Contemporary Mathematics

# Regular Free Length Functions on Lyndon's Free $\mathbb{Z}[t]$-group $F^{\mathbb{Z}[t]}$

Alexei G. Myasnikov, Vladimir N. Remeslennikov, and Denis E. Serbin

Abstract. Let $F = F(X)$ be a free group with basis $X$ and $\mathbb{Z}[t]$ be the ring of integer polynomials in $t$. In this paper we represent elements of Lyndon's free $\mathbb{Z}[t]$-group $F^{\mathbb{Z}[t]}$ by infinite words defined as functions $w : [1, f_w] \to X^{\pm 1}$ over closed intervals $[1, f_w] = \{a \in \mathbb{Z}[t] \mid 1 \leqslant a \leqslant f_w\}$ in the additive group of $\mathbb{Z}[t]$, viewed as an ordered abelian group. This naturally provides a regular free Lyndon length function $L : w \to f_w$ on $F^{\mathbb{Z}[t]}$ with values in $\mathbb{Z}[t]$. It follows that every finitely generated fully residually free group has a free length function with values in a free abelian group $\mathbb{Z}^n$ of finite rank with the lexicographic order. This technique allows one to solve various algorithmic problems for $F^{\mathbb{Z}[t]}$ using the standard Nielsen cancellation argument for the length function $L : F^{\mathbb{Z}[t]} \to \mathbb{Z}[t]$.

Contents



## 1. Introduction

Let $F = F(X)$ be a free non-abelian group with basis $X$ and $\mathbb{Z}[t]$ be the ring of integer polynomials in the variable $t$. In [**27**] Lyndon defined and studied a free $\mathbb{Z}[t]$-group $F^{\mathbb{Z}[t]}$ which admits exponents in the ring $\mathbb{Z}[t]$. The impetus for his study

1991 *Mathematics Subject Classification.* 20E08.
*Key words and phrases.* Lyndon length function, infinite words.
The first author was supported by NSF grant DMS-9970618.
The second author was supported by RFFI grant 02-01-00192.

was to describe solutions sets of equations over $F$ by elements from $F^{\mathbb{Z}[t]}$, viewed as parametric words with parameters in $\mathbb{Z}[t]$. Lyndon proved that one needs only finitely many parametric words to describe solutions of one-variable equations over $F$ [**29**]. Further progress in this direction was made by Appel [**1**] and Lorents [**26**], who gave the exact form of the required parametric words, see also [**11**] for an alternative proof. It was shown later [**2, 42**] that solution sets of equations of more than one variable, in general, cannot be described by a finite set of parametric words.

Recently, a new wave of interest (see, for example, [**5, 36, 14, 19, 20, 22**]) in Lyndon's group $F^{\mathbb{Z}[t]}$ arose with respect to its relation to algebraic geometry over groups and the Tarski problem. In [**19, 20**] Kharlampovich and Myasnikov proved that the coordinate groups of irreducible algebraic sets over $F$ are precisely the finitely generated subgroups of $F^{\mathbb{Z}[t]}$. It follows, for example, that the solution set of an irreducible system of equations over $F$ is equal to the Zariski closure of some set of solutions given by a finite set of parametric words over $F$.

Another recent development related to $F^{\mathbb{Z}[t]}$ concerns fully residually free groups. It was shown in [**4**] that finitely generated fully residually free groups are precisely the coordinate groups of irreducible algebraic sets over $F$, so (by the result above) these groups are embeddable into $F^{\mathbb{Z}[t]}$. On the other hand, in the original paper [**27**] Lyndon proved that $F^{\mathbb{Z}[t]}$ (hence, every subgroup of it) is fully residually free. This gives another characterization of finitely generated fully residually free groups which allows one to study them by means of combinatorial group theory: HNN-extensions and free products with amalgamation, Bass-Serre theory, JSJ-decompositions.

In this paper we represent elements of the group $F^{\mathbb{Z}[t]}$ by infinite words in the alphabet $X^{\pm 1}$. These words are functions of the type

$$w : [1, f_w] \to X^{\pm 1},$$

where $f_w \in \mathbb{Z}[t]$ and $[1, f_w] = \{g \in \mathbb{Z}[t] \mid 1 \leqslant g \leqslant f_w\}$ is a closed interval in $\mathbb{Z}[t]$ with respect to the standard lexicographical order $\leqslant$. The function $L : w \to f_w$ gives rise to a regular free Lyndon length function on $F^{\mathbb{Z}[t]}$ with values in the additive group of $\mathbb{Z}[t]$, viewed as an abelian ordered group. This implies that every finitely generated fully residually free group has a free length function with values in a free abelian group $\mathbb{Z}^n$ of finite rank with the lexicographic order.

Once the presentation of elements of $F^{\mathbb{Z}[t]}$ by infinite words is established, a host of problems about $F^{\mathbb{Z}[t]}$ can be solved precisely in the same way as in the standard free group $F$. To demonstrate this technique we show that the conjugacy and the power problems are decidable in $F^{\mathbb{Z}[t]}$ in the same fashion as in $F$. Notice that decidability of the conjugacy problem has been proven before by Liutikova in [**25**], and also by Ribes and Zalesski in [**43**] using completely different methods.

Another interesting application of these results stems from the regularity of the length function $L$ (this means that if $c(u, v)$ is the length of the common initial segment of elements $u$ and $v$ then there exists an element $c$ of length $c(u, v)$ such that $u = cu_1$, $v = cv_1$ for some $u_1, v_1$ with $c(u_1, v_1) = 0$). The regularity condition is crucial for Nielsen's cancellation method, which is the base for Makanin's technique for solving equations over $F$ [**32**]. It turns out, that if $G$ is a coordinate group of an irreducible algebraic set over $F$ with a computable regular free Lyndon length function $G \to \mathbb{Z}^n$ then a Makanin's type argument can be used for solving equations over $G$ (see [**17, 22**]). This plays an important role in proving the decidability of

the elementary theories of free groups. Since the coordinate group $G$ is a subgroup of $F^{\mathbb{Z}[t]}$ the restriction $L_G$ of $L$ onto $G$ is a length function on $G$ satisfying all the required conditions, except, maybe, the regularity axiom. Using the machinery of infinite words we were able to show that $L_G$ is regular for a wide class of subgroups of $F^{\mathbb{Z}[t]}$.

Observe, that one can derive from the description of $F^{\mathbb{Z}[t]}$ as the union of extensions of centralizers [**36**] and the results of Bass on non-archimedean actions [**3**] that $F^{\mathbb{Z}[t]}$ acts freely on a $\Lambda$-tree, where $\Lambda$ is a free abelian group of countable rank with the lexicographic order. This implies, that $F^{\mathbb{Z}[t]}$, indeed, has a free Lyndon length function with values in $\mathbb{Z}[t]$, but the method does not provide any information whether this length is regular, or computable.

Our method for constructing free length functions on groups is quite general and can be applied to a wide class of groups. It is based on infinite $A$-words in an alphabet $X^{\pm}$, where $A$ is an arbitrary discretely ordered abelian group. An $A$-word is a function $w : [1_A, \alpha_w] \longrightarrow X^{\pm}$, where $1_A$ is the minimal positive element of $A$ and $[1_A, \alpha_w]$ is a closed segment in $A$. One can consider a set $R(A, X)$ of all reduced $A$-words $w$ ($w(a + 1_A) \neq w(a)^{-1}$ for $a \in [1_A, \alpha_w]$) which comes equipped with the natural partial multiplication and length function $w \longrightarrow \alpha_w$. For a given group $G$ every embedding of $G$ into $R(A, X)$ provides a "nice" length function on $G$ inherited from $R(A, X)$. It turned out (quite unexpectedly) that Stalling's pregroups supply the most adequate technique to study $R(A, X)$.

In [**37**] and [**38**] we have constructed a similar length function on $F^{\mathbb{Z}[t]}$ using quite different methods (more direct and computationally heavy). We would like also to mention preprint [**7**] which contains some preliminary results concerning length functions on extensions of centralizers of free groups.

## 2. Preliminaries

**2.1. Lyndon's $\mathbb{Z}[t]$-free group $F^{\mathbb{Z}[t]}$.** Let $A$ be an associative unitary ring. Recall [**36, 6**] that a group $G$ is termed an *$A$-group* if it comes equipped with a function (*exponentiation*) $G \times A \to G$:

$$(g, \alpha) \to g^{\alpha}$$

satisfying the following conditions for arbitrary $g, h \in G$ and $\alpha, \beta \in A$:

(E1) $g^1 = g, \quad g^{\alpha+\beta} = g^{\alpha} g^{\beta}, \quad g^{\alpha\beta} = (g^{\alpha})^{\beta}$;
(E2) $g^{-1} h^{\alpha} g = (g^{-1} h g)^{\alpha}$;
(E3) if $g$ and $h$ commute, then $(gh)^{\alpha} = g^{\alpha} h^{\alpha}$.

The axioms (E1) and (E2) were introduced originally by Lyndon in [**27**], the axiom (E3) was added later in [**35**]. A homomorphism $\phi : G \to H$ between two $A$-groups is termed an $A$-homomorphism if $\phi(g^{\alpha}) = \phi(g)^{\alpha}$ for every $g \in G$ and $\alpha \in A$. It is not hard to prove (see, [**35**] or [**36**]) that for every group $G$ there exists an $A$-group $H$ (which is unique up to an $A$-isomorphism) and a homomorphism $\mu : G \longrightarrow H$ such that for every $A$-group $K$ and every $A$-homomorphism $\theta : G \longrightarrow K$, there exists a unique $A$-homomorphism $\phi : H \longrightarrow K$ such that $\phi\mu = \theta$. We denote $H$ by $G^A$ and call it the *$A$-completion* of $G$. In particular, there exists a $\mathbb{Z}[t]$-completion $F^{\mathbb{Z}[t]}$ of a free group $F$. It was introduced by Lyndon in [**27**] who used different methods, and is now called Lyndon's free $\mathbb{Z}[t]$-group.

In [**36**] an effective construction of $F^{\mathbb{Z}[t]}$ was given in terms of extensions of centralizers. For a group $G$ let $S = \{C_i \mid i \in I\}$ be a set of representatives

of conjugacy classes of proper cyclic centralizers in $G$, i.e., every proper cyclic centralizer in $G$ is conjugate to one from $S$, and no two centralizers from $S$ are conjugate. Then the HNN-extension

$$H = \langle\, G, s_{i,j} \quad (i \in I, j \in \mathbb{N}) \;\mid\; [s_{i,j}, u_i] = [s_{i,j}, s_{i,k}] = 1\, (u_i \in C_i, i \in I, j, k \in \mathbb{N}) \,\rangle,$$

where $\mathbb{N}$ stands for the set of positive natural numbers, is termed an *extension of cyclic centralizers* in $G$. Now the group $F^{\mathbb{Z}[t]}$ is isomorphic to the direct limit of the following infinite chain of groups:

$$F = G_0 < G_1 < \cdots < G_n < \cdots < \cdots, \tag{1}$$

where $G_{i+1}$ is obtained from $G_i$ by extension of all cyclic centralizers in $G_i$. We use this description of Lyndon's free $\mathbb{Z}[t]$-group below to embed $F^{\mathbb{Z}[t]}$ into the set of infinite words $CDR(\mathbb{Z}[t], X)$.

**2.2. Stallings' pregroups and their universal groups.** In papers [**45, 46**] Stallings introduced a notion of a pregroup $P$ and its universal group $U(P)$. A pregroup $P$ provides a very economic way to describe some normal forms of elements of $U(P)$.

A *pregroup* $P$ is a set $P$, with a distinguished element $\epsilon$, equipped with a partial multiplication, that is a function $D \to P$, $(x, y) \to xy$, where $D \subset P \times P$, and an inversion, that is a function $P \to P$, $x \to x^{-1}$, satisfying the following axioms (below $xy$ is *defined* if $(x, y) \in D$):

(P1) for all $u \in P$ $u\epsilon$ and $\epsilon u$ are defined and $u\epsilon = \epsilon u = u$;
(P2) for all $u \in P$, $u^{-1}u$ and $uu^{-1}$ are defined and $u^{-1}u = uu^{-1} = \epsilon$;
(P3) for all $u, v \in P$, if $uv$ is defined, then so is $v^{-1}u^{-1}$, and $(uv)^{-1} = v^{-1}u^{-1}$;
(P4) for all $u, v, w \in P$, if $uv$ and $vw$ are defined, then $(uv)w$ is defined if and only if $u(vw)$ is defined, in which case

$$(uv)w = u(vw);$$

(P5) for all $u, v, w, z \in P$ if $uv, vw$, and $wz$ are all defined then either $uvw$ or $vwz$ is defined.

It was noticed (see [**16**]) that (P3) follows from (P1), (P2), and (P4), hence, can be omitted.

To describe the universal group $U(P)$ recall that a mapping $\phi : P \to Q$ of pregroups is a *morphism* if for any $x, y \in P$ whenever $xy$ is defined in $P$ , $\phi(x)\phi(y)$ is defined in $Q$ and equal to $\phi(xy)$.

Now the group $U(P)$ can be characterized by the following universal property: there is a morphism of pregroups $\lambda : P \to U(P)$, such that, for any morphism $\phi : P \to G$ of $P$ into a group $G$, there is a unique group homomorphism $\psi : U(P) \to G$ for which $\psi\lambda = \phi$. This shows that $U(P)$ is a group with a generating set $P$ and a set of relations $xy = z$, where $x, y \in P$, $xy$ is defined in $P$, and equal to $z$.

There exists an explicit construction of $U(P)$ due to Stallings [**46**]. Namely, a finite sequence $(u_1, \ldots, u_n)$ of elements from $P$ is called a *reduced* $P$-sequence if for any $1 \leqslant i \leqslant n-1$ the product $u_i u_{i+1}$ is not defined in $P$. The group $U(P)$ can be described as the set of equivalence classes on the set of all reduced $P$-sequences modulo equivalence relation $\sim$, where $(u_1, \ldots, u_n) \sim (v_1, \ldots, v_m)$ if and only if $m = n$ and there exist elements $a_1, \ldots, a_{n-1} \in P$ such that $v_i = a_{i-1}^{-1} u_i a_i$ for $1 \leqslant i \leqslant n$ (here $a_0 = a_n = 1$). The multiplication on $U(P)$ is given by concatenation

of representatives and reduction of the resulting sequence. $P$ embeds into $U(P)$ via the canonical map $u \to (u)$.

We use pregroups as a convenient language to describe various presentations of groups by infinite words.

In Section 3.2 we prove that the set $R(A, X)$ with the partial multiplication $*$ and the inversion $^{-1}$ satisfies the axioms (P1) - (P4). In general, $R(A, X)$ does not satisfy (P5), but some subsets of it, which play an important part in our constructions, do.

**2.3. Ordered abelian groups.** In this section some well-known results on ordered abelian groups are collected. For proofs and details we refer to the books [**15**] and [**24**].

DEFINITION 2.1. A set $A$ equipped with addition $+$ and a partial order $\leqslant$ is called a partially ordered abelian group if:

(1) $\langle A, + \rangle$ is an abelian group;
(2) $\langle A, \leqslant \rangle$ is a partially ordered set;
(3) for all $a, b, c \in A$, $a \leqslant b$ implies $a + c \leqslant b + c$.

If the partial ordering is a linear (total) ordering then $A$ is called *an ordered abelian group*

If $A$ is an ordered abelian group then the set of all non-negative elements

$$A^+ = \{a \in A \mid a \geqslant 0\}$$

forms a semigroup, such that $A^+ \cap -A^+ = 0$ and $A^+ \cup -A^+ = A$. Conversely, if $P$ is a subsemigroup of $A$ such that $P \cup -P = A$ and $P \cap -P = 0$ then the relation

$$a \geqslant b \Leftrightarrow a - b \in P$$

turns $A$ into an ordered abelian group. We call $P$ the *positive cone* of the ordered abelian group $A$.

For an element $a \in A$ define a function $sgn : A \to \{-1, 0, 1\}$ as follows:

$$\mathrm{sgn}(a) = \begin{cases} 1 & \text{if } a > 0, \\ 0 & \text{if } a = 0, \\ -1 & \text{if } a < 0. \end{cases}$$

An abelian group $A$ is called *orderable* if there exists a linear order $\leqslant$ on $A$, satisfying the condition (3) above. In general, the ordering on $A$ is not unique.

Observe, that every ordered abelian group is torsion-free, since if $0 < a \in A$ then $0 < na$ for any positive integer $n$. It is easy to see that the reverse is also true, that is, a torsion-free abelian group is orderable. Indeed, by the compactness theorem for first-order logic, a group is orderable if and only if every finitely generated subgroup of it is orderable. Hence, it suffices to show that finite direct sums of copies of the infinite cyclic group $\mathbb{Z}$ are orderable. This is easy, one of the possible orderings is the lexicographical order described below.

Let $A$ and $B$ be ordered abelian groups. Then the direct sum $A \oplus B$ is orderable with respect to the *right lexicographic order*, defined as follows:

$$(a_1, b_1) < (a_2, b_2) \Leftrightarrow b_1 < b_2 \text{ or } b_1 = b_2 \text{ and } a_1 < a_2.$$

Similarly, one can define the right lexicographic order on finite direct sums of ordered abelian groups or even on infinite direct sums if the set of indices is linearly ordered. Indeed, let $I$ be a linearly ordered set of indices and $A_i, i \in I$, be a set

of ordered abelian groups. Then the *right lexicographic order* on the direct sum $A_I = \bigoplus_{i\in I} A_i$ is defined by the following condition: an element $a = (a_i)_{i\in I} \in A_I$ is positive if and only if its greatest non-zero component is positive. It follows that the right lexicographic order on $A_I$ extends the order on each group $A_i$, viewed as a subgroup under the canonical embedding.

For example, let $\langle \mathbb{Z}[t], + \rangle$ be the additive group of the polynomial ring $\mathbb{Z}[t]$ (below we use the notation $\mathbb{Z}[t]$ both for the ring of polynomials and its additive group). Recall, that as a group $\mathbb{Z}[t]$ is an infinite direct sum

$$\mathbb{Z}[t] = \bigoplus_{n=0}^{\infty} \langle t^n \rangle$$

of copies of $\mathbb{Z}$. Hence, $\mathbb{Z}[t]$ has the right lexicographic order induced by this direct decomposition. From now on we fix this right lexicographic order on $\mathbb{Z}[t]$. The ordered abelian group $\mathbb{Z}[t]$ plays a key part in this paper.

Observe, that the construction above allows one to introduce a right lexicographic order on any torsion-free abelian group $A$. Indeed, there exists an embedding (by no means unique) of $A$ into a divisible abelian group $A_{\mathbb{Q}} = A \otimes_{\mathbb{Z}} \mathbb{Q}$, where $\mathbb{Q}$ is the additive group of rational numbers. Clearly, $A_{\mathbb{Q}}$ is a direct sum of copies of $\mathbb{Q}$, $A_{\mathbb{Q}} = \bigoplus_{i\in I} \mathbb{Q}$. Since the set of indices $I$ can be linearly ordered (assuming the axiom of choice) the group $A_{\mathbb{Q}}$ is orderable, as well as its subgroup $A$. The induced order on $A$ is also called lexicographic.

If $A$ is already ordered then the right lexicographic order on $A_{\mathbb{Q}}$, in general, does not extend the order on $A$. Now we introduce an order on $A_{\mathbb{Q}}$ that extends the existing order on $A$. Notice, that elements in $A_{\mathbb{Q}}$ can be described as fractions $\frac{a}{m}$, where $a \in A$ and $m \in \mathbb{Z}, m > 0$. Then the relation

$$\frac{a}{k} \leqslant \frac{b}{m} \Leftrightarrow ma \leqslant kb$$

gives rise to an order on $A_{\mathbb{Q}}$ which extends the order on $A$ under the embedding $a \to \frac{a}{1}$. We will refer to this order as a *fraction* order. Observe that $\mathbb{Z}[t]_{\mathbb{Q}}$ is the additive group of the polynomial ring $\mathbb{Q}[t]$ with the right lexicographic order.

For elements $a, b$ of an ordered group $A$ the *closed segment* $[a, b]$ is defined by

$$[a, b] = \{c \in A \mid a \leqslant c \leqslant b\}.$$

A subset $C \subset A$ is called *convex*, if for every $a, b \in C$ the set $C$ contains $[a, b]$. In particular, a subgroup $B$ of $A$ is convex if $[0, b] \subset B$ for every positive $b \in B$. In this event, the quotient $A/B$ is an ordered abelian group with respect to the order induced from $A$.

A group $A$ is called *archimedean* if it has no non-trivial proper convex subgroups. It is known that $A$ is archimedean if and only if $A$ can be embedded into the ordered abelian group of real numbers $\mathbb{R}_+$, or equivalently, for any $0 < a \in A$ and any $b \in A$ there exists an integer $n$ such that $na > b$.

