Proceedings of the Edinburgh Mathematical Society (2022) **65**, 1080–1132
doi:10.1017/S0013091522000505

RATIONAL GROWTH IN TORUS BUNDLE GROUPS OF ODD TRACE

SEONGJUN CHOI[1], MENG-CHE "TURBO" HO[2] AND MARK PENGITORE[3]

[1] *Purdue University, West Lafayette, IN 47907, USA* (sjchoi235@gmail.com)
[2] *California State University Northridge, Northridge, CA 91330, USA* (turboho@gmail.com)
[3] *University of Virginia, Charlottesville, VA 22903, USA* (waj9cr@virginia.edu)

(Received 6 October 2021; first published online 6 December 2022)

Abstract A group is said to have rational growth with respect to a generating set if the growth series is a rational function. It was shown by Parry that certain torus bundle groups of even trace exhibits rational growth. We generalize this result to a class of torus bundle groups with odd trace.

Keywords: solvable groups; rational growth

2020 *Mathematics subject classification:* Primary 20F16

1. Introduction

The Cayley graph $\Gamma(G;S)$ of a finitely generated group G equipped with a finite generating subset S allows us to study the group G using both combinatorial and geometric methods. One invariant of the group that arises in this viewpoint is the **growth function** $V(n;S)$ which was introduced by Schwarz and Milnor independently and is given by the size of a ball of radius n in $\Gamma(G;S)$. The motivation for this invariant is geometric as seen in case when G is the fundamental group of a Riemannian manifold where the growth function of G gives a discrete approximation of the volume growth of the universal cover of the manifold [19]. Moreover, it has been shown that the growth function has an exponential growth when the manifold is negatively curved and has polynomial growth when G is virtually nilpotent [11, 21].

Milnor asked whether the growth function is always either an exponential function or a polynomial function. Moreover, he asked whether one can classify every group whose growth exponent $\lim \log V(n)/\log n$ exists [12]. It was shown by Tits [20] that there is no linear group of intermediate growth whereas it is known to be not true in general by work of Grigorchuk [8]. For the second problem, Bass showed that virtually nilpotent groups always have an integer degree of polynomial growth [1]. Finally, Gromov showed that a group has polynomial growth if and only if it is virtually nilpotent [9] giving a complete answer to Milnor's question.

For nilpotent groups, one can ask how precisely the growth function $V(n;S)$ behaves like a polynomial over $\mathbb{Q}$. Towards this end, Pansu showed that the limit $\alpha = \lim_{n\to\infty} V(n;S)/n^d$ exists for nilpotent groups [14]. Thus, one may study whether α is a rational number. One approach to this question is to study the **growth series** $\sum V(n;S)t^n$ associated with the growth function and use its analytic properties. If the growth series is a rational function, for instance, one can then show that the limit α is an algebraic integer which is a consequence of the coefficients being linearly recursive.

It turns out the rationality of the growth series has stronger implications to the computability of the group with respect to a finite generating set. As a corollary to the fact that $V(n)$ is linearly recursive when the growth series is rational, one can then see the group G always has a solvable word problem. Cannon showed the growth series for any hyperbolic group is rational by essentially showing that all hyperbolic groups are strongly geodesically automatic [5]. In fact, Neumann and Shapiro showed that the growth series with respect to S is rational when the full language of geodesics in G is regular [13].

Little is known about what groups have rational growth with respect to some finite generating subset. In fact, there are only a handful of classes of finitely generated groups that are known to have rational growth with respect to any finite generating subset. Virtually abelian groups were shown to have rational growth by Benson [2]. For Coxeter groups, it was shown by Paris [15], and for solvable Baumslag–Solitar groups, it was shown by Brazil, and independently by Collins, Edjvet, and Gill [3, 6]. Among these classes of finitely generated groups, hyperbolic groups and virtually abelian groups are also shown to have rational growth with respect to not only some fixed finite generating set, but for all finite generating sets [2, 5]. This property is known as **panrationality** and the only known example of a panrational group outside of virtually abelian groups and hyperbolic groups is the integral Heisenberg group of dimension 3 [7]. In general, the rationality of the growth of a group depends on the choice of generating subset. In particular, this was demonstrated by Stoll [18] in the case of the integral Heisenberg group of dimension 5. Stoll constructed two generating subsets for this group, one for which the generating function associated with the growth function is rational and the other where the generating function is not rational. Thus, a natural direction of research is to investigate when a finitely generated group of interest admits finite generating subsets that are rational, and we may consider the finite generating sets for which the group has rational growth as algorithmically nicer than other generating sets.

Our interests are in the study of rationality of finitely presented solvable groups. Since Kharlampovich [10] constructed examples of finitely presented solvable groups of derived length 3 that have unsolvable word problem, we will focus on metabelian, i.e. solvable of derived length 2, groups in this paper. In particular, we will focus on a family of torus bundle groups given by $G = \mathbb{Z}^2 \rtimes \mathbb{Z}$. Parry showed that when the trace of the action is even and at least 4, these groups have rational growth with respect to some generating set [16]. We extend Parry's result to the traces that are odd and at least 5.

Main Theorem. *Let* $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 2k+1 \end{smallmatrix}\right] \in SL(2,\mathbb{Z})$ *where* $2k+1 \geq 5$. *Then* $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ *has rational growth with respect to the standard generating subset.*

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

It was shown that certain groups of the form $\mathbb{Z}^m \rtimes \mathbb{Z}$ have a finite-index subgroup which have rational growth in some finite generating set [4, 17]. Our work improves on this result for $m = 2$ as we do not require passing to a finite-index subgroup. Moreover, we are able to generalize and to streamline the proof given by Parry. In particular, we define an invariant called the **potential** which makes the proof cleaner. We conjecture that our argument can be applied to all torus bundle groups to get the following:

Conjecture 1. *Any torus bundle group $G = \mathbb{Z}^2 \rtimes_A \mathbb{Z}$ where $A \in SL(2, \mathbb{Z})$ has rational growth with respect to some finite generating set.*

1.1. Outline of the paper

The general structure of this work is as follows:

Section 2. In this section, we first recall the definition of a torus bundle group and its structure and give a description of the word length with a specific choice of generators.

Section 3. Following [16], we reduce the problem of finding the word with the shortest length representing a group element into an optimization problem in the Laurent polynomial ring over the integers. Such minimizing polynomial is called *the n-minimal polynomial*. We also define a related notion called *the n-reduced polynomial* given by a list of rules on coefficients.

Section 4. In this section, we give an explicit algorithm for rewriting any polynomial into *the n-reduced polynomial*. We show that any *n-minimal polynomial* can be rewritten so that it splits into *n-reduced* polynomial part and principal part without increasing the length.

Section 5. With rewriting rules established in the previous section, we classify all cases of *n-reduced polynomials* that require rewriting when you add 1. This will be used to subdivide *n-reduced polynomials* into *n-types and n-classes*.

Section 6. Precise definition for the *n-types and n-classes* are given in this section. The *n-types and n-classes* are defined recursively over the degree of the polynomial. This recursive definition allows us to inductively compute the growth series for *n-reduced polynomials*.

Section 7. In this section, we define *the successor*. We show that any n-reduced polynomial with non-negative leading coefficient can be obtained by applying *successor* repeatedly on 1 and that it is injective. When counting certain *n-classes and n-types* is difficult, we will use the successor to count the corresponding *n-classes and n-types*.

Section 8. Combining the results from § 6, we will find the growth series for the n-reduced polynomial whose leading coefficient is non-negative. We then use this to establish the rationality of the growth of the whole group.

2. Torus bundle groups

In this section, we briefly give the definition of the class of torus bundle groups that we are interested in and a description of their word metrics with respect to a specific choice of finite generating subset. When given a finitely generated group G equipped with a finite generating subset S, we write $\|g\|_S$ to be the minimal length over all representatives of g in the alphabet in S. When the generating subset is clear from context, we will suppress the subscript.

Let T be the automorphism of $\mathbb{Z}^2$ given by the matrix

$$T = \begin{bmatrix} 0 & -1 \\ 1 & 2k+1 \end{bmatrix}$$

with respect to the standard basis $a = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$, $b = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right]$ of $\mathbb{Z}^2$. Let $\langle t \rangle$ be the infinite cyclic group generated by t. We define the action of t on $\mathbb{Z}^2$ by $t\,x\,t^{-1} = T \cdot x$ for any $x \in \mathbb{Z}^2$ and form the semidirect product $G = \mathbb{Z}^2 \rtimes \langle t \rangle$. We will view elements of G as ordered pairs $(x,\, t^n)$ where $x \in \mathbb{Z}^2$ and $n \in \mathbb{Z}$. Thus, we may write G as

$$G = \langle a, b, t \mid [a, b] = 1, a^t = b, b^t = a^{-1} b^{2k+1} \rangle$$

where $g^t = t\,g\,t^{-1}$. In particular, we will investigate the word growth of G with respect to the generating subset $S = \{a,\, b,\, t\}$.

2.1. Length of elements in G

Let $g = (x,\, t^n) \in G$. We may rewrite g where we collect consecutive factors which are either a's or b's but not collecting consecutive factors which are either t's or their inverses. This allows us to write

$$g = t^{n_0} x_1\, t^{n_1}\, x_2\, t^{n_2}\, \ldots x_{e-1} t^{n_{e-1}}\, x_e\, t^{n_e}$$

where $e \in \mathbb{N}$, $n_0,\, n_e \in \{-1,\, 0,\, 1\}$, $n_1,\, \ldots,\, n_{e-1} \in \{-1,\, 1\}$, and $x_1,\, \ldots,\, x_e \in \mathbb{Z}^2$. We may obtain the word length of g by minimizing the sum

$$\sum_{i=0}^{e} |n_i| + \sum_{i=1}^{e} |x_i|, \tag{1}$$

where $|x_i|$ is the length of x_i in $\mathbb{Z}^2$ with respect to the generating subset $\{a,\, b\}$. We rewrite the given expression for g as

$$g = (t^{n_0}\, x_1\, t^{-n_0}) \cdot (t^{n_0+n_1}\, x_2\, t^{-n_0-n_1}) \ldots \left(t^{\sum_{i=0}^{e-1} n_i}\, x_e\, t^{-\sum_{i=0}^{e-1} n_i}\right) \cdot t^{\sum_{i=0}^{e} n_i}. \tag{2}$$

We then note that

$$t^{\sum_{i=0}^{\ell-1} n_i}\, x_\ell\, t^{-\sum_{i=0}^{\ell-1} n_i} \in \mathbb{Z}^2$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

for each $0 \leq \ell \leq e-1$ and that $t^m\, x\, t^{-m} = T^m \cdot x$ for all $m \in \mathbb{Z}$ and $x \in \mathbb{Z}^2$. Therefore, we have that

$$(t^{n_0}\, x_1\, t^{-n_0}) \cdot (t^{n_0+n_1}\, x_2\, t^{-n_0-n_1}) \ldots (t^{\sum_{i=0}^{e-1} n_i}\, x_e\, t^{-\sum_{i=0}^{e-1} n_i}) \in \mathbb{Z}^2.$$

By the above construction, we have that $n = \sum_{i=0}^{e} n_i$.

For notational simplicity, we let

$$q = \max\{0, n_0, n_0 + n_1, n_0 + n_1 + n_2, \ldots, n\}$$

and

$$p = \max\{0, -n_0, -n_0 - n_1, -n_0 - n_1 - n_2, \ldots, -n\}.$$

Assume that $n \geq 0$. By combining terms according to the partial sums $n_0 + \ldots + n_i$, we see that we will not increase the length of the expression in Equation (1). Thus, we may rewrite Equation (2) as

$$\begin{aligned} g &= (t^{-p}\, y_{-p}\, t^{p}) \cdot (t^{-p+1}\, y_{-p+1}\, t^{p-1}) \ldots (t^{q}\, y_q t^{-q}) \cdot t^n \\ &= \left(\sum_{i=-p}^{q} T^i(y_i), t^n \right) \end{aligned}$$

for elements $y_{-p}, \ldots, y_q \in \mathbb{Z}^2$. We furthermore obtain $\|g\|$ by minimizing

$$2p + 2q - n + \sum_{i=-p}^{q} |y_i|.$$

We may suppose that $y_i = r_i\, a + s_i\, b$ with $r_i,\, s_i \in \mathbb{Z}$. Given that $T(a) = b$, we may write $T^i(y_i)$ as

$$T^i(y_i) = r_i\, T^i(a) + s_i T^i(b) = r_i\, T^{i-1}(b) + s_i\, T^i(b)$$

where $i > 0$. If $i < 0$, then we may write $T^i(y_i)$ as

$$T^i(y_i) = r_i\, T^i(a) + s_i T^i(b) = r_i T^i(a) + s_i T^{i+1}(a).$$

We have a similar situation for $n \leq 0$. Thus, if $g = (x,\, t^n) \in G$, then $\|g\|$ is the minimal value of

$$2p + 2q - |n| + \sum_{i=0}^{p} |r'_i| + \sum_{j=0}^{q} |s'_j|$$

over all representatives of x given by

$$x = \sum_{i=0}^{p} r'_i T^{-i}(a) + \sum_{j=0}^{q} s'_j T^j(b)$$

where $r'_0, \ldots, r'_p, s'_0, \ldots, s'_q$ are integers, $p \geq \max\{0, -n\}$, and $q \geq \max\{0, n\}$. Lastly, we observe that $a = T^{-1}(b)$. Therefore, we have the following proposition which expresses

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

the value of $\|g\|$ for $g = (x, t^n)$ in terms of representatives for x constructed in the above discussion.

Proposition 2. *Let $g = (x, t^n) \in G$. We may express $\|g\|$ as the minimal value of*

$$2p + 2q - |n| + \sum_{j=-p}^{q} |c_j|$$

over all representations of x given by

$$x = \sum_{j=-p-1}^{q} c_j T^j(b),$$

where $p \geq \max\{0, -n\}$, $q \geq \max\{0, n\}$, and $c_{-p-1}, \ldots, c_q$ are integers.

3. Polynomial representatives

Following [16, Section 4], we establish a correspondence between Laurent polynomials and elements in the Torus bundle group.

Definition 3. Given a Laurent polynomial $F(X) = \sum_{j=-p-1}^{q} c_j X^j$, we define the **polynomial part** of $F(X)$ to be $\sum_{j=0}^{q} c_j X^j$ and the **principal part** to be $\sum_{j=-p-1}^{-1} c_j X^j$.

For $(x, t^n) \in G$, if $x = F(T)(b)$, we say $F(X)$ is a **representative of** x or **represents** x.

Following the notation, we define $p = \max(\{0, -n\} \cup \{p' \mid c_{-p'-1} \neq 0\})$ and $q = \max(\{0, n\} \cup \{q' \mid c_{q'} \neq 0\})$. It follows that if $p > \max(0, -n)$ then $c_{-p-1} \neq 0$, and if $q > \max(0, n)$ then $c_q \neq 0$. We then define the n**-length** of $F(X)$ to be

$$L_n(F(X)) = 2p + 2q - |n| + \sum_{j=-p-1}^{q} |c_j|.$$

Note that $L_n(F(X))$ is always a non-negative integer. For an $F(X)$ representing x, we say $F(X)$ is an n**-minimal representative** of x if $L_n(F(X)) = \|(x, t^n)\|$.

By Proposition 2, $\|(x, t^n)\|$ is realized by some Laurent polynomial and we have the following theorem:

Theorem 4. *Suppose that $g = (x, t^n)$ is an element of G. Then g has an n-minimal representative.*

In this context, the relation $b^t = (b^{-1})^{t^{-1}} b^{2k+1}$ becomes $T - (2k+1)I + T^{-1} = 0$. Hence, finding $\|g\|$ translates to minimizing L_n over all polynomial representatives $F(X)$ of x up to adding multiples of $(X^2 - (2k+1)X + 1)$.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Observe that when given a representative for x

$$F(X) = \sum_{j=-p-1}^{q} c_j X^j$$

where $|c_j| > k+2$ for some j, we can find another polynomial representative by adding polynomial multiples of $(X^2 - (2k+1)X + 1)$ which yields

$$\sum_{j=-p'-1}^{q'} c'_j X^j$$

where the coefficient $|c'_j| < |c_j|$. For example, the polynomial $2X^2 + (-k+2)X + 4$ is preferred to $X^2 + (k+3)X + 3$ which is obtained by adding $(X^2 - (2k+1)X + 1)$. In fact, one can use this cancellation repeatedly to deduce that large coefficients cannot be adjacent to each other too often in an n-minimal polynomial. We will later call this phenomenon an instance of the **global rules**.

Example 5. Consider the polynomial

$$F(X) = X^6 + (k+1)X^5 + (k-1)X^4 + kX^3 + kX^2 + kX + 2.$$

By direct computation, one can show that the 7-length is given by

$$L_7(F(X)) = 8 + 5k.$$

By adding

$$X^6 + (-2k)X^5 + (-2k+1)X^4 + (-2k+1)X^3 + (-2k+1)X^2 + (-2k)X + 1,$$

we get the polynomial

$$Q(X) = 2X^6 + (-k+1)X^5 + (-k)X^4 + (-k+1)X^3 + (-k+1)X^2 + (-k)X + 3.$$

Through direct computation, we have

$$L_7(Q(X)) = 12 - 7 + 2 + (-k+1) - k + (-k+1)(-k+1) - k + 3 = 13 - 4k$$

which has a shorter 7-length.

More precise conditions on the coefficients will be described below.

3.1. n-reduced polynomials

In this subsection, we define n**-reduced polynomials** in $\mathbb{Z}[X]$. Later, we show in Theorem 24 that any n-minimal Laurent polynomial can be written as the sum of two n-reduced polynomials, namely, the polynomial part and the principal part. Since the set of n-reduced polynomials has a natural grading given by the degree of a polynomial, we will be using n-reduced polynomials instead of n-minimal Laurent polynomials for counting purposes. For convenience, we denote a polynomial $F(X) = \sum_{i=0}^{m} c_i X^i$ by a

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

string of coefficients $(c_m, c_{m-1}, \ldots, c_1, c_0)$ which we call the **word**. Here indices are understood as the degree of X and the entries as the coefficient of that power of X. A contiguous substring of this will be called a **subword** of a word. We adopt the following convention of sign functions:

$$\operatorname{sign}(x) = \begin{cases} 1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}, \quad \operatorname{sign}^+(x) = \begin{cases} 1 & x \geq 0 \\ -1 & x < 0 \end{cases}, \quad \operatorname{sign}^-(x) = -\operatorname{sign}^+(-x)$$

with the inequality $\operatorname{sign}^-(x+1) \leq \operatorname{sign}^+(x)$ for all $x \in \mathbb{Z}$. We start with the following definition.

Definition 6. For a word $(c_m, \ldots, c_{m-i})$, we define its **potential** as

$$\operatorname{Pot}(c_m, \ldots, c_{m-i}) = \sum_{c_j \in (c_m, \ldots, c_{m-i})} (2k-1) - 2|c_j|.$$

In particular, when the string only contains coefficients whose absolute values are $k-2$, $k-1$, k or $k+1$, then the potential can be written as

$$\operatorname{Pot}(c_m, \ldots, c_{m-i}) = 3N_{k-2} + N_{k-1} - N_k - 3N_{k+1}$$

where $N_t = |\{j \mid c_j = |t|\}|$.

