, s+1 \neq i \in I\} \cup \{r,s\} & \text{if } s+1 \in I. \end{cases}$$

If $s+1 \notin I$, the definition (5.5) of π implies that $I' = \pi(I) \smallsetminus \{s\}$, and we are done. For the rest of the proof we therefore assume that $s+1 \in I$.

If $1 \in J_{w_n}$, we have $1 \in I$ by Lemma 5.15. Since also $s+1 \in I$, the definition of π now implies that $I' = \pi(I)$, and again we are done. For the rest of the proof we therefore assume that $1 \notin J_{w_n}$.

Then $\mathrm{sgn}_1(w_n) = +1$ and hence $w_n = (u,v)$. Also, one of its entries is w_{n+1}, and the word representing it contains all ℓ occurrences of letters in $\{b_{s+1},\ldots,b_r\}$ that result from letters $b_{i_j} \in \{b_{s+1},\ldots,b_r\}$. In particular, the word representing w_{n+1} contains all occurrences of the letter b_r resulting from a letter $b_{i_j} = b_{s+1}$. Each such b_{i_j} contributes a letter b_s to the other entry of (u,v). Since the letter b_s does not arise in any other way from the recursion relations, it follows that the letter b_s does not occur in the word representing w_{n+1}. Therefore w_{n+1} is of type $I' \smallsetminus \{s\}$. But the definition (5.5) of π implies that $I' \smallsetminus \{s\} = \pi(I) \smallsetminus \{s\}$, so we are done. □

Next we fix a subset $I_0 \subset \{1,\ldots,r\}$ of minimal cardinality such that w_0 is of type I_0. For every $n \geqslant 0$ we set $I_n := \pi^n(I_0)$.

Lemma 5.19 *For every $n \geqslant 0$, the set $I_n \subset \{1,\ldots,r\}$ is a subset of minimal cardinality such that w_n is of type I_n.*

Proof. By induction on n, Lemma 5.18 implies that w_n is of type I_n for all $n \geqslant 0$. Suppose that for some $n \geqslant 0$ there exists a subset $I'_n \subset \{1,\ldots,r\}$ with $|I'_n| < |I_n|$ such that w_n is of type I'_n. Then again by Lemma 5.18, the element $w_{n'}$ is of type $\pi^{n'-n}(I'_n)$ for every $n' \geqslant n$. By Lemma 5.17 we can choose $n' \geqslant n$ such that $w_{n'} = w_0$. Then w_0 is of type $\pi^{n'-n}(I'_n)$ with $|\pi^{n'-n}(I'_n)| = |I'_n| < |I_n| = |I_0|$, contradicting the minimality of $|I_0|$. □

Lemma 5.20 *For any $n \geqslant 0$ we have $1 \in J_{w_n}$ if and only if $1 \in I_n$.*

Proof. The 'only if' part follows from Lemmas 5.15 and 5.19. For the 'if' part suppose that $1 \notin J_{w_n}$. Then w_{n+1} is of type $\pi(I_n) \smallsetminus \{s\}$ by Lemma 5.18. The minimality of $I_{n+1} = \pi(I_n)$ from Lemma 5.19 then implies that $\pi(I_n) \smallsetminus \{s\} = \pi(I_n)$. Thus $s \notin \pi(I_n)$, and hence $1 = \pi^{-1}(s) \notin I_n$, proving the converse. □

Lemma 5.21 *For any $n \geqslant 0$ with $1 \notin I_n$, the values x_i are equal for all $i \in I_n$, and w_n is equal to $(w_{n+1}, b_s^{\nu_n})$ or $(b_s^{\nu_n}, w_{n+1})$ for $\nu_n \in \mathbb{Z}$ such that $\mathrm{sgn}_{s+1}(w_n) = (-1)^{\nu_n}$.*

Proof. Assume that $1 \notin I_n$ and abbreviate $I_n^x := \{i \in I_n \mid x_i = x\}$ for all $x \in \{0,1\}$. Write $w_n = b_{i_1} \cdots b_{i_k}$ as a minimal word with all $i_j \in I_n$. Since $1 \notin I_n$, the recursion relations (5.1) show that all factors have the form

$$\begin{cases} (b_r, b_s) & \text{if } s+1 \in I_n^0, \\ (b_s, b_r) & \text{if } s+1 \in I_n^1, \\ (b_{i-1}, 1) & \text{for } i \in I_n^0 \smallsetminus \{s+1\}, \\ (1, b_{i-1}) & \text{for } i \in I_n^1 \smallsetminus \{s+1\}. \end{cases}$$

By Lemma 5.16 we have $w_n = (w_{n+1}, \delta)$ or (δ, w_{n+1}) for some $\delta \in \Delta$. Moreover, in the proof of Lemma 5.18 we have seen that the expansions in the above list yield a minimal word for w_{n+1}. Set $x := 0$ if $w_n = (w_{n+1}, \delta)$, and $x := 1$ otherwise. Then the above list implies that the resulting word for w_{n+1} is a product of certain b_j for $j \in \pi(I_n^x) \cup \{s\}$. But in the proof of Lemma 5.18 we have already seen that in this case all occurrences of b_s must go into δ. Thus w_{n+1} is of type $\pi(I_n^x)$.

Now the minimality in Lemma 5.19 implies that the inclusion $\pi(I_n^x) \subset \pi(I_n) = I_{n+1}$ is an equality. Thus $I_n^x = I_n$, proving the first assertion. Plugging this back into the above list now shows that the only non-trivial factors going into δ are the b_s arising from all $b_{i_j} = b_{s+1}$. Thus if ν_n denotes the number of factors $b_{i_j} = b_{s+1}$, we have $\delta = b_s^{\nu_n}$. But then Lemma 5.14 shows that $\mathrm{sgn}_{s+1}(w_n) = (-1)^{\nu_n}$, and we are done. □

Lemma 5.22 *For any $n \geqslant 0$ the element w_n is W-conjugate to*

$$\begin{array}{ll} (w_{n+1}, 1)\,\sigma & \textit{if } 1 \in J_{w_n}, \\ (w_{n+1}, b_s) & \textit{if } 1 \notin J_{w_n} \textit{ and } s+1 \in J_{w_n}, \\ (w_{n+1}, 1) & \textit{if } 1 \notin J_{w_n} \textit{ and } s+1 \notin J_{w_n}. \end{array}$$

Proof. If $1 \in J_{w_n}$, that is, if $\mathrm{sgn}_1(w_n) = -1$, this follows from Lemma 5.16. Otherwise we have $1 \notin I_n$ by Lemma 5.20, and so the remaining cases follow from Lemma 5.21. □

Lemma 5.23 *For every $n \geqslant 0$ we have:*

(a) For all $i \geqslant 2$ with $i \neq s+1$ we have $\mathrm{sgn}_i(w_n) = \mathrm{sgn}_{i-1}(w_{n+1})$.