Obviously, if the set of indices $I$ has at least two elements then the direct sum $A_I$ with the right lexicographic order is non-archimedean. On the other hand, if $A$ is an archimedean ordered abelian group then the fraction order on its $\mathbb{Q}$-completion $A_{\mathbb{Q}}$ is also archimedean.

It is not hard to see that the set of convex subgroups of an ordered abelian group $A$ is linearly ordered by inclusion (see, for example, [**15**]), it is called *the*

*complete chain of convex subgroups* in $A$. Notice that

$$E_n = \{f(t) \in \mathbb{Z}[t] \mid \deg(f(t)) \leqslant n\}$$

is a convex subgroup of $\mathbb{Z}[t]$ (here $\deg(f(t))$ is the degree of $f(t)$) and

$$0 < E_0 < E_1 < \cdots < E_n < \cdots$$

is the complete chain of convex subgroups of $\mathbb{Z}[t]$.

If $A$ is finitely generated then the complete chain of convex subgroups of $A$:

$$0 = A_0 < A_1 < \ldots < A_n = A$$

is finite. The following result (see, for example, [**10**]) shows that this chain completely determines the order on $A$, as well as the structure of $A$. Namely, the groups $A_i/A_{i-1}$ are archimedean (with respect to the induced order) and $A$ is isomorphic (as an ordered group) to the direct sum

$$A_1 \oplus A_2/A_1 \oplus \cdots \oplus A_n/A_{n-1} \tag{2}$$

with the right lexicographic order.

An ordered abelian group $A$ is called *discretely ordered* if $A^+$ has a minimal non-trivial element (we denote it by $1_A$). In this event, for any $a \in A$ the following hold:

1) $a + 1_A = \min\{b \mid b > a\}$,

2) $a - 1_A = \max\{b \mid b < a\}$.

For example, $A = \mathbb{Z}^n$ with the right lexicographic order is descretely ordered with $1_{\mathbb{Z}^n} = (1, 0, \ldots, 0)$. The additive group of integer polynomials $\mathbb{Z}[t]$ is descretely ordered with $1_{\mathbb{Z}[t]} = 1$.

LEMMA 2.2. *A finitely generated discretely ordered archimedean abelian group is infinite cyclic.*

PROOF. Let $H = \langle a_1, \ldots, a_n \rangle$ be a finitely generated archimedean discretely ordered abelian group and $b = 1_H$. We can assume that $H < \mathbb{R}^+$. Then $a_i = m_i b + r_i$, where $m_i \in Z, 0 \leqslant r_i < b$, hence, $r_i = 0$ and $b$ generates $H$. □

It follows from Lemma 2.2 that a discrete abelian ordered group $A$ has a minimal nontrivial convex subgroup, namely, the infinite cyclic subgroup $\langle 1_A \rangle$ generated by $1_A$. We denote this subgroup by $\mathbb{Z}$ and refer to its elements as *finite* elements of $A$, and to elements from $A - \mathbb{Z}$ as to *infinite* or *non-standard* elements. In particular, if $A = \mathbb{Z}[t]$ then the constant polynomials are the only finite elements of $A$.

Every convex subgroup of a discretely ordered abelian group $A$ is also discretely ordered (with respect to the induced order), but ordered images of $A$ may not be discrete. For example, if $\alpha \in \mathbb{R}$ is irrational then the ordered subgroup $H = \langle \alpha, 1_{\mathbb{R}} \rangle \leqslant \mathbb{R}$ (with the induced order) is finitely generated archimedean non-discrete, hence, the group $A = \mathbb{Z} \oplus H$ with the right lexicographic order is discrete, and $H \simeq A/\mathbb{Z}$ is not.

We call an ordered abelian group $A$ *hereditary discrete* if for any convex subgroup $E \leqslant A$ the quotient $A/E$ is discrete with respect to the induced order. The equality (2) and Lemma 2.2 imply

COROLLARY 2.3. *Let $A$ be a finitely generated hereditary discrete ordered abelian group. Then $A$ is isomorphic to the direct product of finitely many copies of $\mathbb{Z}$ with the lexicographic order.*

**2.4. Lyndon length functions.** Let $G$ be a group and $A$ be an ordered abelian group. Then a function $l : G \to A$ is called a *(Lyndon) length function* on $G$ if the following conditions hold:

(L1) $\forall\ x \in G :\ l(x) \geqslant 0$ and $l(1) = 0$;
(L2) $\forall\ x \in G :\ l(x) = l(x^{-1})$;
(L3) $\forall\ x, y, z \in G :\ c(x, y) > c(x, z) \to c(x, z) = c(y, z)$,
where $c(x, y) = \frac{1}{2}(l(x) + l(y) - l(x^{-1}y))$.

In general $c(x, y) \notin A$, but $c(x, y) \in A_{\mathbb{Q}}$, so, in the axiom (L3) we view $A$ as a subgroup of $A_{\mathbb{Q}}$.

It is not difficult to derive the following two properties of Lyndon length functions from the axioms (L1)-(L3):

- $\forall\ x, y \in G :\ l(xy) \leqslant l(x) + l(y)$;
- $\forall\ x, y \in G :\ 0 \leqslant c(x, y) \leqslant min\{l(x), l(y)\}$.

Below we list several extra axioms which describe some special classes of Lyndon length functions.

(L4) $\forall\ x \in G :\ c(x, y) \in A$.

A length function $l : G \to A$ is called *free*, if it satisfies

(L5) $\forall\ x \in G :\ x \neq 1 \to l(x^2) > l(x)$.

A group $G$ has a Lyndon length function $l : G \to A$, which satisfies axioms (L4)-(L5) if and only if $G$ acts freely on some $A$-tree. This is a remarkable result due to Chiswell (see [**9**]). Lyndon himself proved that groups with free length functions with values in $\mathbb{Z}$ are just subgroups of free groups with the induced length functions [**28**]. A joint effort of several researchers culminated in a description of finitely generated groups with real-valued free length function [**34, 40, 8, 13**] which is now known as Rips' theorem: a finitely generated group acts freely on an $\mathbb{R}$-tree if and only if it is a free product of free abelian groups and surface groups (with exception of non-orientable groups of genus 1, 2, and 3). The case of non-archimedean free length functions is wide open. In [**3**] Bass studied finitely generated groups acting freely on a $(\Lambda \oplus \mathbb{Z})$-tree with lexicographic order on $\Lambda \oplus \mathbb{Z}$.

In Section 4 we define a subset $CDR(A, X) \subset R(A, X)$ of all reduced infinite words which admit cyclic decomposition and prove the following result: for a discretely ordered abelian group $A$ the function $l : CDR(A, X) \to A$, defined as $l(w) = |w|$, satisfies all the axioms (L1)–(L5), whenever corresponding products of elements in these axioms are defined. This implies that every group embeddable into $CDR(A, X)$ has a free length function with values in $A$. Moreover, in the special case when $A = \mathbb{Z}[t]$, some subgroups of $CDR(A, X)$, in particular, the free $\mathbb{Z}[t]$-group $F^{\mathbb{Z}[t]}$, have free length functions which are easily computable and satisfy the following extra axiom (L6). Below for elements $x_1, \dots, x_n \in G$ we write $x = x_1 \circ \cdots \circ x_n$ if $x = x_1 \cdots x_n$ and $l(x) = l(x_1) + \cdots + l(x_n)$. Also, for $\alpha \in A$ we write $x = x_1 \circ_\alpha x_2$ if $x = x_1 x_2$ and $c(x_1^{-1}, x_2) < \alpha$.

The length function $l : G \to A$ is called *regular* if it satisfies the following *regularity* axiom:

(L6) $\forall x, y \in G, \exists u, x_1, y_1 \in G :$

$$x = u \circ x_1\ \&\ y = u \circ y_1\ \&\ l(u) = c(x, y).$$

The regularity condition is crucial for Nielsen's cancellation method, which is the base for Makanin's technique for solving equations over $F$ [**32**].

## 3. $A$-words

**3.1. Definitions.** Let $A$ be a discretely ordered abelian group. Recall that $1_A$ is the minimal positive element of $A$ and if $a, b \in A$ then $[a, b] = \{x \in A \mid a \leqslant x \leqslant b\}$. For a function $f : B \to C$ by $dom(f)$ we denote the domain $B$ of $f$.

Let $X = \{x_i \mid i \in I\}$ be a set. Put $X^{-1} = \{x_i^{-1} \mid i \in I\}$ and $X^{\pm} = X \cup X^{-1}$. As usual we define an involution $^{-1}$ on $X^{\pm}$ by $(x)^{-1} = x^{-1}$ and $(x^{-1})^{-1} = x$.

Definition 3.1. An $A$-word is a function of the type

$$w : [1_A, \alpha] \to X^{\pm},$$

where $\alpha \in A, \alpha \geqslant 0$. The element $\alpha$ is called the length $|w|$ of $w$.

By $W(A, X)$ we denote the set of all $A$-words. Observe, that $|w| = 0$ if and only if the domain of $w$ is empty ($[1_A, 0] = \emptyset$), i.e. the function $w$ is empty. We denote this function by $\varepsilon$. Also, we say that an element $w \in W(A, X)$ has a *finite length* if $|w| \in \mathbb{Z}$.

*Concatenation* $uv$ of two words $u, v \in W(A, X)$ is an $A$-word of length $|u| + |v|$ and such that:

$$(uv)(a) = \begin{cases} u(a) & \text{if } 1_A \leqslant a \leqslant |u| \\ v(a - |u|) & \text{if } |u| < a \leqslant |u| + |v| \end{cases}$$

In particular, $\varepsilon u = u\varepsilon = u$ for any $u \in W(A, X)$. For any $A$-word $w$ we define an *inverse* $w^{-1}$ as an $A$-word of the length $|w|$ and such that

$$w^{-1}(\beta) = w(|w| + 1_A - \beta)^{-1} \quad (\beta \in [1_A, |w|]).$$

An $A$-word $w$ is *reduced* if $w(\beta + 1_A) \neq w(\beta)^{-1}$ for each $1_A \leqslant \beta < |w|$. We denote by $R(A, X)$ the set of all reduced $A$-words. Clearly, $\varepsilon \in R(A, X)$.

Of course, concatenation $uv$ of two reduced words $u, v$ may not be reduced. We write $u \circ v$ instead of $uv$ in the case when $uv$ is reduced, i.e. $u(|u|) \neq v(1_A)^{-1}$. We will show below that this notation agrees with the one given in Section 2.4 via length functions. Obviously, $\circ$ satisfies the following cancellation conditions:

$$x \circ y = x \circ z \Longrightarrow y = z, \quad y \circ x = z \circ x \Longrightarrow y = z.$$

If $w = w_1 \circ u \circ w_2$ then $u$ is called a *subword* of $w$.

**3.2. Multiplication.** In this subsection we introduce a (partial) multiplication on $R(A, X)$ and show that it satisfies the axioms (P1)–(P4) of pregroups.

For $u \in W(A, X)$ and $\beta \in \mathrm{dom}(u)$ by $u_\beta = u\,|_\beta$ we denote the restriction of $u$ on $[1_A, \beta]$. If $u$ is reduced and $\beta \in \mathrm{dom}(u)$ then

$$u = u_\beta \circ \tilde{u}_\beta,$$

for some uniquely defined $\tilde{u}_\beta$.

An element $\mathrm{com}(u, v) \in R(A, X)$ is called the (*longest*) *common initial segment* of $A$-words $u$ and $v$ if

$$u = \mathrm{com}(u, v) \circ \tilde{u}, \quad v = \mathrm{com}(u, v) \circ \tilde{v}$$

for some (uniquely defined) $A$-words $\tilde{u}, \tilde{v}$ such that $\tilde{u}(1_A) \neq \tilde{v}(1_A)$. Notice that, there are words $u, v \in R(A, X)$ for which $\mathrm{com}(u, v)$ does not exist. In fact, $\mathrm{com}(u, v)$

exists if and only if the following element from $A$ is defined:

$$\delta(u,v) = \begin{cases} 0 & \text{if } u(1_A) \neq v(1_A) \\ \sup\{\beta \mid u_\beta = v_\beta\} & \text{if it exists} \\ \text{undefined} & \text{otherwise} \end{cases}$$

In this case

$$\mathrm{com}(u,v) = u\mid_{\delta(u,v)} = v\mid_{\delta(u,v)}.$$

Clearly, if the length of $u$ is finite then $\delta(u,v)$ and $\delta(v,u)$ are defined for every $v \in R(A,X)$.

Definition 3.2. Let $u, v \in R(A,X)$. If $\mathrm{com}(u^{-1},v)$ is defined then

$$u^{-1} = \mathrm{com}(u^{-1},v)\circ\tilde{u}, \quad v = \mathrm{com}(u^{-1},v)\circ\tilde{v},$$

for some uniquely defined $\tilde{u}$ and $\tilde{v}$. In this event put

$$u * v = \tilde{u}^{-1}\circ\tilde{v}.$$

The product $*$ is a partial binary operation on $R(A,X)$.

Example 3.3. Let $A = \mathbb{Z}^2$ with the right lexicographic order (in this case $1_A = (1,0)$). Put

$$w(\beta) = \begin{cases} x & \text{if } \beta = (s,0) \text{ and } s \geqslant 1 \\ x^{-1} & \text{if } \beta = (s,1) \text{ and } s \leqslant 0 \end{cases}$$

Then

$$w : [1_A, (0,1)] \to X^{\pm}$$

is a reduced $A$-word. Clearly, $w^{-1} = w$ so $w * w = \varepsilon$. In particular, $R(A,X)$ has 2-torsion with respect to $*$.

If $u, v \in R(\mathbb{Z}[t], X)$ and $u * v$ is defined, then we write sometimes $u \circ_\alpha v$ instead of $u * v$ provided $|\mathrm{com}(u^{-1},v)| < \alpha$.

The main result of this section is the following theorem.

Theorem 3.4. *Let $A$ be a discretely ordered abelian group and $X$ be a set. Then the set of reduced $A$-words $R(A,X)$ with the partial binary operation $*$ satisfies the axioms* (P1)–(P4) *of a pregroup.*

Proof. The axioms (P1), (P2), and (P3) follow immediately from definitions.

Let $u, v, w$ be reduced $A$-words such that the products $u * v, v * w$ are defined. Suppose that one of the products $(u * v) * w, u * (v * w)$, say $(u * v) * w$, is defined (the other case is similar). We need to show that the product $u * (v * w)$ is also defined and the equality

$$(u * v) * w = u * (v * w). \tag{3}$$

holds.

Since $v * w$ is defined we have

$$v = v_1 \circ c, \quad w = c^{-1} \circ w_1, \quad v * w = v_1 * w_1 = v_1 \circ w_2 \tag{4}$$

for some (perhaps, trivial) $v_1, w_1, c \in R(A,X)$, where $c = \mathrm{com}(v^{-1}, w)$.

Consider several cases.

C1). $u * v = u \circ v$.

a) Let $v_1 \neq \varepsilon$. In this case

$$(u * v) * w = (u \circ v_1 \circ c) * (c^{-1} \circ w_1) = u \circ v_1 \circ w_1.$$

On the other hand,

$$u * (v * w) = u * \big((v_1 \circ c) * (c^{-1} \circ w_2)\big) = u * (v_1 \circ w_1) = u \circ v_1 \circ w_1,$$

so it is defined and (3) holds.

b) Let $v_1 = \varepsilon$. Then $w = v^{-1} \circ w_1$ and in this case

$$(u * v) * w = (u \circ v) * (v^{-1} \circ w_1) = u * w_1,$$

which is defined. On the other hand,

$$u * (v * w) = u * (v * (v^{-1} \circ w_1)) = u * w_1,$$

which is also defined and equal to $(u * v) * w$.

C2) $u = v^{-1}$.

In this case

$$(u * v) * w = (v^{-1} * v) * w = w.$$

On the other hand, in notations from (4), we have

$$u * (v * w) = v^{-1} * (v * w) = (c^{-1} \circ v_1^{-1}) * \big((v_1 \circ c) * (c^{-1} \circ w_1)\big) =$$

$$= (c^{-1} \circ v_1^{-1}) * (v_1 \circ w_1) = c^{-1} \circ w_1 = w,$$

hence, it is defined and (3) holds.

Now we are ready to prove the general case.

C3) Let $u = u_1 \circ u_2^{-1}$ and $v = u_2 \circ v_2$ for some (perhaps trivial) elements $u_1, u_2, v_2 \in R(A, X)$. Then $u * v = u_1 \circ v_2$ and the triple $u_1, v_2, w$ satisfies all conditions of C1) (observe, that $v_2 * w$ is defined since $v * w$ is defined). Hence,

$$(u * v) * w = (u_1 * v_2) * w \overset{C1}{=} u_1 * (v_2 * w).$$

Finally,

$$u * (v * w) = (u_1 \circ u_2^{-1}) * ((u_2 \circ v_2) * w) \overset{C1}{=} (u_1 \circ u_2^{-1}) * (u_2 * (v_2 * w)) \overset{C1}{=}$$

$$u_1 * \big(u_2^{-1} * (u_2 * (v_2 * w))\big) \overset{C2}{=} u_1 * (v_2 * w) = (u * v) * w,$$

as desired. □

A subset $G \leqslant R(A, X)$ is called a *subgroup* of $R(A, X)$ if $G$ is a group with respect to $*$. We say that a subset $Y \subset R(A, X)$ *generates a subgroup* $\langle Y \rangle$ in $R(A, X)$ if the product $y_1 * \ldots * y_n$ is defined for any finite sequence of elements $y_1, \ldots, y_n \in Y^{\pm 1}$.

Example 3.5. Let $A$ be a direct sum of copies of $\mathbb{Z}$ with the right lexicographic order. Then the set of all elements of finite length in $R(A, X)$ forms a subgroup which is isomorphic to a free group with basis $X$.

**3.3. Standard Exponentiation, roots, and conjugation.** In this section we study properties of the "standard exponentiation" (by integers) in $R(A, X)$, roots of elements, and conjugation.

Observe, that there are elements $w \in R(A, X)$ for which even the square $w * w$ is not defined. We have to exclude such elements from our considerations related to exponentiation. Put

$$\begin{aligned} E_n R(A, X) &= \{w \in R(A, X) \mid w^k \text{ is defined for every } k \leqslant n\} \\ E_\infty R(A, X) &= \bigcap_n E_n R(A, X). \end{aligned}$$

Then the set $E_\infty R(A,X)$ is closed under the "standard" exponentiation by elements of $\mathbb{Z}$. Notice, that $E_\infty R(A,X)$ is precisely the set of elements from $R(A,X)$ for which the notion of order is defined. The following definitions provide some tools to classify orders of elements from $E_\infty R(A,X)$. An element $v \in R(A,X)$ is termed *cyclically reduced* if $v(1_A)^{-1} \neq v(|v|)$. We say that an element $v \in R(A,X)$ admits a *cyclic decomposition* if $v = c^{-1} \circ u \circ c$, where $c, u \in R(A,X)$ and $u$ is cyclically reduced. Observe that a cyclic decomposition is unique (whenever it exists). Denote by $CR(A,X)$ the set of all cyclically reduced words in $R(A,X)$ and by $CDR(A,X)$ the set of all words from $R(A,X)$ which admit a cyclic decomposition. Obviously, $CDR(A,X) \subset E_\infty R(A,X)$. Not all elements in $E_\infty R(A,X)$ admit cyclic decomposition, for instance, the element $w$ of order 2 from Example 3.3 in Section 3.2 does not. We will show below that such elements are the only elements in $E_\infty R(A,X)$ which do not admit cyclic decomposition. Put

$$T_2R(A,X) = \{w \in R(A,X) \mid w * w = \varepsilon\}.$$

Clearly, $T_2R(A,X) \subset E_\infty R(A,X)$.

LEMMA 3.6. *Let $A$ be a discretely ordered abelian group and $X$ be a set. Then:*

1) $E_2R(A,X) = CDR(A,X) \cup T_2R(A,X)$;
2) $E_\infty R(A,X) = E_2R(A,X)$;
3) *every element from $CDR(A,X)$ has infinite order.*

PROOF. Let $v \in E_2R(A,X), v \neq \varepsilon$. Then $v = v_1 \circ c = c^{-1} \circ v_2$ for some $v_1, v_2, c \in R(A,X)$ such that $v_1 * v_2 = v_1 \circ v_2$.

If $|v_2| \geqslant |c|$ then $v_2 = v_3 \circ c$, so $v = c^{-1} \circ v_3 \circ c$ and $v_3 * v_3 = v_3 \circ v_3$. In this case $v_3$ is cyclically reduced and $v \in CDR(A,X)$.

If $|v_2| < |c|$ then $c = c_1 \circ v_2$, therefore

$$v = v_1 \circ c_1 \circ v_2 = v_2^{-1} \circ c_1^{-1} \circ v_2$$

which implies $c_1 = c_1^{-1}$ and hence, $v * v = \varepsilon$, i.e., $v \in T_2R(A,X)$. Now 1) follows.