By definition, the potential is additive under concatenating two strings. In order to describe the change in the potential under any rewriting, we analyse the potential change in different cases on a single coefficient which is listed out in the following lemma. Since it follows from definition, we omit the proof.

Lemma 7. *Let a be such that $|a| < k + 2$. We then have the following*:

- $\operatorname{Pot}(a+1) = \operatorname{Pot}(a) - 2\operatorname{sign}^+(a)$
- $\operatorname{Pot}(a-1) = \operatorname{Pot}(a) + 2\operatorname{sign}^-(a)$
- $\operatorname{Pot}(a-(2k-1)) = -\operatorname{Pot}(a) \quad (a > 0)$
- $\operatorname{Pot}(a+(2k-1)) = -\operatorname{Pot}(a) \quad (a < 0)$
- $\operatorname{Pot}(a-2k) = -\operatorname{Pot}(a) - 2 \quad (a > 0)$
- $\operatorname{Pot}(a+2k) = -\operatorname{Pot}(a) - 2 \quad (a < 0)$.

The potential value of an n-minimal polynomial serves as a test function that determines whether a rewriting is needed. We are now ready to define n-reduced polynomials.

Definition 8. Let n be a fixed integer and $P(X) = (c_m, \ldots, c_1, c_0)$ be a polynomial of degree m. $P(X)$ is n**-reduced** if the following rules are satisfied.

Rule 1 (Local top rule) For $m \geq n$,

$$|c_m| \leq k+2,$$
$$|c_m| \leq k+1 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-1}) < 0.$$

Rule 2 (Local non-top rule) For $i = m < n$ or $i < m$,

$$|c_i| \leq k+1,$$
$$|c_i| \leq k \quad \text{if } \operatorname{sign}(c_{i+1} \cdot c_i) < 0 \text{ or } \operatorname{sign}(c_i \cdot c_{i-1}) < 0,$$
$$|c_i| \leq k-1 \quad \text{if } \operatorname{sign}(c_{i+1} \cdot c_i) < 0 \text{ and } \operatorname{sign}(c_i \cdot c_{i-1}) < 0.$$

Rule 3 (Local top rule) For $m > n$,

$$(c_m, c_{m-1}) \neq \pm(1, -k),$$
$$(c_m, c_{m-1}) \neq \pm(1, -k+1) \quad \text{if } \operatorname{sign}(c_{m-1} \cdot c_{m-2}) < 0.$$

Rule 4 (Global top rule)
For $m > n$ and $i \geq 1$, and

$$(c_m, \ldots, c_{m-i}) = \pm(1, c'_{m-1}, \ldots, c'_{m-i})$$

where $c'_{m-1} \in \{-k+1, -k+2\}$, $c'_{m-j} \in \{-k+1, -k\}$ for $1 < j < i$, and $c'_{m-i} \in \{-k, -k-1\}$.

$$\operatorname{Pot}(c'_{m-1}, \ldots, c'_{m-i}) \geq 2 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-i-1}) > 0,$$

$$\operatorname{Pot}(c'_{m-1}, \ldots, c'_{m-i}) > 0 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-i-1}) \leq 0.$$

Rule 5 (Global top rule)
For $m \geq n$, $i \geq 1$, and

$$(c_m, \ldots, c_{m-i}) = \pm(c'_m, c'_{m-1}, \ldots, c'_{m-i})$$

where $c'_m \in \{k+1, k+2\}$, $c'_{m-i'} \in \{k-1, k\}$ for $i' \neq i$, and $c'_{m-i} \in \{k, k+1\}$.

$$\operatorname{Pot}(c'_m, \ldots, c'_{m-i}) > -6 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-i-1}) \geq 0,$$

$$\operatorname{Pot}(c'_m, \ldots, c'_{m-i}) \geq -4 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-i-1}) < 0.$$

Rule 6 (Global non-top rule)
For $0 \le \ell < j$ and either $0 < j < m$ or $0 < j = m < n$, and

$$(c_j, c_{j-1}, \ldots, c_\ell) = \pm(c'_j, c'_{j-1}, \ldots, c'_\ell)$$

where c'_j, $c'_\ell \in \{k,\, k+1\}$,
and $c'_s \in \{k-1,\, k\}$ for $s \neq j,\, \ell$.

$$\mathrm{Pot}(c_j, \ldots, c_\ell) > -3 - \mathrm{sign}^+(c_j \cdot c_{j+1}) \quad \text{if } \mathrm{sign}(c_j \cdot c_{\ell-1}) \ge 0,$$

$$\mathrm{Pot}(c_j, \ldots, c_\ell) \ge -1 - \mathrm{sign}^+(c_j \cdot c_{j+1}) \quad \text{if } \mathrm{sign}(c_j \cdot c_{\ell-1}) < 0.$$

Similarly, for $F(X) \in \mathbb{Z}[X^{-1}]$, we say $F(X)$ is n**-reduced** if $F(X^{-1}) \in \mathbb{Z}[X]$ is n-reduced.

Rule 1, **Rule 2** and **Rule 3** are called **local rules**. These rules determine whether a single coefficient requires rewriting. **Rule 4**, **Rule 5** and **Rule 6** are called **global rules**. These determine whether a string of coefficients requires rewriting. The local rules can be considered as the degenerate cases of the corresponding global rules. Note that the local rules for a single coefficient cannot be violated at the same time, and that **Rule 4** and **Rule 5** cannot be violated at the same time for the same sequence of coefficients. Of course, both rules can be violated at the same time if the violations occur in different locations, and these locations may overlap.

Definition 9. For the global rules, a subword $(c_j,\, c_{j-1},\, \ldots,\, c_{j-i})$ used in the potential condition will be called the **subword associated with the rule**. For the local rules, the associated subword will be understood as a single coefficient $\pm(k-1)$, $\pm k$, $\pm(k+1)$, or $\pm(k+2)$ in question.

For convenience, we introduce an alternative definition of global rules.

Lemma 10. *Assuming the same conditions for subwords, the potential condition for the global rules can be restated as follows:*

Rule 4 *(Global top rule)*

$$\mathrm{Pot}(c'_{m-1}, \ldots, c'_{m-i}) \ge 1 + \tfrac{1}{2}\,\mathrm{sign}^-(c_m \cdot c_{m-i-1}).$$

Rule 5 *(Global top rule)*

$$\mathrm{Pot}(c'_m, \ldots, c'_{m-i}) \ge -5 - \tfrac{1}{2}\,\mathrm{sign}^+(c_m \cdot c_{m-i-1}).$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Rule 6 *(Global non-top rule)*

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_\ell) \geq -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(c_j \cdot c_{\ell-1})$$

Proof. We first consider **Rule 4**. When $\mathrm{sign}(c_m \cdot c_{m-i-1}) > 0$, we have that $\mathrm{sign}^-(c_m \cdot c_{m-i-1}) = 1$, so

$$\mathrm{Pot}(c'_{m-1}, \ldots, c'_{m-i}) \geq 1 + \tfrac{1}{2}\,\mathrm{sign}^-(c_m \cdot c_{m-i-1}) = 1 + \tfrac{1}{2}.$$

Since potentials are integers, this is equivalent to $\mathrm{Pot}(c'_{m-1}, \ldots, c'_{m-i}) \geq 2$, the potential condition stipulated in Definition 8 in this case.

Similarly, when $\mathrm{sign}(c_m \cdot c_{m-i-1}) \leq 0$, we have that $\mathrm{sign}^-(c_m \cdot c_{m-i-1}) = -1$, so

$$\mathrm{Pot}(c'_{m-1}, \ldots, c'_{m-i}) \geq 1 + \tfrac{1}{2}\,\mathrm{sign}^-(c_m \cdot c_{m-i-1}) = 1 - \tfrac{1}{2}.$$

Since potentials are integers, this is equivalent to $\mathrm{Pot}(c'_{m-1}, \ldots, c'_{m-i}) > 0$, the potential condition stipulated in Definition 8 in this case.

The proofs for **Rule 5** and **Rule 6** follow in the same fashion. □

Since $\mathrm{Pot}(\cdot)$ is integer valued, there is no distinction between strict inequality and inequality. This allows us to reduce the number of cases one needs to check. We will use this alternative definition when appropriate.

We note that not all n-minimal polynomials are n-reduced which means that we may have to rewrite the polynomial to obtain an n-reduced polynomial representative. Thus, for each violation, we assign **rewriting rules** that do not increase n-length.

Definition 11. Suppose that $P(X) = (0, c_m, \ldots, c_0)$ is not n-reduced. For each violation of the rules, we define **the rewriting associated with the given rule** as the following operations.

Rule 1
For $m \geq n$, assume that $|c_m| > k + 2$ or $|c_m| > k + 1$ if $\mathrm{sign}(c_m \cdot c_{m-1}) < 0$, then the rewriting rule is given by

$$(0, c_m, c_{m-1}) - \mathrm{sign}(c_m)(-1, 2k + 1, -1).$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Rule 2
For $i = m < n$ or $i < m$, assume that

$$
\begin{aligned}
&|c_i| > k+1,\\
&|c_i| > k \text{ if } \operatorname{sign}(c_{i+1}\cdot c_i) < 0 \text{ or } \operatorname{sign}(c_i \cdot c_{i-1}) < 0, \text{ or}\\
&|c_i| > k-1\text{if } \operatorname{sign}(c_{i+1}\cdot c_i) < 0 \text{ and } \operatorname{sign}(c_i\cdot c_{i-1}) < 0.
\end{aligned}
$$

Then the rewriting rule is given by

$$(c_{i+1}, c_i, c_{i-1}) - \operatorname{sign}(c_i)(-1, 2k+1, -1).$$

Rule 3 (Local top rule) For $m > n$, assume that

$$
\begin{aligned}
&(c_m, c_{m-1}) = \pm(1, -k), \text{ or}\\
&(c_m, c_{m-1}) = \pm(1, -k+1) \quad \text{if } \operatorname{sign}(c_{m-1}\cdot c_{m-2}) < 0.
\end{aligned}
$$

Then the associated rewriting rule is given by

$$
\begin{aligned}
&(1, c_{m-1}, c_{m-2}) + (-1, 2k+1, -1), \text{ or}\\
&(-1, c_{m-1}, c_{m-2}) + (1, -2k-1, 1).
\end{aligned}
$$

Rule 4 (Global top rule)
For $m > n$ and $i \geq 1$, and

$$(c_m, \ldots, c_{m-i}) = \pm(1, c'_{m-1}, \ldots, c'_{m-i})$$

where $c'_{m-1} \in \{-k+1, -k+2\}$, $c'_{m-j} \in \{-k+1, -k\}$ for $1 < j < i$, and $c'_{m-i} \in \{-k, -k-1\}$, assume that

$$
\begin{aligned}
&\operatorname{Pot}(c'_{m-1}, \ldots, c'_{m-i}) < 2 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-i-1}) > 0, \text{ or}\\
&\operatorname{Pot}(c'_{m-1}, \ldots, c'_{m-i}) \leq 0 \quad \text{if } \operatorname{sign}(c_m \cdot c_{m-i-1}) \leq 0.
\end{aligned}
$$

Then the rewriting rule is given by

$$(1, c'_{m-1}, \ldots, c'_{m-i}, c'_{m-i-1}) + (-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1).$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Rule 5 (Global top rule)
For $m \geq n$, $i \geq 1$, and

$$(c_m, \ldots, c_{m-i}) = \pm(c'_m, c'_{m-1}, \ldots, c'_{m-i})$$

where $c'_m \in \{k+1, k+2\}$, $c'_{m-i'} \in \{k-1, k\}$ for $i' \neq i$, and $c'_{m-i} \in \{k, k+1\}$, assume that

$$\begin{aligned} &\mathrm{Pot}(c'_m, \ldots, c'_{m-i}) \leq -6 \quad \text{if } \mathrm{sign}(c_m \cdot c_{m-i-1}) < 0, \text{ or} \\ &\mathrm{Pot}(c'_m, \ldots, c'_{m-i}) \geq -4 \quad \text{if } \mathrm{sign}(c_m \cdot c_{m-i-1}) < 0. \end{aligned}$$

Then the rewriting rule is given by

$$(0, c_m, \ldots, c_{m-i}, c_{m-i-1}) - \mathrm{sign}(c_m)(-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1).$$

Rule 6 (Global non-top rule)
For $0 \leq l < j$ and either $0 < j < m$ or $0 < j = m < n$, and

$$(c_j, c_{j-1}, \ldots, c_l) = \pm(c'_j, c'_{j-1}, \ldots, c'_\ell)$$

where c'_j, $c'_\ell \in \{k, k+1\}$,
and $c'_s \in \{k-1, k\}$ for $s \neq j$, ℓ, assume that

$$\begin{aligned} &\mathrm{Pot}(c_j, \ldots, c_{j-i}) \leq -3 - \mathrm{sign}^+(c_j \cdot c_{j+1}) \quad \text{if } \mathrm{sign}(c_j \cdot c_{\ell-1}) \geq 0, \text{ or} \\ &\mathrm{Pot}(c_j, \ldots, c_{j-i}) < -1 - \mathrm{sign}^+(c_j \cdot c_{j+1}) \quad \text{if } \mathrm{sign}(c_j \cdot c_{\ell-1}) < 0. \end{aligned}$$

Then the rewriting rule is given by

$$(c_{j+1}, c_j \ldots, c_l, c_{l-1}) - \mathrm{sign}(c_j)(-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1).$$

Since the rewriting rules may take place at the constant term c_0, the resulting polynomial may have a non-zero coefficient in front of X^{-1}. For example, if $F(X) = k+2$, the rewriting will give us $F'(X) = X + (-k+1) + X^{-1}$. However, if we start with $F(X) \in \mathbb{Z}[X]$, after rewriting, the coefficient for X^{-1} can only be 0 or ± 1. While this may seem problematic, as the rules don't apply to a polynomial with X^{-1}, we will show later that once the rewriting is done on the constant coefficient, any subword associated with rules for future violations will not include X^{-1} nor the constant coefficient; thus, X^{-1} part can be ignored in effect.

In this view, Example 5 can be rephrased using the established definitions above as follows: suppose that $n = 7$. For a polynomial

$$(1, k+1, k-1, k, k, k, 2)$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

a subword $(k+1,\ k-1,\ k,\ k,\ k)$ is tested with **Rule 6**. Since

$$\mathrm{Pot}(k+1,k-1,k,k,k) = -5 < -3 - \mathrm{sign}((k+1)\cdot 1) = -4,$$

we see that **Rule 6** is violated. The rewriting rule for this violation is to add another polynomial

$$(1,-2k,-2k+1,-2k+1,-2k+1,-2k,1)$$

as prescribed in the definition 11, which gives us

$$(2,-k+1,-k,-k+1,-k+1,-k,3).$$

As demonstrated in the example, new polynomial has a shorter 7-length compared to the polynomial we started with. We show that this is the case with all rewriting rules.

Lemma 12. *The rewriting associated with the rules will not increase the n-length of the sequence.*

Proof. We split this proof into two sections. The first section is devoted to the local rules and the second is devoted to global rules. For local rules, we check the n-length change for each case.

(1) **Local Rules**

- **Rule 1**. The associated rewriting rule is given by

$$(0,k+3,b,\dots)+(1,-2k-1,1)=(1,-k+2,b+1,\dots).$$

  The n-length is changed by $3-5+\mathrm{sign}^+(b)<0$.

- **Rule 2**. The associated rewriting rule is given by

$$(\dots,b,k+2,c,\dots)+(1,-2k-1,1)=(\dots,b+1,-k+1,c+1,\dots).$$

  The n-length is changed by $\mathrm{sign}^+(b)-3+\mathrm{sign}^+(c)<0$.

- **Rule 3**. The associated rewriting rule is given by

$$(1,-k,c,\dots)+(-1,2k+1,-1)=(0,k+1,c-1,\dots).$$

  The n-length is changed by $-3+1-\mathrm{sign}^+(c)<0$.

(2) **Global Rules**

Suppose that $c_i<0$ is a coefficient in the subword associated with the rule. We see that adding $(2k-1)$ to c_i for all possible values of c_i yields

$$\begin{aligned} -k-1 &\mapsto k-2 \\ -k &\mapsto k-1 \\ -k+1 &\mapsto k \\ -k+2 &\mapsto k+1, \end{aligned}$$

and for each case, the absolute value of the coefficient changes by -3, -1, 1 and 3, respectively. We will prove the lemma for **Rule 6**, the proofs for other global rules are similar.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

- **Rule 6**. Assuming $c_j < 0$, the associated rewriting rule is given by

$$\begin{aligned}(c_{j+1}, c_j, \ldots, c_l, c_{l-1}) &- \operatorname{sign}(c_j)(-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1)\\ &= (c_{j+1}, c_j, c_{j-1}, \ldots, c_{l+1}, c_l, c_{l-1})\\ &\quad + (-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1)\\ &= (c_{j+1}-1, c_j+2k, c_{j-1}+2k-1, \ldots, c_{l+1}+2k-1, c_l+2k, c_{l-1}-1)\end{aligned}$$

The n-length on the first and last coordinates depend on the sign of c_{j+1} and c_{l-1}. For $l+1 \le s \le j-1$, we have $c_s = -k$ or $-k+1$, and from the above discussion, the corresponding n-length change is -1 or 1, namely $\operatorname{Pot}(c_s)$. For $s = j$ or l, we have $c_s = -k$ or $-k-1$, and $c_s + 2k = k$ or $k-1$, so the n-length change is 0 or -2, namely $\operatorname{Pot}(c_s)+1$. Thus, the total n-length is changed by

$$\begin{aligned}&-\operatorname{sign}^+(c_{j+1}) - \operatorname{sign}^+(c_{l-1}) + \operatorname{Pot}(c_j, \ldots, c_l) + 2\\ &\quad= \operatorname{sign}^+(c_{j+1}\cdot c_j) + \operatorname{sign}^+(c_{l-1}\cdot c_j) + \operatorname{Pot}(c_j, \ldots, c_l) + 2\\ &\quad< \operatorname{sign}^+(c_{j+1}\cdot c_j) + \operatorname{sign}^+(c_{l-1}\cdot c_j)\\ &\qquad + (-2 - \operatorname{sign}^+(c_{j+1}\cdot c_j) - \tfrac{1}{2}\operatorname{sign}^+(c_{l-1}\cdot c_j)) + 2\\ &\quad= \tfrac{1}{2}\operatorname{sign}^+(c_{l-1}\cdot c_j)\end{aligned}$$

As everything is an integer here, we have the total n-length change must be non-positive. □

In some cases, a polynomial after the rewriting will have the same n-length. We demonstrate this in the example below.

Example 13. Consider the sequence $(2, 2, k, k, k, k, 2)$. The subsequence (k, k, k, k) has potential -4, and thus violates **Rule 6** as $\operatorname{Pot}(k, k, k, k) = -4 < -2 - \operatorname{sign}^+(2\cdot k) - \frac{1}{2}\operatorname{sign}^+(k\cdot 2) = -3 - \frac{1}{2}$. The rewriting associated with this rule would be $(2, 2, k, k, k, k, 2) - (0, -1, 2k, 2k-1, 2k-1, 2k, -1) = (2, 3, -k, -k+1, -k+1, k, 3)$. In each coordinate, the n-length is changed by 0, 1, 0, -1, -1, 0, 1, so the total n-length is unchanged.

4. Rewriting procedures

In this section, we show how n-reduced polynomials can be obtained by applying the rewriting rules listed above. As noted, while some rules are mutually exclusive, it is possible that a word violates multiple rules at the same time. Moreover, after rewriting, another rule violation may appear somewhere else. For that reason, it is not immediately clear how any polynomial can be uniquely rewritten to an n-reduced polynomial.

We first establish that there is a smallest unit of rewriting called a *minimal poison subword*, which can be made unique by picking the subword with the lowest degree. The main idea is to first rewrite on this unique subword, then find the minimal poison subword for the new polynomial to rewrite and repeat the process. For this algorithm to work, we will need to show that subsequent minimal poison subwords are eventually away from the minimal poison subword that appeared first.

With the algorithm for n-reduced polynomials established, we investigate the relationship between the n-reduced polynomial and the n-minimal polynomial. While there may be multiple n-minimal representatives for a group element g, we show that by applying the algorithm introduced earlier to both the principal part and the polynomial part, possibly multiple times, that one can get the unique n- minimal representative of the polynomial.

We begin by defining the minimal poison subword.

Definition 14. If a word violates the unique rule, it is called a **poison word**. The shortest subword that violates the unique rule is called a **minimal poison subword**. A minimal poison subword that has the smallest leading degree is called the **rightmost minimal poison subword**.

By the natural ordering by inclusion, we know there has to be a minimal subword, which includes the case when a single coefficient violates one of the local rules. As noted, the local rules are mutually exclusive, and **Rule 4** and **Rule 5** cannot be tested simultaneously on the same subword. We show that the minimal poison subword can always be obtained.

Lemma 15. *If a word violates multiple rules simultaneously, then there is a shorter subword in it that violates only one of the rules.*

Proof. We show for **Rule 6** first. Suppose that

$$(c_j, c_{j-1}, \dots, c_\ell)$$

violates **Rule 6**. Since a non-top rule applies, the subword can only violate either **Rule 2** or **Rule 6** on a strict smaller subword. If it violates **Rule 2**, then we pick the coefficient as the poison subword. If it violates **Rule 6** on a smaller subword, we pick this subword and repeat the process until we get the minimal poison subword.

For top rules, we only show for **Rule 4**. Suppose that the subword

$$(c_m, \dots, c_{m-i}) = (1, c_{m-1}, \dots, c_{m-i})$$

violates **Rule 4**. If this subword violates some other rules, the violation can only come from **Rule 1**, **Rule 3**, **Rule 4** and **Rule 6**. If it violates any of the local rules, then we pick the coefficient in question as the poison subword as before. If it violates **Rule 4** on a strictly smaller subword contained in the original, we pick the smaller subword and repeat the same argument again. Hence, it remains to show that if **Rule 6** is violated, the violation occurs on a strictly smaller subword. For

$$(1, c_{m-1}, \dots, c'_{m-i}),$$

we observe that c_{m-1} is either $-k+1$ or $-k+2$. Since **Rule 6** requires the leading coefficient to be $-k$ or $-k-1$, c_{m-1} is not contained in the subword that violates **Rule 6**. By repeating this process for a strictly smaller subword, we get a poison subword. The case for **Rule 5** can be worked out similarly. □

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

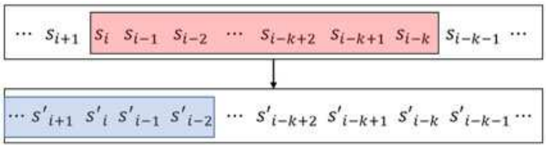

Figure 1. Given a word (top), we perform a rewriting with respect to the minimal poison subword (in red). After rewriting, a new minimal poison subword always appears on the left (in blue).

There may be multiple minimal poison subwords, however, by preferring the smaller degree for the leading coefficient, the algorithm above always gives the unique minimal poison subword.

We now have established that the rightmost minimal poison subword exists and is unique. We will repeatedly rewrite the rightmost minimal poison subword to obtain the n-reduced polynomial. Once a rewriting on the rightmost minimal poison subword is done, the consequent poison subword should move left in order for this process to terminate eventually. We start with a definition for two subwords for their relative positions.

Definition 16. Let $(c_i, \ldots, c_{i-k})$ and $(c_j, \ldots, c_{j-l})$ be two subwords that violate any of the rules. If there is no common subword that is contained in both, i.e., if $i - k > j$ or $j - l > i$, then the two subwords are said to be **disjoint**. In the same manner, two rewriting rules are disjoint if their associated subwords are disjoint.

Two disjoint rules do not necessarily commute unless their associated subwords are separated by another non-trivial subword. Thus, the ordering of the rules is important. We are now ready to show this sequence of rewriting progresses to the left without backtracking. See Figure 1.

Theorem 17. *Let $(s_i, \ldots, s_{i-k})$ be the rightmost minimal poison subword of a given word. Let $(s'_i, \ldots, s'_{i-k})$ be the subword obtained from rewriting, and let $(s'_j, \ldots, s'_{j-l})$ be the rightmost minimal poison subword for the new word. Then $j > i$ and $j - l > i - k$. Subsequently, rewriting rules are eventually disjoint from the initial rewriting.*

Proof. We rule out all of the other possible cases using the potential of subwords. We have a number of cases based on the inclusion relationship between the subwords $(s'_i, \ldots, s'_{i-k})$ and $(s'_j, \ldots, s'_{j-l})$.

(1) The subword $(s'_j, \ldots, s'_{j-l})$ is contained in the subword $(s'_i, \ldots, s'_{i-k})$. This case is handled by Lemma 18.

(2) The subword $(s'_i, \ldots, s'_{i-k})$ is contained in the subword $(s'_j, \ldots, s'_{j-l})$. This case is handled in Lemma 19. See Figure 3.

(3) The subword $(s'_j, \ldots, s'_{j-l})$ is on the right of the subword $(s'_i, \ldots, s'_{i-k})$. This last case is handled in Lemma 20. See Figure 4.

□

By dividing the proof into three different cases, we have control over what rules need to be checked after the initial rewriting. For instance, in Lemma 20, we only need to check

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

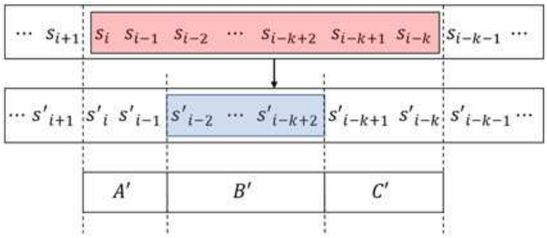

Figure 2. The new minimal poison subword cannot be contained in where the previous minimal poison subword was. (Lemma 18.).

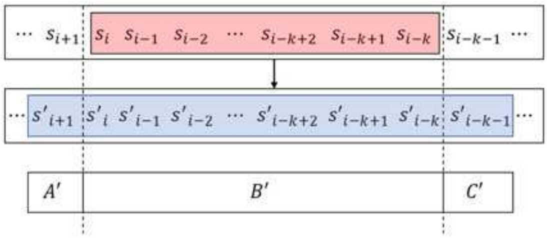

Figure 3. New minimal poison subword cannot contain a subword corresponding to the previous minimal poison subword. (Lemma 19).

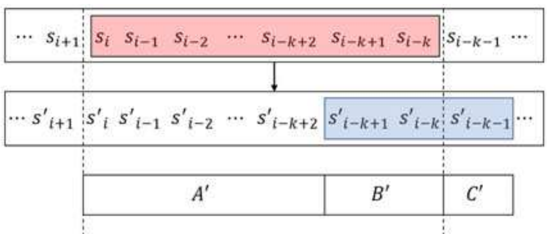

Figure 4. New minimal poison subword cannot appear on the right. (Lemma 20).

Rule 2 and **Rule 6** after rewriting as these are the only non-top rules. If followed by a minimal poison subword for any of the top rules, this would fall into the case covered in Lemma 19 instead.

Throughout the proof, we will denote the subword (not necessarily poison) as a whole letter such as A, B and C. Once the rewriting has been applied, new subwords will be denoted as A', B' and C', respectively. Instead of writing the sign of the leading coefficient and end coefficient of A, we will be using $\operatorname{sign}^+(A)$ to indicate the sign of the coefficient and $\operatorname{sign}^+(A \cdot B)$ when we need to use the signs of the coefficients from two subwords; since all coefficients in the minimal poison subword have the same sign, there is no ambiguity here.

Lemma 18. *Assume that the subword* $(s_i, \ldots, s_{i-k})$ *is the rightmost minimal poison subword of a given word. Let* $(s'_i, \ldots, s'_{i-k})$ *be the subword obtained from rewriting, and*

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Table 1. *For Lemma 18, we only need to check these rules.*

Initial rule violation	Next rule violation
Rule 4	**Rule 1, 2, 5, 6**
Rule 5	**Rule 2, 3, 4, 6**
Rule 6	**Rule 2, 6**

let $(s'_j, \ldots, s'_{j-l})$ be the rightmost minimal poison subword for the new word. Then the subword $(s'_j, \ldots, s'_{j-l})$ cannot be contained in the subword $(s'_i, \ldots, s'_{i-k})$. Namely, we cannot have both $i \geq j$ and $j - l \geq i - k$.

Proof. We first show that the new poison subword $(s'_j, \ldots, s'_{j-l})$ cannot be contained in the subword $(s'_i, \ldots, s'_{i-k})$ (see Figure 2.)

We first list rules we need to check. (See Table 1.) We note that if the initial minimal poison subword violates a local rule, then the next minimal poison subword that appears after rewriting can only violate a local rule because we assumed containment. More specifically, once (s_{i+1}, s_i) violates **Rule 3**, we can only check (s'_i) for **Rule 1** and vice versa. Similarly, once (s_i) violates **Rule 2**, we can only check (s'_i) for **Rule 2**. However, by Definition 8, we know this is impossible. So assume that the initial minimal poison subword violates a global rule as listed in Table 1. We also point out that, because of containment, if the initial rule violation is from a non-top rule, then the next rule violation cannot be from a top rule.

For simplicity, denote the initial minimal poison subword as

$$(s_i, \ldots, s_{i-k}) = (A|B|C)$$

as 3 disjoint subwords concatenated into one word. After rewriting, this subword becomes $(s'_i, \ldots, s'_{i-k})$, which we denote $(A'|B'|C')$ where $(s'_j, \ldots, s'_{j-l}) = (B')$. The rewriting rule in this case is

$$\begin{aligned}&(s_{i+1}, |A|B|C|, s_{i-k-1}) - \operatorname{sign}(s_i)(-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1)\\&= (s'_{i+1}, |A'|B'|C'|, s'_{i-k-1}).\end{aligned}$$

For a top rule, subword (A) is empty. Obviously, the subwords (A) and (C) cannot be empty at the same time, as the rules cannot be applied to the same subword twice by Definition 8.

We argue in the following way: because the subword $(A'|B'|C')$ was obtained from rewriting, there's a bound on the value $\operatorname{Pot}(A'|B'|C')$ from which comes from the value $\operatorname{Pot}(A|B|C)$. Since the subword (B') violates one of the rules, we can combine with alternate bounds on the values $\operatorname{Pot}(A')$ and $\operatorname{Pot}(C')$ to get another bound on the value $\operatorname{Pot}(A'|B'|C')$ which contradicts the previous bound on the value of $\operatorname{Pot}(A'|B'|C')$. We proceed through our proof based on the particular rule that the subword $(A|B|C)$ violates. In each case, we assume that either $j \leq i$ or $j - l \leq i - k$ for our contradiction.

1. $(A|B|C)$ **violates Rule 4 or Rule 5**.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

As mentioned, (A) and (C) cannot be both empty. We proceed based on whether (A), (C), or (A) and (C) are both empty.

(1) **Suppose that both (A) and (C) are nonempty.**
It then follows that the word (B') can only violate **Rule 2** or **Rule 6**. Since all coefficients in (B') have values either $\pm k$ or $\pm(k-1)$, and all coefficients in $(A'|B'|C')$ have the same sign, **Rule 2** cannot be violated. As for **Rule 6**, when $(A|B|C)$ violates **Rule 4**, we then have

$$\begin{aligned} \operatorname{Pot}(A|B|C) &\leq 1 + \tfrac{1}{2}\operatorname{sign}^-(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(A') &= -\operatorname{Pot}(A) - 2 \leq -4, \\ \operatorname{Pot}(C') &= -\operatorname{Pot}(C) - 2 \leq 1 + \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(B') &\leq -4. \end{aligned}$$

This implies that

$$\operatorname{Pot}(A'|B'|C') \leq -7 + \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}).$$

But $\operatorname{Pot}(A'|B'|C') \geq -5 - \frac{1}{2}\operatorname{sign}^-(s_{i-k} \cdot s_{i-k-1})$ which is impossible.
Similarly, when $(A|B|C)$ violates **Rule 5** and (B') violates **Rule 6**, we have

$$\begin{aligned} \operatorname{Pot}(A|B|C) &\leq -5 - \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(A') &= -\operatorname{Pot}(A) - 2 \leq 3, \\ \operatorname{Pot}(C') &= -\operatorname{Pot}(C) - 2 \leq 1 + \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(B') &\leq -4. \end{aligned}$$

Taking this all together, we may write

$$\operatorname{Pot}(A'|B'|C') \leq \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}).$$

But $\operatorname{Pot}(A'|B'|C') \geq 1 + \frac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1})$ which is impossible.

(2) **(C) is empty.**
The above argument works identically. Assuming that (B) is violating **Rule 6**, the potential is bounded

$$\begin{aligned} \operatorname{Pot}(A|B) &\leq 1 + \tfrac{1}{2}\operatorname{sign}^-(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(A') &= -\operatorname{Pot}(A) - 2 \leq -4, \\ \operatorname{Pot}(B') &\leq -3 - \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(A'|B') &\leq -7 - \tfrac{1}{2}\operatorname{sign}^+(s_{i-k} \cdot s_{i-k-1}), \\ \operatorname{Pot}(A'|B') &\geq -5 - \tfrac{1}{2}\operatorname{sign}^-(s_{i-k} \cdot s_{i-k-1}) \end{aligned}$$

for **Rule 4**, which is impossible. For **Rule 5**, we have that

$$\begin{aligned}\mathrm{Pot}(A|B) &\leq -5 - \tfrac{1}{2}\,\mathrm{sign}^{+}(s_{i-k}\cdot s_{i-k-1}),\\ \mathrm{Pot}(A') &= -\,\mathrm{Pot}(A) - 2 \leq 3,\\ \mathrm{Pot}(B') &\leq -3 - \tfrac{1}{2}\,\mathrm{sign}^{+}(s_{i-k}\cdot s_{i-k-1}),\\ \mathrm{Pot}(A'|B') &\leq -\tfrac{1}{2}\,\mathrm{sign}^{+}(s_{i-k}\cdot s_{i-k-1}),\\ \mathrm{Pot}(A'|B') &\geq 1 + \tfrac{1}{2}\,\mathrm{sign}^{+}(s_{i-k}\cdot s_{i-k-1}).\end{aligned}$$

which is impossible. For **Rule 2**, we only need to consider $(B') = s'_{i-k}$. The only possible coefficients for s'_{i-k} are $\pm k$ and $\pm(k-1)$, and s'_{i-k+1} has the same sign as s'_{i-k}, so s'_{i-k} cannot violate **Rule 2**.

(3) (A) **is empty.**
If $(B|C)$ violates **Rule 4** then (B') violates **Rule 1** or **Rule 5**, and if $(B|C)$ violates **Rule 5**, then (B') violates **Rule 3** or **Rule 4**. Suppose that $(B|C)$ violates **Rule 4**. Since (s'_i) is either $\pm(k+1)$ or $\pm(k+1)$ with (s'_{i-1}) having the same sign as (s'_i), **Rule 1** cannot be violated. As for **Rule 5**, we check the potential

$$\begin{aligned}\mathrm{Pot}(B|C) &\leq 1 + \tfrac{1}{2}\,\mathrm{sign}^{-}(s_{i-k}\cdot s_{i-k-1}),\\ \mathrm{Pot}(C') &\geq -3 - \tfrac{1}{2}\,\mathrm{sign}^{+}(s'_{i-k}\cdot s'_{i-k-1}),\\ \mathrm{Pot}(C) &\geq 1 + \tfrac{1}{2}\,\mathrm{sign}^{+}(s'_{i-k}\cdot s'_{i-k-1}),\\ \mathrm{Pot}(B') &\leq -5,\\ \mathrm{Pot}(B) &\geq 3,\\ \mathrm{Pot}(B|C) &\geq 4 + \tfrac{1}{2}\,\mathrm{sign}^{+}(s'_{i-k}\cdot s'_{i-k-1}).\end{aligned}$$

which is impossible. Now suppose that $(B|C)$ violates **Rule 5**. For **Rule 3**, $(B) = s'_i$ is either $\pm(k-1)$ or $\pm(k-2)$, with s'_i having the same sign as s'_i, so **Rule 3** cannot be violated. For **Rule 4**, We have that

$$\begin{aligned}\mathrm{Pot}(B|C) &\leq -5 - \tfrac{1}{2}\,\mathrm{sign}^{+}(s_{i-k}\cdot s_{i-k-1}),\\ \mathrm{Pot}(C') &\geq -3 - \tfrac{1}{2}\,\mathrm{sign}^{+}(s'_{i-k}\cdot s'_{i-k-1}),\\ \mathrm{Pot}(C) &\geq 1 + \tfrac{1}{2}\,\mathrm{sign}^{+}(s'_{i-k}\cdot s'_{i-k-1}),\\ \mathrm{Pot}(B') &\leq 1,\\ \mathrm{Pot}(B) &\geq -3,\\ \mathrm{Pot}(B|C) &\geq -2 + \tfrac{1}{2}\,\mathrm{sign}^{+}(s'_{i-k}\cdot s'_{i-k-1})\end{aligned}$$

which is impossible.

2. The subword $(A|B|C)$ violates Rule 6

First, we can rule out **Rule 2** entirely, as the coefficients appearing in (A'), (B') and (C') are either $\pm k$ or $\pm(k-1)$, with at least one neighbouring coefficient having the same

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

sign. So suppose that (B') violates **Rule 6**. We proceed based on whether A, C or A and C are empty.

(1) **The subwords** (A) **and** (C) **are both nonempty**.
Recall that the subword $(s_i, \ldots, s_{i-k})$ satisfies **Rule 6** if

$$\mathrm{Pot}(s_i, \ldots, s_{i-k}) \geq -2 - \mathrm{sign}^+(s_i \cdot s_{i+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1}).$$

Since the subword $(s_i, \ldots, s_{i-k}) = (A|B|C)$ violates **Rule 6**, we instead have

$$\mathrm{Pot}(A|B|C) \leq -2 - \mathrm{sign}^+(s_i \cdot s_{i+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1}).$$

Since the subword $(A|B|C)$ is minimal, none of the subwords inside $(A|B|C)$ violate any rules which includes **Rule 6**. Thus, we have

$$\begin{aligned}
\mathrm{Pot}(A) &\geq -2 - \mathrm{sign}^+(s_i \cdot s_{i+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(A \cdot B),\\
\mathrm{Pot}(A) &\geq -2 - \mathrm{sign}^+(s_i \cdot s_{i+1}),\\
\mathrm{Pot}(C) &\geq -2 - \mathrm{sign}^+(B \cdot C) - \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1}),\\
\mathrm{Pot}(C) &\geq -3 - \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1}).
\end{aligned}$$

After rewriting, the subword (B') is the rightmost minimal poison subword violating **Rule 6**. Therefore, we have

$$\mathrm{Pot}(B') \leq -2 - \mathrm{sign}^+(A' \cdot B') - \mathrm{sign}^+(B' \cdot C') = -4.$$

Because $(A'|B'|C')$ was obtained from $(A|B|C)$ by rewriting, we have

$$\begin{aligned}
\mathrm{Pot}(A') &= -\mathrm{Pot}(A) - 2 \leq \mathrm{sign}^+(s_i \cdot s_{i+1}),\\
\mathrm{Pot}(C') &= -\mathrm{Pot}(C) - 2 \leq 1 + \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1}).
\end{aligned}$$

Hence, we may write the value $\mathrm{Pot}(A'|B'|C')$ as

$$-\mathrm{Pot}(A|B|C) - 4 \geq -2 + \mathrm{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1}).$$

But $\mathrm{Pot}(B') \leq -4$. Therefore,

$$\mathrm{Pot}(A'|B'|C') \leq -3 + \mathrm{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\,\mathrm{sign}^+(s_i \cdot s_{i-k-1})$$

which is a contradiction.

(2) (A) **is empty.**

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

We may write

$$\begin{aligned}\operatorname{Pot}(B') &\leq -3 - \operatorname{sign}^+(s'_i \cdot s'_{i+1}),\\ \operatorname{Pot}(C') &\leq 1 + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1})\end{aligned}$$

Therefore, we may express $\operatorname{Pot}(B'|C')$ as

$$-\operatorname{Pot}(B|C) - 4 \geq -2 + \operatorname{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1}).$$

However, since $\operatorname{sign}^-(s_i \cdot s'_{i+1}) \leq \operatorname{sign}^+(s_i \cdot s_{i+1})$, we have that

$$\begin{aligned}\operatorname{Pot}(B'|C') &\leq -2 - \operatorname{sign}^+(s'_i \cdot s'_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1}),\\ &= -2 + \operatorname{sign}^-(s_i \cdot s'_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1}),\\ &\leq -2 + \operatorname{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1}),\\ &\leq \operatorname{Pot}(B'|C').\end{aligned}$$

Thus, the equality can only happen when $\operatorname{sign}^+(s_i \cdot s_{i-k-1}) = 0$ which is impossible.

(3) (C) **is empty.**
We then have

$$\begin{aligned}\operatorname{Pot}(A') &= -\operatorname{Pot}(A) - 2 \leq \operatorname{sign}^+(s_i \cdot s_{i+1}),\\ \operatorname{Pot}(B') &\leq -3 + \tfrac{1}{2}\operatorname{sign}^+(s'_i \cdot s'_{i-k-1}).\end{aligned}$$

That implies we may write $\operatorname{Pot}(A'|B')$ as

$$-\operatorname{Pot}(A|B) - 4 \geq -2 + \operatorname{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1}).$$

Hence, we may further write

$$\begin{aligned}\operatorname{Pot}(A'|B') &\leq -3 + \operatorname{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s'_i \cdot s'_{i-k-1}),\\ &\leq -3 + \operatorname{sign}^+(s_i \cdot s_{i+1}) + \tfrac{1}{2}\operatorname{sign}^+(s_i \cdot s_{i-k-1}) < \operatorname{Pot}(A'|B').\end{aligned}$$

□

Lemma 19. *Assume that $(s_i, \ldots, s_{i-k})$ is the rightmost minimal poison subword of a given word. Let $(s'_i, \ldots, s'_{i-k})$ be the subword obtained from rewriting, and let $(s'_j, \ldots, s'_{j-l})$ be the rightmost minimal poison subword for the new word. Then the subword $(s'_i, \ldots, s'_{i-k})$ cannot be contained in the subword $(s'_j, \ldots, s'_{j-l})$. Namely, we cannot have both $j \geq i$ and $i - k \geq j - l$.*

Proof. Again, we begin with listing rules to be checked. (See Table 2.) Because we have already checked the cases when the second violation is from a local rule in Lemma 18, we only need to check global rules for the second violation.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Table 2. *For Lemma 19, we only need to check these rules. by Lemma 18, the second violation from local rules are ruled out.*

Initial rule violation	Next rule violation
Rule 1	**Rule 4**
Rule 2	**Rule 4,5,6**
Rule 3	**Rule 5**
Rule 4	**Rule 5**
Rule 5	**Rule 4**
Rule 6	**Rule 4,5,6**

Suppose (B) violates **Rule 1**. Then (A) is empty and $(B') = s'_{m-1}$ is either $\pm(k-1)$ or $\pm(k-2)$. Since (B) is assumed to be the rightmost minimal poison, (C) does not violate **Rule 6**. By Lemma 10, we have

$$\mathrm{Pot}(C) \geq -1 - \tfrac{1}{2}\,\mathrm{sign}^+(s'_{i-k-1} \cdot s'_{j-\ell-1}).$$

Since (C') is obtained by adding $\mathrm{sign}(B)$ to s_{i-k-1},

$$\mathrm{Pot}(C') \geq 1 - \tfrac{1}{2}\,\mathrm{sign}^+(s'_{i-k-1} \cdot s'_{j-\ell-1}).$$

Since $(B'|C')$ violates **Rule 4**, we have

$$\mathrm{Pot}(B'|C') < 1 + \tfrac{1}{2}\,\mathrm{sign}^-(s'_m \cdot s'_{j-\ell-1}).$$

However, $\mathrm{Pot}(s'_{m-1}) > 0$, so this is impossible. The case when $(A'|B'|C')$ violates the **Rule 4** can be worked out similarly by using a lower bound for $\mathrm{Pot}(B')$ which is obtained from an upper bound for $\mathrm{Pot}(B)$.

Now suppose (B) violates **Rule 3**. Then (A) is empty and $(B') = s'_{m-1}$ is either $\pm k$ or $\pm(k-1)$. Since (C) does not violate **Rule 6**, just like before, we have

$$\mathrm{Pot}(C') \geq 1 - \tfrac{1}{2}\,\mathrm{sign}^+(s'_{i-k-1} \cdot s'_{j-\ell-1}).$$

Since $(B'|C')$ violates **Rule 5**, we have

$$\mathrm{Pot}(B'|C') < -5 - \tfrac{1}{2}\,\mathrm{sign}^+(c_m \cdot c_{j-\ell-1}).$$

However, $\mathrm{Pot}(s'_{m-1}) > -2$, so this is impossible. The case when $(A'|B'|C')$ violates the **Rule 5** can be worked out similarly, again by using a lower bound for $\mathrm{Pot}(B')$ which is obtained from an upper bound for $\mathrm{Pot}(B)$.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Table 3. *For Lemma 20, all other cases have been exhausted except for by Lemma 18 and 19.*

Initial rule violation	Next rule violation
Rule 1,2,3,4,5,6	**Rule 2**
Rule 4,5,6	**Rule 6**

Suppose both (B) and $(A'|B'|C')$ violate **Rule 6**, or (B) violates **Rule 2** and $(A'|B'|C')$ violate **Rule 6**. Since (B) is the rightmost, we have that

$$\mathrm{Pot}(C) \geq -1 - \tfrac{1}{2}\,\mathrm{sign}^+(C \cdot s'_{j-l}).$$

Therefore,

$$\mathrm{Pot}(C') \geq 1 - \tfrac{1}{2}\,\mathrm{sign}^+(C' \cdot s_{j-l}).$$

On the other hand, since $(A'|B'|C')$ violates **Rule 6**, we have that

$$\mathrm{Pot}(A'|B'|C') \leq -2 - \mathrm{sign}^+(s_{j+1} \cdot A') - \tfrac{1}{2}\,\mathrm{sign}^+(C' \cdot s_{j-l}).$$

This gives us a new bound $\mathrm{Pot}(A'|B') \leq -3 - \mathrm{sign}^+(s_{j+1} \cdot A')$ which implies that $(A'|B')$ violates **Rule 6**, contradicting that $(A'|B'|C')$ is minimal poison. Using the same bounds for $\mathrm{Pot}(C')$, we also get a contradiction for $(A'|B'|C')$ violating **Rule 4** or **Rule 5**. $\square$

Lemma 20. *Assume that $(s_i, \ldots, s_{i-k})$ is the rightmost minimal poison subword of a given word. Let $(s'_i, \ldots, s'_{i-k})$ be the subword obtained from rewriting, and let $(s'_j, \ldots, s'_{j-l})$ be the rightmost minimal poison subword for the new word. Assume that $(s'_i, \ldots, s'_{i-k})$ and $(s'_j, \ldots, s'_{j-l})$ intersect such that the first word does not contain the second word and vice versa. Then $j > i$ and $j - l > i - k$.*

Proof. We begin with listing rules to be checked. (See Table 3.) By Lemma 18 and 19, regardless of the initial rule violation, the next rule violation can only be from **Rule 2** or **Rule 6**.

Suppose that $(s_i, \ldots, s_{i-k})$ violates any of the rules. By Lemma 18, the minimal poison subword violating **Rule 2** after rewriting must be disjoint from $(s_i, \ldots, s_{i-k})$, (s'_{i-k-1}) is the minimal poison subword in this case. (s_{i-k-1}) is not a poison subword, so by Definition 8,

$$|s_{i-k-1}| \leq k+1, k, \text{ or } k-1$$

depending on $\mathrm{sign}(s_{i-k}s_{i-k-1})$ and $\mathrm{sign}(s_{i-k-1}s_{i-k-2})$. (s'_{i-k-1}) violates **Rule 2**, so

$$|s'_{i-k-1}| > k+1, k, \text{ or } k-1$$

depending on

$$\mathrm{sign}(s'_{i-k}s'_{i-k-1}) = -\,\mathrm{sign}(s_{i-k}s_{i-k-1})$$

and

$$\mathrm{sign}(s'_{i-k-1}s_{i-k-2}) = \mathrm{sign}(s_{i-k-1}s_{i-k-2}).$$

But this is impossible, since $s'_{i-k-1} = s_{i-k-1} + \mathrm{sign}(s_{i-k})$.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Table 4. *Base case for types and classes.*

Type	n-class of Q	$Q = dX + c$	n
n-initial type	–	0	$n \leq 0$
n-interior type	S_0	$d = 0 \quad c = 0$	$n > 0$
	S_+	$d = 0 \quad 0 < c \leq k$	$n \leq 0$
	U^t_{-3}	$d = 0 \quad c = k + 1$	$n \leq 0$
	S_+	$d = 0 \quad 0 < c \leq k - 1$	$n > 0$
	U_0	$d = 0 \quad c = k$	$n > 0$
n-negative type	E_1	$X - k + 1$	$n \leq 0$
	E_3	$X - k + 2$	$n \leq 0$
n-boundary type	U^t_{-5}	$d = 0 \quad c = k + 2$	$n \leq 0$
	U_{-2}	$d = 0 \quad c = k + 1$	$n > 0$

Table 5. *Inductive case for types and classes.*

Type of Q	n-class of $XP + c$	$(n-1)$-class of P	c
n-interior	S_+	Any	$0 < c \leq k - 2$
	S_0	except E_1, $-U_{-2}$	$c = 0$
	S_+	S_0, S_+, U_0, U^t_{-3}	$c = k - 1$
	U_0	U_{-1}	$c = k - 1$
	U_0	S_0, S_+	$c = k$
	U_0	S_-, E	$c = k - 1$
	U^t_{-3}	U^t_{-4}	$c = k - 1$
n-negative	E_2	E_1	$c = -k + 1$
	E_3	E_2	$c = -k + 1$
	S_-	E_3	$c = -k + 1$
	E_1	E_2	$c = -k$
	E_2	E_3	$c = -k$
	S_-	except above	$c < 0$
n-boundary (P)	U_{-1}	U_{-2}	$c = k - 1$
	U^t_{-4}	U^t_{-5}	$c = k - 1$
	U_{-2}	U_{-1}	$c = k$
	U^t_{-5}	U^t_{-4}	$c = k$
	U_{-1}	U_0	$c = k$
	U^t_{-4}	U^t_{-3}	$c = k$
	U_{-2}	S_-, E	$c = k$
	U_{-2}	S_+, S_0	$c = k + 1$
n-boundary (S)	S_0	$-U_{-2}$	$c = 0$
	S_0	E_1	$c = 0$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Now we have ruled out all local rules. Suppose $i \geq j \geq i-k \geq j-l$. Let the intersection be (B'), $(s'_i, \ldots, s'_{i-k}) = (A'|B')$, and $(s'_j, \ldots, s'_{j-l}) = (B'|C')$ is the minimal poison subword violating **Rule 6**. We show (B') is empty and use the fact that $(A|B)$ is the rightmost minimal poison subword to get a contradiction. In this case, the rewriting is given by

$$\begin{aligned}&(s_{i+1}|A|B|s_{i-k-1}) - \operatorname{sign}(s_i)(-1, 2k, 2k-1, \ldots, 2k-1, 2k, -1)\\ &= (s'_{i+1}|A'|B'|s'_{i-k-1}).\end{aligned}$$

Note that (A) and (B) have the same sign and (B') and (C') have the same sign, since $(A|B)$ and $(B'|C')$ violate some rules. Also, (B) and (B') have opposite signs because of the rewriting. Thus, all coefficients in (A) and (B) have the same sign with all coefficients in (C) the opposite sign.

$(A|B)$ violates **Rule 6**. Thus,

$$\begin{aligned}\operatorname{Pot}(A|B) &\leq -2 - \operatorname{sign}^+(s_i \cdot s_{i+1}),\\ \operatorname{Pot}(A) &\geq -2 - \operatorname{sign}^+(s_i \cdot s_{i+1})(\textbf{Rule 6}),\\ \operatorname{Pot}(B) &\geq -2(\textbf{Rule 6}),\\ \operatorname{Pot}(C) &\geq -1 - \tfrac{1}{2}\operatorname{sign}^+(s_{i-k-1} \cdot s_{j-l-1})(\textbf{Rule 6}),\\ \operatorname{Pot}(B'|C') &\leq -3 - \tfrac{1}{2}\operatorname{sign}^+(s'_{j-l} \cdot s_{j-l-1})(\text{Violation of } \textbf{Rule 6}),\\ \operatorname{Pot}(A') &= -\operatorname{Pot}(A) - 2 \leq \operatorname{sign}^+(s_i \cdot s_{i+1})(\text{Rewriting}),\\ \operatorname{Pot}(A'|B') &\geq -2 + \operatorname{sign}^+(s_i \cdot s_{i+1})(\text{Rewriting}).\end{aligned}$$

By combining the inequalities for $\operatorname{Pot}(A')$ and $\operatorname{Pot}(A'|B')$, we get

$$\operatorname{Pot}(B') \geq -2.$$

Hence, combining the inequalities for $\operatorname{Pot}(B')$ and $\operatorname{Pot}(B'|C')$ allows us to write

$$\operatorname{Pot}(C') \leq -1 - \tfrac{1}{2}\operatorname{sign}^+(s'_{j-l} \cdot s_{j-l-1}).$$

However, it then follows that $\operatorname{Pot}(C) \leq -3 - \frac{1}{2}\operatorname{sign}^+(s'_{j-l} \cdot s_{j-l-1})$ which contradicts the previous bound on $\operatorname{Pot}(C)$. Thus, (B) is empty. Similarly, we can show that (B) is empty assuming $(A|B)$ violates either **Rule 4** or **Rule 5**.

Since the subword (B) is empty, two consecutive poison subwords are disjoint, and thus, we can directly compare the potentials. (C') is a minimal poison subword. Therefore, we have that $\operatorname{Pot}(C') \leq -2 - \operatorname{sign}^+(c_j \cdot c_{j+1}) - \frac{1}{2}\operatorname{sign}^+(c_{j-l} \cdot c_{j-l-1})$. Because (A) and (C) has opposite sign, the rewriting rule suggests that $\operatorname{Pot}(C) = \operatorname{Pot}(C') - 2$, which means that (C) already violates **Rule 6** contradicting the fact (A) is the rightmost minimal poison subword. □

We point out that the proof of Lemma 18 does not require the rightmost minimal poison subword. The purpose of choosing the rightmost one is to prevent the next minimal poison subwords from appearing at other places. If there is only one minimal poison subword to start with, Lemma 19 and Lemma 20 can be modified to give us the following corollary.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Corollary 21. *If a word has only one minimal poison subword, then all consecutive rewriting rules are disjoint. In particular, if P is an n-reduced polynomial, then all consecutive rewriting rules for $P+1$ are disjoint.*

If the only minimal poison subword comes from **Rule 4** or **Rule 5**, then the next minimal poison subword is either contained or contains the initial minimal poison subword. By Lemma 18 and Lemma 19, we know this cannot happen. If the minimal poison subword violates **Rule 6**, then this follows from Lemma 20 applied to the left side instead of the right side.

We now show that there exists an n-minimal representative of a given element $g \in G$ whose polynomial part and principal part are n-reduced. We start with the following lemma.

Lemma 22. *Suppose $F(X) = \sum_{i=\ell}^{m} c_i X^i$ is an n-minimal representative of $g = (x, t^n)$. Then polynomial and principal parts of $F(X)$ satisfy* ***Rule 1***, ***Rule 2***, *and* ***Rule 3***.

Proof. If not, by adding or subtracting $X^d(X^2 - (2k+1)X + 1)$ with some appropriate choice of d, one can obtain a new Laurent polynomial. By Lemma 12, this new Laurent polynomial has strictly less n-length, contradicting the fact $F(X)$ is an n-minimal representative of g. □

With local rules satisfied, we now prescribe how n-minimal Laurent polynomials can be rewritten to have n-reduced polynomial part.

Proposition 23. *Let $F(X) = \sum_{i=\ell}^{m} c_i X^i$ be an n-minimal representative of $g = (x, t^n)$. Let r be an integer, and suppose that $\ell < 0 \leq r \leq m$. Then there exists a deterministic process that takes $F(X)$ to a Laurent polynomial $G(X)$ given by*

$$G(X) = \sum_{i=r}^{M} B_i X^i + (B_{r-1} + c_{r-1}) X^{r-1} + \sum_{i=\ell}^{r-2} c_i X^i$$

such that $G(X)$ is an n-minimal representative of g and where $\sum_{i=r}^{m} B_i X^i$ is n-reduced. Moreover, we have that $B_{r-1} \in \{-1, 0, 1\}$, and if $B_{r-1} = \pm 1$, then $B_r B_{r-1} < 0$ and $c_{r-1} B_r \geq 0$. We have that $B_r \in \{c_r, c_r \pm 1, c_r \pm 2k, c_r \pm (2k+1)\}$. Finally, $M = m$ or $M = m \pm 1$.

Proof. We induct on r reversely, i.e., we apply the rewriting procedure as in Theorem 17 on $F(X)$ inductively from a higher degree. The base case in our case for the induction is when $r = m$. Consider $c_m X^m$. Only local rules apply here, and by Lemma 22, $c_m X^m$ is n-reduced. Thus, $c_m = B_M$ and $m = M$. For the step case, consider

$$F_r(X) = c_m X^m + \ldots + c_r X^r.$$

If it is n-reduced, we are done and $m = M$. If not, Lemma 22 implies that $F_r(X)$ cannot violate local rules. Thus, we need only consider global rules. As in Theorem 17, we start rewriting from the rightmost minimal poison subword of $(c_m, \ldots, c_r)$. We note that since F_{r+1} is already n-reduced, the rightmost minimal poison subword must contain

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

either c_r or c_{r+1}. If it contains c_r, then $B_{r-1} \in \{-1, 1\}$ and $B_r \in \{c_r \pm 2k, c_r \pm (2k+1)\}$, and $B_{r-1} = 0$, $c'_r = c_r \pm 1$ otherwise. Finally, $M = m+1$ or $M = m-1$ depending on whether c_m is contained in the rightmost minimal poison subword in the sequence of rewriting rules. The sequence of rewriting rules terminates as all rewriting rules after the initial rewriting are eventually disjoint from (c_r). □

Theorem 24. *Suppose that $g = (x, t^n)$ is an element of G. Then x has an n-minimal representative whose polynomial and principal part are both n-reduced.*

We show that we can modify any n-minimal representative of x until the desired form is achieved. By Lemma 22, we have any n-minimal representative must satisfy **Rule 1**, **Rule 2** and **Rule 3**. We will apply Proposition 23 with $r = 0$ to the polynomial part. Furthermore, by the symmetry of the polynomial and principal parts, we can apply Proposition 23 to the principal part by applying it to $X^{-1} \cdot F(X^{-1})$. We also need the following proposition.

Proposition 25. *Let $n \in \mathbb{Z}$.*

(1) *If $P(X) = \sum_{i=0}^{m} c_i X^i$ is n-reduced, then so is $\sum_{i=\ell}^{m} c_i X^i$.*

(2) *Let $P(X) \in \mathbb{Z}[X]$. Then $P(X)$ is n-reduced if and only if $XP(X)$ is $(n+1)$-reduced.*

Proof. Let $P_\ell(X) = \sum_{i=\ell}^{m} c_i X^k$. We claim that P_ℓ is n-reduced, and towards that end, we may represent P_ℓ as the string

$$(c_m, \ldots, c_\ell, 0, \ldots, 0)$$

where there are $\ell - 1$ zero's at the end of the string. Since P is n-reduced and $(c_m, \ldots, c_\ell)$ is a substring of $(c_m, \ldots, c_0)$, it is easy to see that **Rule 1**, **Rule 2**, and **Rule 3** are satisfied for coefficients with indices between ℓ and m. Since the coefficients of P_ℓ with index less than ℓ are zero, we have that the **Rule 1**, **Rule 2**, and **Rule 3** are all satisfied.

Let $m \geq t \geq i \geq \ell$, and suppose that $Q = (c_t, \ldots, c_i)$ is a poison subword with respect to either **Rule 4**, **Rule 5**, or **Rule 6**. If $i > \ell$, then $(c_t, \ldots, c_i)$ is a poison subword of P with respect to **Rule 4**, **Rule 5**, or **Rule 6** which is a contradiction. Thus, if P_ℓ contains a poison subword, it must contain the coefficient c_ℓ.

We proceed by contradiction to demonstrate $(c_m, \ldots, c_\ell)$ satisfies **Rule 4**, **Rule 5**, and **Rule 6**. We split this argument based on the rule we are trying to verify.

(1) **Rule 4**.
If $(c_m, \ldots, c_\ell)$ violates **Rule 4**, we then would have that

$$(c_m, \ldots, c_\ell) = \pm(1, c'_{m-1}, \ldots, c'_\ell)$$

where $c'_{m-j} \in \{-k+1, -k\}$ for $0 \leq j < m - \ell$ and $c'_\ell \in \{-k, -k-1\}$. We have that $\operatorname{sign}(c_m \cdot c_{\ell-1}) = \operatorname{sign}(c_m \cdot 0) = \operatorname{sign}(0)$. We then have

$$\operatorname{Pot}(c_m, \ldots, c_\ell) \leq 0.$$

However, since $(c_m, \ldots, c_\ell)$ is a substring of P, we have that $(c_m, \ldots, c_\ell)$ satisfies **Rule 4**. In particular, if $\operatorname{sign}(c_m \cdot c_\ell) > 0$, then $\operatorname{Pot}(c_m, \ldots, c_\ell) \geq 2$ which is a contradiction. If $\text{sign}(c_m \cdot c_{\ell-1}) \leq 0$, then $\text{Pot}(c_m, \ldots, c_\ell) > 0$ which is also a contradiction. Thus, P_ℓ satisfies **Rule 4**.

(2) **Rule 5**.
If $(c_m, \ldots, c_\ell)$ violates **Rule 5**, we would have that $c_t \in \{k+1, k+2\}$ where $c_s \in \pm\{k-1, k\}$ for $s \neq \ell$ and $c_\ell \in \{k, k+1\}$. Since $c_{\ell-1} = 0$, we have that $\text{sign}(c_m \cdot c_{\ell-1}) = 0$. Thus, we have that

$$\text{Pot}(c_m, \ldots, c_\ell) < -6.$$

Since $(c_m, \ldots, c_\ell)$ is a substring of $(c_m, \ldots, c_0)$, we have that $(c_m, \ldots, c_\ell)$ satisfies **Rule 5**. Hence, if $\text{sign}(c_m \cdot c_{i-1}) \geq 0$, then $\text{Pot}(c_m, \ldots, c_\ell) > -6$ which is a contradiction. If $\text{sign}(c_m \cdot c_{\ell-1}) < 0$, then $\text{Pot}(c_t, \ldots, c_\ell) > -4$ which is also a contradiction. Thus, P_ℓ must satisfy **Rule 5**.

(3) **Rule 6**.
If $(c_t, \ldots, c_\ell)$ violates **Rule 6**, we would have that $c_s \in \{k, k+1\}$ for $s \in \{t, \ell\}$ and $c_\ell \in \pm\{k-1, k\}$ otherwise. By definition of **Rule 6**, we have that

$$\text{Pot}(c_t, \ldots, c_\ell) \leq -3 - \text{sign}^+(c_t \cdot c_{t+1}).$$

However, $(c_t, \ldots, c_\ell)$ is a substring of P which implies that it satisfies **Rule 6**. If $\text{sign}(c_t \cdot c_\ell) \geq 0$, then $\text{Pot}(c_j, \ldots, c_\ell) > -3 - \text{sign}^+(c_t \cdot c_{t+1})$ which is a contradiction. If $\text{sign}(c_t \cdot c_{\ell-1}) < 0$, then $\text{Pot}(c_t, \ldots, c_\ell) \geq -1 - \text{sign}^+(c_t \cdot c_{t+1})$ which is also a contradiction. Thus, P_ℓ must satisfy **Rule 6**.

For the second statement, we may proceed using similar arguments as for the first statement. □

Proof of Theorem 24. Suppose that $F(X)$ represents $g = (x, t^n)$ with both non-trivial polynomial and principal parts. We first apply Proposition 23 to the principal part of $F(X)$ (namely, apply it to $X^{-1} \cdot F(X^{-1})$, we obtain $F'(X) = \sum_{i=l<0}^{M} B_i X^i$ which represents g. By applying Proposition 23 to the polynomial part, we obtain

$$G(X) = \sum_{i=0}^{M} C_i X^i + (C_{-1} + B_{-1})X^{-1} + \sum_{i=\ell}^{-2} B_i X^i.$$

If $C_{-1} = 0$, then we are done. If not, we have $C_0 C_{-1} < 0$ and $C_0 B_{-1} \geq 0$. Observe by Proposition 25 that $\sum_{i=\ell}^{-2} B_i X^i$ is n-reduced. By Corollary 21, we have that all rewriting rules for the principal parts are disjoint from the polynomial part except C_0. Rewriting using Proposition 23 on the principal part, we obtain a Laurent polynomial that is n-reduced on the principal part, and $C_0 C_{-1} < 0$ guarantees that the polynomial part is n-reduced as well. □

5. Stability of n-reduced polynomials

In this section, we attempt to count the number of all n-reduced polynomials. Intuitively, we start with $P = 0$ which is trivially n-reduced and keep adding 1 repeatedly until we

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

fail to have an n-reduced polynomial. By quantifying this failure, we classify all n-reduced polynomials with a non-negative leading coefficient. We start with a basic lemma.

Lemma 26. *Suppose that $P = (\ldots, c_1, c_0)$ is an n-reduced polynomial. Then $P+1$ is n-reduced or the rightmost minimal poison subword of $P+1$ contains either c_1 or c_0+1.*

Proof. This is clear from the fact that for any subword not containing c_1 and c_0, there is an identical subword in P. Since the subword follows all of the local and global rules applied on P, it never violates any of the rules. If there is no minimal poison subword of $P+1$ containing any of the coefficients, then $P+1$ is n-reduced. □

For each case, we define the following.

Definition 27. Suppose that $P = (\ldots, c_1, c_0)$ is an n-reduced polynomial where $P+1$ is not n-reduced.

- If the rightmost minimal poison subword contains c_1 but not c_0, we say $P+1$ fails to be n-reduced by a **sign change violation**.
- If the rightmost minimal poison subword contains c_0+1, we say $P+1$ fails to be n-reduced by a **potential value change violation**.

Suppose that P is n-reduced, but $P+1$ is not. This next proposition classifies all possibilities for P based on whether we have a sign change violation or a potential value change and what rule $P+1$ violates.

Proposition 28. *Suppose that P is an n-reduced polynomial of degree m and $P+1$ is not n-reduced. Then, P falls into one of these categories:*

- *Sign change violations*
  (1) *$P+1$ violates **Rule 1**.*
  In this case, $P = (-k-2, 0)$ and $n \leq 1$.

  (2) *$P+1$ violates **Rule 2**.*
  (i) *$P = (-k-1, 0)$ and $n > 1$.*
  (ii) *$P = (\ldots, c_2, -k-1, 0)$ and $c_2 < 0$.*
  (iii) *$P = (\ldots, c_2, -k, 0)$ and $c_2 \geq 0$.*

  (3) *$P+1$ violates **Rule 3**.*
  In this case, $P = (1, -k+1, 0)$ and $n \leq 1$.

  (4) *$P+1$ violates **Rule 4**.*
  For $P = (1, c_{m-1}, \ldots, c_1, 0)$, $m > n$, $c_1 = -k$ and
  $$\mathrm{Pot}(c_{m-1}, \ldots, c_1) = 1.$$

  (5) *$P+1$ violates **Rule 5**.*

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

For $P = (c_m, \ldots, c_1, 0)$, $m \geq n$, $c_1 = -k$ *and*

$$\mathrm{Pot}(c_m, \ldots, c_1) = -5.$$

(6) *If* $P+1$ *violates* **Rule 6**.
Let $P = (\ldots|A|0)$ *and* $(A) = (c_j, \ldots, c_1)$ *be the minimal poison subword of* $P+1$. *Then,* $c_1 = -k$ *and*

$$\mathrm{Pot}(A) = -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}).$$

- *Potential value change violations*

(1) $P+1$ *violates* **Rule 1**.
textrmin this case, $P = k+2$ *and* $n \leq 0$.

(2) $P+1$ *violates* **Rule 2**.
 (i) $P = k+1$, $n > 0$.

 (ii) $P = (\ldots, c_1, k+1)$, $c_1 \geq 0$.

 (iii) $P = (\ldots, c_1, k)$, $c_1 < 0$.

(3) $P+1$ *violates* **Rule 3**.
textrmin this case, $n \leq 0$, $P = (-1, k-1)$.

(4) $P+1$ *violates* **Rule 4**.
For $P = (-1, c_{m-1}, \ldots, c_0)$, $m > n$
 (i) $c_0 = k$ *and*

$$\mathrm{Pot}(c_{m-1}, \ldots, c_1) \in \{2, 3\}.$$

 (ii) $c_0 = k-1$ *and*

$$\mathrm{Pot}(c_{m-1}, \ldots, c_1) = 1.$$

(5) *If* $P+1$ *violates* **Rule 5**.
For $P = (c_m, \ldots, c_1, c_0)$, $m \geq n$
 (i) $c_0 = k-1$ *and*

$$\mathrm{Pot}(c_m, \ldots, c_1) = -5.$$

 (ii) $c_0 = k$ *and*

$$\mathrm{Pot}(c_m, \ldots, c_1) \in \{-4, -3\}.$$

(6) *If* $P+1$ *violates* **Rule 6**.
Let $(A|c_0) = (c_j, \ldots, c_1, c_0)$ *be the minimal poison subword of* $P+1$. *Then,*
 (i) $c_0 = k-1$ *and*

$$\mathrm{Pot}(A) = -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}).$$

 (ii) $c_0 = k$ *and*

$$\mathrm{Pot}(A) \in \{-1 - \mathrm{sign}^+(c_j \cdot c_{j+1}), -\mathrm{sign}^+(c_j \cdot c_{j+1})\}.$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Proof. We work out the case when the minimal poison subword for $P+1$ violates **Rule 6**. Denote the minimal poison subword as $(c_j, \ldots, c_\ell)$ Recall that **Rule 6** is violated if

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_\ell) < -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(c_j \cdot c_{\ell-1})$$

By Lemma 26, either $\ell = 0$ or $\ell = 1$.

(1) $\ell = 1$. In this case, $P+1$ contains a subword $(c_j, \ldots, c_1, c_0 + 1)$. From P, the potential of the subword $(c_j, c_{j-1}, \ldots, c_1)$ is

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_1) \geq -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(c_j \cdot (c_0))$$

but since it is the minimal poison subword of $P+1$, we also have

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_1) < -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}) - \tfrac{1}{2}\,\mathrm{sign}^+(c_j \cdot (c_0 + 1))$$

which can happen only when $c_0 = 0$ and $c_1 < 0$. Furthermore, we have $c_1 = -k$ or $-k-1$. (Note $c_1 = -k-1$ case is already included in Rule 2 violation.)

(2) $\ell = 0$. Again, $P+1$ contains a subword $(c_j, \ldots, c_1, c_0 + 1)$. From P, the potential of the subword $(c_j, c_{j-1}, \ldots, c_1, c_0)$ is

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_1, c_0) \geq -3 - \mathrm{sign}^+(c_j \cdot c_{j+1})$$

because $c_{-1} = 0$. But since it is minimal poison subword of $P+1$, we also have

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_1, c_0 + 1) < -3 - \mathrm{sign}^+(c_j \cdot c_{j+1})$$

which happens only when $c_0 > 0$, that is when adding 1 to the polynomial decreases the potential by 2. If $c_0 = k-1$, then the only possible value of the potential for the subword without c_0 is

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_1) = -2 - \mathrm{sign}^+(c_j \cdot c_{j+1}),$$

whereas if $c_0 = k$,

$$\mathrm{Pot}(c_j, c_{j-1}, \ldots, c_1) \in \{-1 - \mathrm{sign}^+(c_j \cdot c_{j+1}), -\mathrm{sign}^+(c_j \cdot c_{j+1})\}.$$

Other cases can be worked out similarly. □

We note there is a correspondence in these classifications which we shall exploit to reduce the number of cases we consider. We list these by providing a lemma.

Lemma 29. *For an $(n+1)$-reduced polynomial $P = XQ$, if $P+1$ is not $(n+1)$-reduced by a sign change violation for some global rule, then $-Q+1$ is not n-reduced by a potential value change violation for the same rule.*

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Proof. This can be done by simply comparing the conditions for each sign change violation in Proposition 28. Start with an $(n+1)$-reduced polynomial

$$P = (1, c_{m-1}, \dots, c_1, 0)$$

and suppose that $P+1$ violates Rule 4. The condition states that

$$\mathrm{Pot}(c_{m-1}, \dots, c_2, c_1) = 1, \quad c_1 = k.$$

This implies that

$$\mathrm{Pot}(c_{m-1}, \dots, c_2) = 2$$

which is precisely the condition for potential value change violation by Rule 4. For Rule 5, this case corresponds to 5) (ii) with potential -4, and for Rule 6, this corresponds to 6) (ii) with $Pot(A) = -1 - \mathrm{sign}^+(c_j \cdot c_{j+1})$. □

Therefore, in the later section, we will only select a few cases listed here to generate the entire list of n-reduced polynomials. In addition, once rewriting is triggered by a violation, since all rewriting rules for $P+1$ are disjoint (see Corollary 21), if there were to be another rewriting, the poison subword would fall into one of these categories as well. This allows us to break P into smaller pieces which we call *n-types* and *n-classes*.

6. n-Types and n-classes

In this section, we give the precise definition of n-types and n-classes. n-types and n-classes come from a list of cases from Proposition 28 and a list of generic cases, that is, the case when both P and $P+1$ are n-reduced. Intuitively, n-types tells us whether $P+1$ is n-reduced or not when P is n-reduced; if it fails to be n-reduced, it will be subdivided into n-classes using Proposition 28. n-classes serve another purpose here: they capture whether $XP+c$ is $(n+1)$-reduced or not when P is n-reduced. Since XP is always $(n+1)$-reduced by Proposition 25, the case when $XP+c$ is $(n+1)$-reduced can be classified using Proposition 28. More specifically, if $c=1$, then we can use the sign change violation; if $c=k$ or $k+1$, then we can use the potential change violation. The main reason we need both n-types and n-classes is that n-length is not the length that we are interested when computing the growth series for the group, rather, we need to count all n-reduced polynomials for all possible integer n. n-classes provides us a way to increment n from 0-reduced polynomial.

As mentioned after Proposition 28, there is a correspondence between sign change violations and potential value change violations, hence there is a reduction in cases. Here, we will primarily select polynomials whose leading coefficient is non-negative. Thus, we consider potential value change violation for **Rule 5** and **Rule 6**, and the sign change violations by **Rule 4**. Rule 2 will be considered as a degenerate case of **Rule 6**. **Rule 1** and **Rule 3** have only a finite number of cases, so those cases will appear in the base case, but not in the inductive definition of the n-types and n-classes.

We start with the generic case. If both P and $P+1$ are n-reduced and the constant coefficient of P is non-negative, we say P has n-interior type. If the constant coefficient of P is negative, then it follows that $P+1$ is also n-reduced, and we say P has n-negative

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

type. All other polynomials, i.e. when $P+1$ is not n-reduced, are said to have n-boundary type.

Now we discuss n-classes. We begin with the **stable** n-class, denoted as n-class S. This class consists of n-reduced polynomials $P(X)$ such that for any positive c, the rightmost minimal poison subword of $XP(X)+c$ is disjoint from the subword corresponding to $XP(X)$. Necessarily, $P+1$ is n-reduced whenever P has n-class S. These are the most common n-reduced polynomials. The class splits into 3 separate sub-classes S_-, S_0 and S_+ depending on the sign of the constant coefficient.

Violations	Corresponding n-class	Related n-classes
Sign Change, **Rule 4**	E_1	E_2, E_3
Potential Change, **Rule 5**	U^t_{-3}, U^t_{-4}, U^t_{-5}	
Potential Change, **Rule 6**	U_0, U_{-1}, U_{-2}	

Generic classes: S_-, S_0, S_+.

The opposite of the stable n-class is the **unstable** n-class which we write as n-class U. These are the polynomials $P(X)$ where the rightmost minimal poison subword of $XP(X)+c$ violates some global rule for some positive c. These violations are classified in Proposition 28.

Consider a n-reduced polynomial P. Suppose that $XP(X)+k+1$ is not $(n+1)$-reduced by violating **Rule 6** by a potential value change, but $XP(X)+k$ is $(n+1)$-reduced. By Proposition 28, we know that the rightmost minimal poison subword excluding the constant coefficient will have either potential $-\operatorname{sign}^+(c_j \cdot c_{j+1})$ or $-1-\operatorname{sign}^+(c_j \cdot c_{j+1})$. We notice that $XP(X)+k$ also satisfies the condition for the unstable $(n+1)$-class.

For a n-reduced polynomial P, if $XP(X)+k$ is not $(n+1)$-reduced by violating **Rule 6** by a potential value change but $XP(X)+k-1$ is $(n+1)$-reduced, then by Proposition 28, we know that the rightmost minimal poison subword excluding the constant coefficient will have potential $-2-\operatorname{sign}^+(c_j \cdot c_{j+1})$. Again, $XP(X)+k-1$ will be in the unstable $(n+1)$-class.

We split the unstable n-class into sub-classes U_0, U_{-1}, and U_{-2} by their truncated potential of the rightmost minimal poison subword being $-\operatorname{sign}^+(c_j \cdot c_{j+1})$, $-1-\operatorname{sign}^+(c_j \cdot c_{j+1})$, and $-2-\operatorname{sign}^+(c_j \cdot c_{j+1})$, respectively. As observed, multiplying X and adding either k or $k-1$ to P in the unstable n-class will give us a new polynomial in the unstable $(n+1)$-class with a different potential value.

We follow a similar kind of logic to classify n-reduced polynomials. For **Rule 5** in Proposition 28, We will define n-classes U^t_{-3}, U^t_{-4} and U^t_{-5} where the subscript denotes the potential. For **Rule 4**, we will define n-classes E_1, E_2, and E_3. Note that the U^t classes and the E classes are both associated with top rules.

Definition 30 (Base case). Let Q be an integer linear polynomial with a non-negative leading coefficient. The n-class and n-type of Q are given as follows:

- (n**-initial type**) $n \le 0$, $Q=0$.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

- (n**-interior type**) if $Q = dX + c$, and
  $n > 0$. Then $Q = 0$ has n**-class** S_0.

  $d = 0$, $0 < c \le k$, and $n \le 0$. Then Q has n**-class** S_+.

  $d = 0$, $c = k + 1$, and $n \le 0$. Then Q has n**-class** U^t_{-3}.

  $d = 0$, $0 < c \le k - 1$, and $n > 0$. Then Q has n**-class** S_+.

  $d = 0$, $c = k$, and $n > 0$. Then Q has n**-class** U_0.

- (n**-negative type**) if $Q = dX + c$, and
  $d = 1$ and $c = -k + 1$. Then Q has n-class E_1 if $n \le 0$.

  $d = 1$ and $c = -k + 2$. Then Q has n-class E_3 if $n \le 0$.

- (n**-boundary type**)
  If $n \le 0$. Then $Q = k + 2$ has n**-class** U^t_{-5}.

  If $n > 0$. Then $Q = k + 1$ has n**-class** U_{-2}.

We define types and classes for polynomials with a non-negative leading coefficient.

Definition 31. Suppose that $Q(X) = XP(X) + c$ is an n-reduced polynomial whose leading coefficient is positive where $P(X) \neq 0$ and c is constant.

- (n**-interior type**) if
  - For any P and $0 < c \le k - 2$, Q has n-class S_+.
  - P has any $(n-1)$-class except E_1 and $-P$ does not have $(n-1)$-class U_{-2} and $c = 0$. Then Q has n-class S_0.
  - P has $(n-1)$-class S_0, S_+, U_0, or U^t_{-3} and $c = k - 1$. Then Q has n-class S_+.
  - P has $(n-1)$-class U_{-1} and $c = k - 1$. Then Q has U_0.
  - P has $(n-1)$-class S_0 or S_+ and $c = k$. Then Q has n-class U_0.
  - P has $(n-1)$-class S_-, E_1, E_2, or E_3 and $c = k - 1$. Then Q has n-class U_0.
  - P has $(n-1)$-class U^t_{-4} and $c = k - 1$. Then Q has n-class U^t_{-3}.
- (n**-negative type**) if
  - P has $(n-1)$-class E_1 and $c = -k + 1$. Then Q has n-class E_2.
  - P has $(n-1)$-class E_2 and $c = -k + 1$. Then Q has n-class E_3.
  - P has $(n-1)$-class E_3 and $c = -k + 1$. Then Q has n-class S_-.
  - P has $(n-1)$-class E_2 and $c = -k$. Then Q has n-class E_1.
  - P has $(n-1)$-class E_3 and $c = -k$. Then Q has n-class E_2.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

  - $c < 0$. Then Q has n-class S_- unless otherwise stated above.

- (n**-boundary type (P)**) if
  - P has $(n-1)$-class U_{-2} and $c = k-1$. Then Q has n-class U_{-1}.
  - P has $(n-1)$-class U^t_{-5} and $c = k-1$. Then Q has n-class U^t_{-4}.
  - P has $(n-1)$-class U_{-1} and $c = k$. Then Q has n-class U_{-2}.
  - P has $(n-1)$-class U^t_{-4} and $c = k$. Then Q has n-class U^t_{-5}.
  - P has $(n-1)$-class U_0 and $c = k$. Then Q has n-class U_{-1}.
  - P has $(n-1)$-class U^t_{-3} and $c = k$. Then Q has n-class U^t_{-4}.
  - P has $(n-1)$-class S_-, E_1, E_2, or E_3 and $c = k$. Then Q has n-class U_{-2}.
  - P has $(n-1)$-class S_+ or S_0 and $c = k+1$. Then Q has n-class U_{-2}.

- (n**-boundary type (S)**) if
  - P has $(n-1)$-class S_- such that $-P$ has $(n-1)$-class U_{-2} and $c = 0$. Then Q has n-class S_0.
  - P has $(n-1)$-class E_1 and $c = 0$. Then Q has n-class S_0.

Remark 32. Although we gave our definitions recursively, it is straightforward to prove inductively that these do correspond to the cases in Proposition 28. For example, if P has n-boundary type (P) and n-class U_{-1}, then:

- $P = (\ldots|A)$ with $A = (c_j, \ldots, c_0)$ and $\mathrm{Pot}(A) = -1 - \mathrm{sign}^+(c_j \cdot c_{j+1})$,
- $P+1$ is not n-reduced and its minimal poison subword is $A' = (c_j, \ldots, c_1, c_0+1)$,
- $XP + k + 1$ will violate **Rule 6** by a potential violation as described in Proposition 28.

From Proposition 28, it is also easy to check that the n-classes form a partition of all n-reduced polynomials. We record this as lemma.

Lemma 33. *For each n, the n-classes form a partition of all n-reduced polynomials with non-negative leading coefficient.*

7. Successor function

Previously, we have classified any n-reduced polynomial P into n-types and n-classes using an inductive definition. The definition relied on whether $P+1$ is n-reduced and $XP+C$ is $(n+1)$-reduced. While the classification is complete, the definitions for S_0 and S_- are not descriptive enough to give the growth series on its own, and we develop a tool to bypass that.

In this section, we will define the successor of a polynomial to generate all n-reduced polynomials with a non-negative leading coefficient. We will add 1 consecutively to the

n-reduced polynomial until it is no longer n-reduced. When $P(X)+1 \in \mathbb{Z}[X]$ is not n-reduced, Proposition 23 will give us a new polynomial

$$Q(X) = \sum_{i=0}^{d} c_i X^i + c_{-1}X^{-1}$$

where $c_{-1} = 0$ or 1. By Proposition 25, we know that $Q(X) - X^{-1} = \sum_{i=0}^{d} c_i X^i \in \mathbb{Z}[X]$ is also n-reduced. Intuitively, we want to define this to be the **successor** of $P(X)$. However, in some cases, $Q(X) - X^{-1} - 1$ is also n-reduced, and to make sure that the successor function maps onto the set of n-reduced polynomials, we instead define $Q(X) - X^{-1} - 1$ to be the successor of $P(X)$ (see (3) in the formal definition).

Definition 34. Let P be an n-reduced polynomial. The **successor** of P, denoted $\mathcal{S}(P)$, is given by the following:

(1) If P has n-initial, n-interior, or n-negative type, then $\mathcal{S}(P) = P + 1$.

(2) If P has one of the boundary types in the base case, we define the successor as follows. (Note that this is a special case of 3) below.)

P	$\mathcal{S}(P)$
$k+2$ and $n \leq 0$	$X - k + 1$
$k+1$ and $n > 0$	$X - k$

(3) Suppose that P has n-boundary type (P) and n-class U_{-2} or U^t_{-5}. Letting Q be the rewriting of $P+1$ given by Proposition 23, we then set $\mathcal{S}(P) = Q - 1 - X^{-1}$.

(4) Suppose that P has n-boundary type (P) and n-class U_{-1} or U^t_{-4}. Letting Q be the rewriting of $P+1$ given by Proposition 23, we then set $\mathcal{S}(P) = Q - X^{-1}$.

(5) If P has n-boundary type (S), then $\mathcal{S}(P)$ is defined to be the rewriting of $P+1$ given by Proposition 23.

If $\mathcal{S}(P) = P + 1$, it is called a **regular successor**. Otherwise, it is called an **irregular successor**.

It is clear in the definition that $\mathcal{S}(P)$ is n-reduced when it is a regular successor. For irregular successors, as an example, we show that $\mathcal{S}(P)$ is n-reduced when P has n-class U_{-2}. If $P = XR(X) + k$ and $R(X)$ has n-class S_-, or $P = XR(X) + k + 1$ and R has n-class S_0 or n-class S_+, then $P + 1$ violates **Rule 2**. Thus, it can be checked easily that $\mathcal{S}(P)$ is n-reduced. If $P = XR(X) + k$ and R has n-class U_{-1}, there exists d such that

$$P = X^{d+1}B + XA + k$$

where B has stable n-type and $(A|k+1)$ is the rightmost minimal poison subword of $P+1$. After rewriting $P+1$ and subtracting $1 + X^{-1}$, we have $\mathcal{S}(P) = X^{d+1}(B+1) + XA' - k$.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

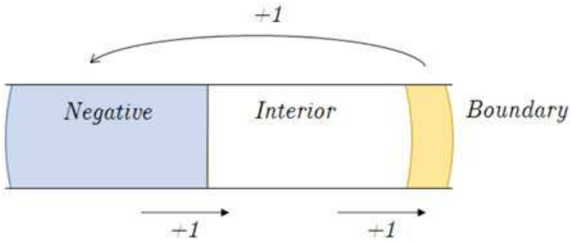

Figure 5. As we add one to our reduced polynomial, we move from the n-negative type (blue region) to the n-interior type (white region). Finally, as we reach the end of the interior region, we reach the n-boundary types (yellow region).

Given that

$$\begin{aligned} \mathrm{Pot}(A) &= -2 - \mathrm{sign}^+(c_d \cdot c_{d+1}) \\ \mathrm{Pot}(A') &= -(-2 - \mathrm{sign}^+(c_d \cdot c_{d+1})) - 2 \\ &= \mathrm{sign}^+(c_d \cdot c_{d+1}) = -\,\mathrm{sign}^+(c'_d \cdot c'_{d+1}) \end{aligned}$$

and for any subword adjacent to $(-k)$ not containing c'_d we also have

$$\mathrm{Pot}(c_d \dots c_j) > -3 - \mathrm{sign}^+(c_d \cdot c_{d+1}),$$

it then follows that

$$\mathrm{Pot}(c_j \dots c_1) \leq 0.$$

Thus, $\mathrm{Pot}(c'_j \dots c'_1) \geq 0$. Since the potential for A' and of any subword of A' is bounded below, we conclude that $\mathcal{S}(P)$ cannot violate **Rule 6**.

Denote the set of polynomials with a non-negative leading coefficient $\mathcal{R}^+$. First, we show that the successor function is a bijection from $\mathcal{R}^+ \cup \{0\}$ onto $\mathcal{R}^+$. See Figure 5.

Proposition 35. *The successor function is a bijection from* $\mathcal{R}^+ \cup \{0\}$ *onto* $\mathcal{R}^+$.

Proof. We show this by showing there is an inverse function $\mathcal{S}^{-1}(P)$, which will be constructed by applying the successor on $-P$.

Since $-P$ can have a negative leading coefficient, only for this proof, we add new n-types to Definition 30 and Definition 31. For the base case, suppose that c is a negative integer. We say c has n-class S_- when $|c| \leq k+1$ and $n > 0$, or $|c| \leq k+2$ and $n \leq 0$. For *any* n-reduced polynomial, we define n-classes and n-types inductively following Definition 31.

Now we define the extension $\tilde{\mathcal{S}}$ of the successor for any n-reduced polynomial. For polynomials with negative leading coefficients, the successor prescribed in Definition 34 will always give an n-reduced polynomial with few exceptions, which can be observed from the potential change violations by **Rule 4** and the sign change violations by **Rule 5** in Proposition 28. We add two cases of irregular successors.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

(1) If P has n-class $-E_2$, we let Q be the rewriting of $P+1$ given by Proposition 23, we then set $\tilde{\mathcal{S}}(P) = Q - X^{-1}$. When P has n-class $-E_1$, we then define $\tilde{\mathcal{S}}(P) = Q - 1 - X^{-1}$

(2) If $P = XR$ and R has $(n-1)$-class $-U^t_{-5}$, then $\tilde{\mathcal{S}}(P)$ is the rewriting of $P+1$ given by Proposition 23.

We see that this extension now is well defined. We first show that $\S^{-1}(\mathcal{S}(P)) = P$ for each case from Definition 34.

Suppose that $\mathcal{S}$ is a regular successor for P. In order for the identity to hold, we need $-(\mathcal{S}(-P-1)) = P$, or equivalently, $\mathcal{S}(-P-1) = -P$. When P has n-initial, n-interior type, since $-P-1$ has n-negative type, the identity holds.

Now suppose that P has n-negative type. We show that $-P-1$ always has n-interior type. We begin with the base cases

n-class of P	$-P-1$	n-class of $-P-1$	n-class of $-P$	n
E_1	$-X+k-2$	S_+	U_0	$n \leq 1$
E_3	$-X+k-3$	S_+	S_+	$n \leq 1$
S_-	$0 < c \leq k$	S_0, S_+ or U_0	S_+, U_0 or U_{-2}	$n > 0$
S_-	$0 < c \leq k+1$	S_0, S_+ or U^t_{-3}	S_+, U^t_{-3} or U^t_{-5}	$n \leq 0$

.

Thus, the claim is true for the base case. Now, in general, if $P = XR + c$, then

n-class of P	$(n-1)$-class of R	$-R$	$c' = -c-1$	$-P-1$
E_2	E_1	U_0	$k-2$	S_+
E_3	E_2	S_+	$k-2$	S_+
S_-	E_3	S_+	$k-2$	S_+
E_1	E_2	S_+	$k-1$	S_+
E_2	E_3	S_+	$k-1$	S_+
S_-	S_0	S_0	$0 \leq c' \leq k$	S_0, S_+, U_0
S_-	$*$	S_-	$0 \leq c' \leq k-1$	S_0, S_+, U_0

.

Working out each case directly shows that $\mathcal{S}(-P-1) = -P$ as desired except when P has n-class S_- and R has $(n-1)$-class S_-. We note that since P is n-reduced, $-R$ having n-class U_{-2} can be ruled out. Furthermore, $-P$ needs to be n-reduced, significantly reducing the number of cases to be considered. In this case, working out explicitly we see that

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

class of P	$-R$	$c' = -c-1$	$-P-1$
S_-	S_+	$0 \le c' \le k$	S_+, U_0
S_-	U_0	$0 \le c' \le k-1$	S_+
S_-	U_{-1}	$0 \le c' \le k-1$	S_+, U_0
S_-	U^t_{-3}	$0 \le c' \le k$	S_+
S_-	U^t_{-4}	$0 \le c' \le k-1$	S_+, U^t_{-3}
S_-	U^t_{-5}	$0 \le c' \le k-2$	S_+

.

Hence, the successor for $-P-1$ is regular.

Now suppose that $\mathcal{S}$ is irregular. For the base case, the identity holds trivially by construction. Let P have n-class U^t_{-4} or U^t_{-5}. It is easy to check that $\mathcal{S}(P)$ has n-class E_2 and E_1, respectively. For $-\mathcal{S}(P)$, by construction of the generalized successor, $\tilde{\mathcal{S}}(-\mathcal{S}(P)) = P$ as required.

Now let P have n-class U. For the base case, we check when $P = XR + c_0$ has n-class U_{-2} where R has n-class S or E. For the recursive case, there exists a smallest $d > 2$ such that

$$P = X^d B + XA + c_0$$

where B has $(n-d)$-class S or E and A is a degree $d-2$ polynomial. Denote $P = (B|A|c_0)$. By choice of d, $XA + c_0 + 1$ corresponds to the rightmost minimal poison subword of $P+1$.

n-class of P	Pot(A)	c_0	$-c'_0$	n-class of $-\mathcal{S}(P)$
U_{-2}	$-2 - \text{sign}^+(c_j \cdot c_{j+1})$	k	k	U_{-2}
U_{-1}	$-1 - \text{sign}^+(c_j \cdot c_{j+1})$	k	k	U_{-1}
U_{-1}	$-1 - \text{sign}^+(c_j \cdot c_{j+1})$	$k-1$	$k-1$	U_{-1}

We observe that $-\mathcal{S}(P)$ can only have n-class U and that the rightmost minimal poison subword for $-\mathcal{S}(P)$ can only be on the same position as A. The rewriting rule for $-\mathcal{S}(P)$ is identical to the rewriting rule for P, and thus, the identity holds.

For n-boundary (S), let $Q = XP$ where P has $(n-1)$-class of E_1. $\mathcal{S}(Q)$ is also of the form XR where R has $(n-1)$-class $-U^t_{-5}$, and the identity follows from construction of the generalized successor. When $Q = XP$ and P has $(n-1)$-class $-U_{-2}$, one can observe $-\mathcal{S}(Q)$ also has n-boundary (S) which completes the proof.

The other direction $\mathcal{S}(\mathcal{S}^{-1}(P)) = \mathcal{S}(-\mathcal{S}(-P))$ follows from symmetry. □

Proposition 36. *Suppose P is an n-reduced polynomial with non-negative leading coefficient that represents x.*

(1) *If P has n-initial type, then $L_n(\mathcal{S}(P)) = L_n(P) + 1$ and $\mathcal{S}(P)$ represents $x + b$.*

(2) *If P has n-interior type, then $L_n(\mathcal{S}(P)) = L_n(P) + 1$ and $\mathcal{S}(P)$ represents $x + b$.*

(3) *If P has n-negative type, then $L_n(\mathcal{S}(P)) = L_n(P) - 1$ and $\mathcal{S}(P)$ represents $x + b$.*

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

(4) *If $P \in U^t_{-5}$ or $P \in U_{-2}$, then $L_n(\mathcal{S}(P)) = L_n(P)$ and $\mathcal{S}(P)$ represents $x - a$.*

(5) *If $P \in U^t_{-4}$ or $P \in U_{-1}$, then $L_n(\mathcal{S}(P)) = L_n(P)$ and $\mathcal{S}(P)$ represents $x + b - a$.*

(6) *If P has n-boundary type (S), then $L_n(\mathcal{S}(P)) = L_n(P)$ and $\mathcal{S}(P)$ represents $x + b$.*

Proof. We will only prove the case when $P \in U_{-2}$. The other cases can be proved similarly.

Suppose $P \in U_{-2}$. We then have $P = (\ldots|A)$ for some A with degree d and potential $-2 - \operatorname{sign}^+(c_j \cdot c_{j+1})$. The rewriting of $P + 1$ is by subtracting $(X^d + X^{d-1} + \ldots + 1)$ $(X - (2k+1) + X^{-1})$, and thus, we may write $\mathcal{S}(P)$ as

$$
\begin{aligned}
&P + 1 + (X^d + X^{d-1} + \ldots + 1)(X - (2k+1) + X^{-1}) - 1 - X^{-1} \\
&\quad = P + 1 + (X^{d+1} - 2kX^d - (2k-1)X^{d-1} - \ldots - (2k-1)X - 2k + X^{-1}) - 1 - X^{-1} \\
&\quad = P + (X^{d+1} - 2kX^d - (2k-1)X^{d-1} - \ldots - (2k-1)X - 2k) \\
&\quad = P + X^{d+1} - X^d - 1 - (2k-1)(X^d + X^{d-1} + \ldots + X + 1).
\end{aligned}
$$

Recall that the potential of a coefficient is exactly the length change when adding $2k - 1$. Therefore, the length difference in the last $d + 1$ digits of P and $\mathcal{S}(P)$ is $-2 - \operatorname{sign}^+(c_j \cdot c_{j+1}) + 2 = -\operatorname{sign}^+(c_j \cdot c_{j+1})$, which with $c_{j+1} > 0$, is exactly the opposite of the effect X^{d+1} has on the length change. Thus, $L_n(\mathcal{S}(P)) = L_n(P)$. We also have $\mathcal{S}(P)$ represents $x - a$ which follows from the fact that rewriting does not change the element the polynomial represents and that X^{-1} represents a. □

For a Laurent polynomial $F(X)$, we will write $\overline{F}(X) = X^{-1} \cdot F(X^{-1})$. We define the successor function on its principal part $Q(X)$ dually to the polynomial part, i.e., the n-successor of $Q(X)$ is $\overline{\mathcal{S}(\overline{Q}(X^{-1})}$, where $\mathcal{S}$ is the $(-n)$-successor function.

Our main interest is in counting minimal length group elements, not n-reduced polynomials. Therefore, we need to count the number of n-minimal polynomials that represent any group element and to take care over the overcount. Therefore, suppose $F(X) = \sum_{j=-p}^{q} c_j X^j$ represents x, and write its polynomials and principal parts as $P(X)$ and $Q(X)$, respectively. In the next Lemma, we show that we can write $P(X) = \pm\mathcal{S}^n(0)$ and $\overline{Q}(X) = \pm\mathcal{S}^m(0)$. Thus, $(\pm\mathcal{S}^n(0)| \pm \overline{\mathcal{S}^m(0)})$ represents x. However, for a fixed x, there may be more than one way to write it as $(\pm\mathcal{S}^n(0)| \pm \overline{\mathcal{S}^m(0)})$. To quantify this, we will also need the *proof* of the following lemma.

We view the sequence $\{\mathcal{S}^i(0)\}$ of successive polynomials as a sequence of points g_i which they represent in $\mathbb{Z}^2 = \langle a, b\rangle$, and the successor corresponds to moving in either b, $-a$ or $b - a$ direction depending on the type. Note that if $\overline{Q}(X)$ represents $ka + tb$ then $Q(X)$ represents $ta + kb$. We state the lemma in a slightly more general setting.

Lemma 37 (Spanning lemma). *Let $G = \langle a, b\rangle$ be a free abelian group. Suppose there exists an infinite sequence $\{g_i\} \subset G$ such that $g_0 = 0$, $g_1 = b$ and $g_{i+1} \in \{g_i + b, g_i + b - a, g_i - a\}$. Moreover, assume that if $g_{i+1} - g_i \in \{b - a, -a\}$, then $g_{i+2} - g_{i+1} = g_{i+3} - g_{i+2} = b$. We also define $\{h_i\}$ such that if $g_i = ka + tb$, then $h_i = ta + kb$. Then for all $\gamma \in G$, there exist $i, j \in \mathbb{N}$ such that $\gamma = \pm g_i \pm h_j$.*

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

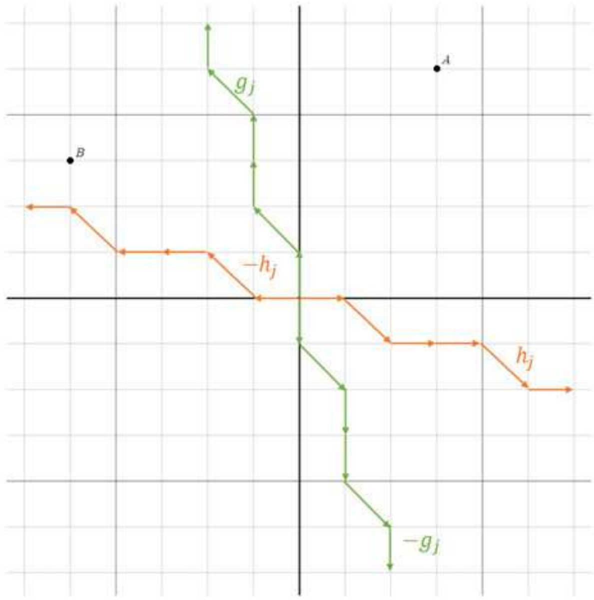

Figure 6. For point A, there is some (i, j) such that $g_i + h_j$ represents A. For point B, the representative to look for is $g_i - h_j$. Instead of actually finding (i, j), we increment by $\pm a$ and $\pm b$ from a known pair.

Proof. We first prove that if some γ is a sum of some g_i and h_j, then any $\gamma + ma + nb$ is also for any $m, n \in \mathbb{N}$. We proceed by induction on n and m. Suppose that $\gamma = g_i + h_j$. We first need to find a pair (i', j') such that $\gamma + b = g_{i'} + h_{j'}$. If $g_{i+1} = g_i + b$, we are done. If $g_{i+1} = g_i + (b - a)$, then

$$\begin{aligned} g_{i+1} + h_{j+1} &= g_i + (b-a) + h_j + (a), \\ g_{i+2} + h_{j+2} &= g_i + (b-a) + (b) + h_j + (-b) + (a), \text{ or} \\ g_{i+2} + h_{j+2} &= g_i + (b-a) + (b) + h_j + (a-b). \end{aligned}$$

On the other hand, if $g_{i+1} = g_i + (-a)$, then

$$\begin{aligned} g_{i+2} + h_{j+1} &= g_i + (-a) + (b) + h_j + (a), \\ g_{i+2} + h_{j+2} &= g_i + (b-a) + (b) + h_j + (-b) + (a), \text{ or} \\ g_{i+3} + h_{j+2} &= g_i + (-a) + (b) + (b) + h_j + (-b) + (a). \end{aligned}$$

We observe that by the symmetry between g_i and h_i, the a's can be incremented in the same manner. This proves the lemma for elements in $\{g_i + ma\} \cup \{h_j + nb\}$, i.e., the upper-right region cut out by the trajectories of g_i and h_i (see Figure 6). By switching signs, any element in $\{-g_i - ma\} \cup \{-h_j - nb\}$ can be expressed as $-g_i - h_j$ as well.

By symmetry, this leaves out the case when $\gamma \in \{g_i - ma\} \cap \{-h_j + nb\}$. We will show that such γ can be written as $g_i - h_j$ for some $i, j \in N$. By induction, let $\gamma = g_i - h_j$ for

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

$j > 1$. We need to find a pair (i', j') such that $\gamma + b = g_{i'} - h_{j'}$ where $i' > i$ and $j' < j$. If $g_{i+1} - g_i = b$, then $\gamma + b = g_i - h_j$, and we are done. If $g_{i+1} - g_i = b - a$, then either

$$g_{i+1} - h_{j-1} = g_i + (b-a) - h_j + (a),$$
$$g_{i+2} - h_{j-1} = g_i + (b-a) + (b) - h_j + (a-b), \text{ or}$$
$$g_{i+2} - h_{j-2} = g_i + (b-a) + (b) - h_j + (-b) + (a) \quad (j > 1)$$

where the last case only appears when $j \geq 2$ as $h_1 = a$. On the other hand, if $g_{i+1} - g_i = -a$, then either

$$g_{i+1} - h_{j-1} = g_i + (-a) + (b) - h_j + (a),$$
$$g_{i+3} - h_{j-1} = g_i + (-a) + (b) + (b) - h_j + (a-b), \text{ or}$$
$$g_{i+3} - h_{j-2} = g_i + (-a) + (b) + (b) - h_j + (-b) + (a). \quad (j > 1)$$

When $j = 0$, $\gamma = g_i$ and $\gamma + b$ will either be g_{i+1} or is covered by the first case of the proof. Hence, any element in the set $\{g_i - ma\} \cap \{-h_j + nb\}$ can be expressed as a difference $g_i - h_j$. By symmetry, this can be done for the set $\{-g_j + ma\} \cap \{h_j - nb\}$. □

For counting, we need to know how many representatives of a single γ exist. We use the same framework as in Lemma 37 to figure out all the cases and then find the appropriate types and classes in relation to the successor function.

As in the lemma, we first look at the sum of two sequences g_i and h_j. We find all possible pairs of sequences satisfying

$$g_i + h_j = g_{i'} + h_{j'}.$$

Equivalently, we can find sequences with weaker conditions whose sum is 0. Here we only require $-a$ and $b - a$ to be followed by two consecutive b's in the sequence $\{g_i\}$ and a similar requirement for the sequence $\{h_j\}$. When any of two sequences is long, the b's (or a's) dominate the sequence. Hence, it suffices to look at combinations shorter than 3 symbols:

$$\begin{aligned} 0 &= (-a) + (a) = (b) + (-b) = (b-a) + (a-b) \\ &= (b-a) + (a + (-b)) = (b-a) + ((-b) + a) \\ &= (b + (-a)) + (a + (-b)) = ((-a) + b) + ((-b) + a) = (b + (-a)) + ((-b) + a) \\ &= ((-a) + b) + (a + (-b)). \end{aligned}$$

Now we consider the Laurent polynomial $F(X) = \sum_{j=-p}^{q} c_j X^j$ that represents γ, and write its polynomials and principal parts as $P(X)$ and $\overline{Q}(X)$, respectively. Suppose both P and $\overline{Q}$ have non-negative leading coefficients. For $n \geq 0$, when P is an n-reduced polynomial and $\overline{Q}$ is a $(-n)$-reduced polynomial, we have P representing some g_i and Q representing some h_j and $x = g_i + h_j$. Thus, the overcountings are in the form $g_i + h_j = g_{i'} + h_{j'}$, and based on the discussion above and Prop 36 can now be classified in terms of types and classes.

$(P|\overline{Q}) = (\mathcal{S}(P)|\overline{\mathcal{S}(Q)})$ occurs when

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

n-classes of P	$(-n)$-classes of $\overline{Q}$
U_{-2}, U^t_{-5}	0, $S_\bullet$, U_0, $E_\bullet$, U^t_{-3}
0, $S_\bullet$, $E_\bullet$, U_0, U^t_{-3}	U_{-2}, U^t_{-5}
U_{-1}, U^t_{-4}	U_{-1}, U^t_{-4}

.

Similarly, $(P|\overline{Q}) = (\mathcal{S}(P)|\overline{\mathcal{S}^2(Q)})$ occurs when

n-classes of P	$(-n)$-classes of $\overline{Q}$	$(-n)$-classes of $\overline{\mathcal{S}(Q)}$
U_{-1}, U^t_{-4}	U_0, U^t_{-3}	U_{-2}, U^t_{-5}
U_{-1}, U^t_{-4}	U_{-2}, U^t_{-5}	S_-, $E_\bullet$

.

And finally, $(P|\overline{Q}) = (\mathcal{S}^2(P)|\overline{\mathcal{S}^2(Q)})$ can be classified.

P	$\mathcal{S}(P)$	$\overline{Q}$	$\overline{\mathcal{S}(Q)}$
U_0, U^t_{-3}	U_{-2}, U^t_{-5}	U_0, U^t_{-3}	U_{-2}, U^t_{-5}
U_{-2}, U^t_{-5}	S_-, $E_\bullet$	U_{-2}, U^t_{-5}	S_-, $E_\bullet$
U_0, U^t_{-3}	U_{-2}, U^t_{-5}	U_{-2}, U^t_{-5}	U_0, U^t_{-3}
U_{-2}, U^t_{-5}	S_-, $E_\bullet$	U_0, U^t_{-3}	U_{-2}, U^t_{-5}

.

Now we consider the case when P is positive and $\overline{Q}$ is negative, so $P+Q$ represents $x = g_i - h_j$:

$$b = (b) - 0 = 0 - (-b) - a = (-a) - 0 = 0 - (a)$$
$$b - a = (b - a) - 0 = 0 - (a - b).$$

In terms of the successor, this corresponds to

$$(\mathcal{S}(P)|\overline{Q}) = (P|\overline{\mathcal{S}(Q)}),$$

and the possible classes for P and Q are described below.

n-classes of P	$(-n)$-classes of $\overline{Q}$
0, $S_\bullet$, U_0, $E_\bullet$, U^t_{-3}	0, $S_\bullet$, U_0, $E_\bullet$, U^t_{-3}
U_{-2}, U^t_{-5}	U_{-2}, U^t_{-5}
U_{-1}, U^t_{-4}	U_{-1}, U^t_{-4}

8. Growth series for n-reduced polynomials

For the reader's convenience, we give a brief summary here. We begin with the main theorem of this article.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Main Theorem. *Let* $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 2k+1 \end{smallmatrix}\right] \in SL(2, \mathbb{Z})$ *where* $2k+1 \geq 5$. *Then* $\mathbb{Z}^2 \rtimes_A \mathbb{Z}$ *has rational growth with respect to the standard generating subset.*

Recall that for any group element $g = (x, t^n) \in \mathbb{Z}^2 \rtimes_A \mathbb{Z}$, we represent this element by a Laurent polynomial $P(X)$, and $\|g\|$ is calculated by the n-length L_n. If

$$P(X) = \sum_{j=-p-1}^{q} c_j X^j,$$

then n-length L_n is defined as

$$L_n(P) = \|g\| = 2p + 2q - |n| + \sum_{j=-p-1}^{q} |c_j|$$

where $p \geq \max\{0, -n\}$ and $q \geq \max\{0, n\}$. Here we assumed the polynomial had zero as its coefficients on both ends if these two conditions are not met. $P(X)$ with minimal n-length is called the n-minimal polynomial. Instead of working with n-minimal polynomials, we defined n-reduced polynomials using a list of rules given in Definition 8.

In Theorem 24, we showed that any n-minimal polynomial can be rewritten as a sum of a polynomial part and a principal part, both of which are n-reduced. So once the growth series for all n-reduced polynomials are set up, the growth series for n-minimal polynomials can be deduced with possible multiplicities.

For the growth series of n-reduced polynomials, we focus on the polynomials with non-negative leading coefficient, as we can easily deduce the series for the polynomial P with negative leading coefficient by looking at $-P$ instead.

For an n-reduced polynomial P, it may be the case that $P + 1$ is not n-reduced; we gave a full classification in Proposition 28. Using this, we divided all n-reduced polynomials into n-types and n-classes in Definition 30 and Definition 31. In this section, each n-type and the degree of a polynomial will serve as a *state*. For any P in that state, we will quantify the state for $XP + C$; this will play the role of transition between two states. Since we know specifically how much length is changed when the successor is applied, we can explicitly write down the transition as a matrix as well as its impact to the generating series.

Since conditions given in Definition 30 and Definition 31 are not descriptive enough, we define a function called the successor (Definition 34). We show we can obtain all n-reduced polynomials with non-negative leading coefficient by starting from 0 and applying the successor function repeatedly, which is shown to be injective (Proposition 35) and spans all polynomials (Lemma 37). This allows us to count other n-types by looking at the image of the successor instead. In the same lemma, we also listed a finite number of ways to represent the same element where both polynomial and principal parts are n-reduced. From this, we can conclude that once the generating functions for each types are rational, the growth of the group is rational.

We begin by defining the generating function for polynomials having a given n-class of degree d with a non-negative leading coefficient and use the inductive definition given in Definition 30 and Definition 31 to find the recursive relation using the following table.

Definition 38. We denote the generating function having the stable n-classes with given degree as follows

Stable n-class S_+	$S_+^{n,d} = \sum_{P \in S_+, \deg(P)=d} t^{L_n(P)}$
Stable n-class S_0	$S_0^{n,d} = \sum_{P \in S_0, \deg(P)=d} t^{L_n(P)}$
Stable n-class S_-	$S_-^{n,d} = \sum_{P \in S_-, \deg(P)=d} t^{L_n(P)}$

We denote the sum of generating functions for all polynomials of degree d having stable n-classes as

$$S^{n,d}(t) = S_0^{n,d}(t) + S_+^{n,d}(t) + S_-^{n,d}(t).$$

We also introduce the vector notation for the generating function:

$$\vec{S}^{n,d}(t) = \begin{pmatrix} S_+^{n,d}(t) \\ S_0^{n,d}(t) \\ S_-^{n,d}(t) \end{pmatrix}.$$

Definition 39. We denote the generating functions having the unstable classes associated with potential value change violations associated with **Rule 5** and **Rule 6** as in Proposition 28 as follows:

Unstable n-class U_0	$U_0^{n,d} = \sum_{P \in U_0, \deg(P)=d} t^{L_n(P)}$
Unstable n-class U_{-1}	$U_{-1}^{n,d} = \sum_{P \in U_{-1},\, \deg(P)=d} t^{L_n(P)}$
Unstable n-class U_{-2}	$U_{-2}^{n,d} = \sum_{P \in U_{-2},\, \deg(P)=d} t^{L_n(P)}$
Unstable n-class U^t_{-3}	$T_{-3}^{n,d} = \sum_{P \in U^t_{-3},\, \deg(P)=d} t^{L_n(P)}$
Unstable n-class U^t_{-4}	$T_{-4}^{n,d} = \sum_{P \in U^t_{-4},\, \deg(P)=d} t^{L_n(P)}$
Unstable n-class U^t_{-5}	$T_{-5}^{n,d} = \sum_{P \in U^t_{-5},\, \deg(P)=d} t^{L_n(P)}.$

We denote the generating function of all polynomials of degree d having unstable n-classes associated with **Rule 6** as

$$U^{n,d}(t) = U_0^{n,d}(t) + U_{-1}^{n,d}(t) + U_{-2}^{n,d}(t)$$

and denote the generating function of all polynomials of degree d having unstable n-classes associated with **Rule 5** as

$$T^{n,d}(t) = T_{-3}^{n,d}(t) + T_{-4}^{n,d}(t) + T_{-5}^{n,d}(t).$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

As a vector notation, we have

$$\vec{U}^{n,d}(t) = \begin{pmatrix} U_0^{n,d}(t) \\ U_{-1}^{n,d}(t) \\ U_{-2}^{n,d}(t) \end{pmatrix} \quad \text{and} \quad \vec{T}^{n,d}(t) = \begin{pmatrix} T_{-3}^{n,d}(t) \\ T_{-4}^{n,d}(t) \\ T_{-5}^{n,d}(t) \end{pmatrix}.$$

Definition 40. We denote the generating functions having unstable classes associated with potential value changes violations associated with **Rule 4** using the following table:

Unstable n-class E_1	$E_1^{n,d} = \sum_{P \in E_1, \deg(P)=d} t^{L_n(P)}$
Unstable n-class E_2	$E_2^{n,d} = \sum_{P \in E_2, \deg(P)=d} t^{L_n(P)}$
Unstable n-class E_3	$E_3^{n,d} = \sum_{P \in E_3, \deg(P)=d} t^{L_n(P)}$,

and we denote the generating function of all polynomials of degree d having unstable n-classes as

$$E^{n,d}(t) = E_1^{n,d}(t) + E_2^{n,d}(t) + E_3^{n,d}(t).$$

Finally, as a vector notation, we write

$$\vec{E}^{n,d}(t) = \begin{pmatrix} E_1^{n,d}(t) \\ E_2^{n,d}(t) \\ E_3^{n,d}(t) \end{pmatrix}$$

When there is no restriction on the degree, the generating functions will be denoted as

$$S^n = \sum_{d=0}^{\infty} S^{n,d} U^n = \sum_{d=0}^{\infty} U^{n,d}$$

$$T^n = \sum_{d=0}^{\infty} T^{n,d} E^n = \sum_{d=0}^{\infty} E^{n,d}.$$

We begin computing these generating functions with small d by computing the n-length for every item in the base case. (Definition 30.)

Proposition 41.

$$\vec{S}^{0,0}(t) = \begin{pmatrix} t + \ldots + t^k \\ 0 \\ 0 \end{pmatrix} = \frac{1}{t-1} \begin{pmatrix} t^k - t \\ 0 \\ 0 \end{pmatrix}$$

$$\vec{S}^{n,0}(t) = t^n \begin{pmatrix} t + \ldots + t^{k-1} \\ 1 \\ 0 \end{pmatrix} = \frac{1}{t-1} \begin{pmatrix} t^{k+1} - t \\ t-1 \\ 0 \end{pmatrix} \quad \textit{if } n > 0.$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Similarly,

$$\vec{U}^{0,0}(t) = 0, \quad \vec{T}^{0,0}(t) = \begin{pmatrix} t^{k+1} \\ 0 \\ t^{k+2} \end{pmatrix}$$

$$\vec{U}^{n,0}(t) = \begin{pmatrix} t^{k} \\ 0 \\ t^{k+1} \end{pmatrix}, \quad \vec{T}^{n,0}(t) = 0 \text{ if } n > 0.$$

$$\vec{E}^{n,0}(t) = 0 \text{ for all } n.$$

Proof. Let $d = 0$. When $n > 0$, we have n-classes S_0, S_+, U_0 and U_{-2}, and $L_n(c_0) = n + |c_0|$. For stable n-types, $0 \leq c_0 \leq k-1$. $c_0 = k$ and $c_0 = k+1$ corresponds to U_0 and U_{-2} respectively. On the other hand, if $n \leq 0$, we have n-classes S_+, U^t_{-3} and U^t_{-5}. In this case, $L_n(c_0) = -n + |c_0|$. For stable n-types, $0 \leq c_0 \leq k$. $c_0 = k+1$ and $c_0 = k+2$ corresponds to U^t_{-3} and U^t_{-5}, respectively. □

Remark 42. We exclude the initial type since it plays no role in the recursive definition of n-types.

Lemma 43.

$$\vec{E}^{n,1}(t) = 0 \text{ if } n > 0$$

$$\vec{E}^{0,1}(t) = \begin{pmatrix} t^{k+2} \\ 0 \\ t^{k+1} \end{pmatrix}.$$

Proof. The n-class E appears only when the degree is greater than 1 and $n < d$. There are two cases we need to consider: $P(X) = X - k + 1$ has 0-class E_1 and $P(X) = X - k + 2$ has 0-class E_3. □

Now we introduce recursion using Definition 31. We begin with n-class E.

Proposition 44.

$$\vec{E}^{(n+1,d+1)}(t) = t \begin{bmatrix} 0 & t^k & 0 \\ t^{k-1} & 0 & t^k \\ 0 & t^{k-1} & 0 \end{bmatrix} \vec{E}^{n,d}(t) = P_{E,E}\vec{E}^{n,d}(t).$$

Proof. Suppose that P has n-class E_2. By Definition 31,

$$XP + (-k+1)$$

has $(n+1)$-class E_3, and the difference between the $(n+1)$-length of $XP + (-k+1)$ and the n-length of P is k. Similarly, if P has n-class E_1, $XP + (-k+1)$ has $(n+1)$-class E_2 and the length increases by k.

On the other hand, if P has n-class E_3, $XP - k$ has $(n+1)$-class E_2; and if P has n-class E_2, $XP - k$ has $(n+1)$-class E_1. In both cases, the length increases by $k+1$. □

Note that when P has n-class E_3, $XP + (-k+1)$ has $(n+1)$-class S_-, so this recursive definition will not appear here; this will appear when we consider a transition between E-classes and S-classes later.

For the next proposition, we introduce the following matrices

$$P_{U,S} = t\begin{bmatrix} t^k & t^k & t^{k-1} \\ 0 & 0 & 0 \\ t^{k+1} & t^{k+1} & t^{k+1} \end{bmatrix} \quad \text{and } P_{U,U} = t\begin{bmatrix} 0 & t^{k-1} & 0 \\ t^k & 0 & t^{k-1} \\ 0 & t^k & 0 \end{bmatrix}.$$

Proposition 45. $\vec{U}^{(n+1,d+1)}(t) = P_{U,S}\vec{S}^{n,d}(t) + P_{U,U}\vec{U}^{n,d}(t)$

Similarly, for other classes except stable classes, we have

Proposition 46.

$$\vec{T}^{(n+1,d+1)}(t) = t\begin{bmatrix} 0 & t^{k-1} & 0 \\ t^k & 0 & t^{k-1} \\ 0 & t^k & 0 \end{bmatrix}\vec{T}^{n,d}(t) = P_{T,T}\vec{T}^{n,d}(t).$$

The proofs for both propositions are similar to that of Proposition 44.

For the next proposition, we define the following matrices:

$$P_{S,S} = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^k - t & t^{k-1} - t & & \\ t-1 & t-1 & t-1* & * & * \end{bmatrix},$$

$$P_{S,U} = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^{k-1} - t & t^{k-1} - t & & \\ t-1 & t-1 & t-1* & * & * \end{bmatrix},$$

$$P_{S,T} = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^{k-1} - t & t^{k-1} - t & & \\ t-1 & t-1 & t-1* & * & * \end{bmatrix},$$

$$P_{S,E} = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^k - t & t^k - t \\ 0 & t-1 & t-1 \\ t^{k-1} - t & t^{k-1} - t & t^k - t \end{bmatrix}$$

For stable classes, we set

$$\vec{S}^{(n+1,d+1)} = P_{S,S}\vec{S}^{n,d}(t) + P_{S,U}\vec{U}^{n,d}(t) + P_{S,T}\vec{T}^{n,d}(t) + P_{S,E}\vec{E}^{n,d}(t).$$

For the $*$ in these matrices, the recursive definition does not explicitly state what coefficients can be attached at the end to get n-class S_0. Instead of pursuing the exact condition, we note that for any polynomial P having n-class E or S_-, we know the n-class of $-P$ by the proof of Proposition 35. Exploiting this symmetry, we have

$$S_-^{(n,d)} + E^{(n,d)} = \begin{cases} S_+^{(n,d)} + S_0^{(n,d)} + U_0^{(n,d)} + U_{-2}^{(n,d)} & \text{if } n \geq d \\ S_+^{(n,d)} + S_0^{(n,d)} + T_{-3}^{(n,d)} + T_{-5}^{(n,d)} & \text{if } n < d \end{cases}$$

which can be used to fill the missing entries for $P_{S,S}$, $P_{S,U}$, $P_{S,T}$ and $P_{S,E}$.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

Denote

$$\mathcal{P} = \begin{bmatrix} P_{S,S} & P_{S,U} & P_{S,T} & P_{S,E} \\ P_{U,S} & P_{U,U} & 0 & 0 \\ 0 & 0 & P_{T,T} & 0 \\ 0 & 0 & 0 & P_{E,E} \end{bmatrix}.$$

by the mentioned symmetry, we have the following identity

$$\mathcal{P}\begin{pmatrix} \vec{S}^{(n,d)} \\ \vec{U}^{(n,d)} \\ \vec{T}^{(n,d)} \\ \vec{E}^{(n,d)} \end{pmatrix} = \begin{bmatrix} A & B & C & D \\ P_{U,S} & P_{U,U} & 0 & 0 \\ 0 & 0 & P_{T,T} & 0 \\ 0 & 0 & 0 & P_{E,E} \end{bmatrix}\begin{pmatrix} \vec{S}^{(n,d)} \\ \vec{U}^{(n,d)} \\ \vec{T}^{(n,d)} \\ \vec{E}^{(n,d)} \end{pmatrix}$$

where

$$A = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^k - t & t^{k-1} - t \\ t-1 & t-1 & t-1 \\ t^k - 1 & t^k - 1 & t^{k-1} - 1 \end{bmatrix} + P_{U,S}$$

$$B = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^{k-1} - t & t^{k-1} - t \\ t-1 & t-1 & t-1 \\ t^k - 1 & t^{k-1} - 1 & t^{k-1} - 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} P_{U,U}$$

$$C = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^{k-1} - t & t^{k-1} - t \\ t-1 & t-1 & t-1 \\ t^k - 1 & t^{k-1} - 1 & t^{k-1} - 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} P_{T,T}$$

$$D = \frac{t}{t-1}\begin{bmatrix} t^k - t & t^k - t & t^k - t \\ 0 & t-1 & t-1 \\ t^{k-1} - t & t^{k-1} - t & t^k - t \end{bmatrix} - P_{E,E}$$

and we will use this new block matrix instead of $\mathcal{P}$.

So far, the degree of polynomials having n-classes is fixed. The induction provided above increments d by 1 at the cost of increasing n. To work around this, we will use the following lemma:

Lemma 47. *Suppose that $n \leq 0$, then*

$$\vec{S}^{n,d}(t) = t^{-n}\vec{S}^{0,d}(t), \quad \vec{U}^{n,d}(t) = t^{-n}\vec{U}^{0,d}(t)$$
$$\vec{T}^{n,d}(t) = t^{-n}\vec{T}^{0,d}(t), \quad \vec{E}^{n,d}(t) = t^{-n}\vec{E}^{0,d}(t)$$

Proof. When $n < 0$, the rules for n-reduced polynomials are identical to that of $n = 0$ except the n-length increase by $|n|$. In other words, for $n < 0$, each 0-reduced polynomial with 0-length ℓ can be considered as an n-reduced polynomial with n-length $\ell + |n|$. □

Now we compute the generating function for each class without restrictions on the degree by summing over all possible degrees. First, observe that

$$\sum_{d=0}^{\infty} \mathcal{P}^d = (1 - \mathcal{P})^{-1}$$

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

which allows us to write

$$\begin{pmatrix} \vec{S}^0 \\ \vec{U}^0 \\ \vec{T}^0 \\ \vec{E}^0 \end{pmatrix} = \begin{pmatrix} \vec{S}^{0,1} \\ \vec{U}^{0,1} \\ \vec{T}^{0,1} \\ \vec{E}^{0,1} \end{pmatrix} + \sum_{d=0}^{\infty} \mathcal{P}^d \begin{pmatrix} \vec{S}^{0,1} \\ \vec{U}^{0,1} \\ \vec{T}^{0,1} \\ \vec{E}^{0,1} \end{pmatrix} = \begin{pmatrix} \vec{S}^{0,1} \\ \vec{U}^{0,1} \\ \vec{T}^{0,1} \\ \vec{E}^{0,1} \end{pmatrix} + (1-\mathcal{P})^{-1} \begin{pmatrix} \vec{S}^{0,1} \\ \vec{U}^{0,1} \\ \vec{T}^{0,1} \\ \vec{E}^{0,1} \end{pmatrix},$$

and for n-classes, we have

$$\begin{pmatrix} \vec{S}^n \\ \vec{U}^n \\ \vec{T}^n \\ \vec{E}^n \end{pmatrix} = (\mathcal{P}/t)^n \begin{pmatrix} \vec{S}^0 \\ \vec{U}^0 \\ \vec{T}^0 \\ \vec{E}^0 \end{pmatrix}.$$

which follows from Lemma 47.

Since $\mathcal{P}$ is a 12×12 matrix with polynomial entries, $(1-\mathcal{P})^{-1}$ is a matrix with rational function entries. Thus, S^n, U^n, T^n and E^n are all rational for fixed n. $(1-\mathcal{P}/t)^{-1}$ is also a matrix with rational function entries, hence the sum of S^n, U^n, T^n and E^n over all n are rational. Since every n-*minimal* polynomial representing a group element can be decomposed into an n-reduced polynomial and $-n$-reduced polynomial with possibly multiplicities described in Proposition 37, the set of all n-minimal polynomials exhibits a rational growth. Furthermore, taking account of the multiplicities in representing group elements only changes the end function by rational functions because U^n, T^n and E^n are all rational.

Acknowledgements. The authors would like to thank the referee for suggestions that improved the exposition of this article.

The first author is partially supported by NSF grant DMS-1600857 "Von Neumann Algebras: Rigidity, Applications to Measurable Dynamics, and Model Theory".

The second author acknowledges support from U.S. National Science Foundation grants DMS-1107452, 1107263, 1107367 "RNMS: Geometric Structures and Representation Varieties" (the GEAR Network) and DMS-2054558 "RUI: Randomness, Computability, and Complexity in Groups".

References

1. H. Bass, The degree of polynomial growth of finitely generated nilpotent groups, *Proc. London Math. Soc.* **3**(4) (1972), 603–614.
2. M. Benson, Growth series of finite extensions of Z^n are rational, *Invent. Math.* **73**(2) (1983), 251–269.
3. M. Brazil, Growth functions for some nonautomatic Baumslag-Solitar groups, *Trans. Amer. Math. Soc.* **342**(1) (1994), 137–154.
4. C. Bregman, Rational growth and almost convexity of higher-dimensional torus bundles, *Int. Math. Res. Not. IMRN* **2019**(13) (2019), 4004–4046.
5. J. W. Cannon, The combinatorial structure of cocompact discrete hyperbolic groups, *Geom. Dedicata* **16**(2) (1984), 123–148.
6. D. J. Collins, M. Edjvet and C. P. Gill, Growth series for the group $\langle x, y | x^-1yx = y^l \rangle$, *Arch. Math. (Basel)* **62**(1) (1994), 1–11.

https://doi.org/10.1017/S0013091522000505 Published online by Cambridge University Press

7. M. Duchin and M. Shapiro, The Heisenberg group is pan-rational, *Adv. Math.* **346** (2019), 219–263.
8. R. I. Grigorchuk, *On the milnor problem of group growth*, Doklady Akademii Nauk, vol. 271 (Russian Academy of Sciences, 1983), pp. 30–33.
9. M. Gromov, Groups of polynomial growth and expanding maps, *Inst. Hautes Études Sci. Publ. Math.* **1981**(53) (1981), 53–73.
10. O. Kharlampovich, A finitely presented solvable group with unsolvable word problem, *Izv. Akad. Nauk SSSR Ser. Mat.* **45**(4) (1981), 852–873.
11. J. Milnor, A note on curvature and fundamental group, *J. Differ. Geom.* **2**(1) (1968), 1–7.
12. J. Milnor, Problem 5603, *Amer. Math. Monthly* **75**(6) (1968), 685–686.
13. W. D Neumann and M. Shapiro, Automatic structures, rational growth, and geometrically finite hyperbolic groups, *Invent. Mathe.* **120**(1) (1995), 259–287.
14. P. Pansu, Croissance des boules et des géodésiques fermées dans les nilvariétés, *Ergodic Theory Dynm. Syst.* **3**(3) (1983), 415–445.
15. L. Paris, *Growth series of coxeter groups*, Group Theory from Geometrical Point of View (eds. E. Ghys, A. Haefliger and A. Verjovsky), World Scientific (1991), 302–310
16. W. Parry, Examples of growth series of torus bundle groups, *J. Group Theory* **10**(2) (2007), 245–266.
17. A. Putman, The rationality of Sol-manifolds, *J. Algebra* **304**(1) (2006), 190–215.
18. M. Stoll, Rational and transcendental growth series for the higher Heisenberg groups, *Invent. Math.* **126**(1) (1996), 85–109.
19. A.S. Švarc, A volume invariant of coverings, *Dokl. Akad. Nauk SSSR (NS)* **105**, 1955), 32–34.
20. J. Tits, Free subgroups in linear groups, *J. Algebra* **20**(2) (1972), 250–270.
21. J. Wolf, Growth of finitely generated solvable groups and curvature of Riemannian manifolds, *J. Differ. Geom.* **2**(4) (1968), 421–446.