FUNDAMENTAL SEARCH PROBLEMS IN GROUP THEORY

by

ALEXANDER USHAKOV

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2005

UMI Number: 3187428

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

05/06/06 — Alexei Miasnikov
Date — Chair of Examining Committee

05/06/06 — Jozef Dodziuk
Date — Executive Officer

Michael Anshel

Robert Gilman

Janos Pach

Vladimir Shpilrain
Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

FUNDAMENTAL SEARCH PROBLEMS IN GROUP THEORY

by

Alexander Ushakov

Advisor: Alexei Miasnikov

We consider search variations of the fundamental problems of the group theory: the Word search problem and the Conjugacy search problem. For each of these problems we propose effective algorithms for solving the problem and prove the efficiency of the algorithm. More precisely, we show that each algorithm has polynomial-time generic-case complexity.

Acknowledgments

First and foremost, I would like to thank my adviser Alexei Miasnikov for his generous time and commitment, for his guidance through all my research, for inspiring advice, support and encouragement not only in mathematics but in everyday life for the past five years of my Ph.D studies. Throughout my doctoral work he continually stimulated my analytical thinking and greatly assisted me with scientific writing. Also, I am extremely grateful to Vladimir Remeslennikov, who was my undergraduate advisor in Omsk State University.

I would like to thank my thesis committee members, Michael Anshel, Bob Gilman, Janos Pach, Vladimir Shpilrain, and Alphonse Vasquez for their time, patience and positive feedback on my dissertation.

I am grateful to the faculty and staff of Mathematics and Computer Science Departments for providing several years of valuable coursework, and for funding this work as part of my doctoral research. I give special thanks to Jozef Dodziuk, Alvany Rocha, Ted Brown, Joseph Driscoll, and Robert Landsman.

I wish to thank all my friends and colleagues, especially Parisa Babaali, Dmitry Bormotov, Alexei Kvaschuk, Alexei D. Miasnikov, Denis Serbin, and Dong Wook Wong.

My thanks to Robert Haralick for allowing me to use a cluster at his lab at the Graduate Center and Stephen Altmuller for his help with the cluster. Also, I thank Jin Mao for his help with my webpage.

Finally, my special thanks go to my parents for their emotional support throughout this very long process.

This work is partially supported from Umbanet Inc. through an award from the U.S. Department of Commerce National Institute of Standards and Technology, Advanced Technology Program, #70NANB2H3012.

Contents

List of Figures

List of Notation

I Word Problem

II Conjugacy Problem

1 Preface

Any presentation $\langle X; R\rangle$ always determines a unique group G (up to isomorphism) (see [30]). But it might be very hard to get any specific information about G (e.g., is G trivial, finite, abelian, etc.) – global properties of G, or about elements of G (e.g., is trivial, of finite order, etc.) – local properties of G. The problem of deciding whether a word in G defines the identity is the first of the fundamental decision problems formulated by Max Dehn in 1911:

(WP) For an arbitrary word w in the generators of G decide in a finite number of steps whether w defines the identity element of G, or not.

(CP) For two arbitrary words w_1 and w_2 in generators of G decide in a finite number of steps whether w_1 and w_2 define conjugate elements of G, or not.

(IP) For two group presentations decide in a finite number of steps whether the groups the represent are isomorphic, or not.

These problems are called the Word problem, the Conjugacy problem, and the isomorphism problem.

The Word problem is, probably, the easiest problem from those listed above. Nevertheless, in 1952 Novikov proved that it is unsolvable in general (later Boone and others). More precisely, these authors presented the particular group presentations for which there is no general and effective procedure to determine whether a word defines the trivial element of the group. Later, it was shown that almost all natural local and global group-theoretic questions have no solutions. In particular, all fundamental problems are undecidable in general. (See [3] for more information on decidability/undecidability of the Word problem in groups and semigroups and [28], [29] for more general results on undecidability of different problems in groups.)

Nevertheless, many algorithmic problems are considered as tractable (or tractable almost everywhere) due to the observation called Gromov's theorem (explicitly

proved by A. Olshanskii in [35]). Olshanskii proved that the asymptotic density of presentations defining word-hyperbolic groups (even more, small cancellation $C'(\frac{1}{6})$) in the class of all presentations is 1. Now, since the time-complexity of many problems (e.g., word and conjugacy, but not membership) for hyperbolic groups is small, it follows that for almost all group presentations those problems are efficiently solvable. This approach has a small flaw though. Even if one has a hyperbolic group presentation, to perform actual computations sometimes one has to precompute certain values (e.g., the constant of hyperbolicity or the Dehn presentation) which might be very hard. So, asymptotically the computations will be fast, but, perhaps, with a huge constant.

Another very important for us result is due to Kapovich, Miasnikov, Schupp, and Shpilrain (see [19]). It can be informally formulated as follows. There exists a generic class of group presentations (does not coincide with the class of hyperbolic groups) in which the word and the conjugacy problems have linear time generic-case complexity. So, these problems might be very hard (even unsolvable) for a presentation from that class but almost all pairs of words in generators are non-conjugate and are easy to recognize as being non-conjugate. Moreover, it is very easy to recognize whether a given presentation $\langle X; R\rangle$ belongs to the class under consideration in contrast to hyperbolic groups.

The downside of the algorithms proposed in [19] is that they produce only the negative answers, e.g., a word does not define the identity of a group, or a pair of words does not define conjugate elements of a group, while in most of the applications the situation is directly opposite. For example, the security of key-exchange scheme proposed in [21] is based mostly on the hardness of the question:

Suppose that $w_1 \sim_G w_2$. Find an element x such that $w_1 = x^{-1}w_2x$.

The quoted above problem is called the Conjugacy search problem. This is one of the following fundamental search problems:

(WSP) For an arbitrary word w in the generators of G decide in a finite number of steps whether w defines the identity element of G (and present a proof of this fact). If w does not define the identity element of G then either never stop, or output No or $DontKnow$.

(CSP) For two arbitrary words w_1 and w_2 in generators of G decide in a finite number of steps whether w_1 and w_2 define conjugate elements of G (and present a proof). If w_1 and w_2 does not define conjugate elements of G then either never stop, or output No or $DontKnow$.

(ISP) For two group presentations decide in a finite number of steps whether the groups the represent are isomorphic (and present a proof). If presentations are not isomorphic then either never stop, or output No or $DontKnow$.

These problems are called the Word search problem, the Conjugacy search problem, and the Isomorphism search problem. The positive answer to each of these problems implies that there exists an algorithm which recognizes the Yes-part of the problem and ignores the No-part. A proof for the Yes-part can be any object using which it is straightforward to check that the element(s) possesses the property. For example, the conjugator for the Conjugacy search problem.

In this paper we consider the first two of these problems for finitely presented groups. For each problem we propose the algorithm solving it and prove its generic polynomial-time efficiency. There is the main obstacle on our way to show the efficiency of the algorithms. It is the measure on the Yes-parts of the problems. We cannot define the standard asymptotic density on, say trivial, words, since the non-constructive definition of the trivial words is the source of insolvability of the Word problem. We cannot capture algorithmically the set of all words defining identity of a fixed length. So, first we will define probability measures on the diagrams (van Kampen and annular) and then we will induce the probability measure from

diagrams onto the words (trivial words and pairs of conjugate words resp.).

1.1 Main results of the first part (Word search problem)

- Discrete probability measure $P_{\mathcal{L}}$ on the set $\mathcal{L}$ of all diagrams over a finite symmetrized reduced presentation $\langle X; R\rangle$.

- New original parameter of a van Kampen diagram which we refer to as depth (denoted by δ).

- Asymptotic density $\rho_{\mathcal{L}}$ on the set of all van Kampen diagrams $\mathcal{L}$ over a finite symmetrized reduced presentation $\langle X; R\rangle$.

- The next corollary states that the set of van Kampen diagrams over $\langle X; R\rangle$ in which the length of a perimeter is greater than the half of the size (total number of cells and free edges) and the depth is less than double of a logarithm of the size has asymptotic density 1 in the set of all van Kampen diagrams.

Corollary 8.11 Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation. Let

$$\mathcal{L}'' = \{D \in \mathcal{L} \mid \delta(D) < 2\log\chi(D) \ \&\ l(D) \geq \tfrac{1}{2}\chi(D)\} \subseteq \mathcal{L}.$$

Then $\rho_{\mathcal{L}}(\mathcal{L}'') = 1$.

This implies that the isoperimetric function for a finite symmetrized reduced presentation is generically linear.

- Algorithms $\mathcal{A}$ and $\mathcal{B}$ (Algorithms 5.1 and 5.8) for solving the Word search problem.

- Asymptotic density ρ_{WP} on the set $WP(X; R)$ of all words defining the identity of $G = \langle X; R\rangle$.

• The next theorem states that for words from the set $CW^{(\alpha)} \subseteq WP(X;R)$ Algorithms $\mathcal{A}$ and $\mathcal{B}$ have polynomial time complexity.

Theorem 9.4 Let $\langle X;R\rangle$ be a finite symmetrized reduced presentation and $G = \langle X;R\rangle$. Then the following holds.

1) The time complexity function for Algorithm $\mathcal{A}$ (the decision algorithm for the word problem in G) on the set of inputs $w \in CW^{(\alpha)}$ is bounded from above by the polynomial

$$O(|w|^{2+2\log L(R)}).$$

2) The time complexity function for Algorithm $\mathcal{B}$ (the algorithm for the Word search problem in G) on the set of inputs $w \in CW^{(\alpha)}$ is bounded by the polynomial

$$O(|w|^{4+4\log L(R)}).$$

where $CW^{(\alpha)}$ is a subset of $WP(X;R)$ of asymptotic density 1.

1.2 Main results of the second part (Conjugacy search problem)

• Discrete probability measure $P_{\mathcal{L}_w}$ on the set $\mathcal{L}_w$ of all annular diagrams (containing a base loop labelled with w) over a finite symmetrized reduced presentation $\langle X;R\rangle$.

• New original parameter of annular diagrams which we refer to as depth (denoted by δ).

• Asymptotic density $\rho_{\mathcal{L}_w}$ on the set of all annular diagrams $\mathcal{L}_w$ (containing a base loop labelled with w) over a finite symmetrized reduced presentation $\langle X;R\rangle$.

- The next corollary states that the set of diagrams over $\langle X; R\rangle$ in which the depth is not greater than double of a logarithm of double of the length of the perimeter has asymptotic density 1 in the set of annular diagrams $\mathcal{L}_w$.

Corollary 19.5 Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation, $w = w(X)$ such that w does not belong to the conjugacy class of a word of length less or equal to 1. Let

$$\mathcal{L}''_w = \{D \in \mathcal{L}_w \mid \delta(D) \leq 2\log(2l(D))\}.$$

Then $\rho_{\mathcal{L}_w}(\mathcal{L}''_w) = 1$.

- Algorithm $\mathcal{A}_C$ (Algorithm 17.11) for solving the Conjugacy search problem.

- Asymptotic density ρ_{CP_w} on the set $CP_w(X; R)$ of all pairs (w_1, w_2) of cyclic words such that $w_1 \sim_G w \sim_G w_2$, where $G = \langle X; R\rangle$.

- The next theorem states that for pairs of words from the generic set $CP_w^{(\alpha)} \subseteq CP_w(X; R)$ the Algorithm $\mathcal{A}_C$ has polynomial time complexity.

Theorem 20.4 Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation, $G = \langle X; R\rangle$, and $w = w(X)$ be a word the conjugacy class of which does not contain words of length less than 2. Then the the time complexity function for Algorithm 17.11 (the search algorithm for the conjugacy problem in G) on the set of inputs $(w_1, w_2) \in CP_w^{(\alpha)}$ is bounded from above by the polynomial

$$O((|w_1| + |w_2|)^{2+4\log L(R)}).$$

where $CP_w^{(\alpha)}$ is a subset of $CP_w(X; R)$ of asymptotic density 1.

Part I

Word Search Problem

2 Introduction

The history of the development of the Word problem in group theory dates back one hundred years now and started, perhaps, from the formulation of the fundamental problems in 1911 mentioned in the preface. (See [6] for more information on the history of the combinatorial group theory.) We will mention here several positive results about the Word problem in groups.

One of the first positive results about the solvability of this problem was obtained by Max Dehn. In 1912 he proved [8] that the word problem for the fundamental groups of closed, two-dimensional, orientable surfaces of a genus $g \geq 2$ can be solved by a monotone reduction process, which is now referred to as Dehn's algorithm. The groups under consideration are one-relator groups.

In 1932 Magnus proved ([24] and [25]) that the Word problem for any one-relator presentation is solvable. The method and the proof of its correctness are rather complicated. The precise time-complexity of the method is still unknown. It is unknown whether one can bound the complexity by any fixed tower of exponents. Though for some special classes of one-relator presentations there exist very efficient algorithms. For instance, for one-relator groups with torsion or for small cancellation presentations the Dehn's algorithm solves the Word problem.

In 1945 Markov [26] (and later Artin [4]) proved that the Word problem in braid groups is solvable by finding normal forms for pure braids. The original algorithm had exponential time-complexity and was later improved by Garside [10] and Birman [5] to quadratic complexity.

In 1960 Greendlinger proved [11] that the Dehn algorithm works for any small cancellation presentation from the class $C(\frac{1}{6})$.

A lot of results were generalized with the introduction of hyperbolic groups by Gromov. Lysenok proved that the group has Dehn's presentation (admitting Dehn's algorithm) if and only if it is hyperbolic and, so, the Word problem in hyperbolic groups has linear-time complexity.

Later the class of hyperbolic groups was generalized by Cannon, Epstein, Gilman to the class of automatic groups in which it was shown that the Word problem has quadratic time-complexity. See [9] for more information on automatic groups.

In certain special classes of groups the solution to the Word problem is straightforward. For example, in linear (matrix) groups the word problem is solvable in at most quadratic time. In the symmetric group S_n the Word problem has linear time complexity. In the group $Aut(F_n)$ of automorphisms of the free group of rank $n \geq 2$ the straightforward solution is at most exponential. It is an open question whether there exists a better upper bound for the worst case time-complexity of the Word problem in $Aut(F_n)$. Also, it was known that abelian and nilpotent groups and polycyclic groups have solvable Word problems.

Moreover, the number of presentations defining groups with undecidable word problem is negligible relative to its complement. Consider the class of word-hyperbolic groups. A. Olshanskii in [Olsh] showed that the asymptotic density of presentations defining word-hyperbolic groups (in fact, small cancellation $C'(\lambda)$, torsion free) is 1. This means that if $\langle a_1, \ldots, a_n; r_1, \ldots, r_k \rangle$ is a group presentation with a fixed numbers n and k of generators and relators then the chance that the corresponding group is hyperbolic tends to 1 exponentially fast as the total length of relators $L(R) = \sum_{i=1}^{k} |r_i|$ tends to ∞. At the same time each word-hyperbolic group has a Dehn presentation and, so, the complexity of the Word problem is linear. Algorithmically that means that almost every randomly generated group presentation we

can solve the word problem in linear time.

In this paper we move this idea further. We will show that there exists a larger class of presentations $\langle X; R\rangle$ (which includes word-hyperbolic groups and all known to us examples of group presentations with undecidable word problem) such that the amount of words $w = w(X)$ that cannot be recognized as non-trivial or trivial in polynomial time in terms of $|w|$ is negligible in the set of all words in the generators of the given group. This is the class of R-reduced group presentations, defined and studied in Section 3. The first part – recognition of the non trivial words – is already accomplished in [19], were the authors use homomorphisms onto certain classes of groups. So we are left with the trivial words only. This leads us to the Word search problem.

The Word search problem is a variation of the Word problem and can be stated as follows. For a group presentation $\langle X; R\rangle$ and a word $w = w(X)$ such that $w =_G 1$ give a proof that w, indeed, represents the trivial element in G. The proof can be any object using which one can check in a straightforward way the triviality of w. We propose two algorithms $\mathcal{A}$ and $\mathcal{B}$ for the Word search problem. The first algorithms outputs a part of the Cayley graph (referred to as approximation) which contains a loop labelled with w. The second algorithm outputs a rewriting system using which one can represent w in a product of conjugates of elements of R.

3 Presentations of groups

Let X be a set. Denote by $X^{-1} = \{x^{-1} \mid x \in X\}$ the set of formal *inverses* of elements of X. The map $x \to x^{-1} (x \in X)$ naturally extends to an involution on the set $X^{\pm 1} = X \cup X^{-1}$, where we define $(x^{-1})^{-1} = x$. Let $M(X)$ be the *free monoid* with basis $X^{\pm 1}$ viewed as the set of all words in the alphabet $X^{\pm 1}$ with concatenation as the multiplication and $F = F(X)$ be a *free group* with basis X

viewed as the set of all *reduced* words in $X^{\pm 1}$ with concatenation and subsequent reduction as the multiplication. For $R \subseteq F(X)$ and a group G we write

$$G = \langle X; R \rangle \tag{1}$$

if $G \simeq F(X)/gp_F(R)$, where $gp_F(R)$ is the normal closure of R in F. In this event X is a set of *generators* of G, R is a set of *relators* of G, and $\mathcal{P} = \langle X; R \rangle$ is a *presentation* of G. For a presentation $\langle X; R \rangle$ we define the total length $L(R)$ and the maximal length $M(R)$ of relators as

$$L(R) = \sum_{r \in R} |r|, \quad M(R) = \max_{r \in R} \{|r|\}.$$

A presentation $\mathcal{P} = \langle X; R \rangle$ is finite if the sets X and R are finite. A group G is called *finitely presented* if $G = \langle X; R \rangle$ for some finite presentation $\langle X; R \rangle$. In this paper we concern only with finite presentations, though some results admit natural generalization for infinite presentations. A finite presentation $\langle X; R \rangle$ has *decidable word problem* if the set $gp_F(R)$ is recursive. It is not hard to see that if one finite presentation of G has decidable word problem then any finite presentation of G has decidable word problem. Therefore, we often refer to G as a group with decidable word problem.

For a subset $Y \subseteq F$ define $Y^{-1} = \{y^{-1} \mid y \in Y\}$.

Definition 3.1. A set $R \subseteq F$ is called *symmetric* if the following holds:

1) every $r \in R$ is cyclically reduced;

2) $R^{-1} = R$;

3) if $r \in R$ then R contains every cyclic permutation of r.

For a given finite subset $R \subseteq F$ one can effectively construct a finite symmetric set R_{sym} such that $gp_F(R) = gp_F(R_{sym})$, so the groups defined by presentations

$\langle X; R\rangle$ and $\langle X; R_{sym}\rangle$ are isomorphic. This allows one to consider only *symmetrized presentations*, i.e., presentations $\langle X; R\rangle$ with $R = R_{sym}$.

Given a group $G = \langle X; R\rangle$ we say that a set S' is obtain from a set $S \subseteq F$ by a G-reduction (and write $S \to_G S'$) if there exists a word $s \in S$ such that some cyclic permutation of s has the form $s_1 \circ s_2$, where $s_1, s_2 \neq \varepsilon$, $s_1 \in gp_F(R)$ (and hence $s_2 \in gp_F(R)$), and

$$S' = (S - \{s\}) \cup \{s_1, s_2\}.$$

Obviously, if S is finite then the rewriting process

$$S \to_G S' \to_G (S')' \to_G \dots$$

terminates in finitely many steps, resulting in a set S^* for which $\to_G$ does not apply. We call S^* a *G-reduced form* of S. In general, it could be several reduction processes for a given S resulting in different sets S^*, but in each case

$$G = \langle X; R\rangle = \langle X; R^*\rangle.$$

Moreover, if the word problem is decidable in G then given a finite set $S \subseteq F$ one can find *effectively* all G-reduced forms S^* of S.

Definition 3.2. We say that a presentation $G = \langle X; R\rangle$ is *G-reduced* if $R = R^*$ and $x \neq_G 1$ for every $x \in X$.

Proposition 3.3. If $G = \langle X; R\rangle$ is a finitely presented group with decidable word problem then one can effectively find a finite symmetrized G-reduced presentation of G.

Proof. It follows from decidability of the word problem that if a finite set $R \subset F(X)$ is not G-reduced then one can effectively find a reduction $S \to_G S'$. Therefore, starting with R in finitely many steps one can effectively find the reduced form

R^* of R. Now, it suffices to delete letters $x \in X^{\pm 1}$ from R^* (if there are any) and delete the same letters from X. The resulting presentation $G = \langle Y; T \rangle$ is G-reduced. Hence the presentation $G = \langle Y; T_{sym} \rangle$ is G-reduced and symmetrized. □

There are many known finite reduced presentations. For example, if $r \in F$ is a cyclically reduced word then one relator presentation $G = \langle X; r \rangle$ is G-reduced (this is due to Weinbaum [39], see also Theorem 5.29 in [23]); the standard presentation of the braid group B_n is B_n-reduced, as well as the canonical finite presentation of the Thompson group

$$F = \langle x_0, x_1, x_2, x_3, x_4 \mid x_i^{-1} x_k x_i = x_{k+1} \ (k > i, \ k < 4) \rangle$$

is F-reduced. In fact, most of the standard presentations of groups are reduced.

4 Approximating Cayley graphs of finitely presented groups

4.1 Cayley graph approximations and singular subcomplexes

Let

$$G = \langle X; R \rangle \tag{2}$$

be a symmetrized presentation of a group G. Recall that the Cayley graph $\Gamma(G, X)$ of G with respect to a generating set $X^{\pm 1}$ is a directed graph labelled by elements from $X^{\pm 1}$ (shortly X-*digraph*) such that elements of G form the vertex set of $\Gamma(G, X)$ and two vertices u and v are connected by a directed edge (u, v) (from u to v) with label $x \in X^{\pm 1}$ if and only if $v = ux$ in G. The edge (ux, u) is the inverse of (u, ux), it has a label x^{-1}. One can turn $\Gamma(G, X)$ into a 2-dimensional *Cayley* complex $C(X, R)$ by adding a face for every loop in $\Gamma(G, X)$ with a label from $R^{\pm 1}$ (see [23]).

An X-digraph Γ is called an *approximation* of the Cayley graph $\Gamma(G, X)$ of G if it comes equipped with an X-digraph morphism

$$\phi : \Gamma \to \Gamma(G, X).$$

Each approximation (Γ, ϕ) of $\Gamma(G, X)$ gives rise to a 2-dimensional complex C_Γ over $\langle X; R\rangle$ (by adding cells for every closed path in Γ with labels from $R^{\pm 1}$) and a morphism of complexes (that preserves dimension, incidence, and labelling) $\phi^* : C_\Gamma \to C(X, R)$. Such a pair (C_Γ, ϕ^*) is called a *singular subcomplex* of $C(X, R)$ (see [23]) or just an *R-complex*. We will freely switch from approximation graphs to the induced singular subcomplexes and back. Observe, that if Γ is connected then the map ϕ is unique up to the choice of vertices $v \in \Gamma$ and $v' \in \Gamma(G, X)$ such that $\phi(v) = v'$.

In general, there is no any algorithm to check whether a given finite X-digraph Γ is an approximation of $\Gamma(G, X)$ or not (this problem is decidable if and only if the word problem in G is decidable). Below we describe a procedure to generate arbitrary large approximations of $\Gamma(G, X)$ with respect to a given presentation $\langle X; R\rangle$. This construction makes use of the Stallings' *folding algorithm* (see [37]). For an X-digraph K by $S(K)$ we denote a *folded* X-digraph obtained from K by the Stalling's folding procedure. The graph $S(K)$ is uniquely determined by K and there exists a canonical epimorphism $\phi_S : K \to S(K)$ (see [37] and [18]). It is not hard to see that ϕ_S is a functor from the category of X-digraphs into the category of folded X-digraphs. For a graph Γ by $V(\Gamma)$ and $E(\Gamma)$ we denote, correspondingly, the sets of vertices and edges in Γ. The worst-case complexity for computing $S(K)$ is bounded from above by $O(|K| \log(K))$, where $|K| = |V(K)| + |E(K)|$. Actually, in all practical computations the time complexity function is bounded by $O(|K|)$.

Recall, that the *core* of K is a subgraph $Core(K)$ of K formed by all closed

cyclically reduced paths in K. If K has a fixed base point v then the *core* $Core_v(K)$ *of* K *at* v is formed by all closed reduced paths in K at the base point v. By definition K is a *core graph* (*core graph at* v) if $Core(K) = K$ ($Core_v(K) = K$).

Given a finite symmetrized presentation $\langle X; R\rangle$ and an arbitrary X-digraph K as an input, the procedure below outputs an X-digraph $\mathcal{C}(K)$ together with a morphism $\phi_{\mathcal{C}} : K \to \mathcal{C}(K)$. We call $\mathcal{C}(K)$ the *R-extension* of K.

Algorithm 4.1. (**R-extension of K**).

INPUT: A directed X-digraph K.

OUTPUT: A directed X-digraph $\mathcal{C}(K)$ together with a morphism of X-digraphs $\phi_{\mathcal{C}} : K \to \mathcal{C}(K)$.

COMPUTATIONS:

C1) For each vertex $v \in K$ and each $r \in R$ add a cycle labelled by r to v. Denote the resulting graph by $\mathcal{C}_1(K)$ and the canonical embedding by $\phi_{\mathcal{C}_1} : K \to \mathcal{C}_1(K)$.

C2) Apply the Stalling's procedure to fold the graph $\mathcal{C}_1(K)$. Put $\mathcal{C}(K) = S(\mathcal{C}_1(K))$ and $\phi_{\mathcal{C}} = \phi_S \circ \phi_{\mathcal{C}_1}$.

C3) Output $\mathcal{C}(K)$ together with the morphism $\phi_{\mathcal{C}} : K \to \mathcal{C}(K)$.

Remark 4.2. If K has a distinguished based point v then we view $\mathcal{C}(K)$ as a graph with the distinguished based point $\phi_{\mathcal{C}}(v)$.

Lemma 4.3. *Let K be an X-digraph. Then the following holds:*

1) $\mathcal{C}(K)$ and $\mathcal{C}_1(K)$ are well-defined, i.e., they do not depend on a sequence of actual transformations in C1) and C2).

2) If $L(R) > 0$ then $\mathcal{C}_1(K)$ and $\mathcal{C}(K)$ are core graphs.

3) K is an approximation of $\Gamma(G, X)$ if and only if $\mathcal{C}(K)$ is an approximation of $\Gamma(G, X)$.

4) If $L(R) > 0$ then $\phi_{\mathcal{C}}$ is a functor from the category of X-digraphs into the category of folded core X-digraphs.

Proof. 1) A graph $\mathcal{C}_1(K)$ does not depend on the order in which new cells are attached to K. Therefore, $\mathcal{C}_1(K)$ is well-defined. Since $\mathcal{C}(K)$ is obtained from $\mathcal{C}_1(K)$ by Stalling's folding procedure $\mathcal{C}(K)$ well-defined too.

2) Observe that after performing step C1) at every vertex $v \in \mathcal{C}_1(K)$ there is a loop labelled with some $r \in R_{sym}$. Hence $\mathcal{C}_1(K)$ is a core graph. Since $\phi_S : \mathcal{C}_1(K) \to \mathcal{C}(K)$ is an epimorphism the same is true for any vertex of $\mathcal{C}(K)$.

3) First, we show that K is an approximation of $\Gamma(G, X)$ if and only if $\mathcal{C}_1(K)$ is. Since K is a proper subgraph of $\mathcal{C}_1(K)$ the sufficiency is obvious. Assume that K is an approximation of $\Gamma(G, X)$ and $\phi : K \to \Gamma(G, X)$ is an X-digraph morphism. Since $\mathcal{C}_1(K)$ is obtained from K by attaching a number of loops labelled by elements of R_{sym} the morphism ϕ can be extended to $\mathcal{C}_1(K)$.

Finally, since taking the Stalling's folding of a graph is a functor and $\Gamma(G, X)$ is a folded X-digraph it follows that $\mathcal{C}_1(K)$ is an approximation of $\Gamma(G, X)$ if and only if $\mathcal{C}(K)$ is.

4) It follows from the definition of $\mathcal{C}_1$ that any morphism $\phi : K \to L$ can be extended to a morphism $\psi : \mathcal{C}_1(K) \to \mathcal{C}_1(L)$ such that the following diagram commutes.

$$\begin{array}{ccc} K & \hookrightarrow & \mathcal{C}_1(K) \\ \downarrow\phi & & \downarrow\psi \\ L & \hookrightarrow & \mathcal{C}_1(L) \end{array}$$

It is easy to see that $\mathcal{C}_1$ is a functor from the category of X-digraphs into itself. By definition $\phi_{\mathcal{C}} = \phi_S \circ \phi_{\mathcal{C}_1}$. As we have mentioned above ϕ_S is a functor from the category of X-digraphs to the category of folded X-digraphs and by 2) $\mathcal{C}(K)$ is a core graph. Hence the result.

□

Lemma 4.4. *Let $\langle X; R\rangle$ be a symmetric finite presentation and K a finite X-digraph. Then the following inequalities hold for the R-extension $\mathcal{C}(K)$ of K:*
1) $|V(\mathcal{C}(K))| \leq (L(R) - |R| + 1)|V(K)|$,
2) $|E(\mathcal{C}(K))| \leq 2|X|\ |V(\mathcal{C}(K))|$.
Moreover, the time complexity of Algorithm 4.1 is bounded from above by

$$O(L(R)|V(K)|\log(L(R)|V(K)|)).$$

Proof. First, observe that since $\mathcal{C}(K)$ is folded and the degree of each vertex is at most $2|X|$ the second inequality holds. The number of new vertices that are added at each vertex in K is at most $L(R) - |R|$. Hence

$$|V(\mathcal{C}(K))| \leq |V(\mathcal{C}_1(K))| \leq (L(R) - |R| + 1)|V(K)|.$$

The number of new edges that are added at each vertex in K is at most $L(R)$ which gives total of $L(R)|V(K)|$ of new edges in $\mathcal{C}(K)$. Adding vertices and edges into the graph requires time proportional to the number of new vertices and edges and, as we already mentioned, the worst-case complexity of the computation of $S(\Gamma)$ is $O(|\Gamma|\log|\Gamma|)$. Therefore the time complexity of the Algorithm 4.1 is bounded by $O(|K|\log|K|)$, as claimed. □

From now on we assume that every letter from X occurs in R. Starting with an X-digraph K one can iterate the construction above. Put:

$$\mathcal{C}^{(1)}(K) = \mathcal{C}(K), \quad \mathcal{C}^{(m+1)}(K) = \mathcal{C}(\mathcal{C}^{(m)}(K))$$

Similarly, one can define $\mathcal{C}_1^{(m)}(K)$ as the result of m consecutive applications of the

unary operation $\mathcal{C}_1$ starting at K. As a special case define

$$\mathcal{C}^{(0)}(K) = S(K), \quad \mathcal{C}_1^{(0)}(K) = K.$$

Lemma 4.5. *Let K be an X-digraph. Then the following holds for any non-negative integers m, n:*

1) $\mathcal{C}^{(m)}(K) \simeq S(\mathcal{C}_1^{(m)}(K))$;

2) $\mathcal{C}^{m+n}(K) \simeq \mathcal{C}^n(\mathcal{C}^m(K))$;

3) any morphism of X-digraphs $\phi : L \to \mathcal{C}^{(m)}(K)$ gives rise to a morphism $\mathcal{C}^{(n)}(L) \to \mathcal{C}^{(m+n)}(K)$.

4) Let K_0 be a graph consisting of a single vertex (and no edges). Then

$$\Gamma(G, X) \simeq \lim_{m\to\infty} \mathcal{C}^{(m)}(K_0)$$

where $\Gamma(G, X)$ is the Cayley graph of the group $G = \langle X; R\rangle$.

Proof. We prove 1) by induction on m. If $m = 1$ then there is nothing to prove. Suppose then that $\mathcal{C}^{(m-1)}(K) \simeq S(\mathcal{C}_1^{(m-1)}(K))$. Observe that the diagram below commutes for an arbitrary X-digraph Γ.

$$\begin{array}{ccc} \Gamma & \xrightarrow{\phi_{\mathcal{C}_1}} & \mathcal{C}_1(\Gamma) \\ \downarrow{\scriptstyle \phi_S} & & \downarrow{\scriptstyle \phi_S} \\ S(\Gamma) & \xrightarrow{\phi_{\mathcal{C}_1}} \mathcal{C}_1(S(\Gamma)) \xrightarrow{\phi_S} & \mathcal{C}(\Gamma) \end{array}$$

In particular, it commutes for $\Gamma = \mathcal{C}_1^{(m-1)}(K)$, which implies 1).

2) is obvious. 3) follows from 2) and the fact that the map $\phi_{\mathcal{C}}$ is a functor (Lemma 4.3). To see 4) observe that the graphs $\Gamma(G, X)$ and $\lim_{m\to\infty} \mathcal{C}^{(m)}(K_0)$ are both regular folded X-digraphs which both accept (as deterministic automata

with the natural base points) the same language - the normal closure of R in $F(X)$. Hence they are isomorphic as X-digraphs. $\square$

Remark 4.6. The construction above of the Cayley graph $\Gamma(G, X)$ as the direct limit of the graphs $\mathcal{C}^{(m)}(K_0)$ can be viewed as a variation of the coset enumeration procedure as it is described in [23] (chapter III.12).

4.2 van Kampen diagrams

Now we consider a special type of singular subcomplexes of $C(X, R)$, so called *van Kampen diagrams* (or *diagrams*) over $\langle X; R\rangle$.

There are two slightly different types of diagrams: the ones that are not necessary homeomorphic to a Euclidean disc (introduced by Lyndon, see [23]) and the others which are always homeomorphic to a Euclidean disc (here, we refer to the Olshanskii's book [34]). In this paper we focus only on the diagrams of the first type, but a similar technique works for diagrams of the second type.