(b) For all $1 \leqslant i \leqslant s$ we have $\mathrm{sgn}_i(w_n) = -1$ if and only if $i \in I_n$.

(c) For all $1 \leqslant i \leqslant r$ we have $\mathrm{sgn}_i(w_n) = \mathrm{sgn}_{\pi(i)}(w_{n+1})$.

(d) If $\mathrm{sgn}_1(w_n) = -1$, then $\mathrm{sgn}_{s+1}(w_n) = -1$.

Proof. For all $i \geqslant 2$ with $i \neq s+1$ we have $\mathrm{sgn}_i(\sigma) = 1$ and $\mathrm{sgn}_{i-1}(b_s) = 1$ by Lemma 5.14. Thus in each of the cases in Lemma 5.22, the conjugation invariance and the recursion relations for signs imply that $\mathrm{sgn}_i(w_n) = \mathrm{sgn}_{i-1}(w_{n+1})$, proving (a).

Next we prove (b) simultaneously for all n by induction on i. For $i = 1$ the assertion already holds by Lemma 5.20. If $i > 1$, by (a) we have $\mathrm{sgn}_i(w_n) = -1$ if and only if $\mathrm{sgn}_{i-1}(w_{n+1}) = -1$. By the induction hypothesis this is equivalent to $i-1 \in I_{n+1}$, in other words to $\pi(i) = i-1 \in I_{n+1} = \pi(I_n)$, and hence to $i \in I_n$, finishing the induction step.

Assertion (c) for $i \neq 1, s+1$ is the same as (a). For $i = 1$ by (b) we have $\mathrm{sgn}_1(w_n) = -1$ if and only if $1 \in I_n$ if and only if $s = \pi(1) \in \pi(I_n) = I_{n+1}$, which again by (b) is equivalent to $\mathrm{sgn}_{\pi(1)}(w_{n+1}) = -1$. This proves (c) for $i = 1$. For $i = s+1$ by the periodicity in Lemma 5.14 combined with (a) we have $\mathrm{sgn}_{s+1}(w_n) = \mathrm{sgn}_{r+1}(w_n) = \mathrm{sgn}_r(w_{n+1}) = \mathrm{sgn}_{\pi(s+1)}(w_{n+1})$. This proves (c) in all cases.

To show (d) we repeat the argument for (a) with $s+1$ in place of i. Again we have $\mathrm{sgn}_{s+1}(\sigma) = 1$, and since now $\mathrm{sgn}_1(w_n) = -1$, the first case of Lemma 5.22 implies that $\mathrm{sgn}_{s+1}(w_n) = \mathrm{sgn}_s(w_{n+1})$. By (c) this is equal to $\mathrm{sgn}_{\pi(1)}(w_{n+1}) = \mathrm{sgn}_1(w_n) = -1$, as desired. Thus everything is proved. $\square$

Lemma 5.24 *For every $n \geqslant 0$ we have $J_{w_n} = \pi^n(J_{w_0})$.*

Proof. This follows by induction from Lemma 5.23 (c). $\square$

Now consider the following conditions on a subset $J \subset \{1, \ldots, r\}$:

Conditions 5.25 *For all $n \geqslant 0$,*

(a) if $1 \in \pi^n(J)$, then $s+1 \in \pi^n(J)$.

(b) if $1 \notin \pi^n(J)$, then the values x_i are equal for all $i \in \pi^n(J)$.

Proposition 5.26 *For any Φ-irreducible $w \in \Gamma_{\underline{x}}$ the subset J_w satisfies Conditions 5.25.*

Proof. Apply the above with $w_0 := w$, and consider any $n \geqslant 0$. If $1 \in \pi^n(J_{w_0})$, by Lemma 5.24 we have $\mathrm{sgn}_1(w_n) = -1$. By Lemma 5.23 (d) this implies that $\mathrm{sgn}_{s+1}(w_n) = -1$ and therefore $s+1 \in \pi^n(J_{w_0})$, proving the condition 5.25 (a). By contrast, if $1 \notin \pi^n(J_{w_0})$, then $1 \notin I_n$ by Lemma 5.20. From Lemma 5.21 it then follows that the values x_i are equal for all $i \in I_n$. But Lemmas 5.24 and 5.15 together imply that $\pi^n(J_{w_0}) \subset I_n$, so in particular the values x_i are equal for all $i \in \pi^n(J_{w_0})$, proving the condition 5.25 (b). $\square$

Lemma 5.27 *Condition 5.25 (a) is equivalent to:*

(a′) For all $i \in J$ with $i \leqslant s$ and all $s < j \leqslant r$ with $i \equiv j \bmod (s, r-s)$ we have $j \in J$.

Proof. For any $n \geqslant 0$ we have $1 \in \pi^n(J)$ if and only if $\pi^{-n}(1) \in J$, and $\pi^{-n}(1)$ is the unique integer $1 \leqslant i \leqslant s$ with $i \equiv n+1 \bmod (s)$. Similarly, we have $s+1 \in \pi^n(J)$ if and only if $\pi^{-n}(s+1) \in J$, where $\pi^{-n}(s+1)$ is the unique integer $s < j \leqslant r$ with $j \equiv s+n+1 \bmod (r-s)$. Given i and j, the conditions on n just stated are $n+s+1 \equiv i \bmod (s)$ and $n+s+1 \equiv j \bmod (r-s)$, so they are satisfied for some n if and only if $i \equiv j \bmod (s, r-s)$. Now the equivalence follows. $\square$

5.5 Conjugacy classes of Φ-irreducible elements

Lemma 5.28 *Consider any distinct indices $i_1, \ldots, i_k \in \{1, \ldots, r\}$, in any order, and set $J := \{i_1, \ldots, i_k\}$. If $1 \in J$ assume that also $s+1 \in J$. Then $a_{i_1} \cdots a_{i_k}$ is W-conjugate to*

$$\begin{array}{ll} (a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1)\,\sigma & \textit{if } 1 \in J \textit{ and } s+1 \in J, \\ (a_{\pi(i_1)} \cdots a_{\pi(i_k)}, a_s) & \textit{if } 1 \notin J \textit{ and } s+1 \in J, \\ (a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1) & \textit{if } 1 \notin J \textit{ and } s+1 \notin J. \end{array}$$