To see 2) observe that $E_\infty R(A,X) \subset E_2R(A,X)$ and, as we have mentioned above, $CDR(A,X) \cup T_2R(A,X) \subset E_\infty R(A,X)$. Now 2) follows from 1).

If $v = c^{-1} \circ u \circ c$ and $\varepsilon \neq u \in CR(A,X)$, then $v^k = c^{-1} \circ u^k \circ c$ and $|u^k| = k|u| > 0$. It follows that $|v^k| \geqslant |u^k| > 0$, hence, $v^k \neq \varepsilon$. This proves 3), and the lemma. □

Since the set $T_2R(A,X)$ is not very interesting from the exponentiation viewpoint, in what follows we bound our considerations to the set $CDR(A,X)$.

Let $v \in CDR(A,X)$ we say that $u \in CDR(A,X)$ is a *$k$-root* of $v$ if $v = u^k$.

LEMMA 3.7. *Let $A$ be a discretely ordered abelian group, $X$ be a set and let $v \in CDR(A,X)$. Then*

1) *If for a given $k$, $v$ has a $k$-root, then this $k$-root is unique.*
2) *If $A = \mathbb{Z}[t]$ then there are only finitely many numbers $k \in \mathbb{N}$ such that $v$ has a $k$-root.*

PROOF. Let $v \in CDR(A,X)$ and $v = c^{-1} \circ w \circ c$ be its cyclic decomposition. It is easy to see that if $v$ has a $k$-root $u$ then $u = c^{-1} \circ u_1 \circ c$, where $u_1$ is a $k$-root of $w$. The converse is also true, that is there exists a $k$-root of $w$ which after conjugation by $c$ becomes a $k$-root for $v$. Thus, without loss of generality we can assume $v$ to be cyclically reduced.

1) Let $k \in \mathbb{N}$ be fixed. Since any root $u$ of $v$ is an element of $CDR(A, X)$, which is the restriction of $v$ on the segment $[1_A, |v|/k]$, we have uniqueness of roots automatically.

2) A necessary condition for the existence of a $k$-root for $v$ is the divisibility of $|v|$ by $k$ in $\mathbb{Z}[t]$.

Recall, that as a group $\mathbb{Z}[t]$ is the infinite direct sum

$$\mathbb{Z}[t] = \bigoplus_{i=0}^{\infty} \langle t^i \rangle$$

of copies of $\mathbb{Z}$. Hence, there exists $n \in \mathbb{N}$ such that $|v|$ belongs to the subgroup $E_n = \bigoplus_{i=0}^{n} \langle t^i \rangle \geqslant \mathbb{Z}$.

Observe that $E_n$ is a direct summand of the additive group of $\mathbb{Z}[t]$, hence, $E_n$ contains all roots of $v$. Since $E_n$ is finitely generated, $v$ has only finitely many roots in $E_n$, and the result follows. □

Let $u, v \in CDR(A, X)$ we say that $u$ is a *conjugate* of $v$ if there exists $c \in R(A, X)$ such that the products $c^{-1} * v$, $v * c$, and $(c^{-1} * v) * c$ are defined and $u = c^{-1} * v * c$. We say that $u$ is a *cyclic permutation* of $v$ if $v = v_1 \circ v_2$ and $u = v_2 \circ v_1$ for some elements $v_1, v_2 \in R(A, X)$ (observe that there can be infinitely many different cyclic permutations of a given $v$).

Lemma 3.8. *Let $A$ be a discretely ordered abelian group and $X$ be a set. Then the following hold:*

1) *if $u \in CDR(A, X), c \in R(A, X)$ and $v = c^{-1} * u * c$ is defined then $v \in CDR(A, X)$;*
2) *if $u, v \in R(A, X)$ are conjugate and cyclically reduced then $|u| = |v|$. Moreover, if $g^{-1} * u * g = v$ for some $g$ such that $|g| \leqslant |u|$ then $u$ is a cyclic permutation of $v$.*

Proof. 1) Let $v = c^{-1} \circ u \circ c \in CDR(A, X)$ and $d \in R(A, X)$. We assume that $d^{-1} * v$ and $v * d$ are both defined. Then $c * d$ and so $d^{-1} * c^{-1}$ are also defined and

$$d^{-1} * (c^{-1} \circ u \circ c) * d = (c * d)^{-1} * u * (c * d).$$

In other words we can assume from the beginning that $v$ is cyclically reduced. So, assume $c = \varepsilon$ and $v = u$. Since $v$ is cyclically reduced then either $d^{-1} * v = d^{-1} \circ v$ or $v * d = v \circ d$. Assume the latter.

a) $v$ does not cancel completely in $d^{-1} * (v \circ d)$. Then $v = v_1 \circ v_2, d = v_1 \circ d_1$ and $d^{-1} * (v \circ d) = d_1^{-1} \circ v_2 \circ v_1 \circ d_1$, where $v_2 \circ v_1$ is cyclically reduced as a cyclic permutation of $v$.

b) $v$ cancels completely in $d^{-1} * (v \circ d)$. Then $d$ and $v \circ d$ have common initial segment $w$ so that $d = w \circ d_2, v \circ d = w \circ d_1$ and $w = v \circ d_3 \neq \varepsilon$. Thus we have $d = d_3 \circ d_1, d = v \circ d_3 \circ d_2$. It follows that $|d_1| > |d_2|$ and moreover $d_2$ is a terminal segment of $d_1$. Hence, $d_1 = d_4 \circ d_2$ and we have

$$d^{-1} * (v \circ d) = d_2^{-1} \circ d_1 = d_2^{-1} \circ d_4 \circ d_2.$$

Since $d_4$ is cyclically reduced we obtained a cyclic decomposition of $d^{-1} * (v \circ d)$.

So, in both cases we showed that $d^{-1} * (v \circ d) \in CDR(A, X)$.

2) Suppose $g^{-1} * u * g = v$ for some $g$. Then either $g^{-1} * u = g^{-1} \circ u$ or $u * g = u \circ g$ because $u$ is cyclically reduced. Assume the latter. Moreover, $g^{-1}$

cancels completely in $g^{-1} * (u \circ g)$ because $v$ is cyclically reduced, so we have $|v| = |g^{-1} * (u \circ g)| = |u| + |g| - |g^{-1}| = |u|$.

If $|g| \leqslant |u|$ then $u = g \circ u_1$, but $v = u_1 \circ g$, so $u$ is a cyclic permutation of $v$. □

## 4. A free Lyndon length function on $CDR(A, X)$

The main result of this section is the following theorem.

THEOREM 4.1. *Let $A$ be a discretely ordered abelian group and $X$ be a set. Then the function $L : CDR(A, X) \to A$ defined as $L(w) = |w|$ satisfies all the axioms* (L1)–(L5) *of a Lyndon length function whenever the corresponding products of elements in these axioms are defined.*

PROOF. Axioms (L1) and (L2) follow immediately from the definition of the length $|w|$ of an element from $CDR(A, X)$. To prove (L3) recall the definition of the function $\delta(u, v)$ from Subsection 3.2

$$\delta(u,v) = \begin{cases} 0 & \text{if } u(1_A) \neq v(1_A) \\ \max\{\beta \mid u_\beta = v_\beta\} & \text{if such } \beta \text{ exists} \\ \text{undefined} & \text{otherwise} \end{cases}$$

By definition $\delta(u, v)$ measures the length of the longest common initial segment of $u$ and $v$. It was shown that the product $u^{-1} * v$ is defined if and only if $\delta(u, v)$ is defined, in which case

$$\delta(u,v) = \frac{1}{2}(|u| + |v| - |u^{-1} * v|) = c(u,v).$$

Now the axiom (L3) easily holds whenever the products $u^{-1} * v$, $u^{-1} * w$, $v^{-1} * w$ are defined. Moreover, (L4) holds as well, since $\delta(u, v) \in A$, whenever defined.

The axiom (L5) follows from the existence of the cyclic decomposition. This proves the theorem. □

COROLLARY 4.2. *Let $A$ be a discretely ordered abelian group and $X$ be a set. Then any subgroup $G$ of $CDR(A, X)$ has a free Lyndon length function with values in $A$ – the restriction $L|_G$ on $G$ of the standard length function $L$ on $CDR(A, X)$.*

## 5. Lyndon's Exponentiation

In this section we describe a $\mathbb{Z}[t]$-exponentiation on the set $CDR(\mathbb{Z}[t], X)$. This gives a very natural and concrete realization of Lyndon's axiomatic approach to exponentiation by polynomials with integer coefficients. Recall that we view $\mathbb{Z}[t]$ as a discrete abelian group with respect to the lexicographic order described in Section 2.3. Observe that in this case $1_{\mathbb{Z}[t]} = 1$.

Our strategy here is to define first exponentiation on $CR(\mathbb{Z}[t], X)$ and then to extend it to $CDR(\mathbb{Z}[t], X)$ via conjugation.

**5.1. Exponentiation on $CR(\mathbb{Z}[t], X)$.** Recall that as a group $\mathbb{Z}[t]$ is a countable direct sum

$$\mathbb{Z}[t] = \bigoplus_{i=0}^{\infty} \langle t^i \rangle$$

of copies of the infinite cyclic group $\mathbb{Z}$ with the right lexicographic order. Recall that

$$E_n = \{f(t) \in \mathbb{Z}[t] \mid \deg(f(t)) \leqslant n\},$$

where $n \geqslant 0$, form the complete chain of convex subgroups of $\mathbb{Z}[t]$. It is easy to see that $R(\mathbb{Z}[t], X)$ is the union of the following chain

$$R(E_0, X) \subset R(E_1, X) \subset \cdots \subset R(E_n, X) \subset \cdots .$$

For an element $w \in R(E_n, X)$ the length $|w|$ is a polynomial $g(t) \in \mathbb{Z}[t]$:

$$|w| = g(t) = a_0 + a_1 t + \cdots + a_n t^n,$$

where $a_n > 0$. In this event we say that $w$ has *height* $n$ and write $h(w) = n$. Clearly,

$$h(w) = n \Leftrightarrow |w| \in E_n - E_{n-1} \Leftrightarrow w \in R(E_n, X) - R(E_{n-1}, X).$$

Now we define exponents $v^{f(t)}$ for a given element $v \in CR(\mathbb{Z}[t], X)$ and a polynomial $f(t) \in \mathbb{Z}[t]$ according to the following cases.

1) Let $v \in CR(\mathbb{Z}[t], X)$ not be a proper power and

$$|v| = g(t) = a_0 + \cdots + a_n t^n, \quad a_n > 0.$$

We define $v^t$ as an element of $CR(\mathbb{Z}[t], X)$ of length $|v^t| = g(t)t$, so, $v^t$ is a function with the domain $[1, g(t)t]$ and

$$g(t)t = a_0 t + a_1 t^2 + \cdots + a_{n-1} t^n + a_n t^{n+1}, \quad a_n > 0.$$

a) If $a_n = 1$ then set

$$v^t(\beta) = \begin{cases} v(\alpha), & \text{if } \beta = mg(t) + \alpha, m \in \mathbb{N}, m \geqslant 0, 1 \leqslant \alpha \leqslant g(t); \\ v(\alpha), & \text{if } \beta = g(t)t - mg(t) + \alpha, m \in \mathbb{N}, m > 0, 1 \leqslant \alpha \leqslant g(t). \end{cases}$$

We claim that this formula defines $v^t(\beta)$ for any $\beta \in [1, g(t)t]$. Indeed, observe that the formula above defines $v^t(\beta)$ for any $\beta$ which belongs either to some initial subsegment of $[1, g(t)t]$ of the form $[1, mg(t)]$ where $m \geqslant 0$ or to some terminal subsegment of $[1, g(t)t]$ of the form $[g(t)t - mg(t), g(t)t]$ where $m > 0$.

Now, any $\beta \in [1, g(t)t]$ is a polynomial $\beta = r(t) = r_1(t) + b_p t^p \in \mathbb{Z}[t]$, where $b_p > 0$, $\deg(r_1) < p$, and either $p < n + 1$ or $p = n + 1$, $b_p = 1$, $r_1(t) < 0$. In the former case there exists $m \geqslant 0$ such that $mg(t) > r(t)$, so that $[1, \beta]$ is an initial subsegment of $[1, mg(t)]$ and $\beta \in [1, mg(t)]$. In the latter case there exists $m > 0$ such that $g(t)t - mg(t) < r(t)$, so that $[\beta, g(t)t]$ is a terminal subsegment of $[g(t)t - mg(t), g(t)t]$ and $\beta \in [g(t)t - mg(t), g(t)t]$.

b) If $a_n > 1$ then we present $[1, g(t)t]$ as the union of disjoint closed segments

$$\left( \bigcup_{k=0}^{a_n - 2} [kt^{n+1} + 1, (k+1)t^{n+1}] \right) \bigcup [(a_n - 1)t^{n+1} + 1, g(t)t]$$

and define $v^t$ on these segments as follows.

For any $k \in [0, a_n - 2]$ and $\beta \in [kt^{n+1} + 1, (k+1)t^{n+1}]$ we set

$$v^t(\beta) = \begin{cases} v(\alpha), & \text{if } \beta = kt^{n+1} + mg(t) + \alpha, m \geqslant 0, 1 \leqslant \alpha \leqslant g(t); \\ v(\alpha), & \text{if } \beta = (k+1)t^{n+1} - mg(t) + \alpha, m > 0, 1 \leqslant \alpha \leqslant g(t). \end{cases}$$

and for $\beta \in [(a_n - 1)t^{n+1} + 1, g(t)t]$ we set

$$v^t(\beta) = \begin{cases} v(\alpha), & \text{if } \beta = (a_n - 1)t^{n+1} + mg(t) + \alpha, m \geqslant 0, 1 \leqslant \alpha \leqslant g(t); \\ v(\alpha), & \text{if } \beta = g(t)t - mg(t) + \alpha, m > 0, 1 \leqslant \alpha \leqslant g(t). \end{cases}$$

For any $k \in [0, a_n - 2]$, the first formula above defines $v^t(\beta)$ for any $\beta$ which belongs to some initial subsegment of $[kt^{n+1} + 1, (k+1)t^{n+1}]$ of the form
$[kt^{n+1}, kt^{n+1} + mg(t)]$ where $m \geqslant 0$ or to some terminal subsegment of $[kt^{n+1} + 1, (k+1)t^{n+1}]$ of the form $[(k+1)t^{n+1} - mg(t), (k+1)t^{n+1}]$ where $m > 0$. The second formula given above defines $v^t(\beta)$ for any $\beta$ which belongs to any initial subsegment of $[(a_n - 1)t^{n+1}, g(t)t]$ of the form $[(a_n - 1)t^{n+1}, (a_n - 1)t^{n+1} + mg(t)]$ where $m \geqslant 0$ or to any terminal subsegment of $[(a_n - 1)t^{n+1}, g(t)t]$ of the form $[g(t)t - mg(t), g(t)t]$ where $m > 0$.

In the same way as in a) one can show that these formulas define $v^t(\beta)$ for any $\beta \in [1, g(t)t]$.

2) If $v \in CR(\mathbb{Z}[t], X)$ is such that $v = u^k$ for some $u \in CR(\mathbb{Z}[t], X)$ then we set $v^t = (u^t)^k$.

Thus we have defined an exponent $v^t$ for a given $v \in CR(\mathbb{Z}[t], X)$. Notice that it follows from the construction that $|v^t| = g(t)t = |v|t$ and $v^t$ starts with $v$ and ends with $v$. In particular, $v^t \in CR(\mathbb{Z}[t], X)$. It follows that $v^t * v = v^t \circ v = v \circ v^t = v * v^t$, hence, $[v^t, v] = \varepsilon$.

3) Now for $v \in CR(\mathbb{Z}[t], X)$ we define exponents $v^{t^k}$ by induction. Since $v^t \in CR(\mathbb{Z}[t], X)$ one can repeat the construction from 1) and define

$$v^{t^{k+1}} = (v^{t^k})^t.$$

4) Now we define $v^{f(t)}$, where $f(t) \in \mathbb{Z}[t]$, by linearity, that is, if $f(t) = m_0 + m_1 t + \ldots + m_k t^k$ then

$$v^{f(t)} = v^{m_0} * (v^t)^{m_1} * \cdots * (v^{t^k})^{m_k}.$$

Observe that the product above is defined because $v^{t^{m+1}}$ is cyclically reduced, and starts and ends with $v^{t^m}$.

The following result is a direct consequence of the construction.

LEMMA 5.1. *Let $v \in CR(\mathbb{Z}[t], X), f(t) \in \mathbb{Z}[t]$. Then $v^{f(t)} \in CR(\mathbb{Z}[t], X)$ and $|v^{f(t)}| = g(t)|f(t)| = |v||f(t)|, [v^{f(t)}, v] = \varepsilon$.*

The following result shows that $\mathbb{Z}[t]$-exponentiation on $CR(\mathbb{Z}[t], X)$ satisfies the axiom E2).

LEMMA 5.2. *Let $u, v \in CR(\mathbb{Z}[t], X)$ and $u = c^{-1} * v * c$ for some $c \in R(\mathbb{Z}[t], X)$. Then for every $f(t) \in \mathbb{Z}[t]$*

$$u^{f(t)} = c^{-1} * v^{f(t)} * c.$$

PROOF. Since $u$ and $v$ are cyclically reduced and $u = c^{-1} * v * c$ then $v = v_1 \circ v_2, u = v_2 \circ v_1, c = v_1$.

In view of 4) it suffices to show prove the lemma for $f(t) = t^n$. Let $f(t) = t$. We want to show that.

$$(v_2 \circ v_1)^t = v_1^{-1} * (v_1 \circ v_2)^t * v_1.$$

We have $|v_2 \circ v_1| = |v_1 \circ v_2|$ and $(v_2 \circ v_1)^t(\beta) = (v_1 \circ v_2)^t(\beta + |v_1|)$ for $\beta \in [1, |v|t - |v_1|]$. When we conjugate $(v_1 \circ v_2)^t$ by $v_1$ we cancel the initial segment of $(v_1 \circ v_2)^t$ of length $|v_1|$ and add a terminal segment of length $|v_1|$, so we have $(v_2 \circ v_1)^t(\beta) = (v^{-1} * (v_1 \circ v_2)^t * v_1)(\beta)$, $\beta \in [1, |v|t]$, and $(v_2 \circ v_1)^t = v_1^{-1} * (v_1 \circ v_2)^t * v_1$.

Since $v^t$ and $u^t$ are cyclic permutations of each other and both belong to $CR(\mathbb{Z}[t], X)$ one can apply the induction on $\deg f(t)$ and the lemma follows. □

LEMMA 5.3. *Let $u, v \in CR(\mathbb{Z}[t], X)$ and $f(t), g(t) \in \mathbb{Z}[t]$ be such that $u^{f(t)} = v^{g(t)}$. Then $[u, v]$ is defined and is equal to $\varepsilon$.*

PROOF. Since $[u, u^{f(t)}] = \varepsilon$ and $[v, v^{g(t)}] = \varepsilon$ then $[u, v^{g(t)}] = \varepsilon$ and $[v, u^{f(t)}] = \varepsilon$. From the latter equalities we will derive the required statement.

Observe that if $|u| = |v|$ then it follows automatically that $u = v^{\pm 1}$. Indeed, by the definition of exponents $u^{f(t)}$ and $v^{g(t)}$ have correspondingly $u^{\pm 1}$ and $v^{\pm 1}$ as initial segments. Since $u^{f(t)} = v^{g(t)}$ then initial segments of length $|u|$ in both coincide.

We can assume $|u| < |v|$ and consider $[u, v^{g(t)}] = \varepsilon$ (if $|u| > |v|$ then we consider $[v, u^{f(t)}] = \varepsilon$ and apply the same arguments). Also, $g(t) > 1$, otherwise we have nothing to prove.

Thus we have $u * v^{g(t)} = v^{g(t)} * u$. Since $u$ and $v$ are cyclically reduced and equal $\mathbb{Z}[t]$-words have equal initial and terminal segments of the same length then $[u, v]$ is defined and we have two cases.

a) $u * v = u \circ v$.

Thus, automatically we have $v * u = v \circ u$

$u \circ v^{g(t)}$ and $v^{g(t)} \circ u$ have the same initial segment of length $2|v|$. So $v = u \circ v_1 = v_1 \circ v_2$ and $|u| = |v_2|$. Comparing terminal segments of $u \circ v^{g(t)}$ and $v^{g(t)} \circ u$ of length $|u|$ we have $u = v_2$ and from $u \circ v_1 = v_1 \circ u$ it follows that $[u, v] = \varepsilon$.

b) There is a cancellation in $u * v$.