Let R^2 be the Euclidean plane. For a subset $S \subset R^2$ denote by ∂S the boundary of S, and by $\overline{S}$ the closure of S in R^2. Recall that a *map* $\mathcal{M}$ is a finite disjoint union of *vertices* (points in R^2), edges (bounded subsets of R^2 homeomorphic to the open unit interval), and *faces* or *cells* (bounded sets homeomorphic to the open unit disc) which satisfies the following conditions:

1) if e is an edge in $\mathcal{M}$ then there are two vertices $a, b \in \mathcal{M}$ (not necessary distinct) such that $\overline{e} = e \cup \{a\} \cup \{b\}$;

2) for each face $\Pi \in \mathcal{M}$ the boundary $\partial\Pi$ is connected and $\partial\Pi = \overline{e}_1 \cup \ldots \cup \overline{e}_k$ for some edges $e_1, \ldots, e_k \in \mathcal{M}$.

An edge of a map $\mathcal{M}$ is called a *free edge* if it does not belong to the boundary of any cell in $\mathcal{M}$. By $V(\mathcal{M})$, $E(\mathcal{M})$, $FE(\mathcal{M})$, and $C(\mathcal{M})$ we denote the sets of vertices, edges, free edges, and cells in $\mathcal{M}$.

Now a *diagram*, or a *disc diagram* over a symmetrized presentation $\langle X; R\rangle$ is a connected and simply connected map $\mathcal{M}$ such that;

1) every edge is considered as a pair of oppositely oriented edges e and e^{-1};

2) every oriented edge e is assigned a letter $y \in X^{\pm 1}$, which is called the *label* $\phi(e)$ of e, and such that $\phi(e^{-1}) = \phi(e)^{-1}$. The function ϕ is called a *labelling* function;

3) if $p = e_1 \dots e_k$ is a *boundary cycle* or *contour* of a face Π (i.e., a cycle of minimal length containing all edges of $\partial\Pi$) then $\phi(p) = \phi(e_1) \dots \phi(e_k) \in R$. In this case Π is called an R-face.

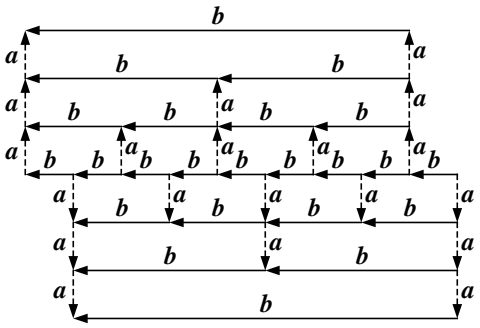

Figure 1: A diagram over a group $G = \langle a, b \ ; \ aba^{-1}b^{-2}\rangle$.

Let v be a vertex of a map $\mathcal{M}$. The *neighborhood* $N_{\mathcal{M}}(v)$ of v in $\mathcal{M}$ is defined as the submap generated by all edges and faces in $\mathcal{M}$ which are incident to v.

Let $\mathcal{M}$ and $\mathcal{N}$ be diagrams over $\langle X; R\rangle$. We say that $\mathcal{M}$ and $\mathcal{N}$ are *isomorphic* if there exists a homeomorphism of the Euclidean plane which induces an isomorphism of corresponding 2-complexes. By $Star_{\mathcal{M}}(v)$ we denote the subgraph generated by all edges incident to v (including their endpoints). If presentation $\langle X; R\rangle$ is reduced and an orientation of the plane is fixed (clockwise or counterclockwise) then for any two edges $e_1, e_2 \in Star_{\mathcal{M}}(v)$ one can unambiguously define the set of all cells in $N_{\mathcal{M}}(v)$ and edges in $Star_{\mathcal{M}}(v)$ between e_1 and e_2.

Diagrams over $\langle X; R\rangle$ satisfy the following important property.

Lemma 4.7. *(van Kampen Lemma, [23]) Let $\langle X; R\rangle$ be a symmetrized presentation and w a word in the alphabet $X^{\pm 1}$. Then $w = 1$ in $G = \langle X; R\rangle$ if and only if there exists a diagram $\mathcal{M}$ over $\langle X; R\rangle$ with a boundary label w.*

4.3 Depth of diagrams and the canonical embeddings

Definition 4.8. Let L be an R-complex. A sequence of vertices $v_1, \dots, v_q$ in L is called a *vertex chain* if for any $i = 1, \dots, q-1$ there is a cell or a free edge c such that $v_i, v_{i+1} \in \partial c$.

Also we will use the following version of chains.

Definition 4.9. Let L be an R-complex. A sequence $c_1, \dots, c_q$ in L, where c_j $(j = 1, \dots, q)$ is a cell or a free edge, is called an *edge-cell chain* if for any $i = 1, \dots, q-1$ $\partial c_i \cap \partial c_{i+1} \neq \emptyset$.

Clearly a vertex chain $v_1, \dots, v_q \in L$ defines at least one chain of cells and free edges $c_1, \dots, c_{q-1} \in L$ such that $v_i, v_{i+1} \in \partial c_i$ for $i = 1, \dots, q-1$.

Let K_1 and K_2 be two subcomplexes of L. We say that K_1 and K_2 are connected by a chain in L if there exists a vertex chain $v_1, \dots, v_q \in L$ such that $v_1 \in K_1$ and $v_q \in K_2$. The length of the shortest vertex chain connecting K_1 and K_2 is called the *chain distance* $d(K_1, K_2)$ between K_1 and K_2.

Definition 4.10. Let K be a subcomplex of an R-complex L. The number $\delta_K(L) = \max\{d(K, \overline{c}) \mid c \in (C(L) \setminus C(K)) \cup (FE(L) \setminus FE(K))\}$ is called the *depth* of L with respect to K.

Definition 4.11. *(Depth of a disc diagram.)* Let M be a map. The depth $\delta(M) = \delta_{\partial M}(M)$ of M with respect to ∂M is called the depth of M.

Let $w = y_1 y_2 \dots y_k$ ($y_i \in X^{\pm 1}$) be a reduced word from $F(X)$. Define an X-digraph $\Gamma(w)$ with the vertex set $V = \{y_1 \dots y_i \mid i = 0, \dots, k\}$ and such that a vertex $y_1 \dots y_i$ is connected to the vertex $y_1 \dots y_i y_{i+1}$ by a directed edge with label y_{i+1} for each $i = 0, \dots, k-1$. So $\Gamma(w)$ is a straight segment with label w. Clearly, there is a graph morphism $\Gamma(w) \to \Gamma(G, X)$.

Proposition 4.12. Let D be a diagram with a boundary label w, $m = \delta(D)$, and $\phi : \Gamma(w) \to \partial D$ be a morphism. Then there exists a morphism of 2-complexes $\psi : D \to \mathcal{C}^{(m)}(\Gamma(w))$ such that the following diagram commutes.

$$\begin{array}{ccc} \Gamma(w) & \xrightarrow{\phi} & D \\ & \overset{\phi_{\mathcal{C}}}{\searrow} & \downarrow \psi \\ & & \mathcal{C}^{(m)}(\Gamma(w)) \end{array}$$

Proof. To prove the assertion of the proposition we first cut a diagram D into a diagram T of a certain type. The diagram T is a forest of cells attached at a line segment graph labelled with w (see Figure 2). The height of the forest (distance from the line segment to cells) is at most m. We will denote the corresponding sewing morphism by $\theta : T \to D$ (read more about cuts and sewing morphisms in Section 7.2).

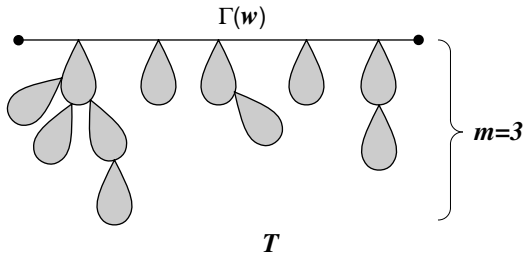

Figure 2: A "forest attached to a line segment" diagram.

We will construct the loop along which we cut D in a sequence of steps. Denote by π_0 the boundary loop ∂D starting at the initial vertex of $\phi(\Gamma(w))$ (from which

w is read). The loop π_0 cuts off a line segment labelled with w (see Figure 3.b).

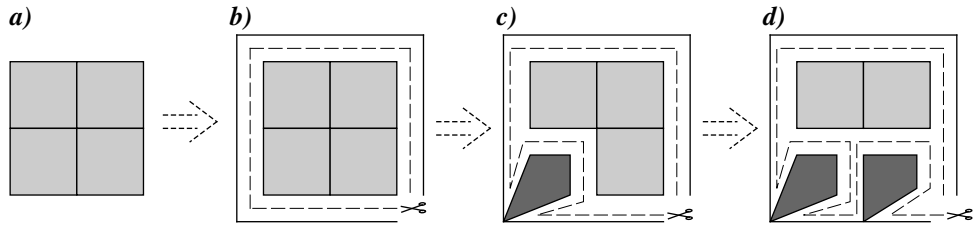

Figure 3: First steps of constructing T.

Assume that π_i is the last constructed loop and T_i is a diagram of a specified type cut off D by π_i. If T_i includes all cells of D then T_i is a required diagram T. Otherwise choose a cell c which does not belong to T_i with the smallest value $d = d(\partial D, c)$. If $d = 1$ then c touches the boundary ∂D at some vertex v in D. In this case pull π_i over c as shown in Figure 3. If $d > 1$ then c touches at some vertex v some cell c' such that $d' = d(\partial D, c') = d - 1$. The cell c' already belongs to T_i. Pull π_i over c at v. Clearly the obtained loop π_{i+1} cuts off a diagram T_{i+1} which includes one additional cell. We continue this process until we have no cells to add to T_i.

Since the result of Stalling's procedure does not depend on the sequence of folds it follows that the following diagram commutes

$$\begin{array}{ccc} T & \xrightarrow{\theta} & D \\ & \overset{\phi_S}{\searrow} & \downarrow \phi_S \\ & & S(T) \end{array} \tag{3}$$

Now it follows from the definition of $\mathcal{C}_1^{(m)}$ and T that there exists a morphism

$\theta' : T \to \mathcal{C}_1^{(m)}$ such that the following diagram commutes

$$\begin{array}{ccc} \Gamma(w) & \hookrightarrow & T \\ & \overset{\phi_{\mathcal{C}_1}}{\searrow} & \downarrow^{\theta'} \\ & & \mathcal{C}_1^{(m)}(\Gamma(m)) \end{array} \tag{4}$$

Using the diagrams (3) and (4) and the fact that operator S is a functor there exists a morphism $\tau : S(T) \to S(\mathcal{C}_1^{(m)}(\Gamma(w)))$ such that the following diagram commutes.

$$\begin{array}{ccccc} \Gamma(w) & \hookrightarrow & T & \overset{\theta}{\to} & D \\ & \overset{\phi_{\mathcal{C}_1}}{\searrow} & \downarrow^{\theta'} & \overset{\phi_S}{\searrow} & \downarrow^{\phi_S} \\ & & \mathcal{C}_1^{(m)}(\Gamma(m)) & & S(T) \\ & & & \overset{\phi_S}{\searrow} & \downarrow^{\tau} \\ & & & & S(\mathcal{C}_1^{(m)}(\Gamma(w))) \end{array}$$

By Lemma 4.5 $S(\mathcal{C}_1^{(m)}(\Gamma(w))) = \mathcal{C}^{(m)}(\Gamma(w))$ which finishes the proof.

□

5 New algorithms for the word search problem in groups

5.1 Search problems in groups

The Word Problem, the Conjugacy Problem, and the Membership Problem are classical algorithmic problems in groups. We refer to surveys [3], [28], and [29] on algorithmic problems in groups.

Let G be a fixed group given by a symmetrized finite presentation $G = \langle X; R \rangle$, and $M(X) = (X^{\pm 1})^*$ a free monoid over the alphabet $X^{\pm 1}$. Sometimes, slightly

abusing notations, we identify words in $M(X)$ with their canonical images in the free group $F(X)$.

An algorithmic problem P over G can be described as a subset $D = D_P$ of a Cartesian power $M(X)^k$ of $M(X)$. The problem is *decidable* if there exists a *decision algorithm* $A = A_P$ which on a given input $w \in M(X)^k$ halts and outputs "Yes" if $w \in D_P$, otherwise it outputs "No". It is convenient to view P as consisting of two parts: the "Yes" (or *positive*) part requires a partial algorithm A_{Yes} which on an input $w \in D$ halts and outputs "Yes", and works forever on inputs from $M(X)^k - D$; the "No" (*negative*) part asks for a partial algorithm for the set $M(X)^k - D$. Recently, it has been shown that for a wide variety of finitely presented groups the "No" part is very easy on *average*, as well as *generically* (see [19], [20]). On the other hand, in many applications it is required to find a decision algorithms A_{Yes} for the "Yes" part of P. Furthermore, very often one has to find a decision algorithm A_{Yes} which on an input $w \in D$ provides a "reasonable proof" that w is, indeed, in D. This leads to the so-called *search* (or *witness*) variations of the algorithmic problems (see [19], [20], and [7]) for a more detailed discussion of the search problems in groups):

Word search problem (WSP) for $G = \langle X; R\rangle$: *For a given $w \in M(X)$ verify if $w = 1$ in G and in this event find a presentation of w as a product of conjugates of relators from R.*

Conjugacy search problem (CSP) for G: *For a given pair $(u, v) \in M(X) \times M(X)$ verify if u and v are conjugate in G, and in this event find a conjugator.*

Membership search problem (MSP) for G: *For a given word $w \in M(X)$ and a finitely generated subgroup H of G (given by a finite set of generators) verify if $w \in H$, and in this event find a presentation of w as a product of the generators of H.*

This new aspect of the search decision problems which requires to provide a "proof", or a "witness", of the correct decision, needs a more detailed explanation.

Let $D \subseteq M(X)^k$ be a search decision problem, $\mathcal{A}$ a decision algorithm for D, $w \in D$ a particular instance of the "Yes" part of the problem, and p_w a "proof" provided by $\mathcal{A}$ that w, indeed, belongs to D. The time complexity function $T_{\mathcal{A}}(x)$ of $\mathcal{A}$ typically takes into account the time required for $\mathcal{A}$ to check whether or not $w \in D$, as well as the time needed for $\mathcal{A}$ to produce p_w on the input w. Hence the time complexity of $\mathcal{A}$ depends on the complexity of the routine to produce p_w, in particular, on the way one represents these p_w as objects (words, graphs, sequence of formal derivations, programs, etc.). It is not clear what kind of representations are the most convenient in computations, this, perhaps, depends on a particular problem and the decision algorithm. But there is another important problem here. Namely, when given a proof p_w it might take a considerable amount of time to confirm, using p_w, that w belongs to D, so obtaining a proof and verification of the decision based on this proof are different processes. Should one add this verification time to the time complexity of the algorithm $\mathcal{A}$ or treat it as a separate issue - is not altogether clear. It is surprising how little was done on this topic in computational algebra. It may happen (see the Membership search problem for free groups below) that the time function $T_V(w, p_w)$ for verification process on the inputs w, p_w is exponentially greater then the time function $T_{\mathcal{A}}(w)$ of the process of constructing the proof p_w. In what follows we treat the time complexities of the decision algorithm $\mathcal{A}$ and that of the verification process as different issues.

5.2 Word search problem in groups. Algorithm $\mathcal{A}$.

In this section we introduce a new algorithm for the Word search problem (**WSP**) in groups and study its worst-case time complexity. Given a finite symmetrized presentation $G = \langle X; R\rangle$ and a word $w \in gp_F(R)$ the algorithm $\mathcal{A}$ produces a proof p_w which is a finite folded X-digraph Γ such that Γ approximates the Cayley graph $\Gamma(G, X)$ and which accepts w (there is a loop with label w at the base point in Γ).

In the worst-case scenario the size of the graph $p_w = \Gamma$ is exponential in the length of w, but given Γ and w the verification procedure is linear in the length of w (one needs only to read w in Γ viewed as a deterministic finite automaton). In this case, the verification time function $T_V(w, p_w)$ is negligible compare to the time function $T_{\mathcal{A}}$.

We would like to emphasize that Algorithm $\mathcal{A}$ is the most efficient general technique for WSP so far. In fact, there are just a few techniques that work for any finite presentation, e.g. Todd-Coxeter algorithm, total enumeration of $gp_F(R)$, Knuth-Bendix procedure, and their numerous modifications. Algorithm $\mathcal{A}$ is itself a modification of a standard Todd-Coxeter procedure. At the end of the paper (in Section 10) we make short comparison of $\mathcal{A}$ with Todd-Coxeter and enumeration of $gp_F(R)$. The good comparison deserves another paper.

We start with a brief description of the algorithm $\mathcal{A}$. Suppose we are given a word $w \in gp_F(R)$. To provide a proof that w belongs to $gp_F(R)$ it suffices to find an approximation Γ of $\Gamma(G, X)$ in which there is a closed path with the label w. Indeed, in this event there exists a closed path with the label w in $\Gamma(G, X)$ so $w \in gp_F(R)$. Now, given a word $w \in F(X)$ the algorithm $\mathcal{A}$ begins to construct some particular approximations Γ of $\Gamma(G, X)$; it stops in finitely many steps if $w \in gp_F(R)$ and works forever otherwise. If $\mathcal{A}$ stops on an input w then the output of $\mathcal{A}$ is an approximation Γ of $\Gamma(G, X)$ in which there exists a loop with label w at the base-point of Γ. The principle idea behind this algorithm is that we do not enumerate all possible approximations Γ of $\Gamma(G, X)$ (as happens in the Todd-Coxeter algorithms), but rather we construct only those approximations which contain a path at the based-point (perhaps, not closed) with the label w.

Recall that $\Gamma(w)$ is an X-digraph which is a line segment labelled with w (see Section 4.3). The starting vertex 1 of the segment is called the *base-point* of the graph $\Gamma(w)$. The canonical image of 1 in $\mathcal{C}^{(m)}(\Gamma(w))$ is the base-point of $\mathcal{C}^{(m)}(\Gamma(w))$,

which we denote again by 1.

We start with the following algorithm.

Algorithm 5.1. *(Decision Algorithm $\mathcal{A}$ for* **WSP** *in groups.)*

INPUT: A finite symmetrized presentation $\langle X; R\rangle$, a word $w \in F(X)$.

OUTPUT: YES if $w \in gp_F(R)$ and a finite approximation Γ of $\Gamma(G, X)$ which accepts w;

COMPUTATIONS:

- Consequently compute $\mathcal{C}^{(i)}(\Gamma(w))$ until the endpoints of the image of $\Gamma(w)$ become equal in $\mathcal{C}^{(i)}(\Gamma(w))$.
- Return YES and $\mathcal{C}^{(i)}(\Gamma(w))$.

Definition 5.2. For a word $w \in gp_F(R)$ define a number

$$\delta(w) = \min\{\delta(D) \mid D \text{ is a diagram over } \langle X; R\rangle \text{ with boundary label } w\}.$$

The number $\delta(w)$ is called the depth of the word w in G.

Observe that by Lemma 4.7 $\delta(w)$ is defined for any $w \in gp_F(R)$.

Theorem 5.3. *The Decision Algorithm $\mathcal{A}$ needs at most $m = \delta(w)$ iterations to stop on an input $w \in gp_F(R)$. The total number of steps required by the algorithm to stop on an input $w \in gp_F(R)$ is bounded from above by $O(m|w|\cdot L(R)^m \log(|w|L(R))$.*

Proof. Let $D(w)$ be a van Kampen diagram such that the label of the boundary ∂D (at some vertex v on ∂D) is w and $\delta(w) = \delta(D(w))$. By Lemma 4.12 there exists an embedding of $D(w)$ into $\Gamma = \mathcal{C}^{(m)}(\Gamma(w))$, where $m = \delta(D(w))$, such that the image of the vertex v is the based-point of Γ. This proves the first part of the theorem. The second part follows from Lemma 4.4. This completes the proof. □

Notice, that it is not easy to extract $D(w)$ from $\mathcal{C}^{(m)}(\Gamma(w))$ even when a morphism $D(w) \to \mathcal{C}^{(m)}(\Gamma(w))$ does exist. In the next section we describe an algorithm to do just that.

5.3 Word search problem in groups. Algorithm $\mathcal{B}$.

In this section we describe a new search decision algorithm $\mathcal{B}$ for **WSP** in groups and study its worst-case time complexity. Given a finite symmetrized presentation $G = \langle X; R\rangle$ and a word $w \in gp_F(R)$ the algorithm $\mathcal{B}$ produces a proof $p_{\mathcal{B}}(w)$ which is a finite sequence of derivations of a certain type. The sequence $p_{\mathcal{B}}(w)$ allows one to rewrite w as a product of conjugates of relators from R - this is the verification process for $\mathcal{B}$ on the inputs $w, p_{\mathcal{B}}(w)$. Thus, the algorithm $\mathcal{B}$ together with the verification procedure for a given $w \in gp_F(R)$ output a decomposition of w as a product of conjugates of relators from R. This is a much more stronger result than the one provided by the algorithm $\mathcal{A}$. Notice that, the size of the proof $p_{\mathcal{B}}(w)$ is comparable to the size of $p_{\mathcal{A}}(w)$, but the verification process is much more time consuming than in $\mathcal{A}$. The worst-case time complexity of $\mathcal{B}$ is still exponential in the length of w. To the best of our knowledge $\mathcal{B}$ is the first general algorithm for **WSP** in groups with a single exponential upper bound on the worst-case complexity.

A brief description of the algorithm $\mathcal{B}$ is the following. Given $\langle X; R\rangle$ and $w \in gp_F(R)$ one starts the algorithm $\mathcal{A}$ on the input w. The algorithm $\mathcal{A}$ returns a X-digraph Γ which accepts w. The graph Γ gives the Stalling's folding (with respect to X) of some finitely generated subgroup H of $gp_F(R)$ which contains w. Afterward, one uses the standard algorithm for Membership search problem for finitely generated subgroups of free groups to find a presentation of w as a product of conjugates of relators from R. This solves **WSP** in G for w in the classical formulation.

Now we give a formal description of the algorithm. For an X-digraph Γ with the

base point 1 define the radius $r(\Gamma)$ of Γ to be the maximum of the distances $d(1, u)$, $u \in \Gamma$, where d is the standard graph metric on Γ.

Lemma 5.4. *Let $\langle X; R\rangle$ be a finite symmetrized presentation, Γ a finite X-digraph with a base point 1, H the subgroup in $F(X)$ accepted by $Core(\Gamma)$. Then the X-digraph $\mathcal{C}(\Gamma)$ (with the base-point induced from Γ) accepts a subgroup of $F(X)$ generated by $H \cup A$, where A is a finite set of conjugates of elements from R satisfying the following conditions:*

1) $|A| \leq |V(\Gamma)| \cdot |R|$.

2) For any $a \in A$ $|a| \leq 2r(\Gamma) + M(R)$.

3) One can find such a generating set A effectively in time

$$O(|V(\Gamma)| \cdot |R| \cdot (2r(\Gamma) + M(R))).$$

Proof. The graph $\mathcal{C}(\Gamma)$ is obtained from Γ by adding to each vertex $v \in \Gamma$ a loop with the label r for each $r \in R$ (since R is symmetrized), which follow by several consecutive foldings. Let c be a loop with the label $r \in R$ added to Γ at a vertex $v \in \Gamma$. Let p_v be the label of a shortest path from the base point 1 to v in Γ. Adding c to Γ results in the same graph as if adding a loop labelled by $p_v r p_v^{-1}$ to the base point of Γ and folding the path with the label p_v into Γ. Since the resulting graph does not depend on a particular sequence of foldings (because $\mathcal{C}_1(\Gamma)$ is a core graph) one can readily see that $\mathcal{C}(\Gamma)$ accepts a subgroup of $F(X)$ generated by H together with a finite set $A = \{p_v r p_v^{-1} \mid v \in V(\Gamma), r \in R\}$. Obviously, $|A| \leq |V(\Gamma)| \cdot |R|$ which proves 1).

Since $|p_v| \leq r(\Gamma)$ and $|r| \leq M(R)$ then for $a = p_v r p_v^{-1}$ we have $|a| \leq |p_v| + |r| + |p_v^{-1}| \leq 2r(\Gamma) + M(R)$. Hence 2) and 3) follow.

□

Proposition 5.5. Let $w \in F(X)$. Then the graph $\mathcal{C}^{(m)}(\Gamma(w))$ is the Stalling's folding of a subgroup of $F(X)$ generated by a finite subset A of elements from R and their conjugates. Moreover,

1) $|A| \leq (|w|+1)|R|^m$.

2) If $a \in A$ then $|a| \leq 2|w| + mM(R)$.

3) One can find such a generating set A effectively in time

$$O(|w| \cdot |R|^m \cdot (2|w| + mM(R))).$$

Proof. 1) and 2) clearly follow from Lemma 5.4 and observation that $|V(\Gamma(w))| = |w|+1 = O(|w|)$. To show 3) notice that adding a loop of length l to an X-digraph increases the radius of the graph at most by $\lfloor M(R)/2 \rfloor$. Now the result follows from this observation and the fact that the radius of the initial graph $\Gamma(w)$ is $|w|$.

□

Let for some natural m the graph $\Gamma' = \mathcal{C}^{(m)}(\Gamma(w))$ accepts w. Let H be the subgroup in $F(X)$ accepted by Γ' and A a set of conjugates of elements from R from Proposition 5.5 that generates the subgroup H. Clearly, $w \in H$ and to present w as a product of conjugates of relators from R it suffices to solve the Membership search problem (**MSP**) for the subgroup $H = \langle A \rangle$ on the given input w. The standard way of solving **MSP** in free groups involves Nielsen minimization method, it gives exponential time estimates on the worst-case complexity. Let's have a look where the exponential time estimates come from in the Nielsen argument. It takes quadratic time for a given tuple of generators $h = (h_1, \ldots, h_k)$ of a subgroup H to find a sequence η of Nielsen moves $\eta_1, \ldots, \eta_s$ which reduces the set h to a Nielsen basis $f = (f_1, \ldots, f_t)$ of H. It takes also at most quadratic time to express w as a word in new generators f. Now, to express w in the old generators h's one needs

to rewrite the new generators f_i's as words in the old generators h, but the length of the resulting words can grow exponentially in terms of $|h|$. Notice, however, that the sequence of Nielsen moves η completely describes the formal expressions of f_i's in terms of h, and the length of η is linear in $|h|$. This leads to the idea to use the sequence η in producing the proof $p_{\mathcal{B}}(w)$ rather then the whole expression of w as a word in h.

To describe this alternative way of producing $p_{\mathcal{B}}(w)$ we need to introduce systems of *derivation rules*. Let H be a subgroup of $F(X)$ generated by a finite set $A = \{a_1(X), \ldots, a_n(X)\} \subset F(X)$, $\widetilde{A} = \{\alpha_1, \ldots, \alpha_n\}$ be a set of formal names for words from A together with a homomorphism $\varphi_A : F(\widetilde{A}) \to \langle A \rangle$ defined by $\varphi_A(\alpha_i) = a_i$, $\Gamma(A)$ be an X-digraph which is the wedge of n loops labelled with words $a_i(X)$, and $S(\Gamma(A))$ be the Stalling's folding of $\Gamma(A)$. Let $Q_0 = \{q_1, \ldots, q_s\}$ and $Q = Q_0 \cup \widetilde{A} \cup E(S(\Gamma(A)))$. A *derivation rule* is a pair $(\alpha, \beta) \in Q \times Q^*$ of one of the following types:

1) (e, q_i), where $e \in E(S(\Gamma(A)))$ and $q_i \in Q_0$;

2) $(q_i, q_j q_k)$, where $q_i, q_j, q_k \in Q_0$ and $i > \max\{j, k\}$;

3) (q_i, α), where $q_i \in Q_0$ and $\alpha \in \widetilde{A}$.

A *derivation system* W is a set of rules satisfying the following properties:

4) for each edge $e \in E(S(\Gamma(A)))$ there exists one rule with the left side e;

5) if $q_i \in Q_0$ is involved in the right side of some rule in W then there exists one rule with the left side q_i.

As usual a derivation is a sequence of applications of the derivation rules to a word from Q^*. Clearly any derivation sequence terminates on any word u from Q^*. The resulting word u^* does not depend on the derivation process. Given a derivation

system W one can define a map α on the set of edges from $S(\Gamma)$ by $e \to e^*$. The map α naturally extends to the set of all paths in $S(\Gamma)$

$$e_1 \dots e_k \overset{\alpha}{\mapsto} e_1^* \dots e_k^*.$$

Now if $a \in \langle A \rangle$ then there exists a unique path p_a in $S(\Gamma)$ with the label a starting at the base point 1 in $S(\Gamma)$. Define $\alpha : A \to F(\widetilde{A})$ by $a \overset{\alpha}{\mapsto} p_a^*$.

A derivation system W is said to be *compatible* with $\langle A \rangle$ if for every $w \in \langle A \rangle$ $\alpha(w) \in F(\widetilde{A})$ correctly represents w in $F(X)$, i.e., $\phi_A(\alpha(w)) = w$. Clearly a folded graph $S(A)$ and a derivation system W compatible with $\langle A \rangle$ give a straightforward solution to **MSP** for $\langle A \rangle$.

Proposition 5.6. ([31]) Let H be a subgroup of $F(X)$ generated by a finite set $A = \{a_1(X), ..., a_n(X)\} \subset F(X)$. Then one can effectively find a finite derivation system compatible with H in at most quadratic time $O(L(A)^2)$.

Corollary 5.5 and Proposition 5.6 give the following result.

Proposition 5.7. Let $G = \langle X; R \rangle$, $w \in F(X)$, and $\mathcal{C}^{(m)}(\Gamma(w))$ a finite approximation of $\Gamma(G, X)$ which accepts w. Then one can effectively find a set of free generators A for $\mathcal{C}^{(m)}(\Gamma(w))$ with a derivation system compatible with $\langle A \rangle$ in at most $O(|w|^2|R|^{2m}(2|w| + mM(R))^2)$ steps.

Proof. Take a set A of generators as in proof of Lemma 5.4. Computation of such a set takes at most $O(M(R)(|w| + 1)|R|^m)$ steps. Clearly $L(A) \leq |A| \max_{a \in A}\{|a|\}$ and hence, using estimates in Lemma 5.5, we get $L(A) \leq (|w| + 1)|R|^m(2|w| + mM)$. By Lemma 5.6 the complexity of computing a derivation system for A is $O(|w|^2|R|^{2m}(2|w| + mM(R))^2)$.

□

Algorithm 5.8. (*Decision Algorithm $\mathcal{B}$ for* **WSP** *in groups.*)

INPUT. A finite symmetrized presentation $\langle X; R\rangle$ and a word $w \in gp_F(R)$.

OUTPUT. A finite approximation Γ of $\Gamma(G, X)$ which accepts w, the set A of free generators of the subgroup H and a derivation system W compatible with A (as described in Proposition 5.5 .

COMPUTATIONS.

1) Compute the approximation $\Gamma = \mathcal{C}^{(m)}(\Gamma(w))$ which accepts w using the algorithm $\mathcal{A}$.

2) Compute a free set of generators A of the subgroup H accepted by Γ as described in Proposition 5.5.

3) Compute the system of derivations W compatible with A as in 5.6.

Combining Theorem 5.3 and Proposition 5.7 we obtain the following result.

Theorem 5.9. *Given a finite symmetrized presentation $\langle X; R\rangle$ and an element $w \in gp_F(R)$ the algorithm $\mathcal{B}$ outputs a finite set A of conjugates of elements from R, the Stollings' folding of the subgroup generated by A in $F(X)$ which accepts w, and a finite derivation system W compatible with A. The worst-case complexity of this algorithm is bounded from above by*

$$O(|w|^2|R|^{2\delta(w)}(2|w| + \delta(w)M(R))^2).$$

6 Random van Kampen diagrams

In this section we describe a class of stochastic procedures, so called *iterative random generators* which generate random van Kampen diagrams over a given finite presentation $\langle X; R\rangle$. Roughly speaking, a random generator RG starts with a given diagram D_0 and then randomly extends it according to some basic pattern (*basic*

random extension). Usually a given random generator depends on a set of distributions that allows one to obtain random diagrams with various properties. One can view such iterative random generators as random walks on *transition* graphs. This allows one to introduce a measure on the set of the corresponding trajectories and then induce this measure on the diagrams produced by the generators.

6.1 Basic random extensions and simple random walks

In this section we define random walks on diagrams and probability spaces on sequences of diagrams. Later it will be used to define asymptotic density on diagrams.

Let $\mathcal{K} = \{D_i \mid i \in \mathbb{N}\}$ be a countable (enumerable) collection of diagrams. In this paper we assume that diagrams from $\mathcal{K}$ are van Kampen diagrams over some fixed presentation $\langle X; R\rangle$ equipped, perhaps, with some extra predicates. Denote by $B : \mathcal{K} \to \mathcal{K}$ a stochastic map that with probability $p_{i,j}$ maps D_i into D_j. Sometimes we write $B(D_i) = D_j$ if $p_{i,j} > 0$. The map B can be viewed as a random walk on $\mathcal{K}$ defined by the infinite stochastic matrix $(p_{i,j})$. We say that B is a *basic extension* if for every diagrams D_i, D_j such that $B(D_i) = D_j$ there exists a diagram morphism $D_i \to D_j$. Given a basic extension B we define the *transition graph* $T_B = (V, E)$ of B which is a directed weighted graph defined as follows:

1) $V = \mathcal{K}$;

2) $E = \{(D_i, D_j) \mid p_{ij} > 0\}$;

3) each edge $e = (D_i, D_j) \in E$ has an associated number $p(e) = p_{ij}$.