Proof. If $1 \notin J$ and $s+1 \notin J$, the recursion relations (5.3) imply that

$$a_{i_1} \cdots a_{i_k} \;=\; (a_{i_1-1}, 1) \cdots (a_{i_k-1}, 1) \;=\; (a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1),$$

and the assertion follows. If $1 \notin J$ and $s+1 \in J$, let j be the unique index with $i_j = s+1$. Then the recursion relations (5.3) imply that

$$\begin{aligned} a_{i_1} \cdots a_{i_k} &= (a_{i_1-1}, 1) \cdots (a_{i_{j-1}-1}, 1) \cdot (a_r, a_s) \cdot (a_{i_{j+1}-1}, 1) \cdots (a_{i_k-1}, 1) \\ &= (a_{\pi(i_1)} \cdots a_{\pi(i_k)}, a_s), \end{aligned}$$

and again the assertion follows. So assume that $1 \in J$ and $s+1 \in J$, and let ℓ and j be the unique indices with $i_\ell = 1$ and $i_j = s+1$. If $\ell < j$, the recursion relations (5.3) imply that

$$\begin{aligned} a_{i_1} \cdots a_{i_k} &= (a_{i_1-1}, 1) \cdots (a_{i_{\ell-1}-1}, 1)\, \sigma\, (a_{i_{\ell+1}-1}, 1) \cdots (a_{i_{j-1}-1}, 1)\, (a_r, a_s)\, (a_{i_{j+1}-1}, 1) \cdots (a_{i_k-1}, 1) \\ &= \big(a_{\pi(i_1)} \cdots a_{\pi(i_{\ell-1})} a_s\,,\; a_{\pi(i_{\ell+1})} \cdots a_{\pi(i_{j-1})} a_r a_{\pi(i_{j+1})} \cdots a_{\pi(i_k)}\big)\, \sigma \\ &= \big(a_{\pi(i_1)} \cdots a_{\pi(i_\ell)}\,,\; a_{\pi(i_{\ell+1})} \cdots a_{\pi(i_k)}\big)\, \sigma \end{aligned}$$

which is conjugate to $(a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1)\, \sigma$, as desired. If $\ell > j$, the same kind of calculation yields

$$\begin{aligned} a_{i_1} \cdots a_{i_k} &= (a_{i_1-1}, 1) \cdots (a_{i_{j-1}-1}, 1)\, (a_r, a_s)\, (a_{i_{j+1}-1}, 1) \cdots (a_{i_{\ell-1}-1}, 1)\, \sigma\, (a_{i_{\ell+1}-1}, 1) \cdots (a_{i_k-1}, 1) \\ &= \big(a_{\pi(i_1)} \cdots a_{\pi(i_{j-1})} a_r a_{\pi(i_{j+1})} \cdots a_{\pi(i_{\ell-1})}\,,\; a_s a_{\pi(i_{\ell+1})} \cdots a_{\pi(i_k)}\big)\, \sigma \\ &= \big(a_{\pi(i_1)} \cdots a_{\pi(i_{\ell-1})}\,,\; a_{\pi(i_\ell)} \cdots a_{\pi(i_k)}\big)\, \sigma \end{aligned}$$

which is again conjugate to $(a_{\pi(i_1)} \cdots a_{\pi(i_k)}, 1)\, \sigma$, as desired. $\square$

Lemma 5.29 *For each $1 \leqslant i \leqslant r$ the element b_i is conjugate to a_i under W.*

Proof. Let $a'_1, \ldots, a'_r$ denote the generators used in [5, §3]. Then the recursion relations (5.1) and the equivalence (a)⇔(b) of [5, Thm. 3.4.1] imply that each b_i is individually conjugate to a'_i under W. Since the elements $a_1, \ldots, a_r$ are a special case of the elements $b_1, \ldots, b_r$, it follows that each b_i is individually conjugate to a_i under W. $\square$

Proposition 5.30 *Consider any Φ-irreducible element $w \in \Gamma_{\underline{x}}$. Let $i_1, \ldots, i_k$ be the distinct elements of J_w in any order. Then w is conjugate to $a_{i_1} \cdots a_{i_k}$ under W.*

Proof. By [5, Lemma 1.3.3] it suffices to show that the restrictions $w|_{T_n}$ and $a_{i_1} \cdots a_{i_k}|_{T_n}$ are conjugate in the automorphism group of T_n for every $n \geqslant 0$. We will achieve this by induction on n. For $n = 0$ the assertion is trivially true, so assume that $n > 0$ and that the assertion is universally true for the restrictions to T_{n-1}.

We apply the above constructions to $w_0 := w$. Then from Lemma 5.24 we know that $\pi(i_1), \ldots, \pi(i_k)$ are the distinct elements of J_{w_1}. By the induction hypothesis the restriction $w_1|_{T_{n-1}}$ is therefore conjugate to $a_{\pi(i_1)} \cdots a_{\pi(i_k)}|_{T_{n-1}}$ under the automorphism group of T_{n-1}. Since J_{w_0} satisfies Condition 5.25 (a), by Lemma 5.28 it follows that $a_{i_1}\cdots a_{i_k}|_{T_n}$ is conjugate to

$$\begin{array}{ll} (w_1,1)\,\sigma|_{T_n} & \text{if } 1\in J_{w_0}, \\ (w_1,a_s)|_{T_n} & \text{if } 1\notin J_{w_0} \text{ and } s+1\in J_{w_0}, \\ (w_1,1)|_{T_n} & \text{if } 1\notin J_{w_0} \text{ and } s+1\notin J_{w_0}, \end{array}$$

under the automorphism group of T_n. Moreover, by Lemma 5.29 the element b_s is conjugate to a_s under W. Comparing the above cases with the respective cases in Lemma 5.28 thus implies that $w_0|T_n$ is conjugate to $a_{i_1}\cdots a_{i_k}|_{T_n}$ under the automorphism group of T_n. This finishes the induction step and thereby the proof. □

Proposition 5.31 *For any subset $J\subset\{1,\ldots,r\}$ satisfying Conditions 5.25 there exists a Φ-irreducible element $w\in\Gamma_{\underline{x}}$ with $J=J_w$.*

Proof. Consider any integer $n\geqslant 0$. For the purpose of this proof we call any element of $\Gamma_{\underline{x}}$ of the form $b_{i_1}\cdots b_{i_k}$, where $i_1,\ldots,i_k$ are the distinct elements of $\pi^n(J)$ in any order, *strictly of type* $\pi^n(J)$. (This is actually a minimal word; hence the element is of type $\pi^n(J)$ in the sense of Definition 5.12, but we will not use that fact.) We claim that any element that is strictly of type $\pi^n(J)$ possesses a first descendant which is strictly of type $\pi^{n+1}(J)$.