Then, from $u^{f(t)} = v^{g(t)}$ it follows that $v^{-1} = v_1^{-1} \circ u$ and so $v = u^{-1} \circ v_1$. Using the same arguments as in a) we obtain $v = u^{-1} \circ v_1 = v_1 \circ v_2$, $|u| = |v_2|$ and $u^{-1} = v_2$. It follows immediately that $[u, v] = \varepsilon$. □

**5.2. Exponentiation on $CDR(\mathbb{Z}[t], X)$.** Let $v \in CDR(\mathbb{Z}[t], X)$ have a cyclic decomposition $v = c^{-1} \circ u \circ c$ and $f(t) \in \mathbb{Z}[t]$. We define $v^{f(t)}$ as follows

$$v^{f(t)} = c^{-1} \circ u^{f(t)} \circ c. \tag{5}$$

Observe that the product above is well defined since $u^{f(t)}$ starts and ends on $u$ if $f(t) > 0$, and starts and ends on $u^{-1}$ if $f(t) < 0$.

Thus we have defined $\mathbb{Z}[t]$-exponentiation function

$$\exp : CDR(\mathbb{Z}[t], X) \times \mathbb{Z}[t] \to CDR(\mathbb{Z}[t], X)$$

on the whole set $CDR(\mathbb{Z}[t], X)$.

There are other ways of defining $\mathbb{Z}[t]$-exponentiation on $CDR(\mathbb{Z}[t], X)$ but from now on we fix the exponentiation described above.

LEMMA 5.4. *Let $u, v \in CDR(\mathbb{Z}[t], X)$ be such that $h(u) = h(v)$ and $[u, v] = \varepsilon$. Then $[u^{f(t)}, v] = \varepsilon$ for any $f(t) \in \mathbb{Z}[t]$ provided $[u^{f(t)}, v]$ is defined.*

PROOF. We can assume that either $u$ or $v$ is cyclically reduced. This is always possible because both elements belong to $CDR(\mathbb{Z}[t], X)$. Suppose we have $v^{-1} * u * v = u$, where $u$ is cyclically reduced.

a) $|u| < |v|$

Since $u$ is cyclically reduced either $v^{-1} * u = v^{-1} \circ u$ or $u * v = u \circ v$. Assume the former. Then $v$ has to cancel completely in $v^{-1} * u * v$ because this product is equal to $u$ which is cyclically reduced. So $v$ has the form $v = u^k \circ w$, where $k < 0$ is the smallest possible and $w$ does not have $u$ as an initial segment. We have then

$$v^{-1} * u * v = w^{-1} * u * w = w^{-1} * (u \circ w) = u.$$

and $w^{-1}$ cancels completely. In this case the only possibility is that $|w| < |u|$ (otherwise we have a contradiction with the choice of $k$) and $[u, w] = \varepsilon$. So now we reduced everything to the case b) because clearly $[u^{f(t)}, u^k] = \varepsilon$ for any $f(t) \in \mathbb{Z}[t]$.

b) $|u| > |v|$

We have $v^{-1} * u * v = u$. $u$ is cyclically reduced, moreover, $u$ is a cyclic permutation of itself that is $v^{-1} * u * v = u$. Finally, since $[u^{f(t)}, v]$ is defined then

$$v^{-1} * u^{f(t)} * v = u^{f(t)}$$

follows from Lemma 5.2. □

We summarize the properties of the exponentiation *exp* in the following theorem.

THEOREM 5.5. *The $\mathbb{Z}[t]$-exponentiation function*

$$\exp : (u, f(t)) \mapsto u^{f(t)}$$

*defined in* (5) *satisfies the following axioms* (*here $u, v \in CDR(\mathbb{Z}[t], X)$ and $f, g \in \mathbb{Z}[t]$*):

E1) $u^1 = u, \quad u^{fg} = (u^f)^g, \quad u^{f+g} = u^f * u^g$,

E2) $(v^{-1} * u * v)^f = v^{-1} * u^f * v$ *provided* $[u, v] = \varepsilon$ *and* $h(u) = h(v)$, *or* $u = v \circ w$, *or* $u = w^\alpha$, $v = w^\beta$ *for some* $w \in CDR(\mathbb{Z}[t], X)$ *and* $\alpha, \beta \in \mathbb{Z}[t]$;

E3) *if* $[u, v] = \varepsilon$ *and* $u = w^\alpha$, $v = w^\beta$ *for some* $w \in CDR(\mathbb{Z}[t], X)$ *and* $\alpha, \beta \in \mathbb{Z}[t]$ *then*

$$(u * v)^f = u^f * v^f$$

PROOF. Let $u \in CDR(\mathbb{Z}[t], X)$ and $\alpha, \beta \in \mathbb{Z}[t]$.

E1) The equalities $u^1 = u$ and $(u^f)^g = u^{fg}$ follow directly from the definition of exponentiation. We need to prove only that $u^{f+g} = u^f * u^g$. Let

$$u = c^{-1} \circ u_1^k \circ c$$

be a cyclic decomposition of $u$. Then

$$u^f = c^{-1} \circ (u_1^f)^k \circ c, \quad u^g = c^{-1} \circ (u_1^g)^k \circ c.$$

Now

$$u^{f+g} = c^{-1} \circ (u_1^{f+g})^k \circ c = (c^{-1} \circ (u_1^f)^k \circ c) * (c^{-1} \circ (u_1^g)^k \circ c),$$

as required.

E2) If $u = w^\alpha, v = w^\beta$ for some $w \in CDR(\mathbb{Z}[t], X)$ and $\alpha, \beta \in \mathbb{Z}[t]$, then the result follows from the definition of exponentiation. If $[u, v] = \varepsilon$ and $h(u) = h(v)$ then result follows from Lemma 5.4. If $u = v \circ w$ then result follows from Lemma 5.2.

E3) We have $(u * v)^f = (w^{\alpha+\beta})^f = w^{(\alpha+\beta)f} = w^{\alpha f} * w^{\beta f} = (w^\alpha)^f * (w^\beta)^f = u^f * v^f$. □

## 6. Extensions of centralizers

In this section we prove that for certain subgroups $G \leqslant CDR(\mathbb{Z}[t], X)$ the extension $H$ of all cyclic centralizers of $G$ by $\mathbb{Z}[t]$ has a natural embedding into $CDR(\mathbb{Z}[t], X)$. This is the main technical result of the paper, it provides the induction argument for our proof that $F^{\mathbb{Z}[t]}$ embeds into $CDR(\mathbb{Z}[t], X)$.

In Subsection 6.1 we introduce and study some conditions on subgroups $G \leqslant CDR(\mathbb{Z}[t], X)$, which allow one to carry out the induction step. In Subsection 6.2 we construct the embedding of $H$ into $CDR(\mathbb{Z}[t], X)$. In Subsection 6.3 we prove that $H$ also satisfies all the induction hypothesis, this finishes the induction step.

### 6.1. Separation, Lyndon's sets, and normal forms.

Definition 6.1. Let $G \leqslant CDR(\mathbb{Z}[t], X)$. We say that $G$ *is subwords-closed* if $G$ contains all sybwords of its elements.

Recall that the set $H_0$ of all words in $CDR(\mathbb{Z}[t], X)$ of finite length is a subgroup which is canonically isomorphic to the free group $F = F(X)$. Moreover, the length function on $F$ induced from $CDR(\mathbb{Z}[t], X)$ is equal to the standard length function on $F$. Throughout this section we identify $F$ with $H_0$ via the canonical isomorphism. Clearly, $F$ is subwords-closed.

Definition 6.2. Let $u, v \in CDR(\mathbb{Z}[t], X)$ and $u = c^{-1} \circ u_1 \circ c, \;\; v = d^{-1} \circ v_1 \circ d$ be their cyclic decompositions. Put $\delta = \delta(u, v) = \max\{|c|, |d|\}$. We say that $u$ and $v$ are *separated* if $u^m * v^n$ is defined for any $n, m \in \mathbb{N}$ and there exists $r = r(u, v) \in \mathbb{N}$ such that for all $m, n > r$

$$u^m * v^n = u^{m-r} \circ_\delta (u^r * v^r) \circ_\delta v^{n-r}.$$

Definition 6.3. A subset $M \subseteq CDR(\mathbb{Z}[t], X)$ is called an *S-set* if any two non-commuting elements of $M$ with cyclic centralizers are separated. In the case when $M$ is a group we call $M$ an *S-subgroup*.

To show that some elements of $CDR(\mathbb{Z}[t], X)$ are separated we need the following lemma, which is well-known in the case of finite words.

Lemma 6.4. *Let $G$ be a subgroup of $CDR(\mathbb{Z}[t], X)$ and $f, h \in G$ be cyclically reduced. If $c(f^m, h^n) \geqslant |f| + |h|$ for some $m, n > 0$ then $[f, h] = \varepsilon$.*

Proof. Suppose $|h| \geqslant |f|$ and $c(f^m, h^n) \geqslant |f| + |h|$ for some $m, n > 0$.

We have $h = f^k \circ h_1, |f| > |h_1|, k \geqslant 1$ and $f = h_1 \circ f_1$. Since $c(f^m, h^n) \geqslant |f| + |h|$ one has $(f^k \circ h_1) \circ f = f^{k+1} \circ h_1$. So, $h_1 \circ h_1 \circ f_1 = h_1 \circ f_1 \circ h_1$ and $f = h_1 \circ f_1 = f_1 \circ h_1$. It follows that $[f_1, h_1] = \varepsilon$, hence, $[h_1, f] = \varepsilon$ and $[f, h] = \varepsilon$. □

The following result is well-known in folklore. Since we could not find a proper reference we provide a complete proof of it.

Lemma 6.5. *The free group $F$ is an S-subgroup of $CDR(\mathbb{Z}[t], X)$.*

Proof. Let $u, v \in F$ and $[u, v] \neq \varepsilon$. We have to show that $u$ and $v$ are separated. Without loss of generality we may assume that $u$ and $v$ are not proper powers.

Assume that $u$ and $v$ are not separated. Hence, for any $M > 0$ and any $r \in \mathbb{N}$ there exist $m = m(M, r) > r$ and $n = n(M, r) > r$ such that $c(u^{-m}, v^n) > M$.

Let $u = a^{-1} \circ \bar{u} \circ a, v = b^{-1} \circ \bar{v} \circ b$ be cyclic decompositions of $u$ and $v$. Without loss of generality we may assume $|a| \geqslant |b|$, so $a = a_1 \circ b$. We may assume also that

$|a_1| \leqslant |\bar{v}|$ (otherwise $a_1 = \bar{v}^k \circ a_2, |a_2| \leqslant |\bar{v}|$ and we can replace $a_1$ by $a_2$). Consider the following cases.

a) $|a_1|+|\bar{u}| \geqslant |\bar{v}|$. If $|a_1|+|\bar{u}| = |\bar{v}|$ then $\bar{v} = a_1^{-1} \circ \bar{u}^{-1}$ and $c(\bar{u}^{-m}, \bar{v}^n) > |\bar{u}|+|\bar{v}|$ (if $M$ is sufficiently big). Hence, (see, for example, Lemma 6.4) $\bar{v} = \bar{u}^{-1}$, so, $a_1 = \varepsilon$. It follows that $a = b$ and $[u, v] = \varepsilon$ - contradiction.

Suppose $|a_1|+|\bar{u}| > |\bar{v}|$. Then $\bar{u}^{-1} = u_1 \circ u_2, a_1^{-1} \circ u_1 = \bar{v}^l, l \geqslant 1, \bar{v} = u_2 \circ v_1$ and $c(\bar{u}^{-m}, (v_1 \circ u_2)^n) > |\bar{u}|+|\bar{v}|$. So, by Lemma 6.4 we have $\bar{u}^{-1} = v_1 \circ u_2$ and $u_1 = v_1$. Thus, $a_1^{-1} \circ v_1 = \bar{v}^l, l \geqslant 1$ and since $|a_1| \leqslant |\bar{v}|$, we have $l = 1, a_1^{-1} \circ v_1 = \bar{v} = u_2 \circ v_1$ and hence, $a_1^{-1} = u_2$. But, in this case we have a cancellation between $a^{-1}$ and $\bar{u}$ - a contradiction with the fact that $a^{-1} \circ \bar{u}^{-1} \circ a$ is the cyclic decomposition of $u^{-1}$.

b) $|a_1|+|\bar{u}| < |\bar{v}|$. In this case we have $\bar{v} = a_1^{-1} \circ \bar{u}^{-k} \circ u_1, k > 0$ and $\bar{u}^{-1} = u_1 \circ u_2$. Hence, $c((u_2 \circ u_1)^m, \bar{v}^n) > |\bar{u}| + |\bar{v}|$ and by Lemma 6.4 we have $v = u_2 \circ u_1$. So, $\bar{u} = \bar{v}$ and $a_1 = u_1 = \varepsilon, k = 1$. It follows that $a = b, \bar{v} = \bar{u}^{-1}$ and $[u, v] = \varepsilon$ - a contradiction.

Thus, our initial assumption is false, so $u$ and $v$ are separated. □

Definition 6.6. Let $M \subseteq CDR(\mathbb{Z}[t], X)$. A subset $R_M \subseteq CR(\mathbb{Z}[t], X)$ is called a set of *representatives of* $M$ if $R_M$ satisfies the following conditions:

1) $R_M$ does not contain proper powers;
2) for any $u, v \in R_M$, $u \neq v^{-1}$;
3) for each $u \in M$ there exist $v \in R_M$, $k \in \mathbb{Z}$, $c \in R(\mathbb{Z}[t], X)$, and a cyclic permutation $\pi(v)$ of $v$ such that
$$u = c^{-1} \circ \pi(v)^k \circ c,$$
moreover, such $v, c, k, \pi(v)$ are unique.

Observe that we do not require $R_M \subset M$.

It is easy to see that a set of representatives $R_M$ exists for any $M \subseteq CDR(\mathbb{Z}[t], X)$. We show how one can obtain $R_M$ from $M$ in three steps.

Step 1. Let $w \in M$ and $w = c^{-1} \circ \overline{w} \circ c$ be its cyclic decomposition. Put $R_1 = \{\overline{w} \mid w \in M\}$.

Step 2. For $w \in R_1$ denote by $M_w$ the subset of $R_1$ consisting of all cyclic permutations of $w$ and $w^{-1}$. Choose a single element $w'$ in each set $M_w$ and put $R_2 = \{w' \mid w \in R_1\}$.

Step 3. For $w \in R_2$ denote by $w^*$ the unique (by Lemma 3.7) maximal root of $w$. Put $R_M = \{w^* \mid w \in R_2\}$. Clearly, $R_M$ satisfies the conditions 1)–3).

Observe that a set of representatives $R_M$ may not be unique for a given $M$, but all such sets have the same cardinality and can be obtained one from another by taking inverses and cyclic permutations of elements.

For a group $G$ put
$$K(G) = \{v \in G \mid C_G(v) = \langle v \rangle\}.$$

Definition 6.7. Let $G$ be a subgroup of $CDR(\mathbb{Z}[t], X)$. Then a *Lyndon's set* of $G$ is a set $R = R_{K(G)}$ of representatives of $K(G)$ which satisfies the following conditions:

1) $R \subset G$;
2) for any $g \in G, u \in R$, and $\alpha \in \mathbb{Z}[t]$ the inner product $c(u^\alpha, g)$ exists and $c(u^\alpha, g) < k|u|$ for some $k \in \mathbb{N}$;
3) no word from $G$ contains a subword $u^\alpha$, where $u \in R$ and $\alpha \in \mathbb{Z}[t]$ with $\deg(\alpha) > 0$.

REMARK 6.8. Let $G$ and $R$ be as above. Then:

a) if $G$ is subwords-closed then 2) implies 3);
b) for any $g \in G, u \in R$, and $\alpha \in \mathbb{Z}[t]$, the products $g * u^\alpha$ and $u^\alpha * g$ are defined.

LEMMA 6.9. *Let $G$ be an $S$-subgroup of $CDR(\mathbb{Z}[t], X)$ and let $R$ be a Lyndon's set of $G$. If $u, v \in R^{\pm 1}$ and $g \in G$ are such that either $[u, v] \neq \varepsilon$ or $[u, g] \neq \varepsilon$ then there exists $r \in \mathbb{N}$ such that for all $m, n \geqslant r$ the following holds:*

$$u^m * g * v^n = u^{m-r} \circ (u^r * g * v^r) \circ v^{n-r}.$$

PROOF. Suppose that the statement of the lemma does not hold for a triple $(u, g, v)$. Then the lemma fails for any triple $(u, g * v^k, v)$ where $k \in \mathbb{Z}$. Since $v \in R$ there exists $k \in \mathbb{Z}$ such that $(g * v^k) * v = (g * v^k) \circ v$. Hence, replacing $g$ by $g * v^k$, we may assume from the beginning that $g * v = g \circ v$.

Similarly, there exists $k \in \mathbb{N}$ such that $u * (u^k * g) = u \circ (u^k * g)$. If $g$ does not cancel completely in $u^k * g$ then

$$u^m * g * v^n = u^{m-k} \circ (u^k * g) \circ v^n$$

for any $m > k$ - contradiction. Hence, $g$ cancels completely and $g = u^p \circ g_1, |g_1| \leqslant |u|$. So, we can assume $g = g_1$ and $|g| \leqslant |u|$.

Consider two cases:

a) Let $[u, v] \neq \varepsilon$. If $|g| = |u|$ then for sufficiently big numbers $m, n$ we have $c(u^{-m}, v^n) \geqslant |u| + |v|$. Hence, by Lemma 6.4, $[u^{-1}, v] = \varepsilon$ - contradiction with our assumption.

If $|g| < |u|$ then $u = u_1 \circ g^{-1}$. If for sufficiently big numbers $m, n$ cancellation between $(u * g)^m$ and $v^n$ is long enough then $c((u_1^{-1} \circ g)^n, v^m) \geqslant |u| + |v| = |u_1^{-1} \circ g| + |v|$. Hence, by Lemma 6.4, $[u_1^{-1} \circ g, v] = \varepsilon$ and a conjugate of $u$ commutes with $v$ - contradiction with the properties of $R$.

b) Let $[u, v] = 1, [g, u] \neq \varepsilon$. Then $u = v^{\pm 1}$ and $|g| < |u|$. Thus $u = u_1 \circ g^{-1}$. It follows that $c((u_1^{-1} \circ g)^n, u^m) \geqslant 2|u| = |u_1^{-1} \circ g| + |u|$ for big enough $m, n > 0$. By Lemma 6.4 $[u_1^{-1} \circ g, v] = \varepsilon$. Hence, $u_1^{-1} \circ g = v$. If $v = u$ then $u_1^{-1} \circ g = u_1 \circ g^{-1}$ and it follows that $u_1^{-1} = u_1$ and $g = g^{-1}$, so $u = \varepsilon$ – contradiction. If $v = u^{-1}$ then $u_1^{-1} \circ g = g \circ u_1^{-1}$, so $[u_1, g] = [u, g] = \varepsilon$ – contradiction.

This shows that our assumption that the triple $(u, g, v)$ does not satisfy the statement of the lemma is false. □

LEMMA 6.10. *Let $G$ be an $S$-subgroup of $CDR(\mathbb{Z}[t], X)$ and $R$ a Lyndon's set of $G$. If $u_1, \ldots, u_n \in R^{\pm 1}$ and $g_1, \ldots, g_{n+1} \in G$ are such that for any $i = 2, \ldots, n$ either $[u_{i-1}, u_i] \neq \varepsilon$ or $[u_i, g_i] \neq \varepsilon$ then there exists $r \in \mathbb{N}$ such that*

$$\begin{aligned} &g_1 * u_1^{m_1} * g_2 * \cdots * u_n^{m_n} * g_{n+1} \\ &\quad = (g_1 * u_1^r) \circ u_1^{m_1 - 2r} \circ (u_1^r * g_2 * u_2^r) \circ u_2^{m_2 - 2r} \circ \cdots \circ u_n^{m_n - 2r} \circ (u_n^r * g_{n+1}) \end{aligned}$$

*for all $m_i \in \mathbb{N}$, $m_i > 2r$, $i \in [1, n]$.*

PROOF. We prove the lemma by induction on $n$. If $n = 1$ then the required result follows from the properties of the Lyndon's set $R$.