For $D \in \mathcal{K}$ we denote by $\Phi = \Phi_B(D)$ the set of all diagrams C in $\mathcal{K}$ such that there exists a path in T_B from D to C. A basic extension B is called $\mathcal{K}$-*complete* if there exists $D \in \mathcal{K}$ such that $\Phi_B(D) = \mathcal{K}$. More generally, if $\varphi : \mathcal{K} \to \mathcal{L}$ is a mapping from $\mathcal{K}$ onto a collection of diagrams $\mathcal{L}$ then we say that B is $\mathcal{L}$-*complete relative to* φ if $\varphi(\Phi) = \mathcal{L}$.

Recall that the neighborhood $N_{\mathcal{M}}(v)$ of a vertex v in a diagram $\mathcal{M}$ is defined as the submap generated by all edges and faces in $\mathcal{M}$ which are incident to v. Let $D \in \mathcal{K}$ and v be a vertex in D. We say that B is *locally stable* at the vertex v if the neighborhood of v eventually stabilizes, i.e., for any infinite path

$$D = C_1 \to C_2 \to \dots$$

in the graph T_B there exists $j_0 \in \mathbb{N}$ such that $N_{C_j}(v) = N_{C_{j_0}}(v)$ for every $j \geq j_0$. A random generator B is called *locally stable* if it is stable at every vertex v of every diagram $D \in \mathcal{K}$.

Given a basic extension B and a diagram $D_0 \in \mathcal{K}$ define a new transition graph (which depends on B and D_0) $\mathcal{T} = (V(\mathcal{T}), E(\mathcal{T}))$, where

$$V(\mathcal{T}) = \{p \mid p \text{ is a finite path in } T_B \text{ starting at } D_0\},$$

and

$$E(\mathcal{T}) = \{(\theta, \theta e) \mid \theta, \theta e \in V(\mathcal{T}), e \in E(T_B)\}.$$

Clearly, $\mathcal{T}$ is a tree. We will refer to $\mathcal{T}$ as the *transition tree* of B (with the empty path ε in the root). For each edge $d = (\theta, \theta e) \in E(\mathcal{T})$ we assign probability $p'(d) = p(e)$.

By $\mathcal{W} = \mathcal{W}_{\mathcal{T}}$ we denote a random walk on the tree $\mathcal{T}$ defined by the transition probabilities p' (we assume here that $\mathcal{W}$ starts with probability 1 at the root ε). As usual one can view the random walk $\mathcal{W}$ as a sequence of random variables Z_n, $n \in \mathbb{N}$, on a suitable probability space $(\Lambda, \mathcal{F}, P)$. To explain this we need a few definitions. An infinite path λ in the directed graph $\mathcal{T}$ which starts at the root ε is called a *trajectory*. For a trajectory λ by λ_i we denote the vertex on λ at distance i from the root ε (the i-th component of λ). Now Λ is the set of all trajectories in $\mathcal{T}$

and $Z_n : \Lambda \to V(\mathcal{T})$ is a random variable such that for $\lambda \in \Lambda$ one has $Z_i(\lambda) = \lambda_i$. A *cone* of $\theta \in V(\mathcal{T})$ is the set of all trajectories passing through θ:

$$Cone(\theta) = \{\lambda \in \Lambda \mid \lambda \text{ is passing through } \theta\}.$$

The σ-algebra $\mathcal{F}$ is generated by all cones $Cone(\theta)$, where $\theta \in V(\mathcal{T})$. For each $\theta = e_1 \dots e_k \in V(\mathcal{T})$ the real number $P(Cone(\theta))$ is defined as the probability to hit the vertex $\theta \in \mathcal{T}$ by the random walk W, i.e.,

$$P(Cone(\theta)) = \prod_{i=1}^{k} p(e_i).$$

By the Kolmogorov's extension theorem the function P extends onto the σ-algebra $\mathcal{F}$ in such a way that $(\Lambda, \mathcal{F}, P)$ is a probability space, so P is a probability measure on Λ.

6.2 Probability and asymptotic measure on diagrams

In this section we define discrete probability measures and asymptotic densities on the sets $V_{\mathcal{T}}$, $\mathcal{K}$, and $\mathcal{L}$ for a given map $\varphi : \mathcal{K} \to \mathcal{L}$.

6.2.1 Probability on $V(\mathcal{T})$

Let (Λ, P) be the probability space defined in the previous section and $Q : \Lambda_{\mathcal{T}} \to \mathbb{N}$ a random variable on Λ. We view the function Q as a *termination condition* for the random walk $\mathcal{W}$ which shows where the walk stops going along a path λ. Define a function $T_Q : \Lambda \to V(\mathcal{T})$ by

$$T_Q(\lambda) = \lambda_{Q(\lambda)}$$

for $\lambda \in \Lambda$.

Lemma 6.1. *For any $\lambda \in \Lambda$ the set $T_Q^{-1}(\lambda_{Q(\overline{\lambda})})$ is measurable in (Λ, P).*

Proof. Follows from the equality

$$T_Q^{-1}(\lambda_{Q(\overline{\lambda})}) = Q^{-1}(Q(\overline{\lambda})) \cap Cone(\lambda_{Q(\overline{\lambda})})$$

and the assumption that Q is a random variable.

□

Denote by V_Q the set of all stop-vertices of $\mathcal{W}$ in $\mathcal{T}$ relative to the termination condition Q, so

$$V_Q = T_Q(\Lambda) \subset V(\mathcal{T}),$$

and define a function $P_Q : V_Q \to \mathbb{R}$ by

$$P_Q(\theta) = P(T_Q^{-1}(\theta))$$

for $\theta \in V_Q$.

Proposition 6.2. The function P_Q is a discrete probability measure on V_Q.

Proof. By Lemma 6.1 $P_Q(\theta)$ is defined and non-negative for every $\theta \in V_Q$. Clearly, if $\theta_1 \neq \theta_2$ then $T_Q^{-1}(\theta_1) \cap T_Q^{-1}(\theta_2) = \emptyset$, so

$$\cup_{\theta \in V_Q} T_Q^{-1}(\theta) = \Lambda$$

is a partition of Λ. Hence

$$P_Q(V_Q) = \sum_{\theta \in V_Q} P_Q(\theta) = 1,$$

as required.

□

Let $Q_i : \Lambda \to \mathbb{N}$, $i \in \mathbb{N}$, be a sequence of random variables (termination conditions) on Λ such that

$$V(\mathcal{T}) = \bigcup_{i \in \mathbb{N}} V_{Q_i} \quad V_{Q_i} \cap V_{Q_j} = \emptyset \ (i \neq j). \tag{5}$$

In this event we say that the sequence $\mathcal{Q} = \{Q_i\}_{i \in \mathbb{N}}$ of termination conditions for W is *complete*. The complete sequence of termination conditions $\mathcal{Q}$ allows one to define an *asymptotic density* $\rho_{V(\mathcal{T})}$ on $V(\mathcal{T})$ with respect to $\mathcal{Q}$. Namely, if $S \subseteq V(\mathcal{T})$ then the asymptotic density $\rho_{V(\mathcal{T})}(S)$ of S in $V(\mathcal{T})$ relative to B, D_0, and $\mathcal{Q}$ is equal to the following limit (if it exists)

$$\rho_{V(\mathcal{T})}(S) = \lim_{i \to \infty} P_{Q_i}(S \cap V_{Q_i}).$$

Let $\mu : \mathbb{N} \to \mathbb{R}$ be a fixed probability distribution on $\mathbb{N}$. Define a probability measure

$$P_{V(\mathcal{T})} : V(\mathcal{T}) \to \mathbb{R}$$

which depends on $\mathcal{Q}$ and μ as follows. For $\theta \in V(\mathcal{T})$ such that $\theta \in V_{Q_i}$ for some $i \in \mathbb{N}$ put

$$P_{V(\mathcal{T})}(\theta) = \mu(i) P_{Q_i}(\theta). \tag{6}$$

Proposition 6.3. The function $P_{V(\mathcal{T})}$ is a discrete probability measure on the set $V(\mathcal{T})$.

Proof. Clearly, the value $P_{V(\mathcal{T})}(\theta)$ is defined for every $\theta \in V(\mathcal{T})$ and is non-negative. Therefore, it suffices to show that $\sum_{\theta \in V(\mathcal{T})} P_{V(\mathcal{T})}(\theta) = 1$. The latter comes from the following equalities:

$$\sum_{\theta \in V(\mathcal{T})} P_{V(\mathcal{T})}(\theta) = \sum_{i \in \mathbb{N}} \sum_{\theta \in V_{Q_i}} P_{V(\mathcal{T})}(\theta) = \sum_{i \in \mathbb{N}} \sum_{\theta \in V_{Q_i}} \mu(i) P_{Q_i}(\theta) = \sum_{i \in \mathbb{N}} \mu(i) = 1$$

□

6.2.2 Probability on $\mathcal{K}$

Next we define a probability measure $P_{\mathcal{K}}$ on diagrams $\mathcal{K}$. Let $\theta \in V(\mathcal{T})$. By definition $\theta = e_1 \dots e_k$ is a path in the transition graph $T = T_B$ with the origin D_0 and the terminus $D(\theta)$. For $D \in \mathcal{K}$ we define a function

$$P_{\mathcal{K}}(D) = \sum_{\theta \in V(\mathcal{T}),\ D(\theta)=D} P_{V(\mathcal{T})}(\theta)$$

(here we assume that $P_{\mathcal{K}}(D) = 0$ if there is no $\theta \in V(\mathcal{T})$ such that $D(\theta) = D$).

Lemma 6.4. *The function $P_{\mathcal{K}}$ is a discrete probability measure on $\mathcal{K}$.*

Proof. Obvious.

□

Finally, define sets

$$\mathcal{K}_i = D(V_{Q_i}) = \{D(\theta) \mid \theta \in V_{Q_i}\}$$

with functions $P_{\mathcal{K}_i} : \mathcal{K}_i \to \mathbb{R}$ such for $D \in \mathcal{K}_i$:

$$P_{\mathcal{K}_i}(D) = \sum_{\theta \in V_{Q_i} \text{ and } D(\theta)=D} P_{Q_i}(\theta).$$

Proposition 6.5. The function $P_{\mathcal{K}_i}$ is a discrete probability measure on $\mathcal{K}_i$.

Notice that if the sets $\mathcal{K}_i$ form a partition of $\mathcal{K}$ then one can define an *asymptotic density* of diagrams from $\mathcal{K}$ as follows. If $S \subseteq \mathcal{K}$ then

$$\rho_{\mathcal{K}}(S) = \lim_{i \to \infty} P_{\mathcal{K}_i}(\mathcal{K}_i \cap S)$$

(if it exists) is an asymptotic density of S in $\mathcal{K}$.

6.2.3 Probability on $\mathcal{L}$

Let $\varphi : \mathcal{K} \to \mathcal{L}$ be a mapping from $\mathcal{K}$ into a collection of diagrams $\mathcal{L}$. We induce a probability $P_{\mathcal{L}}$ on $\mathcal{L}$ from $\mathcal{K}$ through φ: for $D \in \mathcal{L}$

$$P_{\mathcal{L}}(D) = \sum_{\theta \in V(\mathcal{T}) \text{ and } \phi(D(\theta))=D} P_{V(\mathcal{T})}(\theta) = \sum_{D' \in \mathcal{K},\ \varphi(D')=D} P_{\mathcal{K}}(D').$$

Proposition 6.6. The function $P_{\mathcal{L}}$ is a discrete probability measure on $\mathcal{L}$.

Proof. Obvious. □

Define sets

$$\mathcal{L}_i = \varphi(\mathcal{K}_i) = \{\varphi(D(\theta)) \mid \theta \in V_{Q_i}\}$$

with functions $P_{\mathcal{L}_i} : \mathcal{L}_i \to \mathbb{R}$ such for $D \in \mathcal{L}_i$

$$P_{\mathcal{L}_i}(D) = \sum_{\theta \in V_{Q_i} \text{ and } \varphi(D(\theta))=D} P_{V(\mathcal{T})}(\theta).$$

Proposition 6.7. The function $P_{\mathcal{L}_i}$ is a discrete probability measure on $\mathcal{L}_i$.

Notice that if the sets $\mathcal{L}_i$ form a partition of $\mathcal{L}$ then one can define an asymptotic density of diagrams from $\mathcal{L}$ as follows. If $S \subseteq \mathcal{L}$ then

$$\rho_{\mathcal{L}}(S) = \lim_{i \to \infty} P_{\mathcal{L}_i}(\mathcal{L}_i \cap S)$$

(when exists) is an asymptotic density of S in $\mathcal{L}$.

Probability on:	**space**	**subspase**	**relative to**
vertices	$(V_{\mathcal{T}}, P_{V_{\mathcal{T}}})$	(V_{Q_i}, P_{Q_i})	B, μ, D_0, $\{Q_i\}_{i\in\mathbb{N}}$
diagrams (1st level)	$(\mathcal{K}, P_{\mathcal{K}})$	$(\mathcal{K}_i, P_{\mathcal{K}_i})$	all above
diagrams (2nd level)	$(\mathcal{L}, P_{\mathcal{L}})$	$(\mathcal{L}_i, P_{\mathcal{L}_i})$	all above and $\phi : \mathcal{K} \to \mathcal{L}$

Table 1: Probability models.

6.3 Iterative random generator RG_n

In this section we give an example of a complete sequence of termination conditions $\mathcal{Q} = \{Q_n\}_{n\in\mathbb{N}}$ and show that the corresponding probabilities $P_{\mathcal{K}_n}$ are related to a specific random diagram generator RG_n. We freely use notation from Section 6.2.

Let $Q_n : \Lambda_{\mathcal{T}} \to \mathbb{N}$ $(n \in \mathbb{N})$ be a sequence of constant functions:

$$Q_n(\overline{\lambda}) = n, \tag{7}$$

for every $\lambda \in \Lambda$. Clearly, Q_n is a random variable on Λ. So, one can view Q_n as a termination condition from Section 6.2. It follows that $\mathcal{Q} = \{Q_n\}_{n\in\mathbb{N}}$ is a complete sequence of termination conditions for Λ. Let $P_{\mathcal{K}_n}$ be the probability measure on V_{Q_n} from Section 6.2. One can describe the probability measure $P_{\mathcal{K}_n}$ in terms of the following random generator.

Algorithm 6.8. *(Random Generator RG_n relative to the basic generator B)*

Input: A presentation $\langle X; R\rangle$, a diagram $D_0 \in \mathcal{K}$, and $n \in \mathbb{N}$.

Output: A diagram from $\mathcal{K}$.

Initialization: Put $D_{m_0} = D_0$.

Computations:

1) Consequently compute $D_{m_{i+1}} = B(D_{m_i})$, for $i = 0, \ldots, n-1$.

2) Output D_{m_n}.

It is easy to see that the following assertion is true.

Proposition 6.9. Let $D \in \mathcal{K}$. Then

$$P_{\mathcal{K}_n}(D) = \sum_{\theta \in V_{Q_n},\ D(\theta)=D} P_{Q_n}(\theta)$$

is the probability of the event that D will be generated by RG_n.

Remark 6.10. In a similar way one can construct a random generator to produce diagrams from $\mathcal{L}_n$. Indeed, apply RG_n to produce a diagram D from $\mathcal{K}$ and take $\varphi(D)$. The corresponding probability to generate a diagram $\varphi(D)$ equals to $P_{\mathcal{L}_n}(\varphi(D))$.

6.4 Diagram complexity and random generator RG_χ

In this section we define a notion of a size of a diagram and describe a random generator RG_χ which terminates when the diagram reaches a particular size.

For a diagram $D \in \mathcal{K}$ denote by $\chi_e(D)$ and $\chi_c(D)$, correspondingly, the number of *free edges* (i.e. edges which do not belong to the boundary of any cell in D) and the number of cells in D. We refer to the sum $\chi(D) = \chi_e(D) + \chi_c(D)$ as to the *size* of D.

Now, suppose that the basic extension B satisfies the following conditions for every $D \in \mathcal{K}$:

$$0 \leq \chi(B(D)) - \chi(D) \leq 1; \tag{8}$$

$$\limsup_{i \to \infty} \chi(D(\lambda_i)) = \infty, \text{ for each } \lambda \in \Lambda; \tag{9}$$

$$\chi(D_0) = 0. \tag{10}$$

Under these assumptions on B we define the following random variables X_n and $\widehat{Q}_n$. Recall that each $\theta \in V(\mathcal{T})$ is a path $e_1 \dots e_k$ in T_B with the origin at D_0 and

the terminus at some diagram $D(\theta)$. Define a function $X_n : \Lambda \to \mathbb{N}$ by

$$X_n(\lambda) = \min\{i \in \mathbb{N} \mid \chi(D(\lambda_i)) = n\}$$

and put

$$\widehat{Q}_n(\lambda) = \max\{i \in \mathbb{N} \mid \chi(D(\lambda_i)) = n\} = X_{n+1}(\lambda) - 1. \tag{11}$$

Lemma 6.11. *Let B be a basic extension satisfying conditions (8), (9) and (10). Then X_n and $\widehat{Q}_n$ are random variables.*

Proof. It suffices to show that X_n is a random variable for every $n \in \mathbb{N}$, since $\widehat{Q}_n = X_{n+1} - 1$. Fix arbitrary $n, j \in \mathbb{N}$. We claim that $X_n^{-1}(j)$ is a union of at most countable number of cones.

Observe first that if $\lambda \in X_n^{-1}(j)$ then $Cone(\lambda_j) \subseteq X_n^{-1}(j)$. This implies that

$$X_n^{-1}(j) = \cup_{\lambda \in X_n^{-1}(j)} Cone(\lambda_j).$$

It is easy to see that the set above is either countable or finite union of cones and, hence, is measurable.

□

Corollary 6.12. $\{\widehat{Q}_i\}_{n \in \mathbb{N}}$ are termination conditions on Λ.

Lemma 6.11 allows one to define probability spaces $(V_{\widehat{Q}_i}, P_{\widehat{Q}_i})$ (described in Section 6.2) for each $n \in \mathbb{N}$. We show in Proposition 6.14) below that the probability function $P_{\widehat{Q}_i}$ can be described in terms of the following random generator.

Algorithm 6.13. *(Random Generator RG_χ)*

INPUT: A presentation $\langle X; R\rangle$, a diagram D_0, and $n \in \mathbb{N}$.

OUTPUT: A diagram D such that $\chi(D) = n$.

INITIALIZATION: Put $D_{m_0} = D_0$ and $i = 1$.

COMPUTATIONS:

1) Construct $D_{m_i} = B(D_{m_{i-1}})$.

2) If $\chi(D_{m_i}) = n + 1$ then return $D_{m_{i-1}}$. Otherwise increment i and goto 1).

The next proposition is analogous to Proposition 6.9.

Proposition 6.14. Let $\widehat{Q}_n$ be defined as in (11) and $D \in \mathcal{K}$. Then

$$P_{\mathcal{K}_n}(D) = \sum_{\theta \in V_{\widehat{Q}_n},\ D(\theta)=D} P_{\widehat{Q}_n}(\theta)$$

is the probability of the event that D is generated by RG_χ.

Remark 6.15. In a similar way one can construct a random generator to produce diagrams from $\mathcal{L}_n$. Indeed, apply RG_χ to produce a diagram D from $\mathcal{K}$ and take $\varphi(D)$. The corresponding probability to generate a diagram $\varphi(D)$ equals to $P_{\mathcal{L}_n}(\varphi(D))$.

Next, we define probability function $P_{V(\mathcal{T})}$ on $V(\mathcal{T})$ relative to the sequence of random variables $\{\widehat{Q}_i\}_{i\in\mathbb{N}}$ (as in Section 6.2). To do this we need the following lemma.

Lemma 6.16. *Assume that the basic extension B satisfies (8), (9), (10) and also satisfies an extra condition*

$$\textit{for each } D_s \in \mathcal{K} \textit{ there exists } D_t = B(D_s) \textit{ such that } \chi(D_t) - \chi(D_s) = 1. \qquad (12)$$

Then $V(\mathcal{T}) = \cup_{i\in\mathbb{N}} V_{\widehat{Q}_i}$ is a partition of $V(\mathcal{T})$.

Proof. By definition of $\widehat{Q}_i$ if $\theta \in V_{\widehat{Q}_i}$ then $\chi(D(\theta)) = i$. Now, let $\theta \in V(\mathcal{T})$, $\chi(D(\theta)) = i$, and $D_s = D(\theta)$. By assumption of the lemma there exists $D_t = B(D_s)$ such that $\chi(D_t) - \chi(D_s) = 1$. Let (θ, θ') be the edge in $\mathcal{T}$, where $D(\theta') = D_t$. Then, by definition of $\widehat{Q}_i$, $T_{\widehat{Q}_i}(Cone(\theta')) = \{\theta\}$ and $\theta \in V_{\widehat{Q}_i}$. Therefore $V_{\widehat{Q}_i} = \{\theta \mid \chi(D(\theta)) = i\}$ and $V(\mathcal{T}) = \cup_{i\in\mathbb{N}} V_{\widehat{Q}_i}$ is a partition of $V(\mathcal{T})$, as required.

□

Corollary 6.17. $\{\widehat{Q}_i\}_{n\in\mathbb{N}}$ is a complete system of termination conditions on Λ.

Corollary 6.18. Assume that the basic extension B satisfies all conditions (8)-(10) and (12). Then the following holds:

1) If $S \subseteq V(\mathcal{T})$ then

$$\rho_{V(\mathcal{T})}(S) = \lim_{i\to\infty} P_{\widehat{Q}_i}(S \cap V_{\widehat{Q}_i}).$$

defines an asymptotic density of a set S in $V(\mathcal{T})$ with respect to $\{\widehat{Q}_i\}$. We refer to this $\rho_{V(\mathcal{T})}$ as to the asymptotic density relative to the size of diagrams.

2) If μ is a probability distribution on $\mathbb{N}$ then one can define the discrete probability $P_{V(\mathcal{T})}$ on $V(\mathcal{T})$ as in (6).

3) $\mathcal{K} = \cup\mathcal{K}_i$ is a partition of $\mathcal{K}$ and if $\mathcal{K}' \subseteq \mathcal{K}$ then

$$\rho_{V(\mathcal{T})}(\mathcal{K}') = \lim_{i\to\infty} P_{\mathcal{K}_i}(\mathcal{K}' \cap \mathcal{K}_i)$$

defines an asymptotic density of $\mathcal{K}'$ in $\mathcal{K}$.

4) Furthermore, if $\mathcal{L} = \mathcal{L}_i$ is a partition of $\mathcal{L}$ (e.g. when φ preserves the size of diagrams) then

$$\rho_{\mathcal{L}}(\mathcal{L}') = \lim_{i\to\infty} P_{\mathcal{L}_i}(\mathcal{L}' \cap \mathcal{L}_i)$$

defines an asymptotic density of $\mathcal{L}' \subseteq \mathcal{L}$.

7 Basic extension algorithm B_S and relative probability measures

In this section we define a particular basic extension B_S, where S is a set of parameters. In the next section we use B_S to study asymptotic properties of diagrams.

7.1 Basic extension B_S

Let $\langle X; R\rangle$ be a finite presentation. Denote by $\mathcal{L} = \mathcal{L}(X, R)$ a set of representatives (up to isomorphism) of all diagrams D over $\langle X; R\rangle$. In this section we construct a particular basic extension B_S. Roughly speaking, B_S randomly adds cells and edges to the given diagram, and performs random foldings. The extension B_S depends on a set of parameters S (the probabilities with which it adds cells or edges to a diagram and makes foldings) which allow one to obtain random diagrams with different properties.

Let D be a diagram. Suppose a subset $M(D)$ of the set $V(D)$ of vertices of D is chosen. The vertices from $M(D)$ are called "marked vertices" (worked out vertices). Suppose also that a subset $A(D) \subseteq \partial D - M(D)$ of non-marked vertices from D is chosen such that $|A(D)| \leq 1$. We refer to vertices from $A(D)$ as to "active vertices" (vertices in the working). The triple $(D, M(D), A(D))$ is called an *extended diagram*. Morphisms of extended diagrams are morphisms of diagrams that preserve the marked and active vertices. Let $\mathcal{K} = \mathcal{K}(X, R)$ be the set of all extended diagrams from $\mathcal{L}$.

Let $S = (s_1, s_2, s_3, s_4)$ be a sequence of reals such that $s_i \in [0, 1], s_1 + s_2 + s_3 = 1$. The following procedure provides the basic extension B_S.

Algorithm 7.1. (*Basic Extension B_S*)

INPUT: Let D be an extended van Kampen diagram over $\langle X; R\rangle$ such that either $A(D) \neq \emptyset$ or $\partial D - M(D) \neq \emptyset$.

OUTPUT: Diagram $B_S(D) = D$.

1) If $|A(D)| = 1$ then take the only vertex $v \in A(D)$. If $|A(D)| = 0$ then, choose randomly and uniformly an unmarked vertex $v \in \partial D - M(D)$ and put $A(D) = \{v\}$.

2) If v is not the last unmarked vertex in ∂D then with probability s_1 do a), with probability s_2 do b), and with probability $s_3 = 1 - s_1 - s_2$ do c) below:

   a) Take randomly and uniformly a relator $r \in R$. Make a face N with the boundary label r at some vertex $u \in \partial N$. Attach N to v by identifying v with u. Go to 5).

   b) Generate randomly and uniformly a letter $y \in X^{\pm 1}$. Make a free edge $e = (u_1, u_2)$ with the label y. Attach e to v by identifying v with u_1. Go to 5).

   c) Do not attach anything to v and go to 4).

3) If v is the last unmarked vertex in D and $s_1 + s_2 \neq 0$ then with probability $\frac{s_1}{s_1+s_2}$ do a) below, otherwise do b):

   a) Take randomly and uniformly a relator $r \in R$. Make a face N with the boundary label r at some vertex $u \in \partial N$. Attach N to v by identifying v with u. Go to 5).

   b) Generate randomly and uniformly a letter $y \in X^{\pm 1}$. Make a free edge $e = (u_1, u_2)$ with the label y. Attach e to v by identifying v with u_1. Go to 5).

4) a) Let $(e_1, h_1), \ldots, (e_k, h_k)$ be all pairs of edges incident to v and such that for each i the following conditions hold:

   - the path $e_i h_i$ belongs to the boundary of the diagram (with respect to a fixed orientation);
   - all endpoints of e_i and f_i are unmarked;
   - e_i and h_i^{-1} have the same labels (potential fold);
   - edges e_i and h_i are not free.

   Then for each $i = 1, \ldots, k$ with a fixed probability s_4 fold e_i and h_i^{-1}.

b) mark v, and add it to $M(D)$,

c) remove v from $A(D)$. Go to 5).

5) Denote the resulting diagram by $B_S(D)$. Output $B_S(D)$.

Below we list some properties of B_S. Recall that a vertex v is a *cut vertex of a map* $\mathcal{M}$ if there exist two vertices $v_1, v_2 \in \mathcal{M}$ such that any path connecting v_1 and v_2 goes through v.

Lemma 7.2. (Properties of B_S) *Let $D^* = B_S(D)$. Then:*

1) if a vertex v in D is marked then $N_D(v) = N_{D^*}(v)$.

2) if every vertex $v \in D - \partial D$ is marked then every vertex $v \in D^* - \partial D^*$ is marked.

3) if every cut vertex in D is either marked or active then every cut vertex in D^* is either marked or active;

4) Given a diagram D there are only finitely many possible outcomes for D^*.

5) If $\partial D - M(D) \neq \emptyset$ then $\partial D^* - M(D^*) \neq \emptyset$

Proof. Follows from the description of B_S. □

Let D be a diagram. The following notation

$$D^* = B_S^{(n)}(D)$$

means that D^* is a result of n applications of B_S to the diagram D.

Remark 7.3. Let $D^* = B_S^{(n)}(D_0)$ where D_0 is a diagram which consists of one vertex.

1) if $s_2 = 1$ then D^* is a tree;

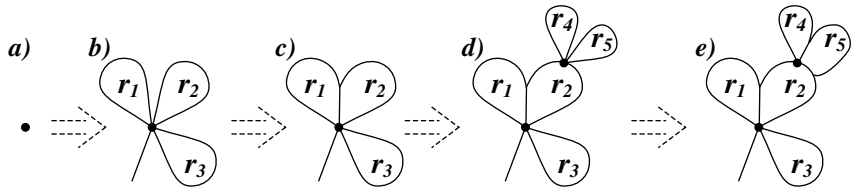

Figure 4: Diagram generation.
Random Generator RG_n starts from the diagram D_0 and then randomly attaches cells and free edges at fixed active vertices. This picture shows eight iterations of RG_n. On step 1) of the first iteration the algorithm chooses the active vertex which must be the only vertex in D_0. Then on iterations 1-4 it randomly adds three cells labelled with relators r_1, r_2, r_3 and a free edge (part b) of the picture). Then on the fifth iteration it determines what pairs of edges in the neighborhood of the active vertex are equally labelled and with probability s_4 folds them. On step 1) of the sixth iteration it again randomly selects a new active vertex and attaches two cells. Finally RG_n randomly folds edges in the neighborhood of the new vertex.

2) if $s_1 = 1$ then D^* is a "tree of cells", i.e., diagram without free edges and such that the dual graph is a tree;

3) if $s_1 + s_2 = 1$ then D^* is a "tree of cells and free edges".

Let $\mathcal{W}_S$ be the random walk corresponding to the random generator RG_S. In the following lemma we collect some basic properties of $\mathcal{W}_S$. By D_∞ we denote a path (perhaps, infinite) in the graph T:

$$D_1 \to D_2 \to \ldots \to D_k \to \ldots$$

Lemma 7.4. *(*Properties of T*) If D_∞ is a path in T and $D_i \in D_\infty$ then the following hold:*

1) every vertex $v \in D_i - \partial D_i$ is marked;

2) for every marked vertex $v \in D_i$ the neighborhood of v does not change in D_j for $j \geq i$, i.e., $N_{D_j}(v) = N_{D_i}(v)$;

3) every unmarked vertex $v \in D_i$ either stays unmarked in all D_j for $j \geq i$ or

eventually it becomes active;

4) every active vertex $v \in D_i$ either stays active in all D_j for $j \geq i$ (and in this event the case 4) in the description of B_S does not occur) or eventually it becomes marked;

Corollary 7.5. The random basic extension B_S is locally stable at every marked vertex v.

7.2 Completeness of the basic extension B_S

In this section we show that B_S is $\mathcal{L}$-complete (provided none of the probabilities in S are zero).

Below we use notation from the previous sections. Recall that $\mathcal{L} = \mathcal{L}(X, R)$ is a set of representatives of all van Kampen diagrams over $\langle X; R\rangle$ up to isomorphisms and $\Phi = \Phi_{B_S}(D_0)$ is the set of all extended diagrams over $\langle X; R\rangle$ that can be produced by a sequence of applications of B_S starting from D_0.

For an extended diagram D denote by $\overline{D}$ the ordinary diagram that results from D by erasing the sets $M(D)$ and $A(D)$. Slightly abusing notations we will identify vertices, edges, and cells in D and $\overline{D}$. This implies, in particular, that for a vertex $v \in D$ one has $N_D(v) = N_{\overline{D}}(v)$. In the situations when D is an extended diagram and $\phi : \overline{D} \to C$ is a morphism of ordinary diagrams the agreement above will allow us to consider unambiguously the image $\phi(v)$ for a vertex $v \in D$. Put

$$\overline{\Phi}_{B_S} = \{\overline{D} \mid D \in \Phi\}.$$

According to the definition of completeness from Section 6.1 the basic extension B_S is $\mathcal{L}$-complete relative to the mapping $\overline{} : \Phi_{B_S} \to \mathcal{L}$ if $\overline{\Phi}_{B_S} = \mathcal{L}$. For notational convenience, further in this section we omit the index B_S in $\overline{\Phi}_{B_S}$ and denote $\overline{\Phi}_{B_S}$ simply by $\overline{\Phi}$.

In the prove of completeness we will use two auxiliary transformations of maps termed *edge cuts* and *vertex cuts*. Let $\mathcal{M}$ be an arbitrary map over $\langle X; R\rangle$ and $e = (v, u)$ be an edge from $\mathcal{M} - \partial\mathcal{M}$ with $v \in \partial\mathcal{M}$. Let f_1 and f_2 be two edges from $\partial\mathcal{M}$ incident to v such that there is no any cell from $N(v)$ or any edge from $Star(v)$ in between f_1 and f_2 according to the fixed orientation (see Section 4.2). Then the cut of the edge v between f_1 and f_2 is the following sequence of transformations:

- replace ("cut") the vertex v and the edge e with their two copies v_1, v_2 and $e_1 = (v_1, u)$, $e_2 = (v_2, u)$;
- replace the vertex v in all edges and cells in $\mathcal{M}$ between e and f_1, including f_1, with v_1;
- replace the vertex v in all edges and cells in $\mathcal{M}$ between f_2 and e, including f_2, with v_2.

Figure 5 illustrates this cut.

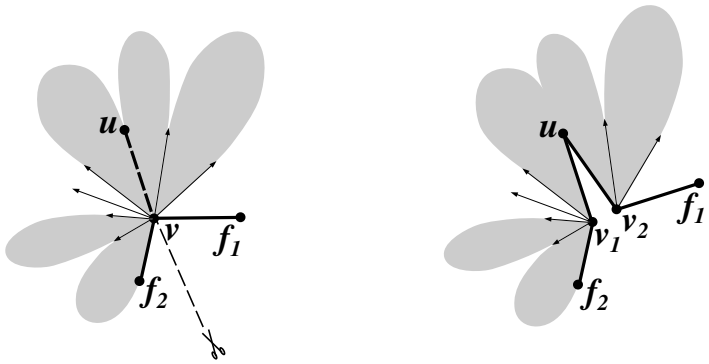

Figure 5: Edge cut.