Granting this, by induction on n it follows that for any $n\geqslant 1$, any element that is strictly of type J possesses a descendant which is strictly of type $\pi^n(J)$. Since π is a permutation of finite order, we deduce that any element that is strictly of type J possesses a descendant which is again strictly of type J. As there are only finitely many elements that are strictly of type J, and being a descendant is a transitive relation, it follows that some element w that is strictly of type J must be its own descendant. This element is therefore Φ-irreducible. Finally, writing $w=b_{i_1}\cdots b_{i_k}$ where $i_1,\ldots,i_k$ are the distinct elements of J, Lemma 5.14 implies that $J=J_w$, as desired.

To prove the claim consider $w:=b_{i_1}\cdots b_{i_k}$ where $i_1,\ldots,i_k$ are the distinct elements of $\pi^n(J)$. Suppose first that $1\notin\pi^n(J)$. Then by Condition 5.25 (b) the values x_i are equal for all $i\in\pi^n(J)$. If this common value is 0, the same calculations as in the proof of Lemma 5.28 show that w is equal to $(b_{\pi(i_1)}\cdots b_{\pi(i_k)},1)$ or $(b_{\pi(i_1)}\cdots b_{\pi(i_k)},b_s)$. If the common value is 1, then w is equal to $(1,b_{\pi(i_1)}\cdots b_{\pi(i_k)})$ or $(b_s,b_{\pi(i_1)}\cdots b_{\pi(i_k)})$. In all these cases w has the first descendant $b_{\pi(i_1)}\cdots b_{\pi(i_k)}$, which is strictly of type $\pi^{n+1}(J)$.

Suppose now that $1\in\pi^n(J)$. Then $\mathrm{sgn}_1(w)=-1$ by Lemma 5.14; hence w has the form $w=(u,v)\,\sigma$. By Condition 5.25 (a) we now also have $s+1\in\pi^n(J)$. By the recursion relations (5.1), any factor $b_{i_j}\neq b_1,b_{s+1}$ of $w=b_{i_1}\cdots b_{i_k}$ contributes precisely one factor $b_{i_j-1}=b_{\pi(i_j)}$ to the product uv. The factor $b_{i_j}=b_{s+1}$ contributes the factors $b_r=b_{\pi(s+1)}$ and $b_s=b_{\pi(1)}$, and the factor $b_{i_j}=b_1$ contributes nothing. Together this shows that uv is a product of the elements $b_{\pi(i_1)},\ldots,b_{\pi(i_k)}$ in some order. It is therefore strictly of type $\pi^{n+1}(J)$, as desired. □

Proposition 5.32 *Any Φ-irreducible element w of $\Gamma_{\underline{x}}$ is W-conjugate to a Φ-irreducible element of $\Gamma_{(0,\ldots,0)}$.*

Proof. By Proposition 5.30 it is conjugate to $a_{i_1} \cdots a_{i_k} \in \Gamma_{(0,\ldots,0)}$, where $i_1, \ldots, i_k$ are the distinct elements of J_w in any order. But the same argument as in the proof of Proposition 5.31 shows that for some order, the element $a_{i_1} \cdots a_{i_k}$ is Φ-irreducible. $\square$

5.6 Some rational functions and their denominators

To any subset $J \subset \{1, \ldots, r\}$ we associate the following power series. For all $m \geqslant 0$ let ℓ_m denote the number of integers $0 \leqslant i < m$ such that $1 \in \pi^i(J)$. Set

$$\Psi_J := \sum_{\substack{m \geqslant 0 \\ 1 \in \pi^m(J)}} X^{\ell_m} Y^{m+1} + \sum_{\substack{m \geqslant 0 \\ 1 \notin \pi^m(J) \ni s+1}} X^{\ell_m} Y^{m+s+1}, \qquad \text{and} \tag{5.33}$$

$$\Phi_J := \frac{1}{1-2Y} + \frac{X-2}{1-2Y} \cdot \Psi_J. \tag{5.34}$$

Abbreviate $p := \gcd(s, r-s)$ and $q := \frac{r-s}{p}$.

Lemma 5.35 *Both Ψ_J and Φ_J are rational functions. More precisely, with $\ell := \big|\{i \in J \mid i \leqslant s\}\big|$ we have*

$$(1 - X^{\ell q} Y^{sq}) \cdot \Psi_J \in \mathbb{Z}[X, Y].$$

Proof. Since π permutes the letters $1, \ldots, s$ transitively, the condition $1 \in \pi^m(J)$ depends only on m mod s, and we have $\ell_{m+s} = \ell_m + \ell$ for all $m \geqslant 0$. Also, since π permutes the letters $s+1, \ldots, r$ transitively, the condition $s+1 \in \pi^m(J)$ depends only on m mod $(r-s)$. The definition of p and q implies that $sq = \operatorname{lcm}(s, r-s)$. Thus in both sums in (5.33), the terms with $m + sq$ in place of m are obtained on multiplying the terms for m by $X^{\ell q} Y^{sq}$. Therefore $(1 - X^{\ell q} Y^{sq}) \cdot \Psi_J \in \mathbb{Z}[X, Y]$, and Ψ_J is rational. By (5.34) so is Φ_J. $\square$

For any $0 \leqslant \ell \leqslant s$ we define:

$$D_\ell := \left[\begin{array}{l} \text{lowest common denominator of the } \Psi_J \text{ for all } J \text{ with} \\ \ell = \big|\{i \in J \mid i \leqslant s\}\big| \text{ satisfying Condition 5.25 (a).} \end{array} \right] \tag{5.36}$$