Suppose the statement holds for $n = k$ and set $n = k + 1$. By the induction hypothesis there exists $r_1 \in \mathbb{N}$ such that

$$g_1 * u_1^{m_1} * g_2 * \cdots * u_k^{m_k} * g_{k+1} =$$

$$= (g_1 * u_1^{r_1}) \circ u_1^{m_1-2r_1} \circ (u_1^{r_1} * g_2 * u_2^{r_1}) \circ \ldots \circ u_k^{m_k-2r_1} \circ (u_k^{r_1} * g_{k+1})$$

for all $m_i > 2r_1$, $i \in [1, k]$. Put

$$w = (g_1 * u_1^{r_1}) \circ u_1^{m_1-2r_1} \circ (u_1^{r_1} * g_2 * u_2^{r_1}) \circ u_2^{m_2-2r_1} \circ \ldots \circ (u_{k-1}^{r_1} * g_k * u_k^{r_1})$$

then we have

$$g_1 * u_1^{m_1} * g_2 * \cdots * u_k^{m_k} * g_{k+1} = w \circ u_k^{m_k-2r_1} \circ (u_k^{r_1} * g_{k+1})$$

and

$$g_1 * u_1^{m_1} * g_2 * \cdots * u_k^{m_k} * g_{k+1} * u_{k+1}^{m_{k+1}} * g_{k+2} = (w \circ u_k^{m_k-2r_1} \circ (u_k^{r_1} * g_{k+1})) * u_{k+1}^{m_{k+1}} * g_{k+2}.$$

Observe that by the properties of $R$ there exists $r_2 \in \mathbb{N}$ such that

$$u_{k+1}^{m_{k+1}} * g_{k+2} = u_{k+1}^{m_{k+1}-r_2} \circ (u_{k+1}^{r_2} * g_{k+2})$$

for all $m_{k+1} > r_2$. Finally, by Lemma 6.9, there exists $r > \max\{r_1, r_2\}$ such that

$$(u_k^{m_k-2r_1} \circ (u_k^{r_1} * g_{k+1})) * u_{k+1}^{m_{k+1}-r_2} = u_k^{m_k-2r} \circ (u_k^r * g_{k+1} * u_{k+1}^r) \circ u_{k+1}^{m_{k+1}-r_2-r}$$

for all $m_k > 2r$, $m_{k+1} > r_2 + r$. Hence,

$$\begin{aligned}(w \circ u_k^{m_k-2r_1} \circ (u_k^{r_1} * g_{k+1})) * u_{k+1}^{m_{k+1}} * g_{k+2} \\ = w \circ u_k^{m_k-2r} \circ (u_k^r * g_{k+1} * u_{k+1}^r) \circ u_{k+1}^{m_{k+1}-2r} \circ (u_{k+1}^r * g_{k+2})\end{aligned}$$

for all $m_i > 2r$, $i \in [1, k+1]$ which proves the lemma. □

Definition 6.11. Let $G$ be a subgroup of $CDR(\mathbb{Z}[t], X)$ with a Lyndon's set $R$. A sequence

$$p = (g_1, u_1^{\alpha_1}, g_2, \ldots, g_n, u_n^{\alpha_n}, g_{n+1}), \tag{6}$$

where $g_i \in G$, $u_i \in R$, $\alpha_i \in \mathbb{Z}[t]$, $n \geqslant 1$, is called an *$R$-form* over $G$.

An $R$-form (6) is *reduced* if $\deg(\alpha_i) > 0, i \in [1, n]$, and if $u_i = u_{i-1}$ then $[u_i, g_i] \neq \varepsilon$.

Denote by $\mathcal{P}(G, R)$ the set of all $R$-forms over $G$. We define a partial function $w : \mathcal{P}(G, R) \to R(\mathbb{Z}[t], X)$ as follows. If

$$p = (g_1, u_1^{\alpha_1}, g_2, \ldots, g_n, u_n^{\alpha_n}, g_{n+1})$$

then

$$w(p) = (\cdots (g_1 * u_1^{\alpha_1}) * g_2) * \cdots * g_n) * u_n^{\alpha_n}) * g_{n+1}$$

if it is defined.

Definition 6.12. An $R$-form $p = (g_1, u_1^{\alpha_1}, g_2, \ldots, g_n, u_n^{\alpha_n}, g_{n+1})$ over $G$ is called *normal* if it is reduced and the following conditions hold:

1) $w(p) = g_1 \circ u_1^{\alpha_1} \circ g_2 \circ \cdots \circ g_n \circ u_n^{\alpha_n} \circ g_{n+1}$,
2) $g_i$ does not have $u_i^{\pm 1}$ as a terminal segment for any $i \in [1, n]$ and $g_i \circ u_i^{\alpha_i}$ does not have $u_{i-1}^{\pm 1}$ as an initial segment for any $i \in [2, n]$.

Lemma 6.13. *Let $G$ be an $S$-subgroup of $CDR(\mathbb{Z}[t], X)$ with a Lyndon's set $R$. Then for every $R$-form $p$ over $G$ the following holds:*

1) *the product $w(p)$ is defined and it does not depend on the placement of parentheses;*
2) *there exists a reduced $R$-form $q$ over $G$ such that $w(q) = w(p)$;*
3) *there exists a unique normal $R$-form $q$ over $G$ such that $w(p) = w(q)$;*
4) *$w(p) \in CDR(\mathbb{Z}[t], X)$.*

PROOF. Let

$$p = (g_1, u_1^{\alpha_1}, g_2, \dots, g_n, u_n^{\alpha_n}, g_{n+1})$$

be an $R$-form over $G$.

We show first that 1) implies 2). Suppose that $w(p)$ is defined for every placement of parentheses and all such products are equal. Denote by $i_1 < i_2 < \cdots < i_k$ the only indices above with $\deg(\alpha_{i_j}) > 0$. Set

$$\begin{aligned} h_1 &= g_1 * \cdots * u_{i_1-1}^{\alpha_{i_1-1}} * g_{i_1} \\ h_{k+1} &= g_{i_k+1} * u_{i_k+1}^{\alpha_{i_k+1}} * \cdots * g_{n+1} \\ h_{j+1} &= g_{i_j+1} * u_{i_j+1}^{\alpha_{i_j+1}} * \cdots g_{i_{j+1}} \end{aligned}$$

where $j \in [2, k-1]$. Notice that $h_j \in G$ for all $j \in [1, k+1]$. It follows from 1) that

$$w(p) = g_1 * u_1^{\alpha_1} * g_2 * \cdots * g_n * u_n^{\alpha_n} * g_{n+1} = h_1 * v_1^{\beta_1} * h_2 * \cdots * v_k^{\beta_k} * h_{k+1},$$

where $\beta_j = \alpha_{i_j}, v_j = u_{i_j}$ for all $j \in [1, k]$. Hence, if we put

$$p_1 = (h_1, v_1^{\beta_1}, h_2, \dots, v_k^{\beta_k}, h_{k+1})$$

then $p_1 \in \mathcal{P}(G, R)$ and $w(p) = w(p_1)$. Now if $p_1$ is not reduced then there exists $j \in [1, k]$ such that $[h_j, v_j] = \varepsilon$ and $v_{j-1} = v_j$. Since the centralizer of $v_j$ in $G$ is cyclic and generated by $v_j$ then $h_j = v_j^m$ for some $m \in \mathbb{Z}$. Therefore

$$v_{j-1}^{\beta_{j-1}} * h_j * v_j^{\beta_j} = v_j^{\beta_{j-1}+m+\beta_j}.$$

Thus, we obtain a new $R$-form

$$p_2 = (h_1, v_1^{\beta_1}, \dots, h_{j-1}, v_j^{\beta_{j-1}+m+\beta_j}, h_{j+1}, \dots, v_k^{\beta_k}, h_{k+1}),$$

which is shorter then $p_1$ and $w(p) = w(p_1) = w(p_2)$. Proceeding this way (or by induction) in a finite number of steps we obtain a reduced $R$-form

$$q = (f_1, v_1^{\gamma_1}, f_2, \dots, v_l^{\gamma_l}, f_{l+1}),$$

such that $w(q) = w(p)$, as required.

Now we show that 1) implies 3). As we have seen above there exists a reduced $R$-form

$$q_1 = (h_1, v_1^{\beta_1}, h_2, \dots, v_k^{\beta_k}, h_{k+1})$$

such that 1) holds for $q_1$ and $w(p) = w(q_1)$. By Lemma 6.10 there exists $r \in \mathbb{N}$ such that

$$\begin{aligned} w(q_1) &= h_1 * v_1^{\beta_1} * \cdots * v_k^{\beta_k} * h_{k+1} \\ &= (h_1 * v_1^{r_1}) \circ v_1^{\beta_1 - 2r_1} \circ (v_1^{r_1} * h_2 * v_2^{r_2}) \circ \cdots \circ v_k^{\beta_k - 2r_k} \circ (v_k^{r_k} * h_{k+1}), \end{aligned}$$

where $r_j = \operatorname{sgn}(\beta_j) \cdot r$, $j \in [1, k]$. Put

$$f_1 = h_1 * v_1^{r_1}, \quad f_{k+1} = v_k^{r_k} * h_{k+1}, \quad f_j = v_{j-1}^{r_{j-1}} * h_j * v_j^{r_j} \quad (j \in [2, k]),$$

where $\gamma_j = \beta_j - 2r_j$. Then if we denote

$$q_2 = (f_1, v_1^{\gamma_1}, f_2, \dots, v_k^{\gamma_k}, f_{k+1}),$$

then $q_2 \in \mathcal{P}(G, R)$, $q_2$ satisfies 1), and $w(q_1) = w(q_2)$.

By the properties of $R$, there exists $M_1 \in \mathbb{Z}$ such that $f_1 = z_1 \circ v_1^{M_1}$ and $z_1$ does not have $v_1^{\pm 1}$ as a terminal segment. Also, by Lemma 6.9, there exists $N_1 \in \mathbb{N}$

such that $f_2 \circ v_2^{\gamma_2} = v_1^{N_1} \circ z'_2 \circ v_2^{\gamma'_2}$ and $z'_2 \circ v_2^{\gamma'_2}$ does not have $v_1^{\pm 1}$ as an initial segment. It follows that

$$w(q_2) = z_1 \circ v_1^{\gamma_1 + M_1 + N_1} \circ z'_2 \circ v_2^{\gamma'_2} \circ \cdots \circ v_k^{\gamma_k} \circ f_{k+1}.$$

Hence, for a reduced $R$-form

$$q_3 = (z_1, v_1^{\gamma_1 + M_1 + N_1}, z'_2, v_2^{\gamma'_2}, \ldots, v_k^{\gamma_k}, f_{k+1})$$

one has $w(q_2) = w(q_3)$.

Now we can proceed with $q_3$ in the same way using properties of $R$ and Lemma 6.9. In a finite number of steps we obtain a normal $R$-form

$$q = (z_1, v_1^{\delta_1}, z_2, v_2^{\delta_2}, \ldots, v_k^{\delta_k}, z_{k+1})$$

such that $w(p) = w(q)$. Uniqueness of $q$ follows from the process above.

Now we prove 1) by induction on $n$. If $n = 1$ then by the condition 2) in the definition of $R$-sets

$$g_1 * u_1^{\alpha_1} = (g_1 * u_1^{k_1}) \circ u_1^{\alpha_1 - k_1}, \quad u_1^{\alpha_1 - k_1} * g_2 = u_1^{\alpha_1 - k_1 - k_2} \circ (u_1^{k_2} * g_2)$$

for some $k_1, k_2 \in \mathbb{N}$. Hence,

$$(g_1 * u_1^{\alpha_1}) * g_2 = ((g_1 * u_1^{k_1}) \circ u_1^{\alpha_1 - k_1}) * g_2 = ((g_1 * u_1^{k_1}) \circ u_1^{\alpha_1 - k_1 - k_2}) \circ (u_1^{k_2} * g_2).$$

By the axiom (P4) of pregroups the product $(g_1 * u_1^{\alpha_1}) * g_2$ does not depend on the placement of parentheses. So 1) holds for $n = 1$.

To show that 1) holds for an arbitrary $p$ above put

$$p_1 = (g_1, u_1^{\alpha_1}, g_2, \ldots, u_{n-1}^{\alpha_{n-1}}, g_n).$$

By induction $w(p_1)$ is defined and it does not depend on the placement of parentheses. By the argument above there exists a normal $R$-form

$$q_1 = (h_1, v_1^{\beta_1}, h_2, \ldots, v_{k-1}^{\beta_{k-1}}, h_k)$$

such that $w(q) = w(q_1)$. Since $q_1$ is a normal $R$-form one has

$$w(q_1) = h_1 \circ v_1^{\beta_1} \circ h_2 \circ \cdots \circ v_{k-1}^{\beta_{k-1}} \circ h_k.$$

To prove that $p$ satisfies 1) it suffices to show that

$$w(q_1) * (u_n^{\alpha_n} * g_{n+1})$$

is defined and does not depend on the placement of parentheses. To show this we consider several cases.

If $\deg(\alpha_n) = 0$ then $h_k * (u_n^{\alpha_n} * g_{n+1}) \in G$ and by the condition 2) of Lyndon's sets

$$v_{k-1}^{\beta_{k-1}} * (h_k * u_n^{\alpha_n} * g_{n+1}) = v_{k-1}^{\beta_{k-1} - r} \circ (v_{k-1}^r * h_k * u_n^{\alpha_n} * g_{n+1})$$

for some $r \in \mathbb{N}$. It follows that $w(p) = w(q_1) * (u_n^{\alpha_n} * g_{n+1})$ is defined and does not depend on the placement of parentheses.

Suppose $\deg(\alpha_n) > 0$. If either $[v_{k-1}, u_n] \neq \varepsilon$ or $[v_{k-1}, h_k] \neq \varepsilon$ then by Lemma 6.9 and the condition 2) in the definition of Lyndon's sets

$$(v_{k-1}^{\beta_{k-1}} \circ h_k) * (u_n^{\alpha_n} * g_{n+1}) = v_{k-1}^{\beta_{k-1} - r} \circ (v_{k-1}^r * h_k * u_n^{s_1}) \circ u_n^{\alpha_n - s_1 - s_2} \circ (u_n^{s_2} * g_{n+1})$$

for some $r, s_1, s_2 \in \mathbb{N}$. In this case $w(q_1) * (u_n^{\alpha_n} * g_{n+1})$ is defined and does not depend on the placement of parentheses.

If $[v_{k-1}, u_n] = \varepsilon$ and $[v_{k-1}, h_k] = \varepsilon$ then $v_{k-1} = u_n$ and $h_k = 1$. Hence,

$$(v_{k-1}^{\beta_{k-1}} \circ h_k) * (u_n^{\alpha_n} * g_{n+1}) = v_{k-1}^{\beta_{k-1}+\alpha_n} * g_{n+1} = v_{k-1}^{\beta_{k-1}+\alpha_n - s_2} \circ (v_{k-1}^{s_2} * g_{n+1})$$

and the statement follows. This proves 1). Hence, 2) and 3) hold.

Now we prove 4). By 3) there exists a normal $R$-form

$$q = (h_1, v_1^{\beta_1}, h_2, \dots, h_k, v_k^{\beta_k}, h_{k+1})$$

such that $w(p) = w(q)$. It follows that

$$w(q) = h_1 \circ v_1^{\beta_1} \circ h_2 \circ \cdots \circ v_k^{\beta_k} \circ h_{k+1}.$$

By Lemma 3.8, to prove that $w(q) \in CDR(\mathbb{Z}[t], X)$ it suffices to show that

$$g^{-1} * w(q) * g \in CDR(\mathbb{Z}[t], X)$$

for some $g \in R(\mathbb{Z}[t], X)$. We consider two cases.

a) If $v_1 \neq v_k$ or $v_1 = v_k$ but $[h_{k+1} * h_1, v_1] \neq \varepsilon$ then by Lemma 6.9, there exists $m \in \mathbb{Z}, m\beta_1 > 0$ such that

$$(v_1^{-n} \circ h_1^{-1}) * w(q) * (h_1 \circ v_1^n) = (v_1^{\beta_1 - n} \circ h_2 \circ \cdots \circ v_k^{\beta_k - m}) \circ (v_k^m * h_{k+1} * h_1 * v_1^m) \circ v_1^{n-m}$$

for any $n \in \mathbb{Z}$, $|n| > |m|$. Thus,

$$(v_1^{-n} \circ h_1^{-1}) * w(q) * (h_1 \circ v_1^n) \in CR(\mathbb{Z}[t], X) \subset CDR(\mathbb{Z}[t], X).$$

b) If $v_1 = v_k, [h_{k+1} * h_1, v_1] = \varepsilon$ then $h_{k+1} * h_1 = v_1^m$ and

$$h_1^{-1} * w(q) * h_1 = v_1^{\beta_1} \circ h_2 \circ \cdots \circ v_k^{\beta_k + m}.$$

If $\operatorname{sgn}(\beta_1) = \operatorname{sgn}(\beta_k)$ then

$$h_1^{-1} * w(q) * h_1 \in CR(\mathbb{Z}[t], X) \subset CDR(\mathbb{Z}[t], X).$$

If $\operatorname{sgn}(\beta_1) \neq \operatorname{sgn}(\beta_k)$ then without loss of generality we can assume $|\beta_1| \geqslant |\beta_k|$ and we have

$$(v_1^{\beta_k + m} * h_1^{-1}) * w(q) * (h_1 * v_1^{-\beta_k - m}) = v_1^{\beta_1 + \beta_k + m} \circ h_2 \circ \cdots \circ h_k,$$

so the number of infinite exponents of elements from R is reduced by one and we can use induction on $k$. This proves 4). □

Let $G$ and $R$ be as above. By Lemma 6.13 for every $g, h \in G$, $u \in R$, $\alpha \in \mathbb{Z}[t]$ the product $g * u^\alpha * h$ is defined and belongs to $CDR(\mathbb{Z}[t], X)$. Put

$$P = P(G, R) = \{g * u^\alpha * h \mid g, h \in G, u \in R, \alpha \in \mathbb{Z}[t]\}.$$

Multiplication $*$ induces a partial multiplication (which we again denote by $*$) on $P$ so that for $p, q \in P$ the product $p * q$ is defined in $P$ if and only if $p * q$ is defined in $R(\mathbb{Z}[t], X)$ and $p * q \in P$. Now we are ready to prove the main technical result of this subsection.

Proposition 6.14. *Let $G$ be an S-subgroup of $CDR(\mathbb{Z}[t], X)$ and let $R$ be a Lyndon's set for $G$. Then the set $P$ forms a pregroup with respect to the multiplication $*$.*

Proof. Since multiplication $*$ in $P$ is induced from $R(\mathbb{Z}[t], X)$ it follows from Theorem 3.4 that axioms (P1)–(P4) hold in $P$. To complete the proof it suffices to check that the following axiom

(P5) for every $u, v, w, z, \in P$ if $u * v, v * w$, and $w * z$ are defined then either $u * v * w$ or $v * w * z$ is defined in $P$

holds in $P$. To show this we need two claims.

**Claim 1.** Let $g_i * c_i^{\alpha_i} * h_i \in P$ and $\deg(\alpha_i) > 0$, $i = 1, 2$. If

$$g_1 * c_1^{\alpha_1} * h_1 = g_2 * c_2^{\alpha_2} * h_2$$

then $c_1 = c_2^{\pm 1}$ and $[h_1 * h_2^{-1}, c_1] = [g_1 * g_2^{-1}, c_1] = \varepsilon$.

Indeed, clearly $a = (g_1, c_1^{\alpha_1}, h_1 * h_2^{-1}, c_2^{-\alpha_2}, g_2^{-1})$ is an $R$-form, so, by Lemma 6.13, $w(a)$ is defined and

$$g_1 * c_1^{\alpha_1} * h_1 * h_2^{-1} * c_2^{-\alpha_2} * g_2^{-1} = \varepsilon.$$

Hence, $a$ is not reduced and the claim follows.

For every $p \in P$ we fix now a representation $p = g_p * c_p^{\alpha_p} * h_p$, where $g_p, h_p \in G, c_p \in R, \alpha_p \in \mathbb{Z}[t]$.

**Claim 2.** Let $p = g_p * c_p^{\alpha_p} * h_p$, $q = g_q * c_q^{\alpha_q} * h_q$ be in $P$. If $\deg(\alpha_p), \deg(\alpha_q) > 0$ and $p * q \in P$ then $c_p = c_q$ and $h_p * g_q \in \langle c_p \rangle$.

Put $x = p * q$. Then $x \in P$ and $x = g_x * c_x^{\alpha_x} * h_x$. Observe that

$$a = (g_p, c_p^{\alpha_p}, h_p * g_q, c_q^{\alpha_q}, h_q * h_x^{-1}, c_x^{-\alpha_x}, g_x^{-1})$$

is an $R$-form, so $w(a)$ is defined and

$$g_p * c_p^{\alpha_p} * h_p * g_q * c_q^{\alpha_q} * h_q * h_x^{-1} * c_x^{-\alpha_x} * g_x^{-1} = \varepsilon.$$

Hence, $a$ is not reduced.

Suppose, first, that $\deg(\alpha_x) > 0$. In this case either $c_p = c_q$, $[h_p * g_q, c_p] = \varepsilon$ or $c_q = c_x$, $[h_q * h_x^{-1}, c_q] = \varepsilon$. In the former case the proof of the claim is complete. In the latter one $h_q * h_x^{-1} = c_q^k$, for some $k \in \mathbb{Z}$, so

$$\begin{aligned} g_p * c_p^{\alpha_p} * h_p &= (g_x * c_x^{\alpha_x} * h_x) * (h_q^{-1} * c_q^{-\alpha_q} * g_q^{-1}) \\ &= g_x * c_q^{\alpha_x} * c_q^{-k} * c_q^{-\alpha_q} * g_q^{-1} = g_x * c_q^{\alpha_x - \alpha_q - k} * g_q^{-1}, \end{aligned}$$

where $\deg(\alpha_x - \alpha_q - k) > 0$ (otherwise $c_p^{\alpha_p} \in G$). Now the result follows form Claim 1.

If $\deg(\alpha_x) = 0$ then $c_p = c_q, [h_p * g_q, c_p] = \varepsilon$ and the claim follows.

Now we are in the position to verify that the axiom (P5) holds in $P$. Put $E = \{\alpha_u, \alpha_v, \alpha_w, \alpha_z\}$ and consider the following cases:

a) $\deg(e) > 0$ for all $e \in E$.

Then by Claim 2, $c_u = c_v = c_w = c_z$ and $h_u * g_v, h_v * g_w, h_w * h_z$ belong to the cyclic subgroup generated by $c_u$. In this case $u * v * w \in P$.

b) There is precisely one element $e \in E$ such that $\deg(e) = 0$.

Then in the sequence $u, v, w, z$ we have a subsequence $a, b, c$ in which either $a, b$ or $b, c$ satisfies a). In this case obviously $a * b * c \in P$.

c) There are precisely two elements $e_1, e_2 \in E$ such that $\deg(e_1) = \deg(e_2) = 0$.

Then in the sequence $u, v, w, z$ we have either a subsequence $a, b, c$ in which either $a, b$ or $b, c$ satisfies a), or a subsequence $a, b, c$ in which only $b$ satisfies a). In both cases $a * b * c \in P$.

d) $\deg(e) = 0$ for all $e \in E$. Hence, $u, v, w, z \in G$ and the axiom (P5) obviously holds.

This completes the proof of the proposition. □

**6.2. Pregroups and non-standard extension of centralizers.** Let $G$ be a fixed S-subgroup of $CDR(\mathbb{Z}[t], X)$ with a Lyndon's set $R$. Below we continue to use notations from the previous section.

By Proposition 6.14

$$P = \{g * u^{\alpha} * h \mid g, h \in G,\ u \in R,\ \alpha \in \mathbb{Z}[t]\}$$

forms a pregroup in $CDR(\mathbb{Z}[t], X)$ with respect to the partial multiplication $*$. The next two results reveal the structure of the universal group $U(P)$ of $P$.

THEOREM 6.15. *$P$ generates a subgroup $\langle P\rangle$ in $CDR(\mathbb{Z}[t], X)$, which is isomorphic to $U(P)$.*

*Proof.* The proof of the theorem is divided into several claims. Below we refer to any tuple $y = (y_1, \dots, y_n) \in P^n$ as a $P$-sequence and we call it *reduced* if $y_i * y_{i+1} \notin P$ for $i \in [1, n-1]$. Observe, that if $y = (y_1, \dots, y_n)$ is a reduced $P$-sequence and $y_i = g_i * c_i^{\alpha_i} * h_i$ then $y$ has the following properties:

1) $\deg(\alpha_i) > 0$ for all $i \in [1, n]$,

2) either $c_i \neq c_{i+1}$ or $c_i = c_{i+1}, [h_i * g_{i+1}, c_i] \neq \varepsilon, i \in [1, n-1]$.

In particular, the following $R$-form over $G$

$$p_y = (g_1,\ c_1^{\alpha_1},\ h_1 * g_2,\ c_2^{\alpha_2},\ \dots,\ h_{n-1} * g_n,\ c_n^{\alpha_n},\ h_n),$$

is reduced as an $R$-form.

Recall, that the group $U(P)$ consists of equivalence classes of reduced $P$-sequences modulo the equivalence relation $\sim$ such that $(y_1, \dots, y_n) \sim (z_1, \dots, z_m)$ if and only if $m = n$ and there exist elements $a_1, \dots, a_{n-1} \in P$ such that $z_i = a_{i-1}^{-1} y_i a_i$ for $1 \leqslant i \leqslant n$ (here $a_0 = a_n = 1$).

**Claim 1**. $P$ generates a subgroup $H = \langle P\rangle$ in $CDR(\mathbb{Z}[t], X)$.

Observe, first, that $P^{-1} = P$. Now if $y_1, \dots, y_n \in P$ then $y_1 * \dots * y_n = w(p_y)$ where $y = (y_1, \dots, y_n)$. Hence, by Lemma 6.13 $y_1 * y_2 * \dots * y_n$ is defined and it belongs to $CDR(\mathbb{Z}[t], X)$. It follows that $P$ generates a subgroup $H$ of $CDR(\mathbb{Z}[t], X)$. It is not hard to see that $H$ consists of all words $w(p)$, where $p$ ranges through all possible $R$-forms over $G$. This proves the claim.

Now we have to prove that $H \simeq U(P)$. By the categorical properties of the universal group $U(P)$ of the pregroup $P$ the canonical inclusion $\psi : P \to H$ (which is obviously a morphism of pregroups) extends to a unique homomorphism of groups $\phi : U(P) \to H$ defined as follows. If $y \in U(P)$ is viewed as a $P$-sequence $y = (y_1, \dots, y_n) \in P^n$, then

$$y^{\phi} = y_1^{\psi} * \dots * y_n^{\psi} \in H.$$

**Claim 2**. $\phi$ is onto.

The claim is obvious since $P \subseteq U(P)$ and $P$ generates $H$.

**Claim 3**. $\phi$ is one-to-one.

Let $y = (y_1, \dots, y_n)$ and $z = (z_1, \dots, z_m)$ be reduced $P$-sequences such that $y^{\phi} = z^{\phi}$. We need to show that in this case $y$ and $z$ define the same element in $U(P)$, i.e., $y \sim z$.

If $y_i = g_{y_i} * c_{y_i}^{\alpha_i} * h_{y_i}$, $i \in [1, n]$, and $z_j = g_{z_j} * c_{z_j}^{\beta_j} * h_{z_j}, j \in [1, m]$, then

$$p_y = (g_{y_1},\ c_{y_1}^{\alpha_1},\ h_{y_1} * g_{y_2},\ c_{y_2}^{\alpha_2},\ \dots,\ h_{y_{n-1}} * g_{y_n},\ c_{y_n}^{\alpha_n},\ h_{y_n}),$$

$$p_z = (g_{z_1},\ c_{z_1}^{\beta_1},\ h_{z_1} * g_{z_2},\ c_{z_2}^{\beta_2},\ \dots,\ h_{z_{m-1}} * g_{z_m},\ c_{z_m}^{\beta_m},\ h_{z_m})$$

are reduced $R$-forms such that $y^\phi = w(p_y)$ and $z^\phi = w(p_z)$.

Following the process described in Lemma 6.13, we find the corresponding normal $R$-forms

$$q_y = (a_0,\ c_{y_1}^{\gamma_1},\ a_1,\ c_{y_2}^{\gamma_2}, \dots, a_{n-1},\ c_{y_n}^{\gamma_n},\ a_n),$$
$$q_z = (b_0,\ c_{z_1}^{\delta_1},\ b_1,\ c_{z_2}^{\delta_2}, \dots, b_{m-1},\ c_{z_m}^{\delta_m},\ b_m),$$

such that $w(p_y) = w(q_y)$ and $w(p_z) = w(q_z)$. Observe that according to the process we have

$$a_0 = g_{y_1} * c_{y_1}^{k_1},\ a_{n-1} = c_{y_n}^{s_n} * h_{y_n},\ a_i = c_{y_i}^{s_i} * (h_{y_i} * g_{y_{i+1}}) * c_{y_{i+1}}^{k_{i+1}},\ i \in [1, n-1],$$
$$b_0 = g_{z_1} * c_{z_1}^{K_1},\ b_{m-1} = c_{z_m}^{S_m} * h_{z_m},\ b_j = c_{z_j}^{S_j} * (h_{z_j} * g_{z_{j+1}}) * c_{z_{j+1}}^{K_{j+1}},\ j \in [1, m-1],$$

where $k_i, s_i, K_j, S_j \in \mathbb{Z},\ i \in [1, n],\ j \in [1, m]$, and

$$\alpha_i = \gamma_i + k_i + s_i,\ \beta_j = \delta_j + K_j + S_j,\ i \in [1, n],\ j \in [1, m].$$

Since $w(q_y) = w(q_z)$, from the uniqueness of normal $R$-forms it follows that $m = n,\ a_i = b_i,\ i \in [0, n]$ and $c_{y_i} = c_{z_i},\ \gamma_i = \delta_i,\ i \in [1, n]$. Now, if we take $P$-sequences

$$y' = (g_{y_1} * c_{y_1}^{\alpha_1} * h_{y_1} * g_{y_2} * c_{y_2}^{k_2},\ \ c_{y_2}^{\alpha_2 - k_2} * h_{y_2} * g_{y_3} * c_{y_3}^{k_3}, \dots, c_{y_{n-k_n}}^{\alpha_n} * h_{y_n}),$$
$$z' = (g_{z_1} * c_{z_1}^{\beta_1} * h_{z_1} * g_{z_2} * c_{z_2}^{K_2},\ \ c_{z_2}^{\beta_2 - K_2} * h_{z_2} * g_{z_3} * c_{z_3}^{K_3}, \dots, c_{z_{m-K_m}}^{\beta_m} * h_{z_m})$$

then $y \sim y', z \sim z'$. Using the equalities above it is easy to see that $y'$ can be obtained from $z'$ by interleaving, that is, $y' \sim z'$ which implies $y \sim z$.

□

Remark 6.16. As we have seen in the proof above every element $h \in H$ can be presented by a reduced $R$-form $p_h$. By Lemma 6.13, $h$ has a unique normal $R$-form $q_h$ such that $w(q_h) = h$. We will refer to this $q_h$ as to the *normal form* of $h$ in $H$.

To describe the algebraic structure of the group $H$ we need the following notation.

Let $R = \{c_i \mid i \in I\}$. Put $S = \{s_{i,j} \mid i \in I, j \in \mathbb{N}\}$. Then the group

$$G(R, S) = \langle G, S \mid [c_i, s_{i,j}] = [s_{i,j}, s_{k,j}] = 1, i \in I, j, k \in \mathbb{N} \rangle$$

is an extension of all cyclic centralizers of $G$ by a direct sum of countably many copies of an infinite cyclic group. Sometimes, we will refer to $G(R, S)$ as an extension of all cyclic centralizers of $G$ by $\mathbb{Z}[t]$.

Theorem 6.17. $H \simeq G(R, S)$.

Proof. We start by defining a map $\phi : P \to G(R, S)$ as follows. Let $g_i * c_i^\alpha * h_i \in P$ and $\alpha = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$. Put

$$g_i * c_i^\alpha * h_i \ \stackrel{\phi}{\to}\ g_i\ s_{i,n}^{a_n}\ s_{i,n-1}^{a_{n-1}}\ \cdots\ s_{i,1}^{a_1}\ c_i^{a_0}\ h_i.$$

It follows from Claim 2 in Proposition 6.14 that $\phi$ is a morphism of pregroups. Since $H \simeq U(P)$, the morphism $\phi$ extends to a unique homomorphism $\psi : H \to G(R, S)$. We claim that $\psi$ is bijective. Indeed, observe first that $G(R, S)$ is generated by $G \cup S$. Now, since $\psi(c_i^{t^j}) = s_{i,j}$ and $\psi$ is identical on $G$, it follows that $\psi$ is onto. To see that $\psi$ is one-to-one it suffices to notice that if

$$y = (g_1 * c_1^{\alpha_1} * h_1, g_2 * c_2^{\alpha_2} * h_2, \dots, g_m * c_m^{\alpha_m} * h_m).$$

is a reduced $R$-form then $y^\psi \neq 1$ by Britton's Lemma (see, for example, [**31**]). This proves that $\psi$ is an isomorphism, as required. □

Now we prove two results about $H$.

LEMMA 6.18. *If $G$ is subwords-closed then so is $H$.*

PROOF. Suppose $G$ is subwords-closed. Let $h$ be an arbitrary element from $H$. Then $h$ can be written in the normal form

$$h = h_1 \circ u_1^{\alpha_1} \circ h_2 \circ u_2^{\alpha_2} \circ \cdots \circ u_m^{\alpha_m} \circ h_{m+1},$$

where $h_i \in G$, $i \in [1, m+1]$, $u_i \in R$, $\alpha_i \in \mathbb{Z}[t]$, $i \in [1, m]$. Now, a subword $h'$ of $h$ has the following form

$$h' = {h'}_k \circ u_k^{\gamma_k} \circ h_{k+1} \circ u_{k+1}^{\alpha_{k+1}} \circ \cdots \circ h_l \circ u_l^{\gamma_l} \circ {h'}_{l+1},$$

where ${h'}_k \circ u_k^{\gamma_k}$ is a terminal segment of $h_k \circ u_k^{\alpha_k}$ and $u_l^{\gamma_l} \circ {h'}_{l+1}$ is an initial segment of $u_l^{\alpha_l} \circ h_{l+1}$. Since $G$ is subwords-closed, it follows that ${h'}_k, {h'}_{l+1} \in G$. Hence, $h' \in H$, as required. □

LEMMA 6.19. *If $G$ is subwords-closed then $H$ is an S-subgroup.*

PROOF. Suppose $f, g \in H$, $[f, g] \neq \varepsilon$, and the centralizers $C_H(f)$ and $C_H(g)$ are cyclic. Since the centralizers in $H$ of elements from $G$ are isomorphic to $\mathbb{Z}[t]$, it follows that $g$ and $h$ are not conjugates of elements from $G$. In particular, if $f = a^{-1} \circ \bar{f} \circ a$ and $g = b^{-1} \circ \bar{g} \circ b$ are cyclic decompositions of $f$ and $g$ then $\bar{f}$ and $\bar{g}$ are not in $G$. Notice that by Lemma 6.18 $H$ is subwords-closed, therefore none of the elements in $H$ contains an infinite power of $\bar{f}$ or infinite power of $\bar{g}$ as a subword.

We have to show that $g$ and $h$ are separated. Suppose to the contrary that they are not separated. Without loss of generality we can assume that $f$ and $g$ are not proper powers. Since $f$ and $g$ are not separated for every $M \in \mathbb{N}$ there are $m, n \in \mathbb{N}$ such that $c(f^{-m}, g^n) \geqslant M$. In particular, $c(f^{-m}, g^n) \geqslant \max\{|a|, |b|\}$ for sufficiently big $m, n$ (i.e., both $a$ and $b^{-1}$ cancel in $f^m * g^n$). We may assume that $|a| \geqslant |b|$, so $a = a_1 \circ b$. Also we may assume that $|a_1| \leqslant |\bar{g}|$ (otherwise $a_1 = \bar{g}^k \circ a_2$, where $|a_2| \leqslant |\bar{g}|$ and $k \in \mathbb{N}$, so we can replace $a_1$ by $a_2$).

Consider the following cases.

a) Let $|a_1| + |\bar{f}| \geqslant |\bar{g}|$. If $|a_1| + |\bar{f}| = |\bar{g}|$ then $\bar{g} = a_1^{-1} \circ \bar{f}^{-1}$. Therefore $f^m * g^n = a^{-1} \circ \bar{f}^m * \bar{g}^n \circ b$, so $c(\bar{f}^{-m}, \bar{g}^n) > |\bar{f}| + |\bar{g}|$. By Lemma 6.4 $\bar{g} = \bar{f}^{-1}$, so $a_1 = \varepsilon$. It follows that $a = b$ and $[f, g] = \varepsilon$ – contradiction.

Suppose $|a_1| + |\bar{f}| > |\bar{g}|$. Then $\bar{f}^{-1} = f_1 \circ f_2, a_1^{-1} \circ f_1 = \bar{g}^p$, $p \geqslant 1$, and $\bar{g} = f_2 \circ g_1$. It follows then that $c(\bar{f}^{-m}, (g_1 \circ f_2)^n) > |\bar{f}| + |\bar{g}|$, so by Lemma 6.4 $\bar{f}^{-1} = g_1 \circ f_2$ and $f_1 = g_1$. Thus, $a_1^{-1} \circ g_1 = \bar{g}^p$, $p \geqslant 1$, and since $|a_1| \leqslant |\bar{g}|$, one has $p = 1$, $a_1^{-1} \circ g_1 = \bar{g} = f_2 \circ g_1$, hence, $a_1^{-1} = f_2$. This shows that there is cancellation between $a^{-1}$ and $\bar{f}$ – contradiction.

b) Let $|a_1| + |\bar{f}| < |\bar{g}|$.

In this case $\bar{g} = a_1^{-1} \circ \bar{f}^{-k} \circ f_1$, $k > 0$ and $\bar{f}^{-1} = f_1 \circ f_2$. It follows then that $c((f_2 \circ f_1)^m, \bar{g}^n) > |\bar{f}| + |\bar{g}|$, so by Lemma 6.4 $g = f_2 \circ f_1$. Hence, $|\bar{f}| = |\bar{g}|$ and $a_1 = f_1 = \varepsilon, k = 1$. This implies $a = b$, $\bar{g} = \bar{f}^{-1}$, and $[f, g] = \varepsilon$ – contradiction.

Thus, our assumption was false and $f, g$ are separated, as required. □

**6.3. Regular free length functions on extensions of centralizers.** Let $G$ be a fixed S-subgroup of $CDR(\mathbb{Z}[t], X)$ with a Lyndon's set $R$. In the previous subsection we showed that the set

$$P = \{g * u^\alpha * h \mid g, h \in G, u \in R, \alpha \in \mathbb{Z}[t]\}$$

generates a subgroup $H = \langle P \rangle$ of $CDR(\mathbb{Z}[t], X)$, which is isomorphic to the extension of all cyclic centralizers of $G$ by $\mathbb{Z}[t]$. It follows that $H$ has a length function induced from $CDR(\mathbb{Z}[t], X)$. In this section we show that this length function is regular, provided the length function on $G$ is regular. Notice that if $G$ is subwords-closed, then by Lemma 6.18 $H$ is subwords-closed too, so the length function on $H$ is obviously regular. In what follows we do not assume that $G$ is subwords-closed.

We begin with a description of the induced length function on $H$. Let $y \in H$ and

$$y = g_0 \circ c_1^{\alpha_1} \circ g_1 \circ c_2^{\alpha_2} \circ g_2 \circ \cdots \circ c_m^{\alpha_m} \circ g_m$$

be the unique normal form for $y$ in $H$. Then

$$|y| = \sum_{i=0}^{m} |g_i| + \sum_{i=1}^{m} |c_i^{\alpha_i}| = \sum_{i=0}^{m} |g_i| + \sum_{i=1}^{m} |c_i||\alpha_i|. \tag{7}$$

LEMMA 6.20. *If the length function on $G$ induced from $CDR(\mathbb{Z}[t], X)$ is regular then so is the length function induced from $CDR(\mathbb{Z}[t], X)$ on $H$.*

PROOF. Suppose that the length function induced from $CDR(\mathbb{Z}[t], X)$ on $G$ is regular. Let $h, g \in H$. One can write them in the normal forms

$$h = h_1 \circ u_1^{\alpha_1} \circ h_2 \circ u_2^{\alpha_2} \circ \cdots \circ u_m^{\alpha_m} \circ h_{m+1},$$

$$g = g_1 \circ v_1^{\beta_1} \circ g_2 \circ v_2^{\beta_2} \circ \cdots \circ v_n^{\beta_n} \circ g_{n+1},$$

where $h_i, g_j \in G,\ i \in [1, m+1],\ j \in [1, n+1],\ u_i, v_j \in R,\ \alpha_i, \beta_j \in \mathbb{Z}[t],\ i \in [1, m]$, $j \in [1, n]$.

If $c(h, g) = 0$ then there is nothing to prove. Suppose $c(h, g) > 0$. Now, comparing representations of $\mathrm{com}(h, g)$ as all possible subwords of $g$ and $h$, consider two cases.

Case 1). Suppose

$$\mathrm{com}(h, g) = g_1 \circ v_1^{\beta_1} \circ \cdots \circ v_{k-1}^{\beta_{k-1}} \circ {g'}_k,$$

where $g_k = {g'}_k \circ {g''}_k$.

a) Assume that

$$\mathrm{com}(h, g) = h_1 \circ u_1^{\alpha_1} \circ \cdots \circ u_{l-1}^{\alpha_{l-1}} \circ {h'}_l,$$

where $h_l = {h'}_l \circ {h''}_l$. From the properties of normal forms it follows that $k = l$, $g_i = h_i,\ u_i = v_i,\ \alpha_i = \beta_i$ for $i \in [1, k-1]$ and ${h'}_k = {g'}_k = \mathrm{com}(h_k, g_k)$. Thus, ${g'}_k \in G$ since the length function on $G$ is regular and it follows that $\mathrm{com}(h, g) \in H$.

b) Assume now that $\mathrm{com}(h, g)$ ends in $h$ inside of $u_l^{\alpha_l}$ for some $l \in [1, m]$, that is,

$$\mathrm{com}(h, g) = h_1 \circ u_1^{\alpha_1} \circ \cdots \circ h_l \circ u_l^{\gamma} \circ u',$$

where $u_l = u' \circ u'',\ \gamma < \alpha_l$.

If $\deg(\gamma) > 0$ then $k = l + 1,\ g_i = h_i,\ u_i = v_i,\ i \in [1, k-1],\ \alpha_i = \beta_i,\ i \in [1, k-2],\ \beta_{k-1} = \gamma$ and ${g'}_k = u' = \mathrm{com}(u_l, g_k) \in G$, thus, $\mathrm{com}(h, g) \in H$.

If $\deg(\gamma) = 0$ then $k = l,\ g_i = h_i,\ u_i = v_i,\ \alpha_i = \beta_i,\ i \in [1, k-1]$ and ${g'}_k = h_k \circ u_k^{\gamma} \circ u'$. Thus, ${g'}_k = \mathrm{com}(h_k \circ u_k^{\gamma+1}, g_k) \in G$ and $\mathrm{com}(h, g) \in H$.

Case 2). Suppose $\mathrm{com}(h, g)$ ends in $g$ inside of $v_k^{\beta_k}$ for some $k \in [1, n]$, that is,

$$\mathrm{com}(h, g) = g_1 \circ v_1^{\beta_1} \circ \cdots \circ g_k \circ v_k^{\delta} \circ v',$$

where $v_k = v' \circ v'',\ \delta < \beta_k$.

a) If

$$\mathrm{com}(h,g) = h_1 \circ u_1^{\alpha_1} \circ \cdots \circ u_{l-1}^{\alpha_{l-1}} \circ {h'}_l,$$

where $h_l = {h'}_l \circ {h''}_l$, then this case is symmetric to Case 1b).

b) Suppose $\mathrm{com}(h,g)$ ends in $h$ inside of $u_l^{\alpha_l}$ for some $l \in [1,m]$, that is,

$$\mathrm{com}(h,g) = h_1 \circ u_1^{\alpha_1} \circ \cdots \circ h_l \circ u_l^{\gamma} \circ u',$$

where $u_l = u' \circ u''$, $\gamma < \alpha_l$.

If $\deg(\gamma), \deg(\delta) > 0$ then $k = l$, $g_i = h_i$, $u_i = v_i$, $i \in [1,k]$, $\alpha_i = \beta_i$, $i \in [1, k-1]$, $\gamma = \delta$, $u' = v'$ and we have a contradiction with the definition of $\mathrm{com}(h,g)$.

If $\deg(\gamma) > 0, \deg(\delta) = 0$ then $k = l+1$, $g_i = h_i$, $u_i = v_i$, $i \in [1, k-1]$, $\alpha_i = \beta_i$, $i \in [1, k-2]$, $\beta_{k-1} = \gamma$ and $u' = g_k \circ v_k^{\delta} \circ v'$. Thus, $u' = \mathrm{com}(u_k, g_k \circ v_k^{\delta+1})$ and $\mathrm{com}(h,g) \in H$. If $\deg(\gamma) = 0$, $\deg(\delta) > 0$ then we apply the same argument.

If $\deg(\gamma) = \deg(\delta) = 0$ then $k = l$, $g_i = h_i$, $u_i = v_i$, $\alpha_i = \beta_i$, $i \in [1, k-1]$ and $g_k \circ v_k^{\delta} \circ v' = h_k \circ u_k^{\gamma} \circ u' = \mathrm{com}(h_k \circ u_k^{\gamma+1}, g_k \circ v_k^{\delta+1}) \in G$. Thus, $\mathrm{com}(h,g) \in H$.

Since in all possible cases $\mathrm{com}(h,g) \in H$, this shows that the length function on $H$ is regular. □

## 7. Embedding of $F^{\mathbb{Z}[t]}$ into $CDR(\mathbb{Z}[t], X)$

Let $F$ be a free non-abelian group. Recall that one can view the group $F^{\mathbb{Z}[t]}$ as a union of the following infinite chain of groups:

$$F = G_0 < G_1 < G_2 < \cdots < G_n < \cdots, \tag{8}$$

where $G_n$ is obtained from $G_{n-1}$ by extension of all cyclic centralizers of $G_{n-1}$ (see Subsection 2.1).

For each $n \in \mathbb{N}$ we construct by induction an embedding

$$\psi_n : G_n \to CDR(\mathbb{Z}[t], X)$$

such that $\psi_{n-1}$ is the restriction of $\psi_n$ to $G_{n-1}$. To this end, let $H_0$ be the set of all words of finite length in $CDR(\mathbb{Z}[t], X)$. Clearly, $F = H_0$. We denote by $\psi_0 : F \to H_0$ the identity isomorphism. It is obvious that $H_0$ is subwords-closed and it is not hard to see that $H_0$ has a Lyndon's set. By Lemma 6.5, $H_0$ is an $S$-subgroup of $CDR(\mathbb{Z}[t], X)$.

Suppose by induction that there exists an embedding

$$\psi_{n-1} : G_{n-1} \to CDR(\mathbb{Z}[t], X)$$

such that the image $H_{n-1} = \psi_{n-1}(G_{n-1})$ is an $S$-subgroup, it is subwords-closed, and there exists a Lyndon's set, say $R_{n-1}$, in $H_{n-1}$. Then by Proposition 6.14 and Theorem 6.15 from Section 6, there exists an embedding $\psi_n : G_n \to CDR(\mathbb{Z}[t], X)$. Moreover, in this case, the image $H_n = \psi_n(G_n)$ is the subgroup of $CDR(\mathbb{Z}[t], X)$ generated by the pregroup

$$P(H_{n-1}, R_{n-1}) = \{ f * u^{\alpha} * h \mid f, h \in H_{n-1},\ u \in R_{n-1},\ \alpha \in \mathbb{Z}[t] \}.$$

Notice that by Lemma 6.19, the group $H_n$ is an $S$-subgroup of $CDR(\mathbb{Z}[t], X)$, and by Lemma 6.18, $H_n$ is subwords-closed. So to finish the proof one needs to show that $H_n$ has a Lyndon's set.

LEMMA 7.1. *Let $H_{n-1}$ from the series (8) be a subwords-closed $S$-subgroup of $CDR(\mathbb{Z}[t], X)$ with a Lyndon's set $R_{n-1}$. Then there exists a Lyndon's set $R_n$ in $H_n$.*

PROOF. Recall that $K = K(H_n) \subset H_n$ is the subset consisting of all elements $v \in H_n$ such that $C_{H_n}(v) = \langle v \rangle$. Denote by $R$ a set of representatives for $K$.

Since $H_n$ is subwords-closed then we may assume that $R \subset H_n$ (see the construction of a set of representatives after Definition 6.6 in Section 6.1). The same argument shows that an element $f \in H_n$ does not contain a subword $u^\alpha$, where $u \in R$ and $\alpha \in \mathbb{Z}[t]$ is infinite. Indeed, in this case it would imply that $u^\alpha \in H_n$, hence, $[u^\alpha, u] = \varepsilon$, so the centralizer of $u$ in $H_n$ is not cyclic – contradiction with $u \in R$. Finally, let $u \in R$, $g \in H_n$. Observe that $u \notin H_{n-1}$, so $u$ has a unique normal form

$$u = f_1 \circ u_1^{\alpha_1} \circ f_2 \circ \cdots \circ u_k^{\alpha_k} \circ f_{k+1},$$

where $f_i \in H_{n-1}$, $u_i \in R_{n-1}$, and $\alpha_i \in \mathbb{Z}[t]$ is infinite for any $i \in [1, k]$. If $g \in H_{n-1}$ then

$$(g * u^m) * u = (g * u^m) \circ u, \quad u * (u^m * g) = u \circ (u^m * g) \tag{9}$$

holds for $m = 1$, since $R_{n-1}$ is a Lyndon's set for $H_{n-1}$. If $g \notin H_{n-1}$ then

$$g = g_1 \circ v_1^{\beta_1} \circ g_2 \circ \cdots \circ v_l^{\beta_l} \circ g_{p+1},$$

where $g_j \in H_{n-1}$, $v_j \in R_{n-1}$ and $\beta_j \in \mathbb{Z}[t]$ is infinite for any $j \in [1, p]$. In this case (9) holds for any $m > p$.

It follows that the set $R_n = R$ is a Lyndon's set for $H_n$. □

## 8. Algorithmic problems for $F^{\mathbb{Z}[t]}$

In this section we discuss some algorithmic problems for $F^{\mathbb{Z}[t]}$. The group $F^{\mathbb{Z}[t]}$ is not finitely generated, as an abstract group, but it is finitely generated as $\mathbb{Z}[t]$-group (a group with operators from $\mathbb{Z}[t]$). Since the ring $\mathbb{Z}[t]$ is finitely generated then every element of $F^{\mathbb{Z}[t]}$ can be represented by a word (so-called *parametric word*) in a finite alphabet. We refer to [**27, 6, 35, 36**] for details on exponential groups. In [**27**] Lyndon showed that the word problem for $F^{\mathbb{Z}[t]}$ is decidable, so this group is *constructible* in the sense of [**33**] or *recursive* in terms of [**41**]. This allows one to represent elements of $F^{\mathbb{Z}[t]}$ effectively by normal forms of various types. In Section 8.1 we discuss how one can effectively rewrite one normal form of an element into another one. Afterward, in Section 8.2, we solve the conjugacy and power problems in $F^{\mathbb{Z}[t]}$.

**8.1. Effective representations of elements of $\mathbb{Z}[t]$.** As we have seen already there are several different ways to describe the group $F^{\mathbb{Z}[t]}$ and its elements. Below we discuss in details various representations of elements of $F^{\mathbb{Z}[t]}$.

**I. Representation by parametric words.** This is Lyndon's original representation [**27**]. We define by induction a set $F_k$ of *parametric* words of level $k$ as follows. Put $F_0 = F = F(X)$. If $F_{k-1}$ is defined then $F_k$ consists of all formal expressions of the type

$$w_1^{\alpha_1} w_2^{\alpha_2} \cdots w_m^{\alpha_m},$$

where $n \in \mathbb{N}$, $w_i \in F_{k-1}$, and $\alpha_i \in \mathbb{Z}[t]$. One can introduce an equivalence relation on $F_k$ such that the equivalence classes form a group with respect to concatenation of parametric words and such that the axioms of exponentiation E1)-E3) (see Subsection 2.1) are satisfied. Abusing notation we denote the resulting group again by $F_k$. Now the group $F^{\mathbb{Z}[t]}$ is defined as a union of the chain of subgroups:

$$F = F_0 < F_1 < \cdots < F_n < \cdots .$$

If $g \in F^{\mathbb{Z}[t]}$ then there exists $k \in \mathbb{N}$ such that $g \in F_k$, so $g$ can be viewed as a parametric word of level $k$

$$g = w_1^{\alpha_1} w_2^{\alpha_2} \cdots w_m^{\alpha_m}.$$

**II. Representation via extensions of centralizers.** This representation of $F^{\mathbb{Z}[t]}$ was introduced in [**36**] by A.Myasnikov and V.Remeslennikov. In this case $F^{\mathbb{Z}[t]}$ is obtained as a union of the chain of extensions of cyclic centralizers (8):

$$F = G_0 < G_1 \cdots < G_n < \cdots,$$

where $G_n$ is the $\mathbb{Z}[t]$-extension of all cyclic centralizers in $G_{n-1}$. Recall that $G_n$ is an HNN-extension of the type

$$G_n = G_{n-1}(R, S) = \langle G_{n-1}, S \mid [c_i, s_{i,j}] = 1, [s_{i,j}, s_{i,k}] = 1, i \in I, j, k \in \mathbb{N} \rangle,$$

where $R = \{c_i \mid i \in I\}$ is a Lyndon's set in $G_{n-1}$ and $S = \{s_{i,j} \mid i \in I, j \in \mathbb{N}\}$. If $g \in F^{\mathbb{Z}[t]}$ then there exists $k \in \mathbb{N}$ such that $g \in G_k$, so $g$ can be represented as a word in generators of $G_k$

$$g = g_1 z_1 g_2 z_2 \cdots z_m g_{m+1},$$

where $g_i \in G_{n-1}$, $z_i \in F(S)$. Moreover, $g$ can be represented in a *reduced form* as an element of an HNN-extension. In this case it does not have subwords of the type $s^{-1}us$ or $sus^{-1}$ where $s \in S$ and $[u, s] = 1$. Furthermore, following [**36**] one can introduce by induction *seminormal* forms of elements from $G_n$.

**III. Representation by infinite words.** In Section 7 we showed that $F^{\mathbb{Z}[t]}$ can be described as a union of the chain of subgroups of $CDR(\mathbb{Z}[t], X)$:

$$F = H_0 < H_1 < \cdots < H_n < \cdots,$$

where $H_n = \langle P(H_{n-1}, R_{n-1}) \rangle$ and $P(H_{n-1}, R_{n-1})$ is the pregroup

$$P(H_{n-1}, R_{n-1}) = \{ f * u^\alpha * h \ \mid \ f, h \in H_{n-1},\ u \in R_{n-1},\ \alpha \in \mathbb{Z}[t] \},$$

formed from $H_{n-1}$ and a Lyndon's set $R_{n-1}$ of $H_{n-1}$.

If $g \in F^{\mathbb{Z}[t]}$ then there exists $n \in \mathbb{N}$ such that $g \in H_n$, so $g$ can be represented by an $R$-form, moreover, it has a unique normal form:

$$g = g_1 \circ u_1^{\beta_1} \circ g_2 \circ \cdots \circ u_m^{\beta_m} \circ g_{m+1},$$

where $g_i \in H_{n-1}$, $u_i \in R_{n-1}$, $\beta_i \in \mathbb{Z}[t]$. We may assume (by induction) that the normal forms of elements from $H_{n-1}$ are already defined. In this event we suppose that the elements $g_i, u_i \in H_{n-1}$ are given in normal forms.

Below we show that given any of the three forms of an element $g \in F^{\mathbb{Z}[t]}$ described above, one can effectively compute the other two. We begin with two auxiliary algorithmic results.

LEMMA 8.1. *Let $f \in H_n$ be given by an $R$-form*

$$f = (f_1, u_1^{\alpha_1}, f_2, \ldots, u_m^{\alpha_m}, f_{m+1}),$$

*where $f_i \in H_{n-1}$, $i \in [1, m+1]$, $u_i \in R_{n-1}$, $\alpha_i \in \mathbb{Z}[t]$, $i \in [1, m]$ and $[f_i, u_{i-1}] \neq \varepsilon$, $[f_i, u_i] \neq \varepsilon$, $i \in [2, m]$. Then one can effectively compute the normal form of $f$ in $H_n$.*

PROOF. We prove by induction on $n$. If $n = 0$ then there is nothing to prove.

Suppose, by induction, that the statement of the lemma holds for $H_{n-1}$. Then one can compute effectively the normal form of any product of the type $u_{i-1}^r * f_i * u_i^r$, where $r_i \in \mathbb{Z}$. By Lemma 6.9 there exists $r_i \in \mathbb{Z}$ such that

$$u_{i-1}^{\alpha_{i-1}} * f_i * u_i^{\alpha_i} = u_{i-1}^{\alpha_{i-1}-r_i} \circ (u_{i-1}^{r_i} * f_i * u_i^{r_i}) \circ u_i^{\alpha_i - r_i}$$

for any $k_1, k_2 > r_i$. Notice that such $r_i$ can be found effectively by checking for $r_i = 1, 2, \ldots$. It follows that one can find effectively a representation of $f$ of the type

$$f = g_1 \circ u_1^{\gamma_1} \circ g_2 \circ \cdots \circ u_m^{\gamma_m} * g_{m+1}.$$

This may not be a normal form for $f$ yet. To obtain the normal form for $f$ one has to check, first, if $g_1$ contains $u_1^{\pm 1}$ as a terminal segment. Using the normal forms for $g_1$ and $u_1$, one can check this effectively. If $g_1 = h_1 \circ u^k$ then

$$f = h_1 \circ u_1^{\gamma_1 + k} \circ g_2 \circ \cdots \circ u_m^{\gamma_m} * g_{m+1}.$$

Now one has to check if $g_2 \circ u_m^{\gamma_m}$ has $u_1^{\pm 1}$ as an initial segment, etc. Induction finishes the proof. □

LEMMA 8.2. *For an element $g \in G_{n-1}$ and $f \in \mathbb{Z}[t]$ one can effectively find the element $g^f \in G_n$, i.e., $\mathbb{Z}[t]$-exponentiation in $F^{\mathbb{Z}[t]}$ (given in the form II) is effective.*

PROOF. To show this we follow the argument from [**36**]. By induction we may assume that $\mathbb{Z}[t]$-exponentiation is defined effectively in $G_{n-2}$ (we put $G_{-1} = 1$ for the base of induction). Recall that every element $g \in G_{n-1} \setminus G_{n-2}$ is a conjugate of some element $u_i \in R_{n-1}$. The axiom (E2) of exponentiation makes it sufficient to define $\mathbb{Z}[t]$-exponentiation on $u_i$ and then extend it by conjugation onto $g$. By the construction the centralizer $C_{G_n}(u_i)$ is isomorphic to the infinite direct sum

$$C_{G_n}(u_i) \simeq \bigoplus_{j=0}^{\infty} \langle s_{i,j} \rangle$$

The map

$$\lambda_i : \mathbb{Z}[t] \to \bigoplus_{j=0}^{\infty} \langle s_{i,j} \rangle$$

defined as

$$a_0 + a_1 t + \cdots + a_k t^k \quad \mapsto \quad a_0 s_{i,0} + a_1 s_{i,1} + \cdots + a_k s_{i,k}$$

is an isomorphism of abelian groups. For $f \in \mathbb{Z}[t]$ put $u_i^f = \lambda_i(f)$. It has been shown in [**36**] that this defines a $\mathbb{Z}[t]$-exponentiation on $G_{n-1}$ (with values in $G_n$), which extends (by induction) to a $\mathbb{Z}[t]$-exponentiation on $F^{\mathbb{Z}[t]}$. Since the isomorphism $\lambda_i$ is effective one can effectively find the element $u_i^f$. To finish the proof it suffices to show now that for a given element $g \in G_{n-1} \setminus G_{n-2}$ one can effectively find the unique element $u_i \in R_{n-1}$ which is a conjugate of $g$. Since the conjugacy problem is decidable in $F^{\mathbb{Z}[t]}$ one can effectively check whether $g$ is conjugate to $u_1$, if not – then to $u_2$, and so on, until the required $u_i$ will be found. This process is effective because the set of representatives $R_{n-1}$ is recursive enumerable (since we started with a recursive representation of $F^{\mathbb{Z}[t]}$ of type II). This finishes the lemma. □

PROPOSITION 8.3. *If $g \in F^{\mathbb{Z}[t]}$ is given by one of the representations I, II, III then one can effectively find the other two representations of $g$.*

PROOF. $I \Longrightarrow II$. Suppose $g \in F^{\mathbb{Z}[t]}$ is given by a parametric word of level $n$

$$g = w_1^{\alpha_1} w_2^{\alpha_2} \cdots w_m^{\alpha_m},$$

where $w_i \in F_{n-1}$, $\alpha_i \in \mathbb{Z}[t]$, $m \in \mathbb{N}$. By induction on $n$ (the base of induction $n = 0$ is obvious) we may assume that for every element $w \in F_{n-1}$, given as a parametric word of level $n-1$, one can effectively compute its representation $\phi_{n-1}(w)$ of the type II, as an element of the HNN-extension $G_{n-1}$. Thus, $\phi_{n-1} : F_{n-1} \to G_{n-1}$ is an effective isomorphism. Now we define $\phi_n : F_n \to G_n$ as follows:

$$\phi_n(g) = \phi_{n-1}(w_1)^{\alpha_1} \dots \phi_{n-1}(w_m)^{\alpha_m}.$$

By Lemma 8.2, $\mathbb{Z}[t]$-exponentiation in $F^{\mathbb{Z}[t]}$ (relative to the representation II) is effective, which implies effectiveness of $\phi_n$.

$II \Longrightarrow III$. Suppose, by induction, we are given an effective isomorphism $\psi_{n-1} : G_{n-1} \to H_{n-1}$. To construct $\psi_n : G_n \to H_n$ one needs only to define $\psi_n$ on elements from $S$. To this end for $s_{i,j} \in S$ put

$$\psi_n(s_{i,j}) = \psi_{n-1}(u_i)^{t^j}$$

This effectively defines $\psi_n$.

$III \Longrightarrow I$. Suppose by induction we are given an effective isomorphism $\psi_{n-1} : H_{n-1} \to F_{n-1}$. If $g \in H_n$ is given as an $R$-form:

$$g = (g_1, u_1^{\beta_1}, g_2, \dots, u_m^{\beta_m}, g_{m+1}),$$

where $g_i \in H_{n-1}, u_i \in R_{n-1}, \beta_i \in \mathbb{Z}[t]$, then put

$$\psi_n(g) = \psi_{n-1}(g_1)\psi_{n-1}(u_1)^{\beta_1}\psi_{n-1}(g_2)\dots\psi_{n-1}(u_m)^{\beta_m}\psi_{n-1}(g_{m+1}).$$

Clearly, $\psi_n : H_n \to F_n$ is an effective isomorphism. □

In view of Proposition 8.3 one may use any of the representations I, II, III of elements from $F^{\mathbb{Z}[t]}$, in which case there is no need to specify a particular one.

It is easy to see that Lemma 8.1 gives one the opportunity to compute the length of elements from $F^{\mathbb{Z}[t]}$ effectively.

COROLLARY 8.4. *Given $f \in F^{\mathbb{Z}[t]}$, one can effectively compute the length $|f|$ of $f$.*

PROOF. In view of Proposition 8.3 we may assume that $f \in H_n$ and it is given by an $R$-form

$$f = (f_1, u_1^{\beta_1}, f_2, \dots, u_k^{\beta_k}, f_{k+1}),$$

where $f_i \in H_{n-1}, i \in [1, k+1], u_i \in R_{n-1}, \beta_i \in \mathbb{Z}[t], i \in [1, k]$. By Lemma 8.1 one can effectively compute the normal form of $f$:

$$f = g_0 \circ u_1^{\alpha_1} \circ g_1 \circ u_2^{\alpha_2} \circ g_2 \circ \dots \circ u_m^{\alpha_m} \circ g_m.$$

Now the length of $f$ is given by the formula (7) from Subsection 6.3:

$$|f| = \sum_{i=0}^{m} |g_i| + \sum_{i=1}^{m} |u_i^{\alpha_i}| = \sum_{i=0}^{m} |g_i| + \sum_{i=1}^{m} |u_i||\alpha_i|.$$

By induction on $n$ we can compute effectively the length of elements $g_i \in H_{n-1}$, hence, the length of $|f|$. □

LEMMA 8.5. *Given the normal forms of $g, h \in F^{\mathbb{Z}[t]}$, one can effectively compute the normal form of* $\mathrm{com}(g, h)$.

PROOF. There exists $n \in \mathbb{N}$ such that $g, h \in H_n$. We prove that the lemma holds for every $H_n$ by induction on $n$. Then the required result will follow for $F^{\mathbb{Z}[t]}$.

If $n = 0$, that is, $g, h \in F$ then $\mathrm{com}(g, h)$ can be computed in the obvious way. Assume $n > 0$ and that the statement is proved for $H_{n-1}$. We can also assume without loss of generality that both $g$ and $h$ belong to $H_n - H_{n-1}$. Thus

$$g = g_1 \circ u_1^{\alpha_1} \circ g_2 \circ \cdots \circ u_k^{\alpha_m} \circ g_{k+1},$$

$$h = h_1 \circ v_1^{\beta_1} \circ h_2 \circ \cdots \circ v_m^{\beta_m} \circ h_{m+1},$$

where $g_i, h_j \in H_{n-1}$, $i \in [1, k+1]$, $i \in [1, m+1]$, $u_i, v_j \in R_{n-1}$, $\alpha_i, \beta_j \in \mathbb{Z}[t]$, $i \in [1, k], j \in [1, m]$.

Suppose $|g_1| \geqslant |h_1|$. By the induction hypothesis we can compute $\mathrm{com}(g_1, h_1)$ effectively. If $c(g_1, h_1) < |h|$ then we are done. Suppose $c(g_1, h_1) = |h|$.

a) If $|g_1| = |h_1|$ then by Lemma 6.4 either $c(u_1^{\alpha_1}, v_1^{\beta_1}) < |u_1| + |v_1|$ or $u_1 = v_1, \mathrm{sgn}(\alpha_1) = \mathrm{sgn}(\beta_1)$. In the former case $\mathrm{com}(g, h) = \mathrm{com}(g_1 \circ u_1^2, h_1 \circ v_1^2)$, which can be computed effectively by the induction hypothesis. In the latter case $\mathrm{com}(u_1^{\alpha_1}, v_1^{\beta_1}) = u^\gamma, \gamma = \mathrm{sgn}(\alpha_1) \min\{|\alpha_1|, |\beta_1|\}$ and we can proceed by the induction on $k + m$.

b) If $|g_1| > |h_1|$ then $g_1 = h_1 \circ f$. By Lemma 6.9 there exists $r \in \mathbb{N}$ such that $c(f \circ u_1^{\alpha_1}, v_1^{\beta_1}) \leqslant r|v_1|$ thus $\mathrm{com}(g, h) = \mathrm{com}(g_1 \circ u_1^{r'}, h_1 \circ v_1^{r''})$, where $r' = \mathrm{sgn}(\alpha_1)r$, $r'' = \mathrm{sgn}(\beta_1)r$ and can be computed effectively by the induction hypothesis. □

COROLLARY 8.6. *Given an element $g \in F^{\mathbb{Z}[t]}$ one can effectively compute its cyclically reduced decomposition $c^{-1} \circ \bar{g} \circ c$.*

**8.2. Conjugacy and power problems for $F^{\mathbb{Z}[t]}$.** In this section we apply the infinite words technique to the conjugacy and power problems for $F^{\mathbb{Z}[t]}$.

Recall that the *conjugacy problem* is decidable in $F^{\mathbb{Z}[t]}$ if there exists an algorithm which, given two elements $f, g \in F^{\mathbb{Z}[t]}$, determines if there exists $x \in F^{\mathbb{Z}[t]}$ such that $x^{-1} f x = g$.

In view of Corollary 8.6 it suffices to solve the conjugacy problem for cyclically reduced $f$ and $g$.

LEMMA 8.7. *Let $f, g \in F^{\mathbb{Z}[t]}, f \neq g$ be cyclically reduced and $w \in F^{\mathbb{Z}[t]}$ be such that $w^{-1} * f * w = g$. Then $w = w_1 \circ h$, where $[w_1, f] = \varepsilon$, $|h| < |f|$ and $g$ is a cyclic permutation of $f$.*

PROOF. We can represent $w$ as a product $w = w_1 \circ h$, where $w_1$ belongs to the centralizer of $f$ and $h$ does not contain any element commuting with $f$ as an initial segment. Thus we have to show that $|h| < |f|$, which implies automatically that $g$ is a cyclic permutation of $f$.

Assume on the contrary $|h| \geqslant |f|$. Since $f$ is cyclically reduced we have either $h^{-1} * f = h^{-1} \circ f$ or $f * h = f \circ h$. Assume the former. Then we have

$$w^{-1} * f * w = (h^{-1} \circ f) * h$$

and $h$ has to cancel completely in $(h^{-1} \circ f) * h$. Thus we have that $h$ has $f^{-1}$ as an initial segment – a contradiction, which proves the lemma. □

Thus, by Lemma 3.8, to check if two elements of $F^{\mathbb{Z}[t]}$ are conjugate we have to compare their cyclic permutations. But unlike free groups, there are infinitely many cyclic permutations of an element in $F^{\mathbb{Z}[t]}$. Thus, we have to reduce the checking procedure to finitely many cyclic permutations.

Let $f, g \in F^{\mathbb{Z}[t]}$ be cyclically reduced. There exist $n_1, n_2 \in \mathbb{N}$ such that $f \in H_{n_1+1} - H_{n_1}$, and $g \in H_{n_2+1} - H_{n_2}$. Observe that if $n_1 < n_2$ then $f$ can not be a cyclic permutation of $g$ because $f$ does not contain infinite exponents of elements from $H_{n_2}$. Thus, if $f$ is conjugate to $g$ then $n_1 = n_2$.

LEMMA 8.8. *Let $f \in H_{n+1} - H_n, n \in \mathbb{N}$ and let*

$$f = f_1 \circ v_1^{\alpha_1} \circ f_2 \circ \cdots \circ v_k^{\alpha_k} \circ f_{k+1}$$

*be its unique reduced form. Then there exists a finite set $C_f$ of cyclic permutations of $f$ such that any $\overline{f} \in C_f$ has an infinite exponent of $v_i, i \in [1, k]$ as an initial segment and does not have $v_i^{\pm 1}$ as a terminal segment.*

PROOF. Consider

$$f(i) = (f_1 \circ v_1^{\alpha_1} \circ \cdots \circ f_i)^{-1} * f * (f_1 \circ v_1^{\alpha_1} \circ \cdots \circ f_i).$$

Then, its unique reduced form is

$$f(i) = v_i^{\gamma_i} \circ h_{i+1} \circ v_i^{\gamma_{i+1}} \circ \cdots \circ v_{i-1}^{\gamma_{i-1}} \circ h_i.$$

Now, if $f(i)$ has $v_i^{\alpha}$ as a terminal segment we can assume this exponent to be maximal possible and set $\overline{f(i)} = v_1^{\alpha} * f(i) * v_1^{-\alpha}$. Observe that $\overline{f(i)}$ satisfies the required conditions.

Since $f$ contains only finitely many infinite exponents of elements of $H_n$, the set $\{f(i)\}$ is finite. Thus, $\{\overline{f(i)}\}$ is also. Finally, it is easy to see that any cyclic permutation of $f$ which has an infinite exponent of $v_i, i \in [1, k]$ as an initial segment and does not have $v_i^{\pm 1}$ as a terminal segment can be obtained in the way we obtained $\{\overline{f(i)}\}$. So, $C_f = \{\overline{f(i)}\}$. □

Observe that $C_f$ can be found effectively for any $f \in F^{\mathbb{Z}[t]}$.

Now we are ready to present the solution of the conjugacy problem for $F^{\mathbb{Z}[t]}$.

LEMMA 8.9. *Elements $f$ and $g$ of $F^{\mathbb{Z}[t]}$ are conjugate in $F^{\mathbb{Z}[t]}$ if and only if $C_f \cap C_g \neq \emptyset$.*

PROOF. If $C_f \cap C_g \neq \emptyset$ then $C_f = C_g$ and obviously $f$ is conjugate to $g$ by the construction of sets $C_f$ and $C_g$.

Suppose $f$ is conjugate to $g$. Observe that if

$$f = f_1 \circ v_1^{\alpha_1} \circ f_2 \circ \cdots \circ v_k^{\alpha_k} \circ f_{k+1},$$

$$g = g_1 \circ u_1^{\beta_1} \circ g_2 \circ \cdots \circ u_l^{\beta_l} \circ g_{l+1}$$

then by Lemma 3.8 we have $\{v_1, \ldots, v_k\} = \{u_1, \ldots, u_l\}$ because $f = w^{-1} * g * w$ for some initial segment $w$ of $g$. But then $C_f = C_g$. □

The *power problem* is decidable in $F^{\mathbb{Z}[t]}$ if there exists an algorithm which, given $g \in F^{\mathbb{Z}[t]}$, determines if there exists $n \in \mathbb{N}$ such that $g = f^n$ for some $f \in F^{\mathbb{Z}[t]}$.

Let $g \in H_{n+1} - H_n$. If the power problem is decidable for cyclically reduced elements then obviously it is decidable for arbitrary ones. Thus, in view of Corollary 8.6 we can assume $g$ to be cyclically reduced.

Let $g$ have the unique reduced form

$$g = g_1 \circ u_1^{\beta_1} \circ g_2 \circ \cdots \circ u_l^{\beta_l} \circ g_{l+1},$$

where $l \geqslant 1$, $g_i, u_i \in H_n$ and $\beta_i \in \mathbb{Z}[t]$ is infinite for any $i \in [1, l]$.

a) $l = 1$

If $g_1 \neq \varepsilon$ then $g$ is not a proper power unless $g_1$ is a power of $u_1$ which is impossible. Now let $g_1 = \varepsilon$, $g = u_1^{\beta_1}$. In this case everything reduces to computations in a free abelian group of finite rank, where we can check easily if an element $\beta_1$ is a proper power.

b) $l > 1$

Compose a set $D$ of all divisors of $l$. Since $D$ is finite we have $D = \{d_1, \ldots, d_k\}$. Consider $s_i = g_{\alpha_j}$, $i \in [1, k]$, where $\alpha_i = |g|/d_i$, $i \in [1, k]$ is such that $|g|$ can be divided by $d_i$ coordinatewise. $\{s_i\}$ is finite because $D$ is finite.

Finally, we check if $g = s_i^{d_i}$ for some $s_i$. If it is for some $i$, then $g$ is a proper power of an element $s_i \in F^{\mathbb{Z}[t]}$, otherwise it is not. This follows from the fact that we have a regular length function on $F^{\mathbb{Z}[t]}$.

## References


[1] K. Appel, *One-variable equations in free groups.* Proc. Amer. Math. Soc., **19** (1968), 912–918.

[2] K. Appel, *On two variable equations in free groups.* Proc. Amer. Math. Soc., **21** (1969), 179–184.

[3] H. Bass, *Groups acting on non-arhimedean trees.* In: Arboreal group theory, MSRI Publications **19** (1991), New York: Springer-Verlag, pp. 69–130.

[4] G. Baumslag, A. Myasnikov and V. Remeslennikov, *Residually hyperbolic groups.* Proc. Inst. Appl. Math. Russian Acad. Sci., **24** (1995), 3–37.

[5] G. Baumslag, A. Myasnikov and V. Remeslennikov, *Algebraic geometry over groups I. Algebraic sets and ideal theory.* J. Algebra, **219** (1999), 16–79.

[6] G. Baumslag, A. Myasnikov and V. Remeslennikov, *Discriminating completions of hyperbolic groups.* Geometriae Dedicata, **92** (2002), 115–143.

[7] I. Belenkov, D. Mosunov and V. Remeslennikov, *Free A-groups.* Preprint.

[8] M. Bestvina and M. Feighn, *Stable actions of groups on real trees.* Invent. Math., **121** no. 2 (1995), 287–321.

[9] I. Chiswell, *Abstract length functions in groups.* Math. Proc. Cambridge Philos. Soc., **80** no. 3 (1976), 451–463.

[10] I. Chiswell, *Introduction to* $\Lambda$*-trees.* World Scientific, 2001.

[11] I. Chiswell and V. Remeslennikov, *Equations in free groups with one variable I.* J. Group Theory, **3** no. 4 (2000), 445–466.

[12] D. E. Cohen, *Combinatorial group theory: a topological approach*, London Math. Soc. Student Texts, **14**, Cambridge University Press, Cambridge, 1989.

[13] D. Gaboriau, G. Levitt and F. Paulin, *Pseudogroups of isometries of R and Rips' theorem on free actions on R-trees.* Israel J. Math., **87** no. 1–3 (1994), 403–428.

[14] D. Gildenhuys, O. Kharlampovich and A. Myasnikov, *CSA-groups and separated free constructions.* Bull. Austral. Math. Soc., **52** no. 1 (1995), 63–84.

[15] A. M. W. Glass, *Partially ordered groups.* Series in Algebra, **7**, World Scientific, 1999.

[16] A. Hoare, *Pregroups and length functions.* Math. Proc. Cambridge Philos. Soc., **104** no. 1 (1988), 21–30.

[17] O. Kharlampovich, *Equations over free and fully residually free groups. Formal power series and algebraic combinatorics.* Proceedings of the 12th Inter. Conf. (FPSAC'00) held in Moscow, Springer, Berlin, 2000, pp. 45–53.

[18] O. Kharlampovich and A. Myasnikov, *Description of fully residually free groups and irreducible affine varieties over a free group.* Center de Recherchers Matematiques, CRM Proceedings and Lecture Notes, **17** (1999), 71–80.

[19] O. Kharlampovich and A. Myasnikov, *Irreducible affine varieties over a free group. I: Irreducibility of quadratic equations and Nullstellensatz.* J. Algebra, **200** no. 2 (1998), 472–516.

[20] O. Kharlampovich and A. Myasnikov, *Irreducible affine varieties over a free group. II: Systems in triangular quasi-quadratic form and description of residually free groups.* J. Algebra, **200** no. 2 (1998), 517–570.
[21] O. Kharlampovich and A. Myasnikov, *Implicit function theorems over free groups.* Preprint.
[22] O. Kharlampovich and A. Myasnikov, *Elementary theory of free groups. The Tarski problem.* Preprint.
[23] O. Kharlampovich, A. Myasnikov and V. Remeslennikov, *Logical languages and axioms for groups with a length function.* Proc. Inst. Appl. Math. Russian Acad. Sci., **20** (1995), 1–8.
[24] V. Kopytov and N. Medvedev, *Right-ordered groups.* Siberian School of Algebra and Logic. Consultants Bureau, New York, 1996.
[25] E. Lioutikova, *Lyndon's group is conjugately residually free.* Internat. J. Algebra and Comput., **13** no. 3 (2003), 255–276.
[26] A. Lorenc, *Coefficient-free equations in free groups.* (Russian) Dokl. Akad. Nauk SSSR, **160** (1965), 538–540.
[27] R. Lyndon, *Groups with parametric exponents.* Trans. Amer. Math. Soc., **9** no. 6 (1960), 518–533.
[28] R. Lyndon, *Length functions in groups.* Math. Scand., **12** (1963), 209–234.
[29] R. Lyndon, *Equations in free groups.* Trans. Amer. Math. Soc., **96** (1960), 445–457.
[30] R. Lyndon and P. Schupp, *Combinatorial group theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete, **89**, Springer-Verlag, Berlin, Heidelberg, New York, 1977.
[31] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: presentations of groups in terms of generators and relators.* Dover Publications, New York, 1976.
[32] G. S. Makanin, *Equations in a free group.* (Russian) Izv. Akad. Nauk SSSR, Ser. Mat., **46** (1982), 1199–1273.
[33] A. I. Mal'cev, *Constructive algebras. I.* (Russian) Uspehi Mat. Nauk, **16** no. 3(99) (1961), 3–60.
[34] J. Morgan and P. Shalen, *Free actions of surface groups on R-trees.* Topology, **30** no. 2 (1991), 143–154.
[35] A. Myasnikov and V. Remeslennikov, *Exponential groups I: foundations of the theory and tensor completion.* Siberian Math. J., **35** no. 5 (1994), 1106–1118 (Russian).
[36] A. Myasnikov and V. Remeslennikov, *Exponential groups II: extensions of centralizers and tensor completion of CSA-groups.* Internat. J. Algebra and Comput., **6** no. 6 (1996), 687–711.
[37] A. Myasnikov and V. Remeslennikov, *Length functions on free exponential groups.* Proc. Internat. Conf. on Groups in Analysis and Geometry, Omsk, 1995, pp. 59–61.
[38] A. Myasnikov and V. Remeslennikov, *Length functions on free exponential groups.* Proc. IITPM SO RAN, Omsk, 1996, no. 26, 1–34.
[39] A. Yu. Ol'shanskii, *On residualing homomorphisms and G-subgroups of hyperbolic groups.* Internat. J. Algebra and Comput., **3** no. 4 (1993), 365–409.
[40] D. Promislow, *Equivalence classes of length functions on groups.* Proc. London Math. Soc. (3), **51** no. 3 (1985), 449–477.
[41] M. O. Rabin, *Computable algebra, general theory and theory of computable fields.* Trans. Amer. Math. Soc., **95** no. 2 (1960), 341–360.
[42] A. Razborov, *On the parameterization of solutions for equations in free groups.* Internat. J. Algebra Comput., **3** no. 3 (1993), 251–273.
[43] L. Ribes and P. Zalesskii, *Conjugacy separability of amalgamated free products of groups.* J. Algebra, **179** no. 3 (1996), 751–774.
[44] F.S. Rimlinger, *Pregroups and Bass-Serre Theory.* Mem. Amer. Math. Soc., Providence, **65**, no. 361 (1987).
[45] J.R. Stallings, *Groups of cohomological dimension one.* Proc. Sympos. Pure Math. Amer. Math. Soc., 1970, **17**, 124–128.
[46] J.R. Stallings, *Group theory and three dimensional manifolds.* New Haven, London, Yale Univ. Press, 1971.

City College of CUNY, Department of Mathematics, Convent Ave. & 138 st. New York NY 10031
*E-mail address*: alexeim@att.net
*URL*: http://www.cs.gc.cuny.edu/ amyasnikov/

Vladimir N. Remeslennikov, Omsk Branch of the Mathematical Institute SB RAS, 13 Pevtsova Street, 644099 Omsk, Russia
*E-mail address*: remesl@iitam.omsk.net.ru

City College of CUNY, Department of Mathematics, Convent Ave. & 138 st. New York NY 10031
*E-mail address*: zloidyadya@yahoo.com