Now let v be a vertex on $\partial\mathcal{M}$ and (f_1, f_2) and (g_1, g_2) be distinct pairs of edges from $\partial\mathcal{M}$ incident to v such that there is no any cell from $N(v)$ or any edge from $Star(v)$ in between f_1 and f_2 and, also, in between g_1 and g_2 (according to the fixed orientation). Then the cut of v between (f_1, f_2) and (g_1, g_2) is the following sequence of transformations:

- replace ("cut") the vertex v with two copies v_1, v_2;
- replace the vertex v in all edges and cells in $\mathcal{M}$ between f_2 and g_1, including f_2 and g_1, with v_1;
- replace the vertex v in all edges and cells in $\mathcal{M}$ between g_2 and f_1, including g_2 and f_1, with v_2.

Figure 6 illustrates vertex cut. We allow only those vertex cuts which result in a connected map.

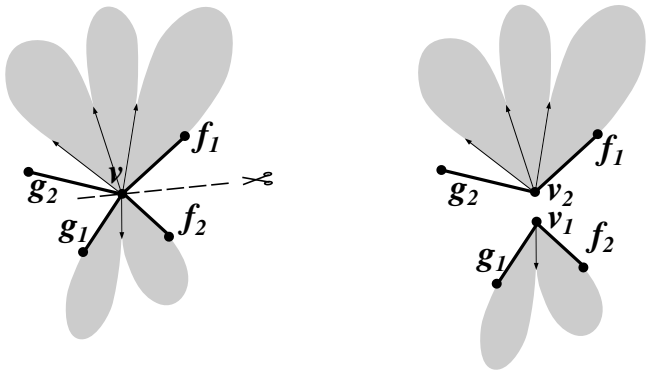

Figure 6: Vertex cut.

We refer to these vertex and edge cuts as *simple cuts*. If σ is a simple cut of $\mathcal{M}$ which results in a map $\mathcal{M}'$ then we write $\mathcal{M} \stackrel{\sigma}{\to} \mathcal{M}'$. There exists a natural *sewing* morphism $\phi : \mathcal{M}' \to \mathcal{M}$ which sews up $\mathcal{M}'$ back into $\mathcal{M}$ (ϕ identifies v_1 with v_2 and e_1 with e_2 from the definitions above). We say that a map $\mathcal{M}'$ is a *cut* of $\mathcal{M}$ if $\mathcal{M}'$ can be obtained from $\mathcal{M}$ by a sequence of simple cuts $\sigma = (\sigma_1, \ldots, \sigma_k)$. We allow here the empty sequences too (i.e., $\mathcal{M}$ is a cut of itself). If $\mathcal{M}'$ is a cut of $\mathcal{M}$ then there exists a natural *sewing* morphism $\mathcal{M}' \to \mathcal{M}$ which is a composition of the sewing morphisms corresponding to the sequence of simple cuts from $\mathcal{M}'$ to $\mathcal{M}$.

Theorem 7.6. *Let $\langle X; R\rangle$ be a symmetrized finite presentation and D be a van Kampen diagram over $\langle X; R\rangle$ which*

1) does not contain loops of length 1 *and*

2) for each cell c the boundary ∂c is vertex-simple (does not touch itself).

If none of the probabilities in S is zero then $D = \overline{B_S^n(D_0)}$ *for some* $n \in \mathbb{N}$*, i.e., the diagram D can be generated by RG with non-trivial probability in n iterations.*

Proof. Let $D \in \mathcal{L}$ be a van Kampen diagram. We are going to construct by induction a sequence of extended diagrams

$$D_0, ..., D_n$$

and a sequence of morphisms

$$\phi_0 : \overline{D}_0 \to D, \ldots, \phi_n : \overline{D}_n \to D$$

such that $\phi_n : \overline{D}_n \to D$ is an isomorphism and such that the following conditions hold:

P1) D_i can be obtained from D_{i-1} by a sequence of basic extensions of the following type:

   a) choose some unmarked vertex v in D_{i-1} and make it active;

   b) add finitely many (perhaps zero) cells and free edges to D_{i-1} at v;

   c) fold some edges incident to v;

   d) make v marked and non-active.

P2) $\overline{D}_i$ is a cut of the subcomplex $\phi_i(\overline{D}_i)$ of D and $\phi_i : \overline{D}_i \to \phi_i(\overline{D}_i)$ is the corresponding sewing morphism.

P3) For every marked vertex $v \in D_i$ ϕ_i maps the neighborhood $N_{D_i}(v)$ of v bijectively on the neighborhood $N_D(\phi_i(v))$.

Base of induction $i = 0$**.** Recall that D_0 is an extended diagram consisting of a single unmarked vertex v and such that $M(D_0) = \emptyset, A(D_0) = \emptyset$. Take any vertex v_0 in D and define $\phi_0(v) = v_0$. All properties P1-P3 clearly hold for D_0.

Induction step. Let D_i and ϕ_i satisfying properties P1-P3 have been constructed.

In the following claims we study properties of $\overline{D}_i$, $\phi_i(\overline{D}_i)$, and ϕ_i. Recall that by $FE(D)$ and $C(D)$ we denote sets of free edges and cells of D.

Claim 1. *(Properties of D_i.) The following holds.*

1.1) Every two elements of $FE(D_i) \cup C(D_i)$ are connected by a chain (see Section 4.3 for definitions) of marked vertices (marked chain).

1.2) Cut vertices of D_i are marked.

1.3) Every element of $FE(D_i) \cup C(D_i)$ has a marked vertex.

Proof of Claim 1. Obviously, 1.2) and 1.3) are corollaries of 1.1).

We prove 1.1) by induction on i. For $i = 0$ there is nothing to prove. Assume now that 1.1) holds for $i = l$. By the property P1 D_{l+1} can be obtained from D_l first by choosing an unmarked vertex v, adding free edges and cells to v, folding some edges incident to v, and making v marked and non-active. Clearly, every new cell or free edge in $D_{l+1} - D_l$ contains the marked vertex v which connects them to the rest of the diagram.

□

$\phi_i(\overline{D}_i)$ is a map on a plane $\mathbb{R}^2$. Hence $\mathbb{R}^2 - \phi_i(\overline{D}_i)$ is a disjoint union of open, connected, simply connected components $C_0, \ldots, C_m$, where C_0 is the unbounded component, and all other components are bounded. By ∂C_s we denote the boundary of C_s which is a connected component of $\partial\phi_i(\overline{D}_i)$.

Claim 2. *(Properties of $\phi_i(D_i)$). The following holds.*

2.1) If u is a vertex in D_i and $\phi_i(u) \in \partial C_s$ for some finite component C_s ($s > 0$) then u is unmarked in D_i.

2.2) If $e = (u, v)$ is an edge in ∂C_s ($s > 0$) then there exists a cell $f \in \phi_i(D_i)$ such that $e \in \partial f$.

Proof of Claim 2.

2.1) Let $u \in D_i$ and $\phi_i(u) \in \partial C_s$. Since $\phi_i(u) \in \partial C_s$ the morphism ϕ_i is not bijective on $N_{D_i}(u)$. Hence u is unmarked by the P3.

2.2) Assume that $e = (v, u) \in \partial C_s$ ($s > 0$). Assume e does not belong to the boundary of any cell of $\phi_i(D_i)$. Let $e' = (v', u') \in D_i$ be such that $\phi_i(e') = e$. The vertices v' and u' are unmarked in D_i by 2.1). Clearly, the edge e' does not belong to the boundary of any cell of D_i, because D_i is a cut of $\phi_i(D_i)$. Hence e' is a free edge in D_i. By the property 1.3 at least one of its endpoints is marked – contradiction.

□

By the property P2 $\overline{D}_i$ is obtained from the subcomplex $\phi_i(\overline{D}_i)$ of D by a finite sequence of simple cuts $\sigma = (\sigma_1, \ldots, \sigma_k)$:

$$\phi_i(\overline{D}_i) = B_1 \overset{\sigma_1}{\to} B_2 \overset{\sigma_2}{\to} \ldots \overset{\sigma_k}{\to} B_{k+1} = \overline{D}_i. \tag{13}$$

Notice that $\phi_i(\partial\overline{D}_i) = \partial\phi_i(\overline{D}_i) \cup \Gamma$, where Γ is the set of edges of $\phi_i(D_i)$ that were cut in (13). Edges from Γ have exactly two preimages in ∂D_i and edges from $\partial\phi_i(\overline{D}_i)$ have unique preimages. Since D_i is a diagram it is connected, hence ∂D_i is a closed path, as well as $\phi_i(\partial\overline{D}_i)$. Let $e_0 = (v_0, v') \in \partial D_i$ be an edge such that $\phi_i(e_0) \in \partial C_0$. Denote by P the closed path $\phi_i(\partial\overline{D}_i)$ starting with the edge $\phi_i(e_0)$.

Claim 3. *(Properties of P) Let C_s and C_t be two distinct components. Let $e_1, \ldots, e_p$ be edges of ∂C_s, and $d_1, \ldots, d_r$ be edges of ∂C_t both given in the order they appear in P. Then the following holds:*

1) The boundary ∂C_s, as a path, is a cyclic permutation of $e_1, \ldots, e_p$.

2) The boundary paths ∂C_s and ∂C_s appear in P in one of the following orders:

$$e_1, \ldots, e_{p'}, d_1, \ldots, d_r, e_{p'+1}, \ldots, e_p, \tag{14}$$

or

$$d_1, \ldots, d_{r'}, e_1, \ldots, e_p, d_{r'+1}, \ldots, d_r, \tag{15}$$

where $0 \leq p' \leq p$ and $0 \leq r' \leq r$.

Proof of Claim 3. Induction on the number of simple cuts in (13). Notice that path P might be not simple, it can be a union of disjoint simple loops. If the number of cuts is zero then ϕ_i is an isomorphism, so there is only one component, the infinite component C_0, and the claim is obvious.

Assume the claim is true for $k-1$ simple cuts $\sigma_1, \ldots, \sigma_{k-1}$. Suppose now that σ_k is a cut along some edge $f = (v, u)$. Then $v \in C_j$ for some $0 \leq j \leq q$ and $f \notin \partial C_l$ for any component C_l. Recall that a cut along f replaces the edge e by two new edges f_1 and f_2 incident to u in such a way that the boundary ∂B_{k+1} is obtained from ∂B_k by inserting either a path $f_1^{-1} f_2$ or a path $f_1^{-1} f_2$ (depending on the orientation). Assume for simplicity that the path $f_1^{-1} f_2$ was inserted. If $j \neq s$ and $j \neq t$ then the claim follows by induction. We may assume now that $j = s$. The image of $f_1^{-1} f_2$ in B_k under the sewing morphism $\theta : B_{k+1} \to B_k$ is the path $f^{-1} f$. Observe that f does not belong to components of B_k. Now the claim follows by induction since $\phi_i(D_i)$ is obtained from B_k by a sequence of a sewing morphisms. This case is illustrated on Figure 7.

Assume now that σ_k is a vertex cut. This case is depicted on Figure 8. Here two components of B_k are merged into one component in B_{k+1}. The proof is obvious from the picture and we omit it.

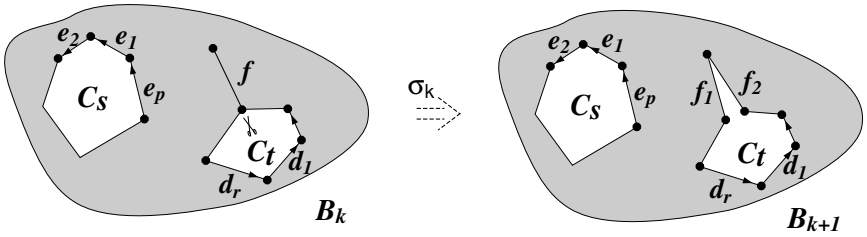

Figure 7: Edge cut starting from the finite component C_t.

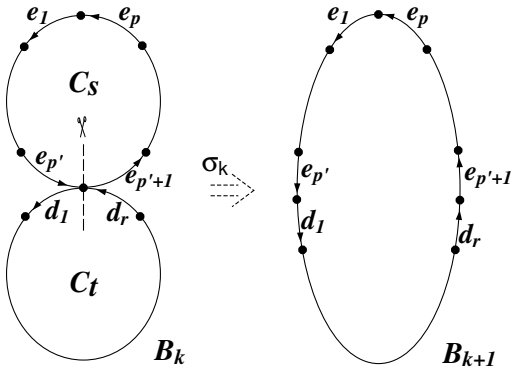

Figure 8: Vertex cut starting from the finite component C_t.

□

It follows from Claim 3 that if P contains a subpath $e_1P_1e_2$ such that $e_1, e_2 \in \partial C_s$ for some component C_s and a subpath P_1 does not contain edges from C_s then:

- The terminus of e_1 is the origin of e_2.
- If P_1 contains an edge $e_3 \in \partial C_t$ for another component C_t then P_1 contains all edges from ∂C_t.

A path Q in $\phi_i(D_i)$ is called *component-complete* provided if Q contains an edge from ∂C_t then Q contains all edges from ∂C_t.

Now we define a directed graph (actually, a forest) $T = T(D_i, \phi_i)$ related to the cut (13). The set of vertices of T is the set of components $C_0, \ldots, C_q$. Two components C_s and C_t are connected by an edge from C_s to C_t if and only if $C_s \neq C_t$ and P contains a subpath $e_1P_1fP_2e_2$ such that

a) $e_1, e_2 \in \partial C_s$;

b) P_1 is component-complete;

c) $f \in \partial C_t$.

It follows from Claim 3 that T does not contain cycles, hence it is a forest. See Figure 9 for an example of a graph T.

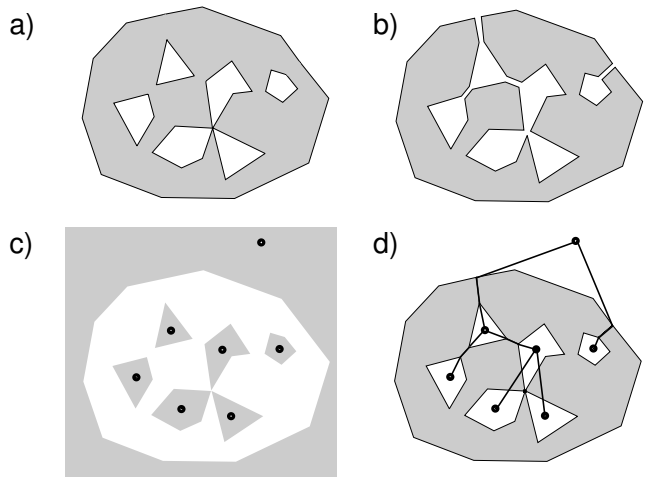

Figure 9: Tree corresponding to the components of $\mathbb{R}^2 - \phi_i(\overline{D}_i)$.
Example for the Case 2.2. Figure a) illustrates $\phi_i(\overline{D}_i)$, b) illustrates $\overline{D}_i$, c) illustrates complement set $\mathbb{R}^2 - \phi_i(\overline{D}_i)$ with components marked by points, d) illustrates graph $T(D_i, \phi_i)$ shown on $\phi_i(\overline{D}_i)$.

Claim 4. *(Existence of an unmarked vertex with a unique image.) If $\phi_i : \overline{D}_i \to D$ is not an isomorphism then there exists an unmarked vertex $v \in \overline{D}_i$ such that*

$$\phi_i(v) \neq \phi_i(v')$$

for every $v' \in \overline{D}_i$ with $v \neq v'$.

Proof of Claim 4. Recall that k is the number of simple cuts in (13). We consider two cases: $k = 0$ and $k > 0$.

Case 1. Let $k = 0$. Then the sewing morphism $\phi_i : \overline{D}_i \to \phi_i(\overline{D}_i)$ is an isomorphism. If $\phi_i(\overline{D}_i) = D$ then we have nothing to prove. If $\phi_i(\overline{D}_i) \neq D$ then

there exists a vertex $u \in \phi_i(\overline{D}_i) \subset D$ such that $N_D(u) \neq N_{\phi_i(\overline{D}_i)}(u)$. Therefore, if $v = \phi_i^{-1}(u) \in D_i$ then $N_D(\phi_i(v)) \not\cong N_{\overline{D}_i}(v)$ (since the latter one is isomorphic to $N_{\phi_i(\overline{D}_i)}(\phi_i(v))$). Now v is unmarked by the property P3. Clearly, $\phi_i(v') \neq \phi_i(v)$ for any $v' \neq v$, since ϕ_i is an isomorphism.

Case 2. Let $k \geq 1$. We say that an edge $e \in \phi_i(\overline{D}_i)$ is cut by a *terminal edge cut* if there exist two edges $e_1 = (u_1, v)$ and $e_2 = (u_2, v)$ in $\overline{D}_i$ mapped to e by ϕ_i. In this event the vertex v is not cut by a simple cut between edges e_1 and e_2. Observe that if the sequence of cuts (13) does not contain a vertex cut then there exists a terminal edge cut.

Case 2.1. Let $e = (\bar{u}, \bar{v}) \in \phi_i(\overline{D}_i)$ be an edge split by a terminal edge cut to edges $e_1 = (u_1, v)$ and $e_2 = (u_2, v)$ in $\overline{D}_i$. We claim that v is a required vertex. Observe first that the vertex v is unmarked. Indeed, e was cut by a simple cut σ_s hence the sewing morphism ϕ_i is not bijective on $N_{\overline{D}_i}(v)$. Therefore v is unmarked by the property P3.

Assume now that there exists a vertex $v' \in \overline{D}_i$ such that $v' \neq v$ and $\phi_i(v') = \phi_i(v)$. Then v is a cut vertex in D_i. Indeed, in this event v is cut by a simple cut from 13. As we have mentioned above this simple cut is not a cut between edges e_1 and e_2. It follows that there are two different pairs of edges in $Star_{D_i}(v)$ which do not have any cells or free edges in between (see Figure 10). Since D_i is simply connected v is a cut vertex. Then v is marked by 1.2 of Claim 1 – contradiction.

Case 2.2. Assume that there is no edge in $\phi_i(\overline{D}_i)$ cut by a terminal edge cut. Let $T = T(\overline{D}_i, \phi_i)$ be the graph related to the cut (13). We claim that there exists at least one finite component in $\mathbb{R}^2 - \phi_i(D_i)$. Indeed, otherwise there is no a vertex cut in (13) (vertex cuts require at least one finite component, since D_i is connected). Hence, as was mentioned above, there is a terminal edge cut in (13) which is not the case.

Let C_s be a leave of T different from C_0 (there are at least two leaves in T,

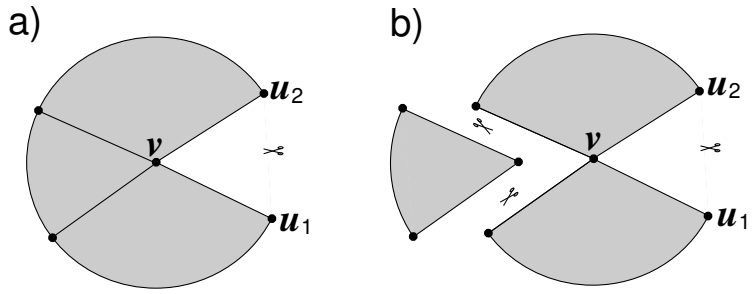

Figure 10: Illustration to the Case 2.1.
a) neighborhood of a rigid vertex of a split edge. b) neighborhood of a rigid vertex of a split edge with one piece cut off.

so such a leave exists). The map $\phi_i(D_i)$ is a submap of the van Kampen diagram D. Hence ∂C_s is a loop in D. Therefore, by assumption of the theorem on D, has length at least 2. So there are at least two vertices on ∂C_s. We claim that there is a vertex on ∂C_s that was not cut by (13). To show this consider the path P. Let $e_1, \dots, e_l$ be edges of ∂C_s in the order they appear in P. By Claim 3.1 e_1 and e_2 are consecutive edges of ∂C_s. Denote by u the terminus of e_1. If u was not cut then this is a vertex we are looking for. Assume now that u was cut. There are two cases here: either e_1 and e_2 are consecutive edges of P or they are not.

In the former case u was not cut in between e_1 and e_2, so it was cut in between two other edges (see Figure 11). In this event there exists a preimage u' of u which is a cut vertex in D_i. By Claim 1.2) u' is marked, but it cannot be marked as a preimage of a vertex from ∂C_s. This contradiction shows that u is cut in between e_1 and e_2.

Therefore, P contains a subpath $e_1 P_1 e_2$, where $P_1 = f_1 \dots f_l$ is a non-empty loop. Since C_s is a leave P_1 does not contain edges from boundaries ∂C_t. Hence P_1 consists only of edges from Γ. Observe that if P_1 does not contain a backtrack then it bounds a cell inside. Indeed, by definition for each edge e from Γ there are two different cells whose boundaries contain e. If $f_l \neq f_1^{-1}$ then one of the cells which contain f_1 on their boundaries is bounded by P_1. If $f_l = f_1^{-1}$ then the subpath

$f_2, \ldots, f_{l-1}$ is a loop in Γ and induction finishes the proof. Now if P_1 bounds a cell inside then D_i is not connected – contradiction. This contradiction shows that there is a backtrack in P_1. Hence there is a terminal edge cut in (13), which is impossible. This shows that u was not cut and hence it has a unique preimage v with respect to ϕ_i. v is unmarked by Claim 2.1). This proves Claim 4.

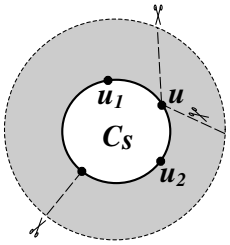

Figure 11: Non-cut vertex u on ∂C_s.

□

At this point we have (D_i, ϕ_i) satisfying properties P1-P3 and an unmarked vertex $v \in \overline{D}_i$ with the unique image in D. We are going to construct a new diagram D_{i+1} and a morphism $\phi_{i+1} : \overline{D}_{i+1} \to D$ satisfying properties P1-P3. Consider a subcomplex E_{i+1} of D generated by $\phi_i(\overline{D}_i)$ and $N_D(\phi_i(v))$ (it is connected, but might be not simply connected, so not a diagram). Let K_{i+1} be the subcomplex generated by elements from of $N_D(\phi_i(v))$ that do not belong to $\phi_i(\overline{D}_i)$ (i.e. $K_{i+1} = N_D(\phi_i(v)) - \phi_i(\overline{D}_i)$).

Claim 5. *There exists an extended diagram D_{i+1} and a sewing morphism $\phi_{i+1} : D_{i+1} \to E_{i+1}$ such that (D_{i+1}, ϕ_{i+1}) satisfies properties P1-P3.*

Proof of Claim 5.

Choose v to be an active vertex and assign $A(D_i) = \{v\}$. Consider cases from the proof of Claim 4.

Case 1. Let $k = 0$. Then the sewing morphism $\phi_i : \overline{D}_i \to \phi_i(\overline{D}_i)$ is an isomorphism. Since $\overline{D}_i$ is a diagram, it is simply connected, so is $\phi_i(\overline{D}_i)$. This

implies that there are no finite components in $\mathbb{R}^2 - \phi_i(\overline{D}_i)$, only the infinite one C_0. The submap K_{i+1} is finite, so it cannot fill in the whole region C_0. Hence there exists an edge $e \in \partial E_{i+1} \cap \partial K_{i+1}$ (see Figure 12).

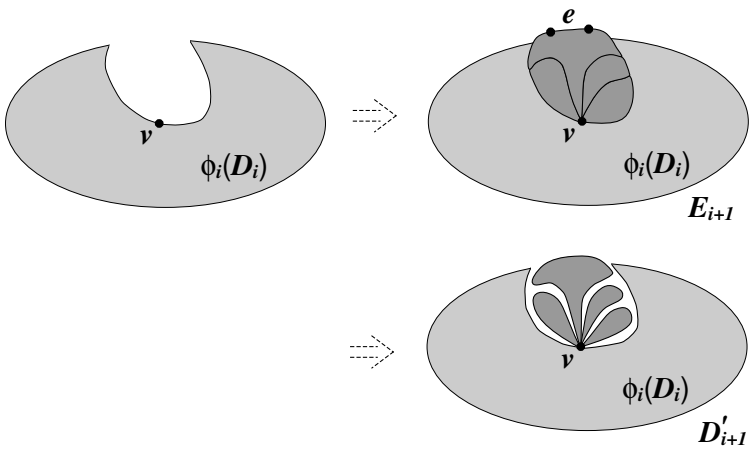

Figure 12: Diagrams $\phi_i(D_i)$, E_{i+1}, and D'_{i+1}.

Now we make a sequence of edge cuts to cut E_{i+1} as follows. We cut all necessary edges in K_{i+1} (not cutting the vertex v) into a bouquet B of free edges and cells attached to the rest of the diagram at the vertex v. Since there exists at least one edge in K_{i+1} on the boundary ∂E_{i+1} we can start the cutting process. Since D does not contain loops of length 1 we can make it into a bouquet without cutting the vertex v. We denote by D'_{i+1} the complex resulted from the cutting of E_{i+1}. From the construction D'_{i+1} is union of $\overline{D}_i$ and the bouquet B, hence it is a diagram.

Now, we fold edges in D'_{i+1} adjacent to v, if they are folded in E_{i+1}, and denote the result by D_{i+1}. Observe that the diagram D_{i+1} can be obtained from D_i as follows:

a) choose the vertex v (which is unmarked and non-active) and make it active;

b) attached finitely many cells and free edges to D_i at v;

c) fold some edges incident to v;

d) make v unmarked and non-active.

We claim that all these steps can be performed by the random extension B_S. The existence of the vertex v comes from Claim 4. Notice that in this case the vertex v was chosen in the proof of Claim 4 in such a way that $N_{\phi_i(\overline{D}_i)}(\phi_i(v))$ is a proper subcomplex of $N_D(\phi_i(v))$. Addition new free edges and cells is allowed in B_S since all the probabilities in S are non-zero. Therefore, even if v is the last unmarked vertex in D_i the extension B_S is allowed to add all required cells and free edges to D_i at v. Notice that any vertex $\partial K_{i+1} \cap \partial\overline{D}_i$ is unmarked. Hence folds of edges between cells in K_{i+1} and D_i are allowed by B_S too. Therefore D_{i+1} can be obtained from D_i by a finite number of application of B_S and the property P1 is satisfied.

D'_{i+1}, as well as D_{i+1}, is a cut of E_{i+1} which is a subcomplex of D. Define $\phi_{i+1} : \overline{D}_{i+1} \to D$ to be the corresponding sewing morphism. Hence we have the property P2. Again it is clearly true (from the way we constructed D_{i+1}) that ϕ_i is an isomorphism of $N_{D_{i+1}}(v)$ onto $N_D(\phi_{i+1}(v))$ which proves P3. This finishes the proof in Case 1.

Case 2.1. Let $k > 0$ and the sequence (13) has a terminal edge cut, say σ_l. In this case there exists an edge $e = (\bar{u}, \bar{v}) \in \phi_i(D_i)$ which is cut by σ_l into two edges $e_1 = (u_1, v)$ and $e_2 = (u_2, v)$ in $\overline{D}_i$. By Claim 4 (see Case 2.1) the vertex v is unmarked and $\phi_i(v) \neq \phi_i(v')$ for any vertex $v' \in \overline{D}_i$, so it can be chosen as the active vertex. It follows (see the proof of Claim 4, Case 2.1) that $K_{i+1} = \emptyset$ and the equality $\phi_i(\overline{D}_i) = E_{i+1}$ holds. In this case we construct the diagram D_{i+1} from D_i as follows:

a) choose the vertex v and make it active;

b) fold edges e_1 and e_2 in D_i and make the vertex v marked and non-active.

Notice that the vertices u_1 and u_2 are unmarked in D_i. Since the probabilities from S are non-zero and there are unmarked vertices in D_i, besides v, it follows that B_S

can add no cells and no free edges at $v \in D_i$. In this case B_S can fold edges e_1 and e_2 in D_i since endpoints of e_1 and e_2 are unmarked. So D_{i+1} satisfies the property P1. It follows from the construction that D_{i+1} is a cut of $E_{i+1} \subset D$. Let ϕ_{i+1} be the corresponding sewing morphism. Clearly the properties P2 and P3 holds.

Case 2.2. Let $k > 0$ and there is no terminal edge cut in (13). Let C_s be a leave in a forest $T(D_i, \phi_i)$ different from C_0. By Claim 4 there is an unmarked vertex $v \in \partial C_s$ that can be chosen as the active vertex. In this case K_{i+1} is not trivial (since C_s is a finite component). The vertex v is not the only unmarked vertex in D_i since all vertices on ∂C_s must be unmarked and the number of vertices on ∂C_s is not less than 2.

In this case E_{i+1} is obtained from $\phi_i(D_i)$ by adding some number of cells and free edges to the vertex v inside the component C_s. The sequence of cuts (13) cuts $\phi_i(D_i)$ into $\overline{D}_i$ starting (by definition) at some vertex from $\partial\phi_i(D_i)$. The path P from Claim 3 starts at some edge $e_0 \in \partial C_0$. The path P naturally defines the sequence of cuts of $\phi_i(D_i)$ which results in D_i. Since P starts on ∂C_0 there exists a sequence σ' of simple cuts starting at the boundary of C_0 and leading to the component C_s and stopping at a vertex w on ∂C_s. Moreover, we may assume that there are no simple cuts in σ' starting at vertices of ∂C_s (σ' corresponds to the initial path of P which reaches ∂C_s the first time). Then being on ∂C_s we can cut K_{i+1} into a bouquet of cells and free edges at the vertex v. After that we can make all cuts required to produce $\overline{D}_i$ from $\phi_i(D_i)$ (it is possible because all the needed boundary vertices of $\phi_i(D_i)$ are available to us now).

Denote the resulting diagram by D'_{i+1}. The diagram D'_{i+1} consists of $\overline{D}_i$ with the bouquet of free edges and cells attached at v. Finally, we fold the edges incident to v that are folded in E_{i+1}, then make v marked and non-active. Denote the resulting diagram by D_{i+1}. The argument similar to the one in Case 2.1 shows that D_{i+1} satisfies all of the properties P1-P3.

□

By Claims 4 and 5 if $\phi_i : \overline{D}_i \to D$ is not an isomorphism one can construct $\phi_{i+1} : \overline{D}_{i+1} \to D$ such that D_{i+1} has strictly more marked vertices than D_i (we do not fold marked vertices from D_i when constructing D_{i+1}). By P2 D_i is a cut of $\phi_i(D_i)$ which is a submap of D. Since every edge can be cut only once one has the following estimate on the number of edges $|E(D_i)| \leq 2|E(D)|$. Hence the number of vertices $|V(D_i)| \leq 4|E(D)|$ has. Hence $\phi_i : \overline{D}_i \to D$ is an isomorphism for some i.

□

Theorem 7.7. (Completeness theorem) *Let $\langle X; R\rangle$ be a reduced finite presentation. If none of the probabilities in S is zero then B_S is $\mathcal{L}$-complete relative to the mapping $D \to \overline{D}$, i.e., $\overline{\Phi}_{B_S} = \mathcal{L}$.*

Proof. Let D be an arbitrary van Kampen diagram over $\langle X; R\rangle$. Since $\langle X; R\rangle$ is reduced it follows that D does not contain loops of length 1 (otherwise some of the generators in X would be trivial in $G = \langle X; R\rangle$) and each cell in D has vertex-simple boundary (otherwise a presentation $\langle X; R\rangle$ could be R-split). Hence, the the result follows from Theorem 7.6.

□

7.3 Some properties of B_S

In this section we consider the random generator RG_χ defined in Section 6.4 relative to the basic extension $B = B_S$ defined in Section 7.1 and show that B_S satisfies properties (8), (9), and (10) from Section 6.4 and, therefore, functions X_n and K_n are random variables and the random generator RG_χ is correctly defined for B_S.

The starting diagram D_0 which is used throughout Section 7 contains no free edges or cells and, hence, equality (10) is satisfied.

Recall that an extended diagram D is a triple $(D, M(D), A(D))$ where $M(D)$ and $A(D)$ are sets of marked and active vertices of D respectively.

Lemma 7.8. *If $D_j = B_S(D_i)$ then*

$$(\chi(D_j) - \chi(D_i)) + (|M(D_j)| - |M(D_i)|) = 1. \tag{16}$$

Therefore, $0 \leq \chi(D_j) - \chi(D_i) \leq 1$ and condition (8) holds for B_S.

Proof. The basic extension B_S performs exactly one of the following actions. It either increases the geometric complexity χ of the input by 1 (when adds a cell or a free edge) or marks a vertex. Hence the result.

□

Proposition 7.9. Let L be the length of a longest relator in the given R-reduced presentation $\langle X; R\rangle$ and $D_0 = D_{m_0}, D_{m_1}, \ldots, D_{m_k}$ be a sequence of marked diagrams such that $D_{m_{i+1}} = B_S(D_{m_i})$. Then $\chi(D_{m_k}) \geq \frac{k}{L+1}$ and the condition (9) holds for B_S.

Proof. As proved in Lemma 7.8 $(\chi(D_{m_{i+1}}) - \chi(D_{m_i})) + (|M(D_{m_{i+1}})| - |M(D_{m_i})|) = 1$. Since $\chi(D_0) + |M(D_0)| = 0$ it follows that $\chi(D_{m_k}) + |M(D_{m_k})| = k$. Assume that $\chi(D_{m_k}) < \frac{k}{L+1}$. Then the number of vertices in D_{m_k} is not greater than $\frac{k}{L+1}L$. Therefore, the number of marked vertices $|M(D_{m_k})|$ is not greater than $\frac{k}{L+1}L$ and

$$\chi(D_{m_k}) + |M(D_{m_k})| < \frac{k}{L+1} + \frac{k}{L+1}L = k.$$

Obtained contradiction finishes the proof.

□

Lemma 7.10. *If probabilities in S are non-zero then for each diagram $D \in \mathcal{K}$ there exists $D^* = B_S(D)$ such that $\chi(D^*) - \chi(D) = 1$, so the condition (12) holds for B_S.*

Proof. A diagram D^* is obtained from D by adding a cell or a free edge at the active vertex of D.

□

Corollary 7.11. If probability in S are non-zero then B_S satisfies all properties (8)-(10) and (12). In particular, $\{Q_n\}_{n\in\mathbb{N}}$ and $\{\widehat{Q}_n\}_{n\in\mathbb{N}}$ are complete sets of termination conditions.

Corollary 7.12. The sets $\mathcal{K}_i = \{D \in \mathcal{K} \mid \chi(D) = i\}$ and $\mathcal{L}_i = \{D \in \mathcal{L} \mid \chi(D) = i\}$ form partitions of $\mathcal{K}$ and $\mathcal{L}$ respectively. Therefore, the asymptotic densities $\rho_{\mathcal{K}}$ and $\rho_{\mathcal{L}}$ on $\mathcal{K}$ and $\mathcal{L}$ (with respect to B_S) are well-defined.

8 Asymptotic properties of diagrams

In this section we describe several asymptotic properties of diagrams relative to the basic extension B_S and, the sequence of termination conditions $\{\widehat{Q}_i\}_{i\in\mathbb{N}}$. In particular, we discuss asymptotic behavior of the length of the perimeter and the depth of diagrams relative to their size.

8.1 Properties related to RG_χ

Let $\langle X; R\rangle$ be a reduced finite presentation, $\mathcal{K}$ the set of all marked diagrams, $\mathcal{L}$ the set of all diagrams over $\langle X; R\rangle$, $\mathcal{K}_n = \{D \in \mathcal{K} \mid \chi(D) = n\}$, and $\mathcal{L}_n = \{\overline{D} \mid D \in \mathcal{K}_n\}$.

In Section 7.3 we introduced a discrete probability $P_{\mathcal{L}_n}$ on the set $\mathcal{L}_n$. The probability $P_{\mathcal{L}_n}$ depends on the basic extension operator B_S from Section 7.1. Below we freely use notation from Section 6 and 7.

If $D_j = B_S(D_k)$ then $\overline{D_j}$ can be obtained from $\overline{D_k}$ by either adding of a free edge or cell, or making a few foldings. Thus going along a trajectory λ the basic extension B_S adds some cells and free edges (we refer to them as *units*). Denote by

$\mathcal{U}_i = \mathcal{U}_i(\lambda)$ the ith unit that was added by B_S along λ. Formally one can express this as

$$\mathcal{U}_i = \mathcal{U}_i(\lambda) = D(\lambda_{X_i(\lambda)}) - D(\lambda_{X_i(\lambda)-1}),$$

where $X_i = \min\{j \mid \chi(D(\lambda_j)) = i\}$.

Now we can introduce random variables $\xi_i : \Lambda \to \{0, 1\}$, $i \in \mathbb{N}$ defined on $\lambda \in \Lambda$ as follows:

$$\xi_i(\lambda) = \begin{cases} 0, & \text{if } \mathcal{U}_i(\lambda) \text{ in } D(\lambda_k) \text{ shares an edge with } \partial D(\lambda_k) \text{ for every } k \geq X_i(\lambda); \\ 1, & \text{otherwise.} \end{cases}$$

Notice that if $\xi_i(\lambda) = 0$ then $\mathcal{U}_i(\lambda)$ has depth one in $D(\lambda_k)$ for every $k \geq X_i(\lambda)$. Similarly one can define ξ_i on $V(\mathcal{T})$. For $\theta \in V(\mathcal{T})$ with $\chi(D(\theta)) \geq i$ denote by $\mathcal{U}_i(\theta)$ the ith unit that B_S added to $D(\theta)$ going along the path θ. Put

$$\xi_i(\theta) = \begin{cases} 0, & \chi(D(\theta)) < i \text{ or } \mathcal{U}_i(\theta) \text{ shares an edge with } \partial D(\theta); \\ 1, & \text{otherwise.} \end{cases}$$

Clearly, if $\lambda = (\lambda_0, \lambda_1, \lambda_2 \ldots)$ than for any $s \leq t$ the following inequality holds

$$\xi_i(\lambda_s) \leq \xi_i(\lambda_t) \leq \xi_i(\lambda). \tag{17}$$

Moreover, $\xi_i(\lambda_r) = \xi_i(\lambda)$ for some r. We denote the minimal such r by $r_i(\lambda)$.

Lemma 8.1. *For any $i \in \mathbb{N}$ the function ξ_i is a random variable on Λ.*

Proof. Since each function ξ_i takes values from $\{0, 1\}$ it is enough to show that $\xi_i^{-1}(1) = \{\overline{\lambda} \mid \xi_i(\lambda) = 1\}$ is measurable in $\Lambda_{\mathcal{T}}$. Let $\lambda \in \xi_i^{-1}(1)$ and $r = r_i(\lambda)$. Then $\xi_i(\lambda_r) = 1$ and for any $\lambda' \in Cone(\lambda_r)$ $\xi_i(\lambda') = 1$. Thus,

$$\xi_i^{-1}(1) = \cup_{\lambda \in \xi_i^{-1}(1)} Cone(\lambda_{r(\lambda)})$$

is a countable union of cones, hence it is measurable, as claimed.

□

Lemma 8.2. *Let $\theta \in V_{\widehat{Q}_n}$. Then for $i \leq n$*

$$P_{\widehat{Q}_n}(\xi_i(\theta) = 1) < \frac{1}{2}. \tag{18}$$

Moreover, for any sequence $(b_1, \ldots, b_n)$ such that $b_1, \ldots, b_n \in \{0, 1\}$,

$$P_{\widehat{Q}_n}(\xi_i(\theta) = 1 \mid \xi_j(\theta) = b_j \text{ where } j = 1, \ldots, i-1, i+1, \ldots, n) < \frac{1}{2}. \tag{19}$$

Proof. Let $\theta = e_1 e_2 \ldots e_m \in V_{\widehat{Q}_n}$ and $\lambda = (\lambda_0, \lambda_1, \lambda_2, \ldots) \in Cone(\theta)$. Notice that $\lambda_i = e_1 \ldots e_i$, for $i = 0, \ldots, m$. For $i = 0, \ldots, m$ define

$$X_i(\theta) = \min\{j = 1, \ldots, m \mid \chi(D(\lambda_j)) = i\}.$$

Clearly, $X_i(\theta)$ is the step at which the ith unit $\mathcal{U}_i = \mathcal{U}_i(\lambda)$ was added to the diagram. Let $D = D(\lambda_{X_i(\theta)})$ and v_i the active vertex of D, so $\mathcal{U}_i$ is attached to v_i.

We define $Y_i(\theta)$ to be the least index $k \in \{1, \ldots, m\}$ such that v_i is marked in $D(\lambda_k)$ and undefined otherwise. At the step $Y_i(\theta)$ the basic extension B_S folds some edges adjacent to v_i in $D(\lambda_{Y_i(\theta)})$. Notice that if Y_i is not defined on θ then $\xi_i(\theta) = 0$. Now, using a total probability formula:

$$P_{\widehat{Q}_n}(\xi_i(\theta) = 1) = P_{\widehat{Q}_n}(\xi_i(\theta) = 1 \mid Y_i \text{ is defined on } \theta) P_{\widehat{Q}_n}(Y_i \text{ is defined on } \theta) +$$

$$+ P_{\widehat{Q}_n}(\xi_i(\theta) = 1 \mid Y_i \text{ is not defined on } \theta) P_{\widehat{Q}_n}(Y_i \text{ is not defined on } \theta) =$$

$$= P_{\widehat{Q}_n}(\xi_i(\theta) = 1 \mid Y_i \text{ is defined on } \theta) P_{\widehat{Q}_n}(Y_i \text{ is defined on } \theta) \leq$$

$$\leq P_{\widehat{Q}_n}(\xi_i(\theta) = 1 \mid Y_i \text{ is defined on } \theta).$$

Therefore, we may assume in the statement of the lemma that Y_i is defined on θ. Denote by E_i the following event: one of the edges in $\mathcal{U}_i(\theta)$ adjacent to v_i belongs to $\partial D(\lambda_{Y_i(\theta)})$. Observe that E_i implies $\xi_i(\theta) = 0$. Clearly

$$P_{\widehat{Q}_n}(\xi_i(\theta) = 1) = 1 - P_{\widehat{Q}_n}(\xi_i(\theta) = 0) \leq 1 - P_{\widehat{Q}_n}(E_i).$$

Now, by formula of total probability

$$P_{\widehat{Q}_n}(E_i) =$$

$$= P_{\widehat{Q}_n}(E_i \mid \mathcal{U}_i \text{ is a cell}) P_{\widehat{Q}_n}(\mathcal{U}_i \text{ is a cell}) +$$

$$+ P_{\widehat{Q}_n}(E_i \mid \mathcal{U}_i \text{ is a free edge}) P_{\widehat{Q}_n}(\mathcal{U}_i \text{ is a free edge}).$$

Observe that

$$P_{\widehat{Q}_n}(E_i \mid \mathcal{U}_i \text{ is a free edge}) = 1$$

and

$$P_{\widehat{Q}_n}(\mathcal{U}_i \text{ is a free edge}) + P_{\widehat{Q}_n}(\mathcal{U}_i \text{ is a cell}) = 1.$$

Thus

$$P_{\widehat{Q}_n}(E_i) > P_{\widehat{Q}_n}(E_i \mid \mathcal{U}_i \text{ is a cell})$$

unless $P_{\widehat{Q}_n}(E_i \mid \mathcal{U}_i \text{ is a cell}) = P_{\widehat{Q}_n}(E_i) = 1$.

Recall that B_s, when attaching a new cell to the current diagram D, chooses cells from R_{sym} uniformly and independently to the previous steps. We represent R_{sym} as a disjoint union of sets

$$R_{sym} = \cup_{x \in X \cup X^{-1}} R^{(x)},$$

where $R^{(x)}$ consists of all relators starting with x. It is easy to see (since $R_{sym}^{-1} =$

R_{sym}) that for any presentation R and for any generator $x \in X \cup X^{-1}$

$$\frac{|R^{(x)}|}{|R_{sym}|} \leq \frac{1}{2}. \tag{20}$$

Hence, for any fixed $x \in X^{\pm 1}$ and a uniformly chosen $r \in R_{sym}$ the probability that $x^{-1}r$ is not freely reduced is at most $\frac{1}{2}$. Thus

$$P_{\widehat{Q}_n}(E_i \mid \mathcal{U}_i \text{ is a cell}) \geq \frac{1}{2}.$$

Therefore, $P_{\widehat{Q}_n}(\xi_i = 1) \leq 1 - P_{\widehat{Q}_n}(E_i) < \frac{1}{2}$.

To see that (19) holds we observe that the argument above is valid for any choice of $\{b_i\}_{i\in\mathbb{N}}$. Indeed, the fold of the edges of $\mathcal{U}_i$ adjacent to v_i depends only on the choice of a cell from R_{sym} which we attach to v_i and the edges on the boundary $\partial D(\lambda_{Y_i})$ adjacent to v_i. Since the cell $\mathcal{U}_i$ is chosen uniformly and independently its choice does not affect the inequality (18). Notice also that the inequality (20) holds for any labels of the edges adjacent to v_i.

□

Define $S_n(\theta) = \sum_{i=1}^{n} \xi_i(\theta)$, for $\theta \in V(\mathcal{T})$.

Lemma 8.3. *Let $\theta \in V_{\widehat{Q}_n}$. Then the length $l(D(\theta))$ of the perimeter of $D(\theta)$ satisfies the following inequality*

$$l(D(\theta)) \geq n - S_n(\theta).$$

Proof. Observe that n is a total number of units in $D(\theta)$ and S_n is a total number of units that do not have edges on the boundary of $D(\theta)$. So $n - S_n(\theta)$ is a number of units that have at least one edge on the boundary, hence the result.

□

Lemma 8.4. *Let $0 < \alpha < 1$. Then*

$$P_{\widehat{Q}_n}\left(S_n \geq \frac{(1+\alpha)}{2}n\right) \leq \exp\left(-\frac{3\alpha^2}{(12+4\alpha)}n\right) \tag{21}$$

Proof. Let Z_n be a binomial random variable with parameters $(n, \frac{1}{2}$. It follows from Lemma 8.2 that

$$P_{\widehat{Q}_n}(S_n \geq i) \leq p(Z_n \geq i).$$

By Chernoff inequality

$$p(Z_n \geq \mathbb{E}Z_n + t) \leq \exp\left(-\frac{t^2}{2(\mathbb{E}Z_n + t/3)}\right).$$

If $t = \alpha\mathbb{E}Z_n$, where $0 < \alpha < 1$, then

$$\begin{aligned} p\left(Z_n \geq (1+\alpha)\mathbb{E}Z_n\right) &\leq \exp\left(-\tfrac{\alpha^2(\mathbb{E}Z_n)^2}{2(\mathbb{E}Z_n + \alpha\mathbb{E}Z_n/3)}\right) = \\ &= \exp\left(-\tfrac{3\alpha^2}{(6+2\alpha)}\mathbb{E}Z_n\right), \end{aligned}$$

and, since $\mathbb{E}Z_n = \frac{n}{2}$, we get

$$P_{\widehat{Q}_n}\left(S_n \geq \frac{(1+\alpha)}{2}n\right) \leq p\left(Z_n \geq \frac{(1+\alpha)}{2}n\right) \leq \exp\left(-\frac{3\alpha^2}{(12+4\alpha)}n\right)$$

as required.

□

Theorem 8.5. *Let $0 < \alpha < 1$. Then the following holds:*

1) *Let $\mathcal{K}'_{n,\alpha} = \{D \in \mathcal{K}_n \mid l(D) < \frac{(1-\alpha)}{2}n\} \subseteq \mathcal{K}_n$. Then $P_{\mathcal{K}_n}(\mathcal{K}'_{n,\alpha}) \to 0$ exponentially fast as $n \to \infty$.*

2) *Let $\mathcal{L}'_{n,\alpha} = \{D \in \mathcal{L}_n \mid l(D) < \frac{(1-\alpha)}{2}n\} \subseteq \mathcal{L}_n$. Then $P_{\mathcal{L}_n}(\mathcal{L}'_{n,\alpha}) \to 0$ exponentially fast as $n \to \infty$.*

Proof. Recall that

$$P_{\mathcal{K}_n}(D) = \sum_{\theta \in V_{\widehat{Q}_n} | D = D(\theta)} P_{\widehat{Q}_n}(\theta).$$

Clearly, $\theta \in V'_{\widehat{Q}_n}$ if and only if $D(\theta) \in \mathcal{K}'_n$ and, thus, $P_{\mathcal{K}_n}(\mathcal{K}'_{n,\alpha}) = P_{\widehat{Q}_n}(V'_{\widehat{Q}_n})$. So, it suffices to show that $P_{\widehat{Q}_n}(V'_{\widehat{Q}_n}) \to 0$ exponentially fast. By Lemma 8.3 $l(D(\theta)) \geq n - S_n(\theta)$. Hence

$$\begin{aligned} 0 \leq P_{\widehat{Q}_n}\left(l(D(\theta)) < \tfrac{(1-\alpha)}{2} n\right) &\leq P_{\widehat{Q}_n}(n - S_n(\theta) < \tfrac{(1-\alpha)}{2} n) = \\ &= P_{\widehat{Q}_n}(S_n(\theta) \geq \tfrac{(1+\alpha)}{2} n). \end{aligned}$$

By (21) we have

$$P_{\widehat{Q}_n}\left(S_n(\theta) \geq \frac{(1+\alpha)}{2} n\right) \leq \exp\left(-\frac{3\alpha^2}{(12+4\alpha)} n\right) \to 0.$$

Hence the result.

Similar argument proves 2).

□

Corollary 8.6. Let $\langle X; R \rangle$ be an R-reduced presentation and $\mathcal{L}$ be a set of representatives of all van Kampen diagrams over $\langle X; R \rangle$ (up to isomorphism). Put

$$\mathcal{L}' = \{D \mid l(D) \geq \tfrac{1}{4}\chi(D)\}.$$

Then

$$\rho_{\mathcal{L}}(\mathcal{L}') = \lim_{i \to \infty} P_{\mathcal{L}_i}(\mathcal{L}_i \cap \mathcal{L}') = 1.$$

Moreover, $P_{\mathcal{L}_i}(\mathcal{L}_i \cap \mathcal{L}') \to 1$ exponentially fast. Thus the set of all diagrams over $\langle X; R \rangle$ with linear isoperimetric function (with coefficient $\frac{1}{4}$) is strongly generic with respect to the asymptotic density.

Let D be a diagram and d be the chain-distance metric on the set of free edges

and cells. We define a ball $B_D(\mathcal{U}_i, r)$ in D with a center at the ith unit $\mathcal{U}_i$ of radius r to be a subcomplex of D generated by $\{\mathcal{U}_j \mid d(\mathcal{U}_i, \mathcal{U}_j) \leq r\}$.

Lemma 8.7. *Let $\theta \in V_{\widehat{Q}_n}(\mathcal{T})$. If $\xi_i(\theta) = 0$ (where $i < n$) then $\mathcal{U}_i(\theta)$ has depth one in $D(\theta)$. Moreover, if there exists an index j such that $\mathcal{U}_j(\theta) \in B_{D(\theta)}(\mathcal{U}_i, r-1)$ and $\xi_j(\theta) = 0$ then the depth of $\mathcal{U}_i(\theta)$ in $D(\theta)$ is not greater than r.*

Proof. Let $D = D(\theta)$. By definition of ξ_i if $\xi_i(\theta) = 0$ then $\mathcal{U}_i$ shares an edge with ∂D and, hence, it has depth one in D.

Similarly, if $\mathcal{U}_j \in B_D(\mathcal{U}_i, r-1)$ and $\xi_j = 0$ then $\mathcal{U}_j$ has depth one in D and by definition of $B_D(\mathcal{U}_i, r-1)$ the chain-distance between CU_i and CU_j is not greater than $r-1$. Hence the result.

□

Proposition 8.8. Let δ be the depth function on diagrams. Then the expectation $\mathbb{E}\delta(D(\theta))$ of the function $\delta(D(\theta))$ on $(V_{\widehat{Q}_n}, P_{\widehat{Q}_n})$ is not greater than $\log n + 2$.

Proof. Let $\theta \in V_{\widehat{Q}_n}(\mathcal{T})$. For $i = 1, \ldots, n$ define

$$d_i(\theta) = \max\{r \mid B(\mathcal{U}_i, r) \text{ does not contain } \mathcal{U}_j \text{ such that } \xi_j(\theta) = 0\} + 1.$$

Notice that if $r < n$ then $|B(\mathcal{U}_i, r)| \geq r + 1$. Then from Lemma 8.2 it follows that

$$P_{\widehat{Q}_n}(d_i(\theta) \geq r) \leq \frac{1}{2^r}.$$

Define a random variable $d(\theta) = \max\{d_i(\theta) \mid i = 1, \ldots, n\}$. From Lemma 8.7 and the definition of d_i it follows that

$$\delta(D(\theta)) \leq d(\theta)$$

and hence

$$\mathbb{E}\delta \leq \mathbb{E}d.$$

On the other hand

$$\begin{aligned} P_{\widehat{Q}_n}(\ d(\theta) \geq r\ ) = P_{\widehat{Q}_n}(\ \textstyle\bigvee_{i=1,\ldots,n}(d_i(\theta) \geq r)\ ) \leq \\ \leq \textstyle\sum_{i=1,\ldots,n} P_{\widehat{Q}_n}(\ d_i(\theta) \geq r\ ) \leq \frac{n}{2^r} \end{aligned} \tag{22}$$

Hence,

$$P_{\widehat{Q}_n}(d(\theta) - \log n \geq r) = P_{\widehat{Q}_n}(d(\theta) \geq r + \log n) \leq \frac{n}{2^{r+\log n}} = \frac{1}{2^r},$$

so

$$\mathbb{E}(d - \log n) \leq \sum_{r=1}^{\infty} \frac{r}{2^r} = 2.$$

Thus, $\mathbb{E}d \leq \log n + 2$, as claimed.

□

Theorem 8.9. *The following holds:*

1) Let $\mathcal{K}_n'' = \{D \in \mathcal{K}_n \mid \delta(D) < 2\log n\} \subseteq \mathcal{K}_n$. *Then* $P_{\mathcal{K}_n}(\mathcal{K}_n'') \to 1$ *as* $n \to \infty$.

2) Let $\mathcal{L}_n'' = \{D \in \mathcal{L}_n \mid \delta(D) < 2\log n\} \subseteq \mathcal{L}_n$. *Then* $P_{\mathcal{L}_n}(\mathcal{L}_n'') \to 1$ *as* $n \to \infty$.

Proof. Let

$$V_{\widehat{Q}_n}'' = \{\theta \in V_{\widehat{Q}_n} \mid \delta(D(\theta)) \leq 2\log n\}.$$

In Proposition 8.8 we defined a random variable $d(\theta)$ on $V_{\widehat{Q}_n}$ such that

$$d(\theta) \geq \delta(D(\theta)) \ \ \textit{and} \ \ P_{\widehat{Q}_n}(\ d(\theta) \geq r\ ) \leq \frac{n}{2^r}.$$

This implies that

$$1 \geq P_{\widehat{Q}_n}(V''_{\widehat{Q}_n}) \geq P_{\widehat{Q}_n}(d(D(\theta)) \leq 2\log n) = 1 - P_{\widehat{Q}_n}(d(D(\theta)) \geq 2\log n) \geq 1 - \frac{1}{n} \to 1$$

as n tends to ∞. Recall that

$$P_{\mathcal{K}_n}(D) = \sum_{\theta \in V_{\widehat{Q}_n}, D=D(\theta)} P_{\widehat{Q}_n}(\theta).$$

Clearly, $\theta \in V''_{\widehat{Q}_n}$ if and only if $D(\theta) \in \mathcal{K}''_n$. Thus,

$$P_{\mathcal{K}_n}(\mathcal{K}''_n) = P_{\widehat{Q}_n}(V''_{\widehat{Q}_n}) \to 1$$

as n tends to infinity.

A similar argument proves 2).

□

Theorem 8.10. *Let $\langle X; R\rangle$ be an R-reduced presentation and $0 < \alpha < 1$. The following holds:*

1) Let $\mathcal{K}'''_{n,\alpha} = \{D \in \mathcal{K}_n \mid \delta(D) < 2\log n \ \&\ l(D) \geq \frac{(1-\alpha)}{2} n\} \subseteq \mathcal{K}_n$. Then $P_{\mathcal{K}_n}(\mathcal{K}'''_{n,\alpha}) \to 1$ as $n \to \infty$.

2) Let $\mathcal{L}'''_{n,\alpha} = \{D \in \mathcal{L}_n \mid \delta(D) < 2\log n \ \&\ l(D) \geq \frac{(1-\alpha)}{2} n\} \subseteq \mathcal{L}_n$. Then $P_{\mathcal{L}_n}(\mathcal{L}'''_{n,\alpha}) \to 1$ as $n \to \infty$.

Proof. Follows from equalities $\mathcal{K}'''_{n,\alpha} = \mathcal{K}'_{n,\alpha} \cap \mathcal{K}''_n$ and $\mathcal{L}'''_{n,\alpha} = \mathcal{L}'_{n,\alpha} \cap \mathcal{L}''_n$ and Theorems 8.5 and 8.9.

□

Corollary 8.11. Let $\langle X; R\rangle$ be an R-reduced presentation. Let

$$\mathcal{K}'' = \{D \in \mathcal{K} \mid \delta(D) < 2\log \chi(D) \ \&\ l(D) \geq \tfrac{1}{2}\chi(D)\} \subseteq \mathcal{K},$$

$$\mathcal{L}'' = \{D \in \mathcal{L} \mid \delta(D) < 2\log\chi(D) \ \&\ l(D) \geq \tfrac{1}{2}\chi(D)\} \subseteq \mathcal{L}.$$

Then $\rho_{\mathcal{K}}(\mathcal{K}'') = 1$ and $\rho_{\mathcal{L}}(\mathcal{L}'') = 1$.

Proof. Take $\alpha = \frac{1}{2}$ and apply Theorem 8.10.

□

9 Generic properties of trivial words

In this section we investigate properties of random trivial words over $\langle X; R\rangle$.

9.1 Random trivial words

Denote by $WP(X;R)$ the set of all cyclic words representing the identity of the group $G = \langle X; R\rangle$. In this section we define a discrete probability measure on $WP(X;R)$.

Recall that $\mathcal{L}_n$ is a set of all van Kampen diagrams over $\langle X; R\rangle$ of a size n and $P_{\mathcal{L}_n}$ is a discrete probability measure on $\mathcal{L}_n$. Denote by CW_i (for $i \in \mathbb{N}$) the set of boundary labels (as cyclic words) of diagrams from $\mathcal{L}_i$ and by $\overline{CW}_n$ the union

$$\overline{CW}_n = \cup_{i=1}^{n} CW_i.$$

It follows from van Kampen Lemma that

$$WP(X;R) \ = \ \cup_{i=1}^{\infty} CW_i \ = \ \cup_{i=1}^{\infty} \overline{CW}_i.$$

Clearly,

$$\overline{CW}_1 \subseteq \overline{CW}_2 \subseteq \overline{CW}_3 \subseteq \ldots.$$

One can induce probability measures from $(\mathcal{L}_n, P_{\mathcal{L}_n})$ onto the sets CW_n and

$\overline{CW_n}$ as follows. For $S \subseteq CW_n$ and $S' \subseteq \overline{CW_n}$ put

$$P_{CW_n}(S) = P_{\mathcal{L}_n}(\{D \in \mathcal{L}_n \mid \text{ the boundary label of } D \text{ belongs to } S\}),$$

$$P_{\overline{CW}_n}(S') = \frac{\sum_{i=1}^{n} P_{CW_i}(S' \cap CW_i)}{n}.$$

It is easy to check that P_{CW_n} and $P_{\overline{CW}_n}$ are discrete probability measures on CW_n and $\overline{CW}_n$.

Using the probability on the sets $\overline{CW}_n$ one can define an asymptotic density of the subsets of $WP(X;R)$ as follows. For $S \subseteq WP(X;R)$ put

$$\rho_{WP}(S) = \lim_{n\to\infty} P_{\overline{CW}_n}(S \cap \overline{CW}_n).$$

One can describe the probability measure P_{CW_n} in terms of the following random generator.

Algorithm 9.1. (*Random Generator I of trivial words*)

INPUT. A number $n \in \mathbb{N}$.

OUTPUT. A word w such that $w =_G 1$.

COMPUTATIONS.

1) Run RG_χ to generate a random diagram D of size n.

2) Output the boundary label of D.

The probability measure $P_{\overline{CW}_n}$ can be described in terms of the following random generator.

Algorithm 9.2. (*Random Generator II of trivial words*)

INPUT. A number $n \in \mathbb{N}$.

OUTPUT. A word w such that $w =_G 1$.

COMPUTATIONS.

1) Generate randomly and uniformly a number i from the set $\{1, \ldots, n\}$.

1) Run RG_χ to generate a random diagram D of size i.

2) Output the boundary label of D.

In view of the random generators above the probability measures P_{CW_n} and $P_{\overline{CW}_n}$ are very natural.

9.2 Generic properties of trivial words

In this section we study generic properties of words representing the trivial element of $G = \langle X; R \rangle$.

Fix α such that $0 < \alpha < 1$ and define

$$\overline{CW}_{n,\alpha} = \{w \in \overline{CW}_n \mid w \text{ is a boundary label of some } D \in \cup_{i=1}^{n} \mathcal{L}'''_{i,\alpha}\}.$$

Theorem 9.3. *Let $G = \langle X; R \rangle$. The following holds:*

$$P_{\overline{CW}_n}(\overline{CW}_{n,\alpha}) \to 1 \text{ as } n \to \infty.$$

Proof. By definition of $P_{\overline{CW}_n}$ and $\overline{CW}_{n,\alpha}$ we have

$$P_{\overline{CW}_n}(\overline{CW}_{n,\alpha}) = \frac{1}{n} \sum_{i=1}^{n} P_{CW_i}(\overline{CW}_{n,\alpha} \cap CW_i) =$$

$$= \frac{1}{n} \sum_{i=1}^{n} P_{CW_i}(\{w \in CW_i \mid w \text{ is a boundary label of some } D \in \mathcal{L}'''_{i,\alpha}\}) =$$

$$= \frac{1}{n} \sum_{i=1}^{n} P_{\mathcal{L}_i}(\mathcal{L}'''_{i,\alpha}). \tag{23}$$

Now, if we denote $\sum_{i=1}^{n} P_{\mathcal{L}_i}(\mathcal{L}'''_{i,\alpha})$ by a_n and put $b_n = n$ then (23) becomes equal to

$\frac{a_n}{b_n}$. Notice that

$$\frac{a_{n+1} - a_n}{b_{n+1} - b_n} = P_{\mathcal{L}_i}(\mathcal{L}'''_{i,\alpha}).$$

Since $b_n = n$ is strictly increasing with n and tending to infinity, and, as proved in Theorem 8.10, $\lim_{i\to\infty} P_{\mathcal{L}_i}(\mathcal{L}'''_{i,\alpha}) = 1$ we can apply Stolz-Cesaro theorem and obtain

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 1$$

and, hence,

$$\lim_{n\to\infty} P_{\overline{CW}_n}(\overline{CW}_{n,\alpha}) = 1.$$

□

Let

$$CW^{(\alpha)} = \cup_{i=0}^{\infty} \overline{CW}_{i,\alpha}.$$

Hence, $\rho_{WP}(CW^{(\alpha)}) = 1$.

Theorem 9.4. *Let $\langle X; R\rangle$ be a finite symmetrized reduced presentation and $G = \langle X; R\rangle$. Then the following holds.*

1) The time complexity function for Algorithm $\mathcal{A}$ (the decision algorithm for the word problem in G) on the set of inputs $w \in CW^{(\alpha)}$ is bounded from above by the polynomial

$$O(|w|^{2+2\log L(R)}).$$

2) The time complexity function for Algorithm $\mathcal{B}$ (the algorithm for the search word problem in G) on the set of inputs $w \in CW^{(\alpha)}$ is bounded by the polynomial

$$O(|w|^{4+4\log L(R)}).$$

Proof. Denote $\frac{2}{1-\alpha}$ by β. Let w be an arbitrary word in $CW^{(\alpha)}$. Then w is a

boundary label of some $D \in \cup_{i=1}^{\infty} \mathcal{L}'''_{i,\alpha}$. Assume that $D \in \mathcal{L}'''_{n,\alpha}$ for some $n \in \mathbb{N}$. It follows from the definition of the sets $\mathcal{L}'''_{i,\alpha}$ that $n < \frac{2|w|}{1-\alpha} = \beta|w|$ and

$$\delta(D) < 2\log n < 2\log \frac{2|w|}{1-\alpha} < 2\log\beta + 2\log|w|. \tag{24}$$

By Theorem 5.3 the number of steps required for Algorithm $\mathcal{A}$ to terminate on the input w is bounded from above by

$$O(\delta(w)|w| \cdot L(R)^{\delta(w)} \log(|w|L(R)),$$

where $\delta(w)$ is a depth of w and $L(R)$ is a total length of R. It follows that $\delta(w) \leq \delta(D) < 2\log\beta + 2\log|w|$. Now the formula above becomes

$$O(2(\log\beta + \log|w|)|w| \cdot L(R)^{2\log\beta + 2\log|w|} \log(|w|L(R)) =$$

$$= O(|w|^2 L(R)^{2\log|w|}) = O(|w|^{2+2\log L(R)}).$$

This proves 1).

By Theorem 5.9 the number of steps required for Algorithm $\mathcal{B}$ to terminate on the input w is bounded from above by

$$O(|w|^2 L(R)^{2\delta(w)}(2|w| + \delta(w)M(R))^2),$$

where $M(R) = \max\{|r| \mid r \in R\}$. From (24) we deduce that

$$O(|w|^2 L(R)^{4\log\beta + 4\log|w|}(2|w| + (2\log\beta + 2\log|w|)M(R))^2) =$$

$$O(|w|^4 L(R)^{4\log|w|}) = O(|w|^{4+4\log L(R)}).$$

□

10 Comparison with standard techniques

In this section we shortly compare Algorithm $\mathcal{A}$ with the general techniques for the Word search problem such as Todd-Coxeter procedure and the total enumeration of $gp_F(R)$. The Knuth-Bendix-like procedures are harder to compare since they dynamically change the presentation of a group, so we omit them.

10.1 Todd-Coxeter algorithm

Let $\langle X; R\rangle$ be a finite symmetrized presentation and $G = \langle X; R\rangle$. Let $\Gamma_0 = \Gamma(\varepsilon)$ be an X-digraph with one vertex (which is a base vertex) denoted by v_0 and no edges. The Todd-Coxeter algorithm works the following way. It starts with Γ_0 and applies R-extensions until there is a loop starting at the base point v_0 labelled with w. Below we are looking for an upperbound for the worst case time complexity for Todd-Coxeter algorithm.

Let D be a van Kampen diagram, v_0 a vertex in ∂D, and w a boundary label of D which is read starting at v_0 in a counterclockwise direction. Denote by $\overline{\delta}(D)$ the depth $\delta_{v_0}(D)$ of D with respect to the vertex v_0 and by $\overline{\delta}(w)$ the minimum among all such diagrams D.