Lemma 5.37 *We have $D_0 = 1 - Y^{pq}$.*

Proof. Consider any subset $J \subset \{s+1, \ldots, r\}$. Then J trivially satisfies Condition 5.25 (a). Also, for all $m \geqslant 0$ we have $1 \notin \pi^m(J)$ and $\ell_m = 0$. Thus the first sum in (5.33) is zero and second is the sum of Y^{m+s+1} for all $m \geqslant 0$ with $s+1 \in \pi^m(J)$. Since the condition $s+1 \in \pi^m(J)$ depends only on m mod $(r-s)$, we deduce that

$$(1 - Y^{r-s}) \cdot \Psi_J = \sum_{\substack{0 \leqslant m < r-s \\ s+1 \in \pi^m(J)}} Y^{m+s+1}.$$

Moreover, for any $0 \leqslant m < r-s$ we have $s+1 \in \pi^m(J)$ if and only if $m+s+1 = \pi^{-m}(s+1)$ lies in J. Therefore

$$(1 - Y^{r-s}) \cdot \Psi_J \ = \sum_{s<j\in J} Y^j.$$

In particular the denominator of Ψ_J divides $(1-Y^{r-s})$. Conversely, in the case $J = \{r\}$ we obtain $(1-Y^{r-s})\cdot\Psi_{\{r\}} = Y^r$. Thus the lowest common denominator is $1-Y^{r-s} = 1-Y^{pq}$, as desired. □

Lemma 5.38 *We have $D_s = 1 - XY$.*

Proof. From Lemma 5.27 we see that the only subset $J \subset \{1,\ldots,r\}$ containing $\{1,\ldots,s\}$ which satisfies Condition 5.25 (a) is $\{1,\ldots,r\}$ itself. For it we have $1 \in \pi^m(J)$ and $\ell_m = m$ for all $m \geqslant 0$. By (5.33) this implies that $\Psi_J = \sum_{m\geqslant 0} X^m Y^{m+1} = Y/(1-XY)$, whose denominator is $1 - XY$, as desired. □

Lemma 5.39 *For any $0 < \ell < s$, the lowest common denominator of the Ψ_J for all subsets $J \subset \{1,\ldots,r\}$ satisfying $\ell = \big|\{i \in J \mid i \leqslant s\}\big|$ and $\{s+1,\ldots,r\} \subset J$ is $1 - X^\ell Y^s$.*

Proof. For any such J we have $s+1 \in \pi^m(J)$ for all $m \geqslant 0$. Thus in both sums in (5.33), the terms with $m+s$ in place of m are obtained on multiplying the terms for m by $X^\ell Y^s$. Therefore

$$(1 - X^\ell Y^s)\Psi_J \ = \sum_{\substack{0\leqslant m<s\\ 1\in\pi^m(J)}} X^{\ell_m}Y^{m+1} \ + \sum_{\substack{0\leqslant m<s\\ 1\notin\pi^m(J)}} X^{\ell_m}Y^{m+s+1}.$$

Thus the lowest common denominator divides $(1 - X^\ell Y^s)$.

For the converse note first that for all $0 \leqslant m < s$ we have $1 \notin \pi^m(J)$ if and only if $m+1 = \pi^{-m}(1) \in J$. Thus for all $0 \leqslant m < s$ we have $\ell_m = |\{i \in J \mid i \leqslant m\}$. Now consider the subsets

$$\begin{aligned} J \ &:= \ \{2,3,\ldots,\ell+1,s+1,\ldots,r\}, \\ J' \ &:= \ \{1,3,\ldots,\ell+1,s+1,\ldots,r\}, \end{aligned}$$

both of which satisfy the given conditions. The preceding remarks show that in the range $0 \leqslant m < s$, the values of ℓ_m associated to J and J' differ only for $m = 1$. Thus the summands for all $m > 1$ in both sums above are the same for J and J', and the others yield

$$(1 - X^\ell Y^s)(\Psi_J - \Psi_{J'}) \ = \ (Y^2 + Y^{s+1}) - (Y + XY^{s+2}).$$

As the right hand side is coprime to $(1 - X^\ell Y^s)$, the lemma follows. □

Lemma 5.40 *For any $s - \frac{s}{p} < \ell < s$ we have $D_\ell = 1 - X^\ell Y^s$.*

Proof. Since p divides s, any residue class modulo p contains precisely $\frac{s}{p}$ elements from $\{1, \ldots, s\}$. Thus if $\{i \in J \mid i \leqslant s\}$ has cardinality $\ell > s - \frac{s}{p}$, it must meet every residue class modulo p. If in addition J satisfies Condition 5.25 (a), then Lemma 5.27 implies that $\{s+1, \ldots, r\} \subset J$. Conversely, any subset $J \subset \{1, \ldots, r\}$ with $\ell = \big|\{i \in J \mid i \leqslant s\}\big|$ and $\{s+1, \ldots, r\} \subset J$ trivially satisfies Condition 5.25 (a). The lemma therefore reduces to Lemma 5.39. $\square$

Lemma 5.41 *Consider any subset* $J \subset \{1, \ldots, r\}$ *with* $\ell = \big|\{i \in J \mid i \leqslant s\}\big|$ *that satisfies Condition 5.25 (a). Then* $\bar{J} := J \cup \{s+1, \ldots, r\}$ *has the same properties and*

$$\Psi_{\bar{J}} - \Psi_J \;=\; \sum_{\substack{m \geqslant 0 \\ s+1 \in \pi^m(\bar{J} \smallsetminus J)}} X^{\ell_m} Y^{m+s+1}.$$

Proof. The statement about $\bar{J}$ follows from the form of Condition 5.25 (a). Next, the condition $1 \in \pi^m(J)$ and the exponent ℓ_m in (5.33) is the same for J as for $\bar{J}$. Thus the difference $\Psi_{\bar{J}} - \Psi_J$ comes only from the terms of the second sum in (5.33) with $1 \notin \pi^m(J)$ and $s{+}1 \in \pi^m(\bar{J} \smallsetminus J)$. But since J satisfies Condition 5.25 (a), any m with $s{+}1 \in \pi^m(\bar{J} \smallsetminus J)$ already satisfies $1 \notin \pi^m(J)$. Thus the indicated formula follows. $\square$

Lemma 5.42 *For any* $0 < \ell < s - \frac{s}{p}$ *we have* $D_\ell = 1 - X^{\ell q} Y^{sq}$.

Proof. Lemma 5.35 already shows that the lowest common denominator D_ℓ divides $1 - X^{\ell q} Y^{sq}$. For the converse we apply Lemma 5.41 to the case that $J \cap \{s+1, \ldots, r\} = \{s+2, \ldots, r\}$. Then the condition $s+1 \in \pi^m(\bar{J} \smallsetminus J) = \{\pi^m(s+1)\}$ is equivalent to $r - s = pq \mid m$. Moreover, as in the proof of Lemma 5.35, the terms of the sum with $m + sq$ in place of m are obtained on multiplying the terms for m by $X^{\ell q} Y^{sq}$. Therefore

$$(1 - X^{\ell q} Y^{sq}) \cdot (\Psi_{\bar{J}} - \Psi_J) \;=\; \sum_{\substack{0 \leqslant m < sq \\ pq \mid m}} X^{\ell_m} Y^{m+s+1}.$$

Thus it suffices to show that some linear combination of this for all possible J is coprime to $1 - X^{\ell q} Y^{sq}$. In fact, the difference for two suitable choices of J will do.

Recall that $p = \gcd(s, r-s)$, so that $s - \frac{s}{p}$ is the cardinality of $\{1 \leqslant i \leqslant s : p \nmid i\}$. Also note that the assumption $0 < \ell < s - \frac{s}{p}$ implies that $p = \gcd(s, r-s) > 1$. Thus we can choose a subset A of $\{1 \leqslant i \leqslant s : p \nmid i\}$ of cardinality ℓ such that $1 \notin A$ and $p+1 \in A$. Then $A' := \{1\} \cup A \smallsetminus \{p+1\}$ is another subset of $\{1 \leqslant i \leqslant s : p \nmid i\}$ of cardinality ℓ. With these choices we set $J := A \cup \{s+2, \ldots, r\}$ and $J' := A' \cup \{s+2, \ldots, r\}$. Then in view of Lemma 5.27, both J and J' satisfy the stated conditions.

Next recall that the exponent ℓ_m for J was defined as $\ell_m := |\{0 \leqslant i < m \mid 1 \in \pi^i(J)\}|$. Define accordingly $\ell'_m := |\{0 \leqslant i < m \mid 1 \in \pi^i(J')\}|$. Since π induces a permutation of order s on $\{1, \ldots, s\}$, these numbers satisfy $\ell_{m+s} = \ell_m + \ell$ and $\ell'_{m+s} = \ell'_m + \ell$. Thus the difference $\ell'_m - \ell_m$ depends only on m mod (s).

Recall also that for all $0 \leqslant m < s$ we have $\ell_m = |\{i \in J \mid i \leqslant m\}$, and similarly $\ell'_m = |\{i \in J' \mid i \leqslant m\}|$. The construction of J and J' thus implies that these values are equal unless $1 \leqslant m \leqslant p$, in which case $\ell'_m = \ell_m + 1$.

Returning now to the above sum, consider any integer $0 \leqslant m < sq$ with $pq|m$. Write $m = np + ks$ with $0 \leqslant np < s$. Then the preceding remarks imply that $\ell'_m - \ell_m = \ell'_{np} - \ell_{np}$ is 0 unless $n = 1$, in which case it is 1. The latter case occurs if and only if $m \equiv p \bmod (s)$. But by the definition of p, the integers $\frac{s}{p}$ and $\frac{r-s}{p} = q$ are relatively prime. Thus there is precisely one integer $0 \leqslant m < sq$ with $pq|m$ and $m \equiv p \bmod (s)$. For this m we then have

$$(1 - X^{\ell q}Y^{sq}) \cdot (\Psi_{J\cup\{s+1\}} - \Psi_J - \Psi_{J'\cup\{s+1\}} + \Psi_{J'}) \;=\; X^{\ell_m}(1-X)Y^{m+s+1}.$$

As the right hand side is coprime to $(1 - X^{\ell q}Y^{sq})$, the lemma follows. □

Lemma 5.43 *For $\ell = s - \frac{s}{p} > 0$ we have*

$$D_\ell \;=\; \frac{(1 - X^\ell Y^s)(1 - X^{pq-q}Y^{pq})}{(1 - X^{p-1}Y^p)}.$$

Proof. Consider any subset $J \subset \{1, \ldots, r\}$ with $\ell = \big|\{i \in J \mid i \leqslant s\}\big|$ that satisfies Condition 5.25 (a). Set $\bar{J} := J \cup \{s+1, \ldots, r\}$, which again has the stated properties. Then by Lemma 5.39 the lowest common denominator of $\Psi_{\bar{J}}$ for all possible J is $1 - X^\ell Y^s$.

Suppose in addition that $J \neq \bar{J}$, and choose an element $j_0 \in \bar{J} \smallsetminus J$. Then Lemma 5.27 implies that

$$\{i \in J \mid i \leqslant s\} \;\subset\; \{1 \leqslant i \leqslant s \mid i \not\equiv j_0 \bmod (p)\}.$$

Since p divides s, the set on the right hand side has cardinality $s - \frac{s}{p} = \ell$, same as the set on the left hand side. Thus the inclusion is an equality, and so

$$\{1 \leqslant i \leqslant r \mid i \not\equiv j_0 \bmod (p)\} \;\subset\; J \;\subset\; \{1 \leqslant i \leqslant r \mid i \not\equiv j_0 \bmod (p) \;\vee\; i > s\}. \tag{5.44}$$

In particular this implies that $\ell_{m+p} = \ell_m + p - 1$ for all $m \geqslant 0$. Moreover, the condition $s + 1 \in \pi^m(\bar{J} \smallsetminus J)$ depends only on $m \bmod (r - s)$ with $r - s = pq$. It follows that in the sum in Lemma 5.41, the terms with $m + pq$ in place of m are obtained on multiplying the terms for m by $X^{pq-p}Y^{pq}$. Therefore

$$(1 - X^{pq-q}Y^{pq}) \cdot (\Psi_{\bar{J}} - \Psi_J) \;=\; \sum_{\substack{0 \leqslant m < pq \\ s+1 \in \pi^m(\bar{J} \smallsetminus J)}} X^{\ell_m}Y^{m+s+1}. \tag{5.45}$$

In particular, the denominator of $\Psi_{\bar{J}} - \Psi_J$ divides $1 - X^{pq-q}Y^{pq}$.

Conversely, the subset $J := \{1 \leqslant i \leqslant r \mid i \not\equiv 1 \bmod (p) \;\vee\; i > s+1\}$ satisfies (5.44) with $j_0 := s + 1$. For it we have $\bar{J} \smallsetminus J = \{s+1\}$, and so the conditions $0 \leqslant m < pq$ and $s + 1 \in \pi^m(\bar{J} \smallsetminus J)$ in (5.45) are satisfied only for $m = 0$. The right hand side of (5.45) is therefore equal to Y^{s+1} in this case. Together it follows that the lowest common denominator of $\Psi_{\bar{J}} - \Psi_J$ for all possible J is $1 - X^{pq-q}Y^{pq}$.

Combining everything, we deduce that D_ℓ is the least common multiple of $1 - X^\ell Y^s$ and $1 - X^{pq-q}Y^{pq}$. But since $\ell = (p-1)\frac{s}{p}$ and, by the definition of p, the integers $\frac{s}{p}$ and q are relatively prime, the greatest common divisor of $1 - X^\ell Y^s$ and $1 - X^{pq-q}Y^{pq}$ is $1 - X^{p-1}Y^p$. Thus the least common multiple has the indicated form. $\square$

Combining the preceding lemmas, we obtain:

Proposition 5.46 *For any $0 \leqslant \ell \leqslant s$ we have*

$$D_\ell = \begin{cases} (1 - Y^{pq}) & \textit{if } \ell = 0, \\ (1 - X^{\ell q}Y^{sq}) & \textit{if } 0 < \ell < s - \frac{s}{p}, \\ \dfrac{(1 - X^\ell Y^s)(1 - X^{pq-q}Y^{pq})}{(1 - X^{p-1}Y^p)} & \textit{if } \ell = s - \frac{s}{p} > 0, \\ (1 - X^\ell Y^s) & \textit{if } s - \frac{s}{p} < \ell < s, \\ (1 - XY) & \textit{if } \ell = s. \end{cases}$$

5.7 Denominators of orbit length generating functions

Lemma 5.47 *For all $1 \leqslant i \leqslant r$ we have*

$$\Psi_{b_i} = \begin{cases} Y^i & \textit{if } i \leqslant s, \\ \dfrac{Y^i}{1 - Y^{r-s}} & \textit{if } i > s. \end{cases}$$

Proof. By the recursion relations (5.1) and Proposition 2.14, and the fact that $\Psi_1 = 0$ by (2.15), we have

$$\Psi_{b_i} = \begin{cases} Y & \text{if } i = 1, \\ Y\Psi_{b_r} + Y\Psi_{b_s} & \text{if } i = s+1, \\ Y\Psi_{b_{i-1}} & \text{otherwise.} \end{cases}$$

By induction on i this implies that $\Psi_{b_i} = Y^i$ for all $1 \leqslant i \leqslant s$. Induction also shows that $\Psi_{b_i} = Y^{i-s-1}\Psi_{b_{s+1}}$ for all $s < i \leqslant r$. Therefore $\Psi_{b_{s+1}} = Y\Psi_{b_r} + Y\Psi_{b_s} = Y^{r-s}\Psi_{b_{s+1}} + Y^{s+1}$ and hence $\Psi_{b_{s+1}} = Y^{s+1}/(1 - Y^{r-s})$. This in turn implies that $\Psi_{b_i} = Y^i/(1 - Y^{r-s})$ for all $s < i \leqslant r$, and we are done. $\square$

Proposition 5.48 *For any Φ-irreducible element $w \in \Gamma_{\underline{x}}$ we have $\Phi_w = \Phi_{J_w}$.*

Proof. We apply the constructions of Subsection 5.4 to $w_0 := w$. Combining Lemma 5.22 for all $n \geqslant 0$ with Proposition 2.14 and the conjugation invariance of orbit length generating functions yields

$$\Psi_{w_n} = \begin{cases} Y + XY\Psi_{w_{n+1}} & \text{if } 1 \in J_{w_n}, \\ Y\Psi_{b_s} + Y\Psi_{w_{n+1}} & \text{if } 1 \notin J_{w_n} \text{ and } s+1 \in J_{w_n}, \\ Y\Psi_1 + Y\Psi_{w_{n+1}} & \text{if } 1 \notin J_{w_n} \text{ and } s+1 \notin J_{w_n}. \end{cases}$$

Here $\Psi_1 = 0$ by (2.15), and $\Psi_{b_s} = Y^s$ by Lemma 5.47. Moreover, by Lemma 5.24 we have $J_{w_n} = \pi^n(J_{w_0})$ for all $n \geqslant 0$. As in (5.33) let ℓ_m denote the number of integers $0 \leqslant \ell < m$ such that $1 \in \pi^\ell(J_{w_0})$. Then by induction on n it follows that

$$\Psi_{w_0} \;=\; \sum_{\substack{0\leqslant m<n \\ 1\in\pi^m(J_{w_0})}} X^{\ell_m}Y^{m+1} \;+\; \sum_{\substack{0\leqslant m<n \\ 1\notin\pi^m(J_{w_0})\ni s+1}} X^{\ell_m}Y^{m+s+1} \;+\; X^{\ell_n}Y^n\Psi_{w_n}$$

In the limit over n this implies that $\Psi_{w_0} = \Psi_{J_{w_0}}$. Using (5.34) and Proposition 2.13 we deduce that $\Phi_{w_0} = \Phi_{J_{w_0}}$, as desired. □

For any $0 \leqslant \ell \leqslant s$ we now define

$$(5.49) \qquad D_{\underline{x},\ell} \;:=\; \left[\begin{array}{l} \text{lowest common denominator of the } \Psi_J \text{ for all } J \text{ with} \\ \ell = \big|\{i \in J \mid i \leqslant s\}\big| \text{ satisfying Conditions 5.25.} \end{array}\right]$$

By construction this is a divisor of the polynomial D_ℓ from (5.36) and Proposition 5.46.

Theorem 5.50 *The power series $\Phi_w \in 1+Y\mathbb{Z}[[X,Y]]$ for all $w \in \Gamma_{\underline{x}}$ are rational functions with the lowest common denominator*

$$D_{\underline{x}} \;:=\; (1-2Y) \cdot \prod_{0\leqslant\ell\leqslant s} D_{\underline{x},\ell} \;\in\; 1+Y\mathbb{Z}[X,Y].$$

Proof. By Proposition 5.11 and Theorem 2.8 the Φ_w for all $w \in \Gamma_{\underline{x}}$ are $\mathbb{Z}[X,Y]$-linear combinations of the Φ_w for all Φ-irreducible elements. By Propositions 5.26 and 5.31 and 5.48 the latter are precisely the Φ_J for all subsets $J \subset \{1,\ldots,r\}$ which satisfy Conditions 5.25. They are therefore rational functions, and in view of (5.34) and (5.49) their lowest common denominator is the least common multiple of the polynomials $(1-2Y)D_{\underline{x},\ell}$ for all ℓ.

Lemma 5.35 shows that each $D_{\underline{x},\ell}$ divides $1-X^{\ell q}Y^{sq}$. Thus $D_{\underline{x},\ell}$ can be chosen congruent to $1 \bmod Y$, and then $D_{\underline{x}}$ has the same property. Moreover, the polynomials $1-2Y$ and $1-X^{\ell q}Y^{sq}$ for all $0 \leqslant \ell \leqslant s$ are pairwise coprime, for instance because, viewed as polynomials in Y, their zeros in an algebraic closure of $\mathbb{Q}(X)$ are mutually distinct. Thus the least common multiple of all $(1-2Y)D_{\underline{x},\ell}$ is $D_{\underline{x}}$, and we are done. □

Proposition 5.51 *(a) For all $\underline{x}$ we have $D_{\underline{x},0} = D_0 = 1-Y^{pq}$ and $D_{\underline{x},s} = D_s = 1-XY$.*

(b) For $\underline{x} = (0,\ldots,0)$ or $(1,\ldots,1)$ we have $D_{\underline{x},\ell} = D_\ell$ for all ℓ.

Proof. The first statement in (a) is a consequence of Lemmas 5.37 and 5.47. The second statement in (a) results from Lemma 5.38 and the fact that $J := \{1,\ldots,r\}$ always satisfies Conditions 5.25. Assertion (b) is a consequence of the fact that for $\underline{x} = (0,\ldots,0)$ or $(1,\ldots,1)$ Condition 5.25 (b) is satisfied for all J. □

In principle, the determination of the lowest common denominator $D_{\underline{x}}$ in Theorem 5.50 is a finite combinatorial problem concerning the data r, s, and $\underline{x}$. The author does not (yet) know a simple direct description in general. However, we determined $D_{\underline{x}}$ in small cases using the computer algebra system Maple: see [6]. The outcome was that whenever $r \leqslant 8$ and $x_2, \dots, x_r$ are not all equal, then $\prod_{0<\ell<s} D_{\underline{x},\ell} = 1$ except in the following cases:

(r,s)	$\prod_{0<\ell<s} D_{\underline{x},\ell}$	Conditions on $\underline{x} = (x_2, \dots, x_r)$
$(4,2)$	$(1{-}XY^2)$	$x_2 = x_4$
$(5,4)$	$(1{-}XY^2)$	$x_2 = x_4 = x_5 \neq x_3$
$(6,2)$	$(1{-}XY^2)$	$x_2 = x_4 = x_6$ but not all x_i equal
$(6,3)$	$(1{-}XY^3)(1{-}X^2Y^3)$	$x_2 = x_3 = x_5 = x_6$
$(6,3)$	$(1{-}XY^3)$	$x_2 = x_5 \neq x_3 = x_6$
$(6,4)$	$(1{-}XY^4)(1{-}XY^2)$	$x_2 = x_4 = x_6 \neq x_3 = x_5$
$(6,4)$	$(1{-}XY^2)$	$x_2 = x_4 = x_6 \ \wedge \ x_3 \neq x_5$
$(7,4)$	$(1{-}XY^2)$	$x_2 = x_4 = x_5 = x_6 = x_7 \neq x_3$
$(7,6)$	$(1{-}XY^3)(1{-}X^2Y^3)$	$x_2 = x_3 = x_5 = x_6 = x_7 \neq x_4$
$(7,6)$	$(1{-}XY^2)$	$x_2 = x_4 = x_6 = x_7$ but not all x_i equal
$(8,2)$	$(1{-}XY^2)$	$x_2 = x_4 = x_6 = x_8$ but not all x_i equal
$(8,4)$	$(1{-}XY^4)(1{-}X^2Y^4)(1{-}X^3Y^4)$	$x_2 = x_3 = x_4 = x_6 = x_7 = x_8$
$(8,4)$	$(1{-}XY^4)(1{-}XY^2)$	$x_2 = x_4 = x_6 = x_8 \neq x_3 = x_7$
$(8,4)$	$(1{-}X^2Y^4)$	$x_2 = x_4 = x_5 = x_6 = x_7 = x_8 \neq x_3$
$(8,4)$	$(1{-}XY^4)$	$x_2 = x_6 \neq x_4 = x_8 \ \wedge \ x_3 = x_7$
$(8,4)$	$(1{-}XY^2)$	$x_2 = x_4 = x_6 = x_8 \ \wedge \ x_3 \neq x_7 \wedge (x_5, x_7) \neq (0,0)$
$(8,6)$	$(1{-}XY^6)(1{-}X^2Y^6)(1{-}XY^2)$	$x_2 = x_4 = x_6 = x_8 \neq x_3 = x_5 = x_7$
$(8,6)$	$(1{-}XY^3)(1{-}X^2Y^3)$	$x_2 = x_3 = x_5 = x_6 = x_7 = x_8 \neq x_4$
$(8,6)$	$(1{-}XY^2)$	$x_2 = x_4 = x_6 = x_8$ but x_3, x_5, x_7 not all equal

References

[1] Bartholdi, L., Nekrashevych, V.: Iterated monodromy groups of quadratic polynomials. I. *Groups Geom. Dyn.* **2** (2008), no. 3, 309–336.

[2] Bartholdi, L., Siegenthaler, O.: The twisted twin of the Grigorchuk group *Internat. J. Algebra Comput.* **20** (2010), no. 4, 465–488.

[3] Jones, R., Boston, N.: Settled polynomials over finite fields. *Proc. Amer. Math. Soc.* **140** (2012), no. 6, 1849–1863.

[4] Nekrashevych, V.: *Self-similar groups.* Mathematical Surveys and Monographs, 117. American Mathematical Society, Providence, RI, 2005.

[5] Pink, R.: *Profinite iterated monodromy groups arising from quadratic polynomials.* Preprint (version 3, September 2013), 85p. `arXiv:1307.5678 [math.GR]`

[6] Pink, R.: Computer algebra calculations for orbit length generating functions: `www.math.ethz.ch/~pink/ftp/OLGFs`