The next proposition is analogous to Proposition 4.12.

Proposition 10.1. Let D be a diagram with a boundary label w, $m = \delta(D)$, and $\phi : \Gamma(w) \to \partial D$ be a morphism. Then there exists a morphism of 2-complexes $\psi : D \to \mathcal{C}^{(m)}(\Gamma_0)$ such that the following diagram commutes.

$$\begin{array}{ccc} \Gamma_0 & \xrightarrow{\phi} & D \\ & \overset{\phi_{\mathcal{C}}}{\searrow} & \downarrow{\scriptstyle \psi} \\ & & \mathcal{C}^{(m)}(\Gamma_0) \end{array}$$

Proof. One can prove the assertion of the proposition in a fashion similar to the

proof of Proposition 4.12.

□

Corollary 10.2. Let $\langle X; R\rangle$ be a finite symmetrized presentation, $G = \langle X; R\rangle$, and w be a word representing identity in G. The upper bound for the worst case time complexity of Todd-Coxeter procedure is

$$O(L(R)^{\overline{\delta}}).$$

So, the fraction of uppebounds of time-complexities of Algorithm $\mathcal{A}$ and the Todd-Coxeter procedure can be roughly estimated by

$$|w|L(R)^{\delta-\overline{\delta}}.$$

Clearly, for each word $w \in gp_F(R)$ we have $\overline{\delta}(w) \geq \delta(w)$, but it is hard to say how large (generically or on average) the difference $\overline{\delta}(w) - \delta(w)$ is. Note that it is easy to construct a series of words for which Todd-Coxeter has exponential time complexity and Algorithm $\mathcal{A}$ is linear. For instance, this happens for $G = \langle a, b; [a, b]\rangle$ and $w_i = (ab)^i(a^{-1}b^{-1})^i$. Since G is aspheric the reduced diagram for w_i is unique and it is easy to see that it consists of i diagonal blocks in the first quarter of the grid. Therefore, $\overline{\delta}(w_i) = i$ and $\delta(w_i) = 1$.

We performed series of experiments for different classes of groups (mostly one-relator groups) and the obtained the following results. For most of the randomly generated words $w \in gp_F(R)$ $\delta(w) = 1$ and $\delta(\overline{w}) = \log|w|$.

10.2 Total enumeration of $gp_F(R)$

Let $G = \langle X; R\rangle$ and $w = w(X)$. For $k \in \mathbb{N}$ define

$$C_k = \{\prod_{i=1}^{m} c_i^{-1} r_{k_i} c_i \mid m \leq k,\ |c_i| \leq k\}.$$

Clearly, the sets C_r are finite and $gp_F(R) = \cup_{k\in\mathbb{N}} C_k$. Total enumeration of $gp_F(R)$ enumerates words from C_0, C_1 and so on, until it finds w. To enumerate C_k one has to enumerate up to k conjugates of length up to k, which has the total time complexity $O(3^{k^2})$ (we do not consider a case of a cyclic group G). Therefore, the complexity of the enumeration of $gp_F(R)$ is bounded from below by $O(3^{\widehat{\delta}^2})$, where $\widehat{\delta} = \widehat{\delta}(w)$ is the least number k such that $w \in C_k$. It is hard to estimate the value $\widehat{\delta}(w)$ in terms of $|w|$. Though the following proposition holds.

Proposition 10.3. Let $\langle X; R\rangle$ be a finite symmetrized presentation, $G = \langle X; R\rangle$, and $w \in gp_F(R)$. Then $\widehat{\delta}(w) \geq \overline{\delta}(w)$.

Proof. Let k be the smallest number such that

$$w = \prod_{i=1}^{m} c_i^{-1} r_{k_i} c_i$$

where $m \leq k$, $|c_i| \leq k$. Let D_1 be a diagram which is a bouquet of diagrams corresponding to $c_i^{-1} r_{k_i} c_i$ and D_2 is a diagram obtained from D_1 by foldings of the boundary ∂D_1 (so w is a boundary label of D_2). Since Stalling's folds preserve the incidence in X-digraph it follows that the chain distance from the initial vertex of D_2 to any cell is less or equal than k. This proves the proposition.

□

The obvious corollary of the proposition above is that the total enumeration has much worse time complexity than that of the standard Todd-Coxeter procedure.

11 Experimental results

We performed series of experiments to test the efficiency of the algorithm $\mathcal{A}$. In each series we fixed a finite symmetrized presentation $\langle X; R\rangle$, generated a sequence of words defining trivial element of $G = \langle X; R\rangle$ using several known to us general methods, and started the algorithm $\mathcal{A}$ on those words. We tested the following presentations:

1) $G = \langle a, b, c, d; [a, b][c, d]\rangle$ which is a small cancellation $C(\frac{1}{8})$ group (and so is hyperbolic).

2) $G = \langle a, b, c; a^2b^2c^7\rangle$ which is a hyperbolic, but not small cancellation group.

3) $G = \langle a, b; a^{-1}bab^{-2}\rangle$ which a non-hyperbolic group with exponential isoperimetric inequality.

4) $G = \langle a, b; a^{-1}baba^{-1}b^{-1}ab^{-2}\rangle$ which a non-hyperbolic group with super exponential isoperimetric inequality.

5) B_n (for $n = 3, 4, 5$) a group of braids on n strands, which a non-hyperbolic, automatic group.

For all listed above presentations we generated a series of 5000 words of length approximately 10000 representing the identity. For all generated words the algorithm $\mathcal{A}$ determined the triviality in just one iteration. Therefore, the time complexity of algorithm $\mathcal{A}$ was just $O(|w|L(R))$ - linear in terms of the input word, which is mush better than our theoretical estimates.

These experiments show that it is very hard to generate a diagram of high depth and that the isoperimetric inequality for a group presentation has a little to do with the actual complexity of the Word problem (also see [32]). Indeed, the isoperimatric inequality for a presentation might be low (say polynomial) which tells us that if the

word w is trivial then the area of the minimal diagram for w is limited by a certain not very large number. But this information does not give us any insight into the structure of that minimal diagram. Clearly, there are exponentially many diagrams of area $A(n)$ over any non-trivial presentation $\langle X; R\rangle$. So, to check the triviality of the given word one has to check if one of such diagrams has the boundary label w, which makes the problem exponentially hard.

We claim that the proposed parameter of trivial words – depth – reflects the complexity of the trivial words much better than the area of a minimal diagram with fixed boundary label. Certainly we can say that the depth is not greater than the area and, as shown in Theorem 5.3, the complexity of the Word problem is also exponential in terms of depth. Therefore, the complexity of the Word problem in terms of the depth is not worse than the complexity in terms of the area. And, in fact, our experiments show that practically (for random words defining identities) the value of depth is always much smaller than the value of area.

We would like to point out that we know a few series of inputs for which the performance of the algorithm $\mathcal{A}$ is slow (exponential and superexponential in terms of length of the input). But the amount of such inputs is negligible relative to all possible inputs. In fact, if $\langle X; R\rangle$ is a presentation with unsolvable Wword problem then for any computable function $f(n)$ there is a sequence of words w_n defining identity such that $\delta(w_n)$ grows faster than $f(n)$. But to find such a sequence is extremely hard. We have developed some methods for generation of diagrams of high depth (limited by any fixed $n \in \mathbb{N}$) with high probability. Unfortunately, all of them require exponential space in terms of n which limits their applications.

Part II

Conjugacy Search Problem

12 Introduction

The Conjugacy problem is the second problem in the list of the fundamental problems. As well as the Word problem, the Conjugacy problem is unsolvable in general [33] (also see [28] and [29]). Clearly, if the Word problem is unsolvable then the Conjugacy problem is unsolvable too. Moreover, for almost all classes with the solvable Conjugacy problem, its actual complexity is higher than the complexity of the Word problem. So, we can say that the Conjugacy problem is harder than the Word problem.

We shortly list some known positive results about the Conjugacy problem in groups. In abelian groups the Conjugacy problem is equivalent to the Word problem and, hence, is solvable by Gauss elimination procedure. For small-cancellation groups it was shown by Greendlinger in [12] that the variation of the Dehn's algorithm solves the Conjugacy problem. For word-hyperbolic it was shown by Holt that the Conjugacy problem is solvable in quadratic time in terms of the lengths of the given words. It is an open problem for automatic groups whether the conjugacy problem is solvable or not, though all interesting automatic groups are known to be biautomatic and, hence have the conjugacy problem solvable in quadratic time. It is solvable for braid groups, though there is no good upperbound on the time-complexity of the algorithm. It is also solvable for nilpotent and polycyclic groups. It is an open question whether it is solvable for $Aut(F_n)$.

In this part of the paper we study the generic-case complexity of the Conjugacy search problem. We design an algorithm (Algorithm $\mathcal{A}_C$, 17.11) for solving

it and show that for almost all presentations (including all known to us examples of groups with undecidable conjugacy problem) the conjugacy search problem is generically polynomial in terms of the lengths of words, where the degree depends on the presentation. Presentations non-covered by our proofs can be considered similarly. Another good part of our algorithm is that it does not require any additional information about a presentation or elements (like a constant of hyperbolicity for hyperbolic groups or existence of a good epimorphism onto an infinite hyperbolic group). One can start the algorithm on any presentation and a pair of words. No precomputation required.

The idea of the proposed algorithm is (somewhat) similar to the well-known Todd-Coxeter algorithm for the Word search problem. We show the existence of some universal construction (we call it the conjugacy graph, compare to the Cayley graph) which reflects the structure if the conjugacy class of the given word. So, the algorithm constructs two conjugacy graphs and if at some step they contain certain loops then algorithm stops with a positive answer. The algorithm does not have the negative answer. If non-conjugate words are plugged in then it never stops.

The proposed algorithm, also, allows one to determine many other numerical characteristics of elements of the given group. For example, if a word w is of finite order then it will find it eventually. Of course, the same can be done by a coset enumeration, but we claim that our algorithm is more efficient. If w_1 and w_2 are two words in generators of $G = \langle X; R\rangle$ such that

$$w_1^{n_1} \sim_G w_2^{n_2}$$

then the algorithm will eventually find (describe) the whole set of pairs with that property.

Finally, we would like to point out that this algorithm is one of its kind. There

are algorithms working for particular classes of groups, but none of them work in a full generality.

13 Weighted graphs

In this section we define main objects of this paper, namely conjugacy graphs and pseudo conjugacy graphs, that are analogous to Schreier graphs of a subgroups of a finitely presented group.

13.1 Definition

We start from the definition of X-digraphs. Let X be a finite alphabet closed under inversions (i.e., $X = X^{-1}$) and $\Gamma = (V, E)$ be a directed graph with an edge labelling function $\mu : E \to X$. For each edge $e = u_1 \to u_2 \in E$ we will assume the existence of the *inverse edge* $e^{-1} = u_2 \to u_1$ labelled with a symbol $\mu(e^{-1}) = \mu(e)^{-1}$ without actually adding it into E. A pair (Γ, μ) is called an *X-digraph*. Often we will refer to (Γ, μ) as to Γ without specifying μ. For more information on X-digraphs see [18].

It will be convenient to use the following notation for X-digraphs. Let Γ be an X-digraph. By $V(\Gamma)$ and $E(\Gamma)$ we denote the set of vertices and edges in Γ respectively. If $e = u \to v \in E(\Gamma)$ then the *origin* u of e will be denoted by $\alpha(e)$ and the *terminus* v by $\beta(e)$. A *path* p in Γ is a sequence of edges $e_1 \dots e_k$ such that $\beta(e_i) = \alpha(e_{i+1})$ for each $1 \leq i \leq k-1$. An origin $\alpha(p)$ of a path p is an origin of its first edge and the terminus $\beta(p)$ of p is the terminus of its last edge. The origin and the terminus of an empty path can be any vertex of Γ, and, hence, are not defined. When we will talk about a concatenation of paths p_1 and p_2 we will assume that $\beta(p_1) = \alpha(p_2)$. One can extend function μ from the edge set E to the set of paths

in a natural way. If $p = d_1 \dots d_k$ is a path in Γ then

$$\mu(p) = \mu(d_1) \dots \mu(d_k).$$

Now, we can define a weighted X-digraph. Let Γ be a connected X-digraph and γ a function $\gamma : E \to \mathbb{Z}$. If

$$\gamma(e) = -\gamma(e^{-1})$$

holds for any edge $e \in E(\Gamma)$ then γ is called a *weight function* on Γ and a pair (Γ, γ) is called a *weighted X-digraph*. Usually we shorten the notation (Γ, γ) omitting γ. In pictures we will depict each edge e of a weighted X-digraph Γ with a pair $(\mu(e), \gamma(e)) \in X \times \mathbb{Z}$ – the label and weight of e.

We extend function γ from the edge set E to the set of paths the following way. If $\pi = d_1 \dots d_k$ is a path in Γ then

$$\gamma(\pi) = \sum_{i=1}^{k} \gamma(d_i).$$

We say that a loop π in a weighted X-digraph (Γ, γ) is a *base loop* if $\gamma(\pi) = 1$.

A path $\pi = e_1 \dots e_k$ in Γ is *non-reduced* if $e_{i+1} = e_i^{-1}$ for some $1 \leq i \leq k-1$. Otherwise π is called *reduced*. To reduce a non-reduced path c means to remove all such pairs from π. Since removing $e_i e_{i+1}$ from c decreases the length of π by 2 in a finite number of steps a reduced path will be obtained. One can show that the final result of reductions does not depend on the sequence of reductions. Let π' be a reduced path obtained from π. Clearly $\gamma(\pi) = \gamma(\pi')$ and $\mu(\pi) =_{F(X)} \mu(\pi')$.

Similarly, π is *non cyclically reduced* if it is not reduced or $e_1 = e_k^{-1}$. Otherwise it is called *cyclically reduced*. From this definition follows that non cyclically reduced c must be a loop. To cyclically reduce a non cyclically reduced path π we first freely reduce π and then remove first and last edges of the result while they are opposite.

The result of such operation is clearly cyclically reduced and is uniquely defined. By induction on the number of single reductions it is easy to see that if π' is a cyclically reduced path obtained from π by a procedure defined above then $\gamma(\pi) = \gamma(\pi')$ and $\mu(\pi) \sim_{F(X)} \mu(\pi')$.

13.2 Conjugacy and pseudo conjugacy graphs

Let G be a group, $X \subseteq G$ a generating set for G such that $X^{-1} = X$, and $w = w(X)$. In this section we define conjugacy and pseudo conjugacy graphs of w in G (relative to X) and show that for any w in generators of G there exists at least one pseudo conjugacy graph. The existence of conjugacy graphs will be shown in Section 15.

Let Γ be a weighted X-digraph (not necessarily connected), w a word in generators $X \cup X^{-1}$, and $N \in \mathbb{N} \cup \{\infty\}$ (here ∞ is a symbol denoting the element which greater than any natural number).

Definition 13.1. We say that a pair (Γ, N) is a *pseudo conjugacy graph* of the word w in G if the following conditions are satisfied:

(PCG1) For any loop π in Γ

$$\mu(\pi) \sim_G w^{\gamma(\pi)}. \tag{25}$$

(PCG2) Either $N = \infty$, or $N < \infty$ and $w^N =_G 1$.

Since cyclic reduction of a loop in a weighted X-digraph does not change its weight and label (as a cyclic word) we can slightly modify the first requirement (PCG1) in the definition of pseudo conjugacy graphs to the following one:

(PCG1)' For any cyclically reduced loop π in Γ $\mu(\pi) \sim_G w^{\gamma(\pi)}$.

The obtained definition is equivalent to the previous. Also, notice that if $N < \infty$ then for any loop π in Γ we have $\mu(\pi)^N =_G 1$.

Definition 13.2. A connected folded pseudo conjugacy graph (Γ, N) of $w \in G$ is called a conjugacy graph of w in G (relative to the generating set X) if the following conditions hold:

(CG1) For every $v \in F(X)$ and $\gamma \in \mathbb{N}$ word v and w^γ conjugate if and only if there exists a loop π in Γ such that $\mu(\pi) = v$ and $\gamma(\pi) \equiv \gamma \mod N$.

(CG2) N is an order of w in G.

Let $w = w_1 \dots w_k$ be a word in generators $X \cup X^{-1}$ of the group G and Γ is the graph $Loop_1(w)$ depicted in Figure 13). Then the pair (Γ, ∞) is a pseudo conjugacy graph of w in G. The graph Γ consists of k vertices $\{1, \dots, k\}$ and k edges $e_i = i \overset{(w_i,0)}{\longrightarrow} i+1$ $(i = 1, \dots, k-1)$ and an edge $e_k = k \overset{(w_k,1)}{\longrightarrow} 1$. It is straightforward to check that $Loop_1(w)$ is, indeed, a pseudo conjugacy graph of w.

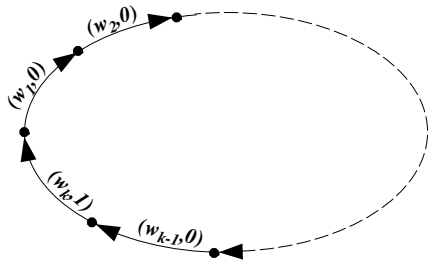

Figure 13: Graph $\Gamma(w)$.

Lemma 13.3. (Conjugators in pseudo conjugacy graphs.) *Let Γ be a pseudo conjugacy graph of w. Suppose that π_0 and π_1 are loops in Γ such that $\gamma(\pi_0) = 1$ and $p = d_1 \dots d_k$ be a path starting at the initial vertex of π_0 (hence $\alpha(p) = \alpha(\pi_0)$) and terminating at the initial vertex of π_1 (hence $\beta(p) = \alpha(\pi_1)$). Then $\mu(\pi_1) =_G \mu(p)^{-1}\mu(\pi_0)^{\gamma(\pi_1)}\mu(p)$.*

Proof. From the assumption put on the path p the sequence of edges $p^{-1}\pi_0^{\gamma(\pi_1)}p\pi_1^{-1}$ is a loop in Γ (perhaps not cyclically reduced). From assumptions put on π_0 and π_1 we

have $\gamma(p^{-1}\pi_0^{\gamma(\pi_1)}p\pi_1^{-1}) = -\gamma(p)+\gamma(\pi_1)\gamma(\pi_0)+\gamma(p)-\gamma(\pi_1) = 0$. Since Γ is a pseudo conjugacy graph we have $\mu(p^{-1}\pi_0^{\gamma(\pi_1)}p\pi_1^{-1}) =_G 1$. Thus $\mu(p)^{-1}\mu(\pi_0)^{\gamma(\pi_1)}\mu(p)\mu(\pi_1)^{-1} =_G 1$.

□

The following assertion is a corollary of Lemma 13.3.

Proposition 13.4. Let G be a group, X be the generating set for G closed under inversions, (Γ, N) a pseudo conjugacy graph of w in G, and π a base loop in (Γ, N). Then (Γ, N) is a pseudo conjugacy graph of $\mu(\pi)$ in G.

The existence of a base loop in a pseudo conjugacy graph is important. Further in the sequel when we say that Γ is a pseudo conjugacy graph of w in G we assume that, in addition to properties (PCG1) and (PCG2), there exists a base loop in Γ labelled with w.

Let (Γ_1, N_1) and (Γ_2, N_2) be pseudo conjugacy graphs of w in G, and $\varphi : \Gamma_1 \to \Gamma_2$ be an X-digraph morphism. We say that φ is a *pseudo conjugacy graph morphism* or, to shorten, *PCG-morphism* if the following conditions hold:

(M1) there exists $c \in \mathbb{N} \cup \{\infty\}$ such that $N_1 = cN_2$;

(M2) for any loop l in Γ_1 $\gamma(l) \equiv \gamma(\varphi(l)) \mod N_2$.

14 Transformations of weighted X-digraphs

In this section we define several transformations of weighted X-digraphs. All together they will be used to construct conjugacy graphs and to solve the conjugacy search problem for finitely presented groups. Let $\langle X; R\rangle$ be a finite group presentation, $w = w(X)$, and Γ a weighted X-digraph. Each of the transformations will be shown to satisfy the following important property. The result of a transformation

of Γ is a pseudo conjugacy graph of w in G if and only if Γ is a pseudo conjugacy graph of w in G.

14.1 Shift operator

Shift operator is a transformation of a weighted X-digraph Γ which preserves its X-digraph structure and changes the weights of edges incident to some vertex in Γ.

Definition 14.1. Let v be a vertex of a weighted X-digraph Γ and $\varepsilon \in \mathbb{Z} \setminus \{0\}$. A *shift* of the weight at the vertex v in Γ by ε is the following transformation of Γ:

1) Each edge $v \overset{(x,\gamma)}{\longrightarrow} u$ (where $v \neq u$) is replaced with an edge $v \overset{(x,\gamma-\varepsilon)}{\longrightarrow} u$.

2) Each edge $u \overset{(x,\gamma)}{\longrightarrow} v$ (where $v \neq u$) is replaced with an edge $u \overset{(x,\gamma+\varepsilon)}{\longrightarrow} v$.

(Observe, that we do not replace edges $v \overset{(x,\gamma)}{\longrightarrow} v$.) The result of a shift operator is denoted by $Shift_{\varepsilon}(\Gamma, v)$. See Figure 14.

Since $Shift_{\varepsilon}$ changes only a weight function γ on an X-digraph Γ there exists a natural X-digraph isomorphism

$$\varphi_{Shift} : \Gamma \to Shift_{\varepsilon}(\Gamma, v).$$

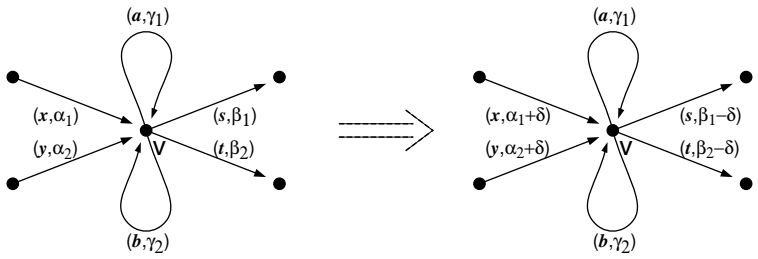

Figure 14: Shift operator.

Proposition 14.2. Let G be a group, X a generating set for G closed under inversions, Γ a weighted X-digraph, $v \in V(\Gamma)$, $\varepsilon \in \mathbb{Z}$, and $N \in \mathbb{N}$. Then the following holds

(Sh1) A pair (Γ, N) is a pseudo conjugacy graph of $w \in G$ if and only if $(Shift_{\varepsilon}(\Gamma, v), N)$ is.

(Sh2) If a pair (Γ, N) is a pseudo conjugacy graph of $w \in G$ then φ_{Shift} is a PCG-morphism.

Proof. Denote $Shift_{\varepsilon}(\Gamma, v)$ by Γ'. Let $\varphi_{Shift} : \Gamma \to \Gamma'$ be a corresponding X-digraph isomorphism, $\pi = e_1 \dots e_k$ an arbitrary loop in Γ and

$$\pi' = \varphi_{Shift}(\pi) = \varphi_{Shift}(e_1) \dots \varphi_{Shift}(e_k)$$

an image of π in Γ'. Clearly $\mu(\pi) = \mu(\pi')$. To finish the proof of (Sh1) and (Sh2) it is enough to show that $\gamma(\pi) = \gamma(\pi')$.

Let $v_1, \dots, v_{k+1}$ $(v_1 = v_{k+1})$ be a sequence of vertices which π passes through in Γ. If for each $i = 1, \dots, k$ $v_i \neq v$ then for each $i = 1, \dots, k$ $\gamma(e_i) = \gamma(\varphi_{Shift}(e_i))$ and hence $\gamma(\pi) = \gamma(\pi')$ due to additivity of γ. If for each $i = 1, \dots, k$ $v = v_i$ then each $e_i = (v, v)$ and, therefore, for each $i = 1, \dots, k$ $\gamma(e_i) = \gamma(\varphi_{Shift}(e_i))$ and $\gamma(\pi) = \gamma(\pi')$.

Now let $v = v_i$ for some $i = 1, \dots, k$ but not for all of them. We may assume that $v \neq v_1$ (take a cyclic permutation of π if required). Let $1 < s, t < k+1$ be such that $v = v_j$ for all $j = s, \dots, t$ and $v \neq v_{s-1}$ and $v \neq v_{t+1}$. Then $e_{s-1} = (u, v)$ (for some $u' \neq v$), $e_j = (v, v)$ $(j = s, \dots, t-1)$ and $e_t = (v, u')$ (for some $u' \neq v$). Using the definition of $Shift_{(v,\varepsilon)}$ we get $\gamma(e_{s-1} \dots e_t) = \gamma(\varphi_{Shift}(e_{s-1} \dots e_t))$. Finally notice that different such subpaths do not overlap in π and weights of edges not belonging to them do not change. Thus $\gamma(\pi) = \gamma(\pi')$.

□

Proposition 14.3. Let $\tau : K_1 \to K_2$ be a PCG-morphism, $K_1' = Shift_{\varepsilon_1}(K_1, v_1)$, and $K_2' = Shift_{\varepsilon_2}(K_2, v_2)$. Then there exists a PCG-morphism $\theta : K_1' \to K_2'$ such

that the diagram commutes:

$$\begin{array}{ccc} (K_1, N_1) & \stackrel{\tau}{\to} & (K_2, N_2) \\ \downarrow^{\phi^{(1)}_{Shift}} & & \downarrow^{\phi^{(2)}_{Shift}} \\ (K_1', N_1) & \stackrel{\theta}{\to} & (K_2', N_2) \end{array}$$

Proof. Since $\phi^{(1)}_{Shift}$ and $\phi^{(2)}_{Shift}$ are X-digraph isomorphisms it is natural to define θ equal to τ on the X-digraph level. To show that so defined X-digraph morphism θ is a PCG-morphism it is enough to prove the property (M2) for θ.

Let π_1' be an arbitrary loop in K_1', $\pi_1 \in K_1$ its preimage, $\pi_2 = \tau(\pi_1)$, and $\pi_2' = \phi^{(2)}_{Shift}(\pi_2)$. Then $\theta(\pi_1') = \pi_2'$. By Proposition 14.2 we have $\gamma(\pi_1) = \gamma(\pi_1')$ and $\gamma(\pi_2) = \gamma(\pi_2')$. Since τ is a PCG-morphism then $\gamma(\pi_1) \equiv \gamma(\pi_2) \mod N_2$. Therefore, $\gamma(\pi_1') \equiv \gamma(\pi_2') \mod N_2$ and (M2) holds for θ.

□

14.2 Stalling's fold

In this section we define Stalling's folds for pseudo conjugacy graphs. Folding procedure of pseudo conjugacy graphs is an extension of Stalling's folding procedure for X-digraphs in the following sense, if Γ' is a result of a fold of a pseudo conjugacy graph Γ then Γ' (as an X-digraph) is a result of a fold of a pseudo conjugacy graph Γ (as an X-digraph). See [18] for more information on Stalling's folding procedure for X-digraphs.

We say that a pseudo conjugacy graph Γ is *not reduced* (*not folded*) if there exist distinct edges $e_1 = v \stackrel{(x,\gamma_1)}{\longrightarrow} u_1$, $e_2 = v \stackrel{(x,\gamma_2)}{\longrightarrow} u_2$ in Γ with the same origin v and the same label x. Otherwise we say that Γ is *reduced* (*folded*). The next algorithm performs a Stalling's fold of e_1 and e_2 in Γ.

Remark 14.4. We assume that ∞ is divisible by any positive number $k \in \mathbb{N}$.

Therefore, $\gcd(\infty, k) = k$ for any $k \in \mathbb{N}$.

Algorithm 14.5. *(Stalling's fold)*

SIGNATURE: $(\Gamma', N', \phi) = Fold(\Gamma, N, e_1, e_2)$.

INPUT: A weighted X-digraph Γ, $N \in \mathbb{N} \cup \{\infty\}$, and a pair of distinct edges $e_1 = v \xrightarrow{(x,\gamma_1)} u_1$, $e_2 = v \xrightarrow{(x,\gamma_2)} u_2$ in Γ.

OUTPUT: A weighted X-digraph Γ', $N' \in \mathbb{N} \cup \{\infty\}$ and a canonical epimorphism $\phi : \Gamma \to \Gamma'$.

COMPUTATIONS:

A) If $u_1 \neq u_2$ (Figure 15):

1) Put

$$u = \begin{cases} u_1, & v \neq u_1; \\ u_2, & \text{otherwise;} \end{cases}$$

and

$$\varepsilon = \begin{cases} \gamma(e_2) - \gamma(e_1), & v \neq u_1; \\ \gamma(e_1) - \gamma(e_2), & \text{otherwise.} \end{cases}$$

2) Let $\Gamma_0 = Shift_{\varepsilon}(\Gamma, u)$ and ϕ_{Shift} a corresponding X-digraph isomorphism $\Gamma \to \Gamma_0$.

3) Identify the vertices u_1 and u_2 in Γ_0 and denote the result by Γ'. Let $\phi_1 : \Gamma_0 \to \Gamma'$ be the corresponding epimorphism.

4) Return a triple $(\Gamma', N, \phi_{Shift} \circ \phi_1)$.

B) If $u_1 = u_2$:

1) If $\gamma(e_1) \neq \gamma(e_2)$ then put $N' = \gcd(N, |\gamma(e_1) - \gamma(e_2)|)$. Otherwise put $N' = N$.

2) Identify the edges e_1 and e_2 in Γ into an edge $e = v \xrightarrow{(x,\gamma_1)} u_1$ and denote the result by Γ'. Let $\phi : \Gamma \to \Gamma'$ be the corresponding epimorphism.

3) Return a triple (Γ', N', ϕ).

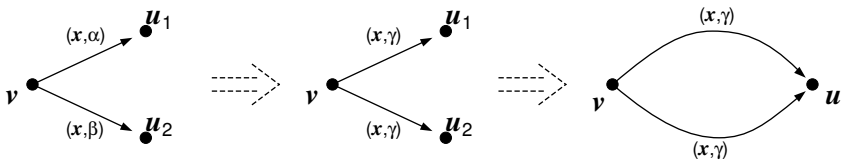

Figure 15: Fold (Case A).

Note that Case B ($u_1 = u_2$) can be viewed as a removal of the edge e_2 and so, in that case, Γ' is a subgraph of Γ.

Proposition 14.6. Let $(\Gamma', N', \phi) = Fold(\Gamma, N, e_1, e_2)$. Then

(F1) (Γ, N) is a pseudo conjugacy graph of w in G if and only if (Γ', N') is.

(F2) If (Γ, N) is a pseudo conjugacy graph of w in G then ϕ is a PCG-morphism.

Proof. We first show (F1).

"$\Longleftarrow$" Clearly, (PCG2) holds for (Γ, N). We will show that (PCG1') holds for (Γ, N) too. Let π be a loop in Γ and $\pi' = \phi(\pi)$. Consider two cases.

Case ($u_1 \neq u_2$). On steps A.1) and A.2) we perform a shift of u_1 or u_2 to make $\gamma(e_1) = \gamma(e_2)$ in Γ_0. By Proposition 14.2 (Γ_0, N) is a pseudo conjugacy graph of $w \in G$ if and only if (Γ, N) is. Hence, we may assume that $\Gamma = \Gamma_0$ and $\gamma(e_1) = \gamma(e_2)$. Clearly, $\mu(\pi) = \mu(\pi')$ and $\gamma(\pi) = \gamma(\pi')$ in Γ_0. Since (Γ', N') is a pseudo conjugacy graph of w in G

$$\mu(\pi) = \mu(\pi') \sim_G w^{\gamma(\pi')} = w^{\gamma(\pi)}.$$

Case ($u_1 = u_2$). Clearly $\mu(\pi) = \mu(\pi')$ and

$$\gamma(\pi) = \gamma(\pi') + k|\gamma(e_1) - \gamma(e_2)|$$

where $k \in \mathbb{Z}$ (the last holds since the mapping ϕ sometimes switches $\gamma(e_2)$ to $\gamma(e_1)$ in Γ'). Since N' divides $|\gamma(e_1) - \gamma(e_2)|$ and (Γ', N') is a pseudo conjugacy graph of

w we have

$$\mu(\pi) = \mu(\pi') \sim_G w^{\gamma(\pi')} =_G w^{\gamma(\pi')} w^{k|\gamma(e_1)-\gamma(e_2)|} = w^{\gamma(\pi)}.$$

"$\Longrightarrow$" Let $\pi' = e'_1, \ldots, e'_k$ be a loop in Γ'. To show that $\mu(\pi') \sim_G w^{\gamma(\pi')}$ we will find a path $\pi \in \Gamma$ such that $\mu(\pi) = \mu(\pi')$ in $F(X)$ and $\gamma(\pi) = \gamma(\pi')$.

Case ($u_1 \neq u_2$). Notice that ϕ is bijection of edges. So we can define a sequence of edges $\pi_0 = \dot{e_1}, \ldots, \dot{e_k} \in \Gamma$ where $\phi(\dot{e_i}) = e'_i$. Since ϕ is not bijective on the vertices of Γ (recall $\phi(u_1) = \phi(u_2)$) π_0 might be not connected at u_1 and u_2. To make π_0 connected we fill the gaps in π_0 with $(e_1^{-1}e_2)^{\pm 1}$ depending on a direction of π_0. Since $\mu(e_1^{-1}e_2) =_{F(X)} \mu(e_2^{-1}e_1) =_{F(X)} 1$ and $\gamma(e_1^{-1}e_2) = \gamma(e_2^{-1}e_1) = 0$ the obtained path π is the required.

Case ($u_1 = u_2$). We first show that obtained N' satisfies the property (PCG2). Indeed, N' changes to $\gcd(N, |\gamma(e_1) - \gamma(e_2)|)$ only when $\gamma(e_1) \neq \gamma(e_2)$. Consider a loop $l = e_1 e_2^{-1}$ in Γ and notice that $\gamma(l) = \gamma(e_1) - \gamma(e_2)$ and $\mu(l) =_F 1$. Finally, since Γ is, by assumption, a pseudo conjugacy graph $1 \sim_G w^{\gamma(l)} = w^{\gamma(e_1)-\gamma(e_2)}$ and $1 = w^N$ which gives us

$$1 = w^{\gcd(N, |\gamma(e_1)-\gamma(e_2)|)}.$$

To finish the proof for this case it remains to show that there exists the claimed above loop c. Since Γ' is a subgraph of Γ we can take π to be a preimage of π' in Γ'. Obviously, it possesses all the claimed properties.

Now we show (F2). Since N', when changed, becomes $\gcd(N, |\gamma(e_1) - \gamma(e_2)|)$ the property (M1) holds. To prove (M2) consider a loop $\pi \in \Gamma_1$ and its image $\pi' = \phi(\pi)$. As proved above $\mu(\pi) = \mu(\pi')$ and $\gamma(\pi) = \gamma(\phi(\pi))$ in the first case and $\gamma(\pi) \equiv \gamma(\pi')$ mod N' in the second case. Therefore, (M2) is proved and ϕ is a PCG-morphism.

□

14.3 Stalling's procedure

Now we are ready to present the algorithm which completely folds weighted X-digraphs.

Algorithm 14.7. *(Stalling's procedure.)*

SIGNATURE: $(\Gamma', N', \phi_S) = S(\Gamma, N)$.

INPUT: A weighted X-digraph Γ, $N \in \mathbb{N} \cup \{\infty\}$.

OUTPUT: A weighted X-digraph Γ', $N' \in \mathbb{N} \cup \{\infty\}$ and a canonical epimorphism $\phi : \Gamma \to \Gamma'$.

INITIALIZATION: Put $\Gamma' = \Gamma$, $N' = N$, and $\phi_S = id$.

COMPUTATIONS:

A) While there is a pair of edges $e_1 = v \xrightarrow{(x,\gamma_1)} u_1$, $e_2 = v \xrightarrow{(x,\gamma_1)} u_2$ in Γ':

   1) Compute $(\Gamma', N', \phi_0) = Fold(\Gamma', N', e_1, e_2)$.

   2) Put $\phi_S = \phi_S \circ \phi_0$.

B) Return a triple (Γ', N', ϕ_S).

Clearly the Staling's procedure for finite weighted X-digraphs terminates in a finitely many steps since each fold decreases $|V(\Gamma')| + |E(\Gamma')|$ by 1. In contrast to X-digraphs the result of Stalling's procedure applied to a weighted X-digraph depends on a sequence of Stalling's folds. One might obtain different values of a weight function γ using different sequences of folds; though the X-digraph structure of a folded Γ does not depend on a particular sequence of folds.

Proposition 14.8. Let G be a group, X a generating set for G, Γ a weighted X-digraph, $N \in \mathbb{N} \cup \{\infty\}$, and $w = w(X)$. If $(\Gamma', N', \phi_S) = S(\Gamma, N)$ then

(S1) (Γ, N) is a pseudo conjugacy graph of w in G if and only if (Γ', N') is.

(S2) If (Γ, N) is a pseudo conjugacy graph of w in G then ϕ_S is a PCG-morphism.

Proof. Follows from Proposition 14.6.

□

Our next goal is to show that the number N' does not depend on a particular sequence of folds in Algorithm 14.8. Define a set of trivial loops in Γ by

$$TL(\Gamma) = \{\pi \mid \pi \text{ is a loop in } \Gamma \text{ s.t. } \mu(\pi) =_{F(X)} 1\}.$$

By a *potential order* of a pseudo conjugacy graph (Γ, N) of w in G we call the following number:

$$PO(\Gamma, N) = \gcd\left(\{|\gamma(\pi)| \mid \pi \in TL(\Gamma),\ \gamma(\pi) \neq 0\} \cup \{N\} \right). \tag{26}$$

Lemma 14.9. *Let (Γ, N) be a folded pseudo conjugacy graph of w in G. Then $N = PO(\Gamma, N)$.*

Proof. Observe that $\{|\gamma(c)| \mid c \in TL(\Gamma),\ \gamma(c) \neq 0\} = \emptyset$ for a folded Γ.

□

Lemma 14.10. *Let (Γ, N) be a non-folded pseudo conjugacy graph of $w \in G$ and $(\Gamma', N', \phi) = Fold(\Gamma, N, e_1, e_2)$. Then $PO(\Gamma, N) = PO(\Gamma', N')$.*

Proof. Let $e_1 = v \stackrel{(x,\gamma_1)}{\longrightarrow} u_1$ and $e_2 = v \stackrel{(x,\gamma_2)}{\longrightarrow} u_2$. Consider two cases ($u_1 \neq u_2$ and $u_1 = u_2$).

If $u_1 \neq u_2$ then $N' = N$ and Γ' is obtained by identification of the vertices u_1 and u_2. For any loop $\pi \in \Gamma$ (we refer to the proof of Proposition 14.6) we have $\gamma(\pi) = \gamma(\phi(\pi))$ and $\mu(\pi) = \mu(\phi(\pi))$. On the other hand, for any loop $\pi' \in \Gamma'$ we can choose (see the proof of Proposition 14.6) a loop $\pi \in \Gamma$ such that $\gamma(\pi) = \gamma(\pi')$ and $\mu(\pi) = \mu(\pi')$ in $F(X)$. Therefore, $PO(\Gamma, N) = PO(\Gamma', N')$ holds.

If $u_1 = u_2$ then $N' = \gcd(N, |\gamma(e_1) - \gamma(e_2)|)$ and Γ' is obtained from Γ by removing e_2. For $\pi \in \Gamma$ we have $\gamma(\pi) \equiv \gamma(\phi(\pi)) \mod N'$ and $\mu(\pi) = \mu(\phi(\pi))$.

Therefore $PO(\Gamma', N')$ divides $PO(\Gamma, N)$. On the other hand, for $\pi' \in \Gamma'$ there exists π such that $\pi' = \phi(\pi)$ such that $\gamma(\pi) = \gamma(\pi')$ and $\mu(\pi) = \mu(\pi')$ (since Γ' is a proper subgraph of Γ). Finally notice that $PO(\Gamma, N)$ divides N' since $\gamma(e_1 e_2^{-1}) = \gamma(e_1) - \gamma(e_1)$ and $\mu(e_1 e_2^{-1}) =_{F(X)} 1$. Therefore, the equality $PO(\Gamma, N) = PO(\Gamma', N')$ holds.

□

Corollary 14.11. Let (Γ, N) be a pseudo conjugacy graph of w in G and $(\Gamma', N', \phi_S) = S(\Gamma, N)$. Then $N' = PO(\Gamma, N)$.

Corollary 14.12. Let (Γ, N) be a pseudo conjugacy graph of $w \in G$ and, $(\Gamma_1, N_1, \phi_1) = S(\Gamma, N)$ and $(\Gamma_2, N_2, \phi_2) = S(\Gamma, N)$ be two results of Stalling's procedure obtained by different sequences of folds. Then $N_1 = N_2$.

In other words, the number N of a folded pseudo conjugacy graph does not depend on a sequence of folds. Besides, we know that the X-digraph structure of Γ does not depend on the sequence of folds. The only thing that changes is a weight function γ.

Lemma 14.13. *Let $\tau : (K_1, N_1) \to (K_2, N_2)$ be a PCG-morphism. Then there exists $c \in \mathbb{N}$ such that $PO(K_1, N_1) = c \cdot PO(K_2, N_2)$ (i.e., $PO(K_2, N_2)$ divides $PO(K_1, N_1)$).*

Proof. An immediate corollary of definitions of a PCG-morphism and a potential order. □

Proposition 14.14. Stalling's procedure is a functor from the category of pseudo conjugacy graphs of w in G to the category of folded pseudo conjugacy graphs of w.

Proof. First, we show that if $\tau : K_1 \to K_2$ is a PCG-morphism, $(K_1', N_1', \phi_1) = S(K_1, N_1)$, and $(K_2', N_2', \phi_2) = S(K_2, N_2)$ then there exists a *PCG*-morphism θ :

$(K_1', N_1') \to (K_2', N_2')$ such that the diagram below commutes.

$$\begin{array}{ccc} (K_1, N_1) & \stackrel{\tau}{\to} & (K_2, N_2) \\ \downarrow^{\phi_1} & & \downarrow^{\phi_2} \\ (K_1', N_1') & \stackrel{\theta}{\to} & (K_2', N_2') \end{array} \tag{27}$$

We already noticed that the Stalling's procedure acts in a usual way on the X-digraph level. Therefore, if the diagram (27) is viewed as the diagram with the corresponding X-digraphs, then it is known that θ exists and unique. We claim that θ is a required PCG-morphism. For that it is sufficient to prove that properties (M1) and (M2) hold.

Property (M1) of θ holds by Lemma 14.13. To show (M2) consider a reduced loop π_1' in K_1'. The loop π_1' can be lifted up to a loop $\pi_1 \in K_1$ such that $\phi_1(\pi_1)$ is π_1' with, perhaps, some backtracks (we refer to the proof of Proposition 14.6). Let $\pi_2 = \tau(\pi_1)$ and $\pi_2' = \phi_2(\pi_2)$. The loop π_2' is $\theta(\pi_1')$ with backtracks. It remains to show that $\gamma(c_1') \equiv \gamma(\pi_2') \mod N_2'$.

Indeed, by Proposition 14.8 ϕ_1 and ϕ_2 are PCG-morphisms. Since τ is also a PCG-morphism we have

$$\begin{aligned} \gamma(\pi_1) &\equiv \gamma(\pi_1') \mod N_1', \\ \gamma(\pi_2) &\equiv \gamma(\pi_2') \mod N_2', \\ \gamma(\pi_1) &\equiv \gamma(\pi_2) \mod N_2 \\ \mu(\pi_1) &=_F \mu(\pi_1'), \\ \mu(\pi_2) &=_F \mu(\pi_2'), \\ \mu(\pi_1) &=_F \mu(\pi_2) \end{aligned}$$

Since N_2' divides N_2, N_1 and N_1'

$$\gamma(\pi_1') \equiv \gamma(\pi_2') \mod N_2'$$

and, hence, (27) commutes. The statement of the proposition easily follows from this.

□

14.4 Basic extension

Definition 14.15. Let Γ be a weighted X-digraph, v a vertex in Γ, and $r = r(X)$. Attach a loop of weight 0 labelled with r at the vertex v and denote the result by $\mathcal{E}_r(\Gamma, v)$. The graph $\mathcal{E}_r(\Gamma, v)$ is called a *basic extension* of Γ with r at v. We denote the corresponding canonical X-digraph embedding $\Gamma \hookrightarrow \mathcal{E}_r(\Gamma, v)$ by $\phi_{\mathcal{E}}$.

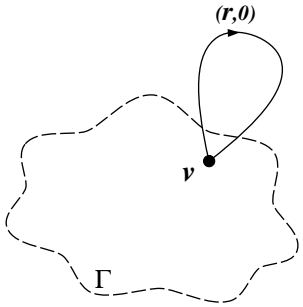

Figure 16: Graph $\mathcal{E}_r(\Gamma, v)$. Edges of a new loop are consequently labelled with generators x_{i_j} (where $r = x_{i_1} \dots x_{i_m}$) and have weight zero.

Proposition 14.16. Let $G = \langle X; R \rangle$ be a finite presentation, Γ a weighted X-digraph, v a vertex in Γ, $N \in \mathbb{N} \cup \{\infty\}$, $r \in R$, and $w = w(X)$. If $(\Gamma', N) = (\mathcal{E}_r(\Gamma, v), N)$ and $\phi_{\mathcal{E}} : \Gamma \hookrightarrow \Gamma'$ the canonical embedding then

(BE1) (Γ, N) is a pseudo conjugacy graph of w in G if and only if (Γ', N) is.

(BE2) If (Γ, N) is a pseudo conjugacy graph of w in G then $\phi_{\mathcal{E}}$ is a PCG-morphism.

Proof. Since N does not change, the property (PCG2) holds for (Γ, N) if and only if it holds for (Γ', N).

Since Γ is a proper subgraph of Γ' the sufficiency in (BE1) is obvious. Prove the necessity. Denote the added loop in Γ' by l. Let π be a cyclically reduced loop in Γ'. We may assume that π starts (and ends) at v. To show that (PCG1) holds for π we consider two cases. If π does not pass through edges of l then π belongs to Γ which is a conjugacy graph and thus (PCG1) holds for π. If π passes through the edges of l then, since π has no backtracks, π goes all the way along edges of l which has label $r^{\pm 1}$ (depending on a direction) and a weight 0. Therefore, removing an occurrence of l inside of π does not change the weight and the label (as an element of G) of π. The obtained loop is shorter than the initial. Hence, after a few removals of $l^{\pm 1}$ we get a loop from Γ of the same weight and with a label equal to the label of the initial loop (as an element of G). As proved above, (PCG1) holds for such a loop and, hence (BE1) holds.

Finally, by (BE1), if (Γ, N) is a pseudo conjugacy graph of $w \in G$ then (Γ', N) is. Therefore, $\phi_{\mathcal{E}}$ is a PCG-morphism and (BE2) is done.

□

Proposition 14.17. Let $G = \langle X; R\rangle$ be a finite presentation, Γ_1 and Γ_2 be a pseudo conjugacy graphs of $w \in G$ and $\tau : \Gamma_1 \to \Gamma_2$ be a PCG-morphism. Let v_1 be a vertex in Γ_1 and $v_2 = \tau(v)$ be its image in Γ_2. Then there exists a PCG-morphism θ such that the following diagram commutes.

$$\begin{array}{ccc} \Gamma_1 & \stackrel{\tau}{\to} & \Gamma_2 \\ \downarrow^{\phi_{\mathcal{E}}} & & \downarrow^{\phi_{\mathcal{E}}} \\ \mathcal{E}_r(\Gamma_1, v_1) & \stackrel{\theta}{\to} & \mathcal{E}_r(\Gamma_2, v_2) \end{array}$$

Proof. The graph $\mathcal{E}_r(\Gamma_1, v_1)$ is a wedge graph of Γ_1 and a loop l_1 labelled with r. Similarly, the graph $\mathcal{E}_r(\Gamma_2, v_2)$ is a wedge graph of Γ_2 and a loop l_2 labelled with r. Define $\theta : \mathcal{E}_r(\Gamma_1, v_1) \to \mathcal{E}_r(\Gamma_2, v_2)$ on a subgraph of $\mathcal{E}_r(\Gamma_1, v_1)$ corresponding to Γ_1 to be equal to τ and on l_1 to be l_2. It is straightforward to check that so defined θ is

a PCG-morphism. □

14.5 R-extension algorithm

In this section we present an R-extension algorithm.

Algorithm 14.18. *(R-extension of weighted graphs.)*

SIGNATURE. $(\Gamma^*, N^*, \phi_{\mathcal{C}}) = \mathcal{C}(\Gamma, N)$.

INPUT. A finite symmetrized presentation $\langle X; R\rangle$, a weighted X-digraph Γ, and $N \in \mathbb{N} \cup \{\infty\}$.

OUTPUT. A weighted X-digraph Γ^*, an X-digraph morphism $\phi_{\mathcal{C}} : \Gamma \to \Gamma^*$, and $N^* \in \mathbb{N} \cup \{\infty\}$.

COMPUTATIONS.

C1) For each vertex $v \in \Gamma$ and each $r \in R$ add a loop labelled by r of weight 0 at v. Denote the resulting graph by $\mathcal{C}_1(\Gamma)$ and the canonical embedding by $\phi_{\mathcal{C}_1} : \Gamma \to \mathcal{C}_1(\Gamma)$.

C2) Let $(\Gamma^*, N^*, \phi_S) = S(\mathcal{C}_1(\Gamma), N)$.

C3) Output a triple (Γ^*, N^*, ϕ_C), where $\phi_{\mathcal{C}} = \phi_{\mathcal{C}_1} \circ \phi_S$.

We will denote the graph Γ^* by $\mathcal{C}(\Gamma)$. In Lemmas 14.19, 14.20, and 14.21 we shortly list properties of the R-extension operator $\mathcal{C}$ and the auxiliary operator $\mathcal{C}_1$. For proofs we refer the reader to part I of this paper (Lemmas 4.3, 4.4, and 4.5).

Lemma 14.19. *Let Γ be a weighted X-digraph and $N \in \mathbb{N} \cup \{\infty\}$. Then the following holds:*

1) $\mathcal{C}_1(\Gamma)$ is well-defined, i.e., it does not depend on a sequence of actual transformations in C1).

2) $\mathcal{C}(\Gamma)$ (as an X-digraph) and N^* are well-defined, i.e., do not depend on a sequence of actual transformations in C1) and C2).

3) If $L(R) > 0$ then $\mathcal{C}_1(\Gamma)$ and $\mathcal{C}(\Gamma)$ are weighted core X-digraphs.

4) If $L(R) > 0$ then $\phi_{\mathcal{C}}$ is a functor from the category of X-digraphs into the category of folded weighted core X-digraphs.

Lemma 14.20. *Let $\langle X; R\rangle$ be a symmetrized finite presentation and Γ a finite X-digraph. Then the following inequalities hold for the R-extension $\mathcal{C}(\Gamma)$ of Γ:*
1) $|V(\mathcal{C}(\Gamma))| \leq (L(R) - |R| + 1)|V(\Gamma)|$,
2) $|E(\mathcal{C}(\Gamma))| \leq 2|X|\ |V(\mathcal{C}(\Gamma))|$.
Moreover, the time complexity of Algorithm 14.18 is bounded from above by

$$O(L(R)|V(\Gamma)|\log(L(R)|V(\Gamma)|)).$$

From now on we assume that every letter in X is non-trivially involved in R. Starting with an X-digraph Γ one can iterate the construction above. Put:

$$\mathcal{C}^{(1)}(\Gamma) = \mathcal{C}(\Gamma), \quad \mathcal{C}^{(m+1)}(\Gamma) = \mathcal{C}(\mathcal{C}^{(m)}(\Gamma))$$

Similarly, one can define $\mathcal{C}_1^{(m)}(\Gamma)$ as the result of m consecutive applications of the unary operation $\mathcal{C}_1$ starting at Γ. As a special case define

$$\mathcal{C}^{(0)}(\Gamma) = S(\Gamma), \quad \mathcal{C}_1^{(0)}(\Gamma) = \Gamma.$$

Lemma 14.21. *Let Γ be an X-digraph. Then the following holds for any non-negative integers m, n:*

1) $\mathcal{C}^{(m)}(\Gamma) \simeq S(\mathcal{C}_1^{(m)}(\Gamma))$;

2) $\mathcal{C}^{m+n}(\Gamma) \simeq \mathcal{C}^n(\mathcal{C}^m(\Gamma))$;

3) any morphism of weighted X-digraphs $\phi : \Delta \to \mathcal{C}^{(m)}(\Gamma)$ gives rise to a morphism $\mathcal{C}^{(n)}(\Delta) \to \mathcal{C}^{(m+n)}(\Gamma)$.

Proposition 14.22. Let $G = \langle X; R\rangle$ be a finite symmetrized presentation, Γ a weighted X-digraph, $N \in \mathbb{N} \cup \{\infty\}$, and $w = w(X)$. If $(\Gamma', N', \phi_{\mathcal{C}}) = S(\Gamma, N)$ then

(C1) (Γ, N) is a pseudo conjugacy graph of w in G if and only if (Γ', N') is.

(C2) If (Γ, N) is a pseudo conjugacy graph of w in G then $\phi_{\mathcal{C}}$ is a PCG-morphism.

Proof. Since (Γ', N) is obtained by a sequence of basic extensions of (Γ, N) with relators of G and then by a Stalling's procedure the statement of the proposition follows from Propositions 14.16 and 14.6.

□

Notice that on the level of X-digraphs Algorithm 14.18 works exactly as its counterpart for the Word problem (Algorithm 4.1).

Proposition 14.23. The R-extension operator is a functor from the category of pseudo conjugacy graphs to a category of folded pseudo conjugacy graphs.

Proof. Since R-extension algorithm is a combination of basic extensions and stalling's fold, the assertion follows from Propositions 14.17 and 14.14. □

Let $\langle X; R\rangle$ be a finite presentation and D be a van Kampen diagram over $\langle X; R\rangle$. The diagram D can be viewed as a weighted X-digraph by assigning weight zero to each edge in D. It is straightforward to check that for any $w = w(X)$ the pair (D, ∞) is a pseudo conjugacy graph of $w \in G$.

Let D_0 be a weighted X-digraph consisting of one vertex v_0 and no edges. Let v be a vertex in ∂D starting from which w is read on ∂D. Let $\tau : D_0 \to D$ be a PCG-morphism such that $\tau(v_0) = v$. The following lemma holds.

Lemma 14.24. *Let $m = \delta_v(D)$ the depth of D with respect to the vertex v. There exists a PCG-morphism $\theta : D_0 \to \mathcal{C}^{(m)}(D_0)$ such that the following diagram com-*

mutes

$$\begin{array}{ccc} (D_0,\infty) & \overset{\tau}{\hookrightarrow} & (D,\infty) \\ & \searrow^{\phi_{\mathcal{C}}} & \downarrow^{\theta} \\ & & \mathcal{C}^{(m)}((D_0,\infty)) \end{array}$$

Therefore, there exists a loop c in $(\Gamma', N') = \mathcal{C}^{(m)}((D_0,\infty))$ such that $\mu(c) = w$ and $\gamma(c) \equiv 0 \mod N'$.

Proof. Similar to a proof of Proposition 4.12. □

15 Conjugacy graphs

Let G be a group, $X \subseteq G$ its generating set closed under inversions, and $w = w(X)$. In Section 15.1 we show that there exists a conjugacy graph of w in G relative to X and it is unique up to isomorphisms of pseudo conjugacy graphs. Further, in Section 15.2, we show that if $\langle X; R\rangle$ is a finite presentation and $G = \langle X; R\rangle$ then the conjugacy graph of w in G can be approximated as a limit of certain weighted X-digraphs.

15.1 Existence

Let G be a group, $X \subseteq G$ its generating set closed under inversions, and $w = w(X)$. We will construct a conjugacy graph of w in G directly. Denote by $\Gamma_H(X)$ the Schreier graph of a subgroup H in G relative to the generating set X.

Lemma 15.1. *Let $u = u(X)$. Then $u \simeq_G w^\gamma$ for some $\gamma \in \mathbb{N}$ if and only $\Gamma_{\langle w\rangle}(X)$ contains a loop labelled with u.*

Proof. Indeed, $u \sim_G w^\gamma$ for some $\gamma \in \mathbb{N}$ if and only there exists $s = s(X)$ such that $sus^{-1} =_G w^\gamma$. Let v be the endpoint of a path in $\Gamma_{\langle w\rangle}(X)$ starting at H and labelled with s. By equality $sus^{-1} =_G w^\gamma$ there exists a loop at v labelled with u.

□

Let $\Gamma = \Gamma_{\langle w \rangle}(X)$ and T a spanning tree in Γ. For each vertex $v \in \Gamma$ denote by π_v the path in T connecting the initial vertex (corresponding to $\langle w \rangle$) and v. Define a function $\gamma : E(\Gamma) \to \mathbb{N}$ as follows. Let $e = v_1 \xrightarrow{x} v_2$. If $e \in T$ then put $\gamma(e) = 0$. If $e \notin T$ then put $\gamma(e) = \gamma$ where $\gamma \in \mathbb{N}$ is the smallest number such that $\mu(p_{v_1} e p_{v_2}^{-1}) = w^\gamma$.

Theorem 15.2. *Let G be a group, $X \subseteq G$ its generating set closed under inversions, and $w = w(X)$. Let $\Gamma = \Gamma_{\langle w \rangle}(X)$ and $N \in \mathbb{N} \cup \{\infty\}$ the order of w in G. Then (Γ, γ, N) is a conjugacy graph of w in G.*

Proof. The property (CG2) is clearly satisfied by the choice of N. Suppose $u \sim w^\gamma$ for some $u = u(X)$ and $\gamma \in \mathbb{N}$. Then by Lemma 15.1 there exists a loop π at some vertex v in Γ labelled with u. Let

$$\pi' = p_v \cdot \pi \cdot p_v^{-1}$$

and $e_1^{\varepsilon_1} \dots e_k^{\varepsilon_k}$ a sequence of edges outside of T π' passes (where $\varepsilon_i = \pm 1$ and $e_i = v_{i,1} \xrightarrow{x_i} v_{i,2}$). Clearly,

$$\mu(\pi') =_{F(X)} \mu\left((p_{v_{1,1}} e_1 p_{v_{1,2}}^{-1})^{\varepsilon_1} \dots (p_{v_{k,1}} e_k p_{v_{k,2}}^{-1})^{\varepsilon_k} \right) =$$

$$= \mu(p_{v_{1,1}} e_1 p_{v_{1,2}}^{-1})^{\varepsilon_1} \dots \mu(p_{v_{k,1}} e_k p_{v_{k,2}}^{-1})^{\varepsilon_k} =$$

$$=_G w^{\varepsilon_1 \gamma(e_1)} \dots w^{\varepsilon_k \gamma(e_k)} =_G w^{\varepsilon_1 \gamma(e_1) + \dots + \varepsilon_k \gamma(e_k)}$$

and

$$\gamma(\pi') = \gamma\left((p_{v_{1,1}} e_1 p_{v_{1,2}}^{-1})^{\varepsilon_1} \dots (p_{v_{k,1}} e_k p_{v_{k,2}}^{-1})^{\varepsilon_k} \right) =$$

$$= \varepsilon_1 \gamma(e_1) + \dots + \varepsilon_k \gamma(e_k).$$

Thus, $\mu(\pi') =_G w^{\gamma(\pi')}$. Finally notice that $\mu(\pi) = \mu(p_v)\mu(\pi')\mu(p_v)^{-1}$ and $\gamma(\pi) = \gamma(\pi')$. Thus, $\mu(\pi) \sim_G w^{\gamma(\pi)}$.

The argument above can be converted to show that if π is a loop in Γ then $\mu(\pi) \sim_G w^{\gamma(\pi)}$. Thus, (CG1) holds for (Γ, γ, N).

□

We would like to finish this section with a remark that a conjugacy graph of $w \in G$ is not unique as a weighted graph. For instance, if (Γ, N) is a conjugacy graph and v is a vertex in Γ then an application of a shift operator $Shift_1(\Gamma, v)$ changes the weight function, while not affecting the property of (Γ, N) to be a conjugacy graph. In the next section we show that Γ is unique up to values of a weight function γ.

15.2 Conjugacy graph approximation

In this section we show that one can construct the conjugacy graph of $w \in G$ as a limit of a certain sequence of pseudo conjugacy graphs of $w \in G$. The procedure is analogous to Todd-Coxeter algorithm enumerating cosets of the Schreier's graph $\Gamma_{\langle w \rangle}(X)$ of $\langle w \rangle$ relative to X.

Let $G = \langle X; R \rangle$ be a finite symmetrized presentation such that all generators X are non-trivially involved in R and $w = w(X)$. We define a sequence of pseudo conjugacy graphs $\{(\Gamma_i, N_i)\}_{i \in \mathbb{N}}$ as follows. Put

$$(\Gamma_0, N_0) = (Loop_1(w), \infty)$$

and, recursively, put

$$(\Gamma_{i+1}, N_{i+1}, \varphi_i) = \mathcal{C}(\Gamma_i, N_i)$$

where $\varphi_i : \Gamma_i \to \Gamma_{i+1}$ is the corresponding canonical morphisms. With φ_i the sequence (Γ_i, N_i) can be viewed as an ascending chain of pseudo conjugacy graphs.

Denote the corresponding limit by

$$(\Gamma_\infty, N_\infty) = \lim_{i\to\infty}(\Gamma_i, N_i).$$

Theorem 15.3. (Approximation of conjugacy graphs) *Let $\langle X; R\rangle$ be a finite symmetrized presentation such that all generators X are non-trivially involved in R, $G = \langle X; R\rangle$, and $w = w(X)$. Then $(\Gamma_\infty, N_\infty)$ is a conjugacy graph of $w \in G$.*

Proof. Let $u = u(X)$ and $\gamma \in \mathbb{N}$ be such that $u =_G s^{-1}w^\gamma s$ for some word $s = s(X)$. Then there exists a van Kampen diagram D over $\langle X; R\rangle$ with a boundary label

$$W = w^\gamma s u^{-1} s^{-1}.$$

Let v be a vertex in ∂D starting from which W is read along ∂D and $m = \delta_v(D)$ the depth of D with respect to v. Let D_0 be an X-digraph containing exactly one vertex v_0 and no edges. Let $\tau : D_0 \to D$ such that $\tau(v_0) = v$ and $\tau_2 : D_0 \to Loop_1(w)$ where $\tau(v_0)$ is the initial vertex of $Loop_1(w)$. By Proposition 14.24 there exists a morphism θ and by Proposition 14.23 there exists a morphism θ_2 such that the following diagram commutes.

$$\begin{array}{ccc}
(D_0, \infty) & \xrightarrow{\tau} & (D, \infty) \\
\downarrow{\scriptstyle \tau_2} & \searrow{\scriptstyle \phi_{\mathcal{C}}} & \downarrow{\scriptstyle \theta} \\
(Loop_1(w), \infty) & & \mathcal{C}^{(m)}((D_0, \infty)) \\
 & \searrow{\scriptstyle \phi_{\mathcal{C}}} & \downarrow{\scriptstyle \theta_2} \\
 & & \mathcal{C}^{(m)}((Loop_1(w), \infty)) \quad = (\Gamma_m, N_m)
\end{array}$$

Therefore, there is a loop π in Γ_m starting at the base vertex v_m of Γ_m such that $\mu(\pi) = w^\gamma s u^{-1} s^{-1}$ and $\gamma(\pi) \equiv 0 \mod N_m$. Since Γ_m is folded and contains a loop π_{Γ_m} at v_m such that $\mu(\pi_{\Gamma_m}) = w$ and $\gamma(\pi_{\Gamma_m}) \equiv 1 \mod N_m$ the path π can be

decomposed into $c^m p^{-1} t p$, where p is a path starting at v_m and is labelled with s and t is a loop starting at $\beta(s)$ labelled with u^{-1}. Hence,

$$\gamma(\pi) = \gamma(\pi_{\Gamma_m}^m) + \gamma(s) + \gamma(t) - \gamma(s) = m\gamma(\pi_{\Gamma_m}) + \gamma(t) \equiv 0 \mod N_m.$$

Thus, $\gamma(t^{-1}) \equiv m \mod N_m$ and $\mu(t^{-1}) = u$ and the property (CG1) holds. Property (CG2), which requires N to be the order of w, can be shown the same way by considering a diagram with the boundary label w^n.

□

Observe, that the action of R-extension on pseudo conjugacy graphs coincides with the action of R-extensions on X-digraphs. Therefore, Γ_∞, if considered as an X-digraph, is the Schreier's graph $\Gamma_{\langle w \rangle}(X)$ of the cyclic subgroup $\langle w \rangle$ in G which is unique up to isomorphism. Moreover, the next proposition holds.

Proposition 15.4. Let (Γ, N) be a conjugacy graph of $w \in G$. Then $N = N_\infty$ and there exists a PCG-morphism $\tau : \Gamma \to \Gamma_\infty$.

Proof. By the property (CG1) of conjugacy graphs $N = N_\infty$. Now, we show that the required morphism $\tau : \Gamma \to \Gamma_\infty$ exists. Let π_Γ be a loop in Γ such that $\mu(\pi_\Gamma) = w$ and $\gamma(\pi_\Gamma) \equiv 1 \mod N$, and v_Γ the initial vertex of π_Γ. If π is a loop in Γ at v_Γ then $\mu(\pi) =_G w^{\gamma(\pi)}$.

Consider Γ_∞. Let π_{Γ_∞} be the base loop in Γ_∞ (the image of the initial graph $Loop_1(w)$) and v_{Γ_∞} be its initial vertex. It follows from the proof of Theorem 15.3 that there is a loop $\pi' \in \Gamma_\infty$ such that $\mu(\pi') = \mu(\pi)$ and $\gamma(\pi') \equiv \gamma(\pi) \mod N$. Therefore, since Γ and Γ_∞ are folded there exists the required PCG-morphism.

□

Proposition 15.5. (*On initial approximation*) For any pseudo conjugacy graph

(Γ, N) of w in G which contains a loop labelled with w

$$\lim_{i\to\infty} \mathcal{C}^{(i)}(\Gamma, N) = (\Gamma_\infty, N_\infty).$$

Proof. By Proposition 14.23 the following diagram commutes:

$$\begin{array}{ccc} (Loop_1(w), \infty) & \to & (\Gamma, N) \\ \downarrow & & \downarrow \\ \mathcal{C}^{(i)}((Loop_1(w), \infty)) & \to & \mathcal{C}^{(i)}((\Gamma, N)) \end{array}$$

Thus, the result.

□

This method can be used for computation of the order of a word w in G. If for some m the number N_m is finite then w has a finite order in G which is a divisor of N_m. Of course, the same result can be obtained by variations of coset enumeration (Todd Coxeter algorithm), but our algorithm seems to be more natural and efficient. Though there are no any experimental evidences of this statement. The principal thing is that on each step we have all powers of w in pseudo conjugacy graph. While using the Todd-Coxeter technique each time we have only a limited number of powers of w. So, if w has a large order n, it will take a long time for the Todd-Coxeter just to construct a path labelled with w^n.

16 Annular (Schupp) diagrams

Let $\langle X; R\rangle$ be a finite presentation and $G = \langle X; R\rangle$. An *annular diagram* or *singular annulus* over $\langle X; R\rangle$ is a pair (S, f), where S is a finite combinatorial annulus, and f a dimension preserving map from S into the Cayley complex $C = C(X; R)$.

Any annular diagram D is bounded by two paths, one of which bounds D from

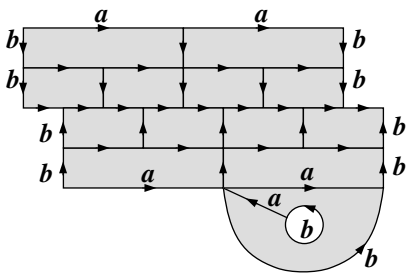

Figure 17: Example of an annular diagrams over $\langle a, b; a^b = a^2\rangle$ with boundary labels (read in counterclockwise direction) b and $b^3a^{-1}b^{-2}a^{-2}b^2ab^{-2}a$. Missing labels of horizontal edge are a's and of vertical edges are b's.

the inner hole and the other bounds D from the outer space. The inner boundary of D will be denoted by $\partial_{in}D$ and the outer boundary of D will be denoted by $\partial_{out}D$. Thus, $\partial D = \partial_{in}D \cup \partial_{out}D$.

Let D_1 and D_2 be diagrams over $\langle X; R\rangle$. We say that D_1 and D_2 are *isomorphic* if there exists a homeomorphism of the Euclidean plane which induces an isomorphism of corresponding 2-complexes.

Proposition 16.1. (*Existence of annular diagrams.*) Let $G = \langle X; R\rangle$ be a finitely presented group and $w_1 = w_1(X)$, $w_2 = w_2(X)$. Words w_1 and w_2 are conjugate in G if and only if there exists an annular diagram D over $\langle X; R\rangle$ such that $\mu(\partial_{in}D) = w_1$ and $\mu(\partial_{out}D) = w_2$.

Proof. If w_1 and w_2 are conjugate in G then there exists $v = v(X)$ such that $w_1 = v^{-1}w_2v$ holds in G. Therefore (by van Kampen Lemma) there exists a van Kampen diagram D' over $\langle X; R\rangle$ with the boundary label $w_1^{-1}v^{-1}w_2v$. Sewing D' along v^{-1} and v we obtain the required diagram D.

To show the converse we define p to be a shortest path in D from $\alpha(\partial_{in}D)$ and $\alpha(\partial_{out}D)$ and cut A along p. Denote the result by D'. Since p is a shortest path in D the diagram D' is connected and simply connected. Hence, D' is a van Kampen diagram labelled with $w_1^{-1}v^{-1}w_2v$ and the statement is proved.

□

Let D be an annular diagram over $\langle X; R\rangle$. We will say that $|\partial_{in} D| + |\partial_{out} D|$ is a *perimeter* of D and denote it by $l(D)$.

16.1 Depth of annular diagrams

Definition 16.2. *(Vertex chain.)* Let D be an annular diagram over $\langle X; R\rangle$. A sequence of vertices $v_1, \dots, v_k$ is called a *vertex chain* if each pair v_i, v_{i+1} $(i = 1, \dots, k-1)$ belongs to some cell or free edge c_i in D. We say that a chain $v_1, \dots, v_k$ has *length* k.

Let K_1 and K_2 be two subcomplexes of D. We say that K_1 and K_2 are connected by a chain in D if there exists a vertex chain $v_1, \dots, v_q \in M$ such that $v_1 \in K_1$ and $v_q \in K_2$. The length of the shortest chain connecting K_1 and K_2 is called the *chain distance* $d(K_1, K_2)$ between K_1 and K_2.

Recall the definition of depth of 2-complexes. Let K be a subcomplex of a 2-complex L. The number

$$\delta_K(L) = \max\{d(K, \overline{c}) \mid c \in (C(L) \setminus C(K)) \cup (FE(L) \setminus FE(K))\}$$

is called the *depth* of L with respect to K.

Definition 16.3. *(Depth of an annular diagram.)* The depth of an annular diagram D is the number

$$\delta(D) = \delta_{\partial D}(D) = \max_{K \in C(D)} \{d(K, \overline{c}) \mid c \in E(\partial D)\}.$$

Definition 16.4. *(Depth of a pair of words.)* Let $\langle X; R\rangle$ be a finite presentation, $w_1 = w_1(X)$, and $w_2 = w_2(X)$. Denote by $D(w_1, w_2)$ the set of all annular diagrams over $\langle X; R\rangle$ with boundary labels w_1 and w_2. Define the depth $\delta(w_1, w_2)$ of a pair

(w_1, w_2) as follows:

$$\delta(w_1, w_2) = \begin{cases} \min\{\delta(D) \mid D \in D(w_1, w_2)\} & \text{if } D(w_1, w_2) \neq \emptyset \\ \infty & \text{otherwise.} \end{cases}$$

16.2 Annular diagrams as pseudo conjugacy graphs

Let $\langle X; R\rangle$ be a finite presentation and D be an annular diagram over $\langle X; R\rangle$ with boundary labels w_1 and w_2. In this section we show that D can be viewed as a pseudo conjugacy graph of w_1 or w_2 in G.

Our goal is to construct a weight function for D. Denote by v_0 the initial vertex of $\partial_{in}D$ (to be treated as the base vertex). Let T be a spanning tree for D. For each vertex $v \in V(D)$ denote by p_v a path from v_0 to v in T. Define a function $\gamma_T : E(D) \to \mathbb{Z}$ the following way. For $e = v_1 \xrightarrow{x} v_2$ put $\gamma(e) = 0$ if $e \in T$ and put $\gamma(e)$ to be the number of times the loop $p_{v_1} e p_{v_2}^{-1}$ goes around the inner hole (in a counter clockwise direction) if $e \notin T$. Denote by D_T the pair (D, γ_T).

Proposition 16.5. Let D be an annular diagram over $\langle X; R\rangle$ such that $\mu(\partial_{in}D) = w_1$ and $\mu(\partial_{out}D) = w_2$. The pair (D_T, ∞) is a pseudo conjugacy graph of w_1 (and w_2) in G.

Proof. Clearly, the property (PCG2) holds for (D_T, ∞). To prove the property (PCG1') consider an arbitrary loop π in D. If $\pi = p_{v_1} e p_{v_2}^{-1}$ for some $e \in E(D) \setminus T$ then, by definition of γ_T, $\mu(\pi) =_G w^{\gamma_T(\pi)}$. If π is some other loop then arguing as in the proof of Theorem 15.2 one can show that $\mu(\pi) \sim_G w^{\gamma_T(\pi)}$.

□

17 Conjugacy search problem

Pseudo conjugacy graphs can be used to solve the Conjugacy search problem in a similar way as approximations of Cayley graphs are used to solve the Word search problem. In this section we use ideas of Sections 14, 15, and 16 to construct an algorithm solving the Conjugacy search problem.

17.1 Annular diagram bisection

In this section we will prove the conjugacy criterion theorem. This theorem will allow us later to express the complexity of the Conjugacy search problem in terms of depth of annular diagrams.

First, we show that any annular diagram D can be cut into two annular diagrams D_1, D_2 in a certain way. Denote $\partial_{out}D$ by l_1 and $\partial_{in}D$ by l_2. Suppose $m = \delta(D)$. Let π be an edge simple, without self-intersections loop in D which goes exactly once around of the annular hole. The loop π cuts D into two annular diagrams D_1 and D_2. Since π is edge simple $\partial D_1 = l_1 \cup \pi$ and $\partial D_2 = l_1 \cup \pi$. We say that π *cuts D in the middle* if $\delta_{l_1}(D_1) \leq m$ and $\delta_{l_2}(D_2) \leq m$, i.e. cells in D_1 and in D_2 are at distance at most m from the outer boundaries l_1 and l_2 resp.

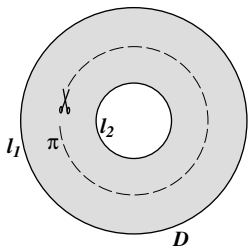

Figure 18: Middle-cut.

Proposition 17.1. Any annular diagram D over $\langle X; R\rangle$ can be cut in the middle.

Proof. Let D be an annular diagram over $\langle X; R\rangle$ and $m = \delta(D)$. Define a function α on the set of cells $C(D)$ into the set $\{1, 2\}$ which will specify to which part (D_1

or D_2) cells will belong. If $d(c, \partial D) = 1$ then put $\alpha(c) = 1$ if c touches l_1 (i.e. $\partial c \cap l_1 \neq \emptyset$) and $\alpha(c) = 2$ otherwise. If $d(c, \partial D) = 2$ then put $\alpha(c) = 1$ if $d(c, l_1) = 2$ and $\alpha(c) = 1$ otherwise. Otherwise put $\alpha(c) = 2$. And so on. The function α defines a partition of $C(D)$ into cells with $\alpha = 1$ and $\alpha = 2$. Observe that free edges in D belong to ∂D. Therefore, using α we can define two submaps P_1 and P_2 of D. The submaps P_1 and P_2 are connected, but, in general, not simply connected.

We say that a sequence of cells $\overline{c} = c_1, \ldots, c_k$ in D is a *cell-chain* if for each $j = 1, \ldots, k-1$

$$\partial c_j \cap \partial c_{j+1} \neq \emptyset.$$

The number k is called the length of $\overline{c}$ and is denoted by $|\overline{c}|$. We say that a cell-chain $c_1, \ldots, c_k$ is geodesic if k is the smallest length of a cell-chain connecting c_1 and c_k. We will be interested in geodesic chains such that $\partial c_k \cap l_i \neq \emptyset$, i.e. geodesics that connect some cell c_1 with the boundary. Note that any such chain entirely belongs to P_1 or P_2.

Let $\overline{c} = c_1, c_2, \ldots, c_k \in P_i$ $(i = 1, 2)$ be a geodesic cell-chain connecting c_k with ∂D. It follows from the definition of α that $d(c_k, l_i) = k$.

Let $\overline{c} = c_1, c_2, \ldots, c_k \in P_1$ be a geodesic connecting c_k with l_1 and $\overline{d} = d_1, d_2, \ldots, d_m \in P_2$ be a geodesic connecting d_m with l_2. We claim that they do not intersect, i.e., the situation in Figure 19 is impossible.

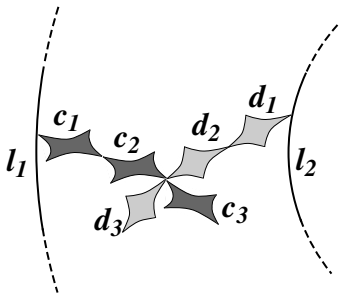

Figure 19: Intersection of geodesic cell-chains in an annular diagram.

Assume to the contrary that two geodesic cell-chains $\overline{c}$ and $\overline{d}$ intersect at a vertex

v. Let c_s, c_{s+1} and d_t, d_{t+1} be cells in $\overline{c}$ and $\overline{d}$ respectively connected to v. Since a part of a geodesic is a geodesic we have $d(c_s, \partial D) = d(c_{s+1}, \partial D) + 1$ and $d(d_t, \partial D) = d(d_{t+1}, \partial D) + 1$. Since all these cells share v we have $d(c_s, \partial D) = d(d_t, \partial D)$ and, hence, $s = t$. But then d_{t+1} must belong to P_1 since it is attached to a cell c_s. Contradiction.

Now, we show that the required loop cutting D in the middle exists. For that we will construct a sequence of loops $\pi_0, \ldots, \pi_m$ which satisfies the following properties:

1) Each π_i $(i = 0, \ldots, m)$ is edge-simple and has no self intersections.

2) Each loop π_i cuts D into two annular diagrams A_i (outer) and B_i (inner) such that if φ_i is a projection of A_i into D then $\varphi_i(A_i) \subseteq P_1$.

3) Moreover, $\varphi_i(A_i)$ is a proper submap of $\varphi_{i+1}(A_{i+1})$ in P_1.

4) Any geodesic from any cell $c \in \varphi_i(A_i)$ is contained in $\varphi_i(A_i)$.

5) Any geodesic from any cell $c \in \varphi_i(B_i) \cap B_i$ is contained in $\varphi_i(B_i)$.

Put $\pi_0' = l_1$. If $\pi_0' = e_1 \ldots e_k$ is not vertex-simple then it contains a proper subloop $\pi = e_i \ldots e_j$ which goes 0 times around the hole. Let c be a cell bounded by π. Clearly, $d(c, l_1) = d(c, \partial A)$ and, hence, $\alpha(c) = 1$. Remove all such subloops from π_0' and denote the result by π_0 (see Figure 20).

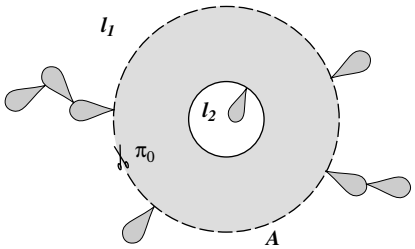

Figure 20: The loop π_0.

Assume that π_i is already constructed and let P_1' a set of cells in P_1 that do not belong to $\varphi_i(A_i)$. Let c be a cell in P_1' with the smallest value $d = d(c, \partial D)$. If $d = 1$

then c touches l_1 at some vertex v. Otherwise, it touches some cell c' which belongs to $\alpha_i(A_i)$ at a vertex v. In both case we perform the following transformations of π_i (see Figure 22.b and 22.c):

a) Let $e_1 \dots e_k$ be a boundary ∂c starting from the vertex v.

b) Insert $e_1 \dots e_k$ in π_i, into the position corresponding to v so that the obtained loop does not intersect itself.

c) Remove backtracks from the obtained path. Denote the result by π'_{i+1}.

Let $e_i \dots e_j$ be a segment of $e_1 \dots e_k$ and $d_1 \dots d_m$ a segment of π_i remained after removing backtracks. It is possible that a loop π'_{i+1} is not edge-simple (and we want π_{i+1} to be edge simple). Consider two cases: ∂c is not edge-simple or ∂c is edge-simple.

Suppose ∂c is not edge-simple, i.e., touches itself (see Figure 21). Since we assume

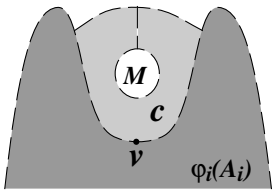

Figure 21: Case when π'_{i+1} is not edge-simple.

that all relators are cyclically reduced, c bounds a van Kampen diagram, denote it by M. It easy to see that for each cell c' in M $d(c', \partial D) = d(c', l_1)$ and, therefore, $\alpha(c') = 1$. Let π''_{i+1} be a loop obtained from π'_{i+1} by removing the boundary of M and then removing backtracks. Clearly, π''_{i+1} is edge-simple and the outer diagram which it cuts has projection in P_1. Denote π''_{i+1} by π_{i+1}.

Suppose that ∂c is edge-simple. Then, since π'_{i+1} is not edge-simple, there are edges d_a and e_b (for some $1 \leq a \leq m$ and $1 \leq b \leq k$) such that $d_a = e_b^{-1}$ (see Figure 22).

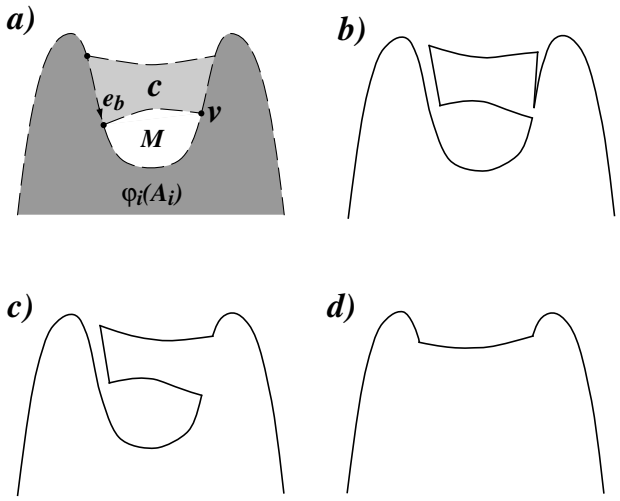

Figure 22: Case when π'_{i+1} is not edge-simple (figure a). Construction of π_{i+1} (cuts after steps b) and c) resp.). Figure d) shows the final result which is obtained by the removal of the internal loop.

Let x be the obtained subloop in π'_{i+1}, M a submap bounded by x, and f a cell in M. Consider two cases. If e_b belongs to l_1 then $d(f, l_1) = 1$. It is easy to see that $\alpha(f) = 1$ in this event. We remove a subloop x from π'_{i+1} and then remove backtracks from the obtained loop.

Assume that e_b does not belong to l_1 (Figure 22). Let c' be a cell such that $c' \neq c$ and $e_b \in \partial c'$. The cell c' belongs to $\varphi_i(A_i)$. Let $\overline{c}'$ be a geodesic cell-chain from c' to l_1 and $\overline{c}$ be a geodesic cell-chain from c to l_1. Both geodesic chains belong to $\varphi_i(A_i)$ and bound M. Therefore, $\alpha(f) = 1$ (otherwise there would be a geodesic from f to l_2 which intersects some geodesic to l_1). As before, remove a subloop x from π'_{i+1} and then remove backtracks from the obtained loop.

Moreover, if adding c to $\alpha_i(A_i)$ introduces a new "hole" and c touches a cell c' such that $d(c, \partial D) = d(c', \partial D) + 1$ at just a vertex then using the same argument one can show that the hole can be added in $\alpha_i(A_i)$ together with c.

Denote the obtained loop by π_{i+1}. The loop π_{i+1} cuts A into two parts: the outer partA_{i+1} and be the inner part B_{i+1}. Let α_{i+1} be a sewing morphism from A_{i+1} into A. Clearly, the obtained π_{i+1} has no self-intersections and is edge-simple

as shown above. Moreover, any geodesic from each cell $c \in \varphi_{i+1}(A_{i+1})$ is contained in $\varphi_{i+1}(A_{i+1})$.

□

Proposition 17.2. Let D be an annular diagram, $l_2 = \partial_{in} D$, $w_2 = \mu(l_2)$, and $m = \delta_{l_1}(A)$. Then there exists a PCG-morphism θ from the pseudo conjugacy graph (D, ∞) of $w_2 \in G$ into $\to \mathcal{C}^{(m)}((Loop_1(w_2), \infty))$ such that the diagram below commutes.

$$\begin{array}{ccc} (Loop_1(w_2), \infty) & \xrightarrow{\tau} & (D, \infty) \\ & \searrow^{\phi_C} & \downarrow^{\theta} \\ & & \mathcal{C}^{(m)}((Loop_1(w_2), \infty)) \end{array}$$

where τ maps $Loop_1(w_2)$ onto ∂D.

Proof. The proof of this proposition is similar to the proof of Proposition 17.1. We say that a diagram D is a "forest on a loop" (see Figure 23) if:

1) its inner boundary is a vertex-simple loop;

2) If $c_1, c_2 \in C(A) \cup FE(A)$ then $|\partial c_1 \cap \partial c_2| \leq 1$.

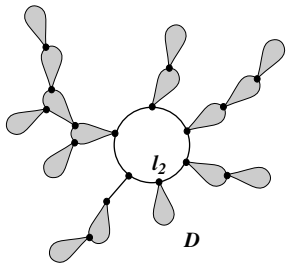

Figure 23: Forest of cells and free edges on a loop.

First we cut D into an annular diagram which is a "forest on a loop l_2". The loop along which we cut D is constructed in a sequence of steps $\pi_0, \ldots, \pi_k$ satisfying the following properties:

1) Each π_i cuts D into two annular diagrams A_i and B_i.

2) A_i is a "forest on a loop l_2" diagram.

3) If φ_i is a projection of A_i into D then $\varphi_i(A_i)$ is a proper submap of $\varphi_{i+1}(A_{i+1})$.

4) If $c \in A_i$ then the chain-distance from c to l_2 in A_i is the same as $d(\varphi_i(c), l_2)$ in D.

Let $\pi_0 = l_2$ – the inner loop of D. The loop π_0 cuts D in two parts: A_0 which is a loop labelled with w_2 ($A_0 = Loop_1(w_2)$) and $B_0 = D$.

Assume that π_i is the last loop constructed in D. If A_i contains all cells from D then we stop. Otherwise take a cell c which does not belong to A_i with the least value $d = \delta_{l_2}(c)$. If $d = 1$ then c touches l_2 (i.e., $\partial c \cap l_2 \neq \emptyset$) at some vertex v. Let $e_1 \dots e_a = \partial c$ (starting from the vertex v). In this case ($d = 1$) we insert $e_1 \dots e_a$ into the corresponding position of π_i (see Figure 22.b). Denote the obtained loop by π_{i+1}.

If $d > 1$ then c touches some cell c' such that $c' \in A_i$ and $\delta_{l_2}(c') = \delta_{l_2}(c) - 1$ at some vertex v. Again, let $e_1 \dots e_a = \partial c$ (starting from the vertex v). Insert $e_1 \dots e_a$ into the corresponding position of π_i. Denote the obtained loop by π_{i+1}.

Clearly, the obtained loop π_{i+1} satisfies all the stated above conditions 1)-4) and the final diagram A_k, denote it by D', is the required annular diagram. Since D' is obtained by cutting D there exists an sewing morphism $\phi_1 : D' \to D$ which maps a boundary l_2 onto itself. Because of the type of D' there exists a graph morphism $\theta' : D' \to \mathcal{C}^{(m)}(Loop_1(w_2))$ such that the following diagram commutes:

$$\begin{array}{ccccc} Loop_1(w_2) & \xrightarrow{\tau} & D' & \xrightarrow{\phi_1} & D \\ & \searrow^{\phi_{\mathcal{C}}} & \downarrow^{\theta'} & & \\ & & \mathcal{C}^{(m)}(Loop_1(w_2)) & & \end{array}$$

Since ϕ_1 is a sewing morphism and $\mathcal{C}^{(m)}(Loop_1(w_2))$ is folded we can continue θ' through ϕ_1. The morphism θ which does that is a required graph morphism.

□

Theorem 17.3. (Conjugacy criterion) *Let D be an annular diagram, $w_1 = \mu(\partial_{out} D)$, $w_2 = \mu(\partial_{in} D)$, and $m = \delta(D)$. Let $\Gamma_1 = Loop_1(w_1)$ and $\Gamma_2 = Loop_1(w_2)$. Then there exist equally labelled paths $p_1 \in \mathcal{C}^{(m)}((\Gamma_1, \infty))$ and $p_2 \in \mathcal{C}^{(m)}((\Gamma_2, \infty))$ of weight 1 (i.e., $\mu(p_1) = \mu(p_2)$ and $\gamma(p_1) = \gamma(p_2) = 1$).*

Conversely, if for w_1, w_2 there exists a number m such that $\mathcal{C}^{(m)}((\Gamma_1, \infty))$ and $\mathcal{C}^{(m)}((\Gamma_1, \infty))$ contain paths p_1 and p_2 as above then $w_1 \sim_G w_2$.

Proof. Let D be an annular diagram of depth m. Let π cuts D in the middle into annular diagrams D_1, D_2 such that $\delta_{l_i}(D_i) \leq m$ $(i = 1, 2)$. By Proposition 17.1 $\partial D_1 = l_1 \cup \pi$ and $\partial D_2 = l_2 \cup \pi$. By Proposition 17.2 there exist graph morphisms $D_i \to \mathcal{C}^{(m)}(Loop_1(w_i))$ $(i = 1, 2)$. Images of c in $\mathcal{C}^{(m)}(Loop_1(w_i))$ are the required paths p_1 and p_2.

□

17.2 Conjugacy search algorithm

In this section, using the ideas of the previous section, mostly Theorem 17.3, we design an algorithm for solving the Conjugacy search problem. At the end of the section we give estimates for time complexity of a proposed algorithm.

By Theorem 17.3 if pseudo conjugacy graphs $\Gamma_1 = \mathcal{C}^{(m)}(Loop_1(w_1))$ and $\Gamma_2 = \mathcal{C}^{(m)}(Loop_1(w_2))$ contain equally labelled loops p_1 and p_2 resp. of weight 1 then $w_1 \sim_G w_1$. The next lemma shows how to find a conjugator for w_1 and w_2 in this situation. Let π_{Γ_i} (where $i = 1, 2$) be a base loop in Γ_i such that $\mu(\pi_{\Gamma_i}) = w_i$ and $v_{\Gamma_i} = \alpha(\pi_{\Gamma_i})$.

Lemma 17.4. *Let q_1 be a path from $\alpha(p_1)$ to v_1 and q_2 a path from $\alpha(p_2)$ to v_2 and $x = \mu(q_2)^{-1}\mu(q_1)$. Then $w_1 =_G x^{-1} w_2 x$.*

Proof. Since $\gamma(p_1 q_1 \pi_{\Gamma_1}^{-1} q_1^{-1}) = 0$ and $\gamma(p_2 q_2 \pi_{\Gamma_2}^{-1} q_2^{-1}) = 0$ we have $\mu(p_1)\mu(q_1)w_1^{-1}\mu(q_1)^{-1} =_G 1$ and $\mu(p_2)\mu(q_2)w_2^{-1}\mu(q_2)^{-1} =_G 1$. Finally, since $\mu(p_1) = \mu(p_2)$ we have

$$\mu(q_1)w_1\mu(q_1)^{-1} =_G \mu(q_2)w_2\mu(q_2)^{-1}$$

and, hence,

$$w_1 =_G \mu(q_1)^{-1}\mu(q_2)w_2\mu(q_2)^{-1}\mu(q_1).$$

□

Next, we show that there exists an effective algorithm for loops p_1 and p_2 (with stated above properties) when they exist in Γ_1 and Γ_2 respectively. The next definition is a generalization of a product of X-digraphs.

Definition 17.5. *(Product of weighted X-digraphs.)* Let Γ_1 and Γ_2 be two weighted X-digraphs. Let $\Gamma = \Gamma_1 \times \Gamma_2$ be a product of Γ_1 and Γ_2 as X-digraphs (see [18]) and let $\pi_1 : \Gamma \to \Gamma_1$ and $\pi_2 : \Gamma \to \Gamma_2$ be projection functions. A *product graph* of Γ_1 and Γ_2 is an X-digraph Γ with a weight functions $\gamma_\Gamma = (\gamma_1, \gamma_2)$ defined on $e \in \Gamma$ the following way:

$$\gamma_\Gamma(e) = (\gamma_{\Gamma_1}(\pi_1(e)), \gamma_{\Gamma_2}(\pi_2(e))).$$

Observe, that $\Gamma_1 \times \Gamma_2$ is not a weighted X-digraph as it is defined in Section 13.1 (since the range of γ_Γ is $\mathbb{N} \times \mathbb{N}$). Nevertheless, one can extend the function γ_Γ on paths in Γ as follows; for $p = e_1 \dots e_k$ (where $e_i = (e_i', e_i'')$) put $\gamma_\Gamma(p) = (\sum_{i=1}^k \gamma_{\Gamma_1}(e_i'), \sum_{i=1}^k \gamma_{\Gamma_2}(e_i''))$. So, we may think of Γ as of a weighted X-digraph.

Let $\Gamma = \Gamma_1 \times \Gamma_2$, $v = (v_1, v_2)$ be a vertex in Γ. Denote the set of all loops in Γ starting at v by L_v. Define the set of indices of L_v by

$$I_v = \{\gamma_\Gamma(\pi) \mid \pi \in L_v\}.$$

Lemma 17.6. (Weights of loops in a product of weighted X-digraphs) *The following holds:*

1) The set I_v is an ideal in $\mathbb{Z} \times \mathbb{Z}$.

2) If vertices u and v are connected in Γ then $I_u = I_v$.

Proof. Immediately follows from the additivity of the weight function. □

Proposition 17.7. Weighted graphs Γ_1 and Γ_2 have equally labelled loops of weight 1 if and only if $(1,1) \in I_v$ for some vertex $v = (v_1, v_2) \in \Gamma_1 \times \Gamma_2$.

Proof. "⇒" Let c_1 and c_2 be two cycles in Γ_1 and Γ_2 respectively such that $u = \mu(c_1) = \mu(c_2)$ and $\gamma_{\Gamma_1}(c_1) = \gamma_{\Gamma_2}(c_2) = 1$. Let $v_1 = \alpha(c_1)$ and $v_2 = \alpha(c_2)$. Clearly, there exists a loop in $\Gamma = \Gamma_1 \times \Gamma_2$ starting (v_1, v_2) labelled with u of weight $(1,1)$. Therefore $(1,1) \in I_v$.

"⇐" Reverse the argument above.

□

Now, our goal is to define an effective algorithm to compute I_v. Let $\Gamma = \Gamma_1 \times \Gamma_2$ and $v = (v_1, v_2)$ a vertex in Γ. Denote by Γ_v a connected component of Γ containing v. Let T be a spanning tree in Γ_v, E' be a subset of edges of Γ_v outside of T. For each $v' \in \Gamma_v$ denote by $p_{v'}$ the shortest path in T with the origin v and the terminus v'. Define a set X_v to be the set of cycles

$$X_v = \{p_{\alpha(e)} e p_{\beta(e)}^{-1} \mid e \in E'\}.$$

Lemma 17.8. (Generators of I_v) *The For any $v \in \Gamma = \Gamma_1 \times \Gamma_2$*

$$I_v = \langle \gamma_\Gamma(\pi) \mid \pi \in X_v \rangle.$$

Proof. The set X_v generates the fundamental group $\pi_0(\Gamma)$ of Γ (see [18]). Hence, any cycle in Γ_v is a product of loops from X_v and their inverses. So, the result follows from additivity of the weight function γ_Γ. □

To determine whether a pair $(1,1)$ belongs to I_v (for some $v = (v_1, v_2) \in \Gamma_1 \times \Gamma_2$) one can apply the Gauss elimination procedure to pairs X_v to compute the generating set for I_v. It is hard to estimate the complexity of this procedure since we do not know a priori the values $\gamma_\Gamma(\pi)$ generating I_v. We will give the final estimate up to the complexity of computation of the generating set for I_v. We would like to point out that any non-trivial value $\gamma_\Gamma(\pi)$ is a valuable information about w_1 and w_2 by itself.

The next algorithm checks whether two pseudo conjugacy graphs of w_1 and w_2 contain equally labelled loops of weight 1 and if they do then finds a conjugator for w_1 and w_2.

Algorithm 17.9. (Common cycle of weight 1)

INPUT: Pseudo conjugacy graphs Γ_1 and Γ_2 of w_1 and w_2 correspondingly with fixed base loops c_{Γ_1} and c_{Γ_2} labelled with w_1 and w_2 of weight 1.

OUTPUT: If equally labelled loops of weight 1 exists then output Yes with a conjugator x (where $w_1 = x^{-1}w_2x$). Otherwise output No.

COMPUTATIONS:

A) Compute $\Gamma = \Gamma_1 \times \Gamma_2$.

B) For each connected component Γ_v (where $v = (v_1, v_2)$):

   1) Compute the generating set $\{\gamma_\Gamma(\pi) \mid \pi \in X_v\}$ for I_v.

   2) Check if I_v contains $(1,1)$.

   3) If it does then compute paths $p_1 \in \Gamma_1$ from $\alpha(c_{\Gamma_1})$ to v_1 and $p_2 \in \Gamma_2$ from $\alpha(c_{\Gamma_2})$ to v_2. Output Yes and a word $\mu(p_2)\mu(p_1)^{-1}$

C) Output No.

Proposition 17.10. Let Γ_1 and Γ_2 be pseudo conjugacy graphs of w_1 and w_2 respectively and $n_1 = |V(\Gamma_1)|$, $n_2 = |V(\Gamma_2)|$. Then Algorithm 17.9 terminates in at most Cn_1n_2 steps (for some constant C) up to operation B.2).

Proof. Consider Algorithm 17.9 step by step. To construct $\Gamma = \Gamma_1 \times \Gamma_2$ it is required $C_1n_1n_2$ steps. Now in each component Γ_v it takes $|\Gamma_v|$ steps to construct a spanning tree and compute a generating set X_v for I_v.

□

Equipped with Algorithm 17.9 we can present an algorithm for the Conjugacy search problem.

Algorithm 17.11. *(Conjugacy search algorithm $\mathcal{A}_C$)*

INPUT: A finite symmetrized presentation $G = \langle X; R\rangle$, and words $w_1 = w_1(X)$ and $w_2 = w_2(X)$.

OUTPUT: If $w_1 \sim_G w_2$ then output Yes with a conjugator x (where $w_1 = x^{-1}w_2x$). Otherwise do not stop.

COMPUTATIONS:

A) Put $n = 0$, $(\Gamma_0, N_0) = (Loop_1(w_1), \infty)$, and $(\Delta_0, N_0') = (Loop_1(w_2), \infty)$.

B) Apply Algorithm 17.9 to graphs Γ_n and Δ_n.

C) If the answer is No then

1) Compute $(\Gamma_{n+1}, N_{n+1}) = \mathcal{C}(\Gamma_n, N_n)$.

2) Compute $(\Delta_{n+1}, N'_{n+1}) = \mathcal{C}(\Delta_n, N'_n)$.

3) Increment n.

4) Goto B).

D) If the answer is (Yes, x) then output (Yes, x).

Theorem 17.12. *Let $G = \langle X; R\rangle$ be a finite presentation, w_1 and w_2 be words in generators $X^{\pm 1}$. Let $m = \delta(w_1, w_2)$ then Algorithm 17.11 requires $C|w_1||w_2|L(R)^{2m}$ (for some constant C) steps to recognize w_1 and w_2 as conjugated (in case $m = \infty$ Algorithm 17.11 does not stop) and find a conjugator.*

Proof. Follows from Lemma 14.20 and Proposition 17.10.

□

18 Random annular diagrams

In this section we define a notion of a random annular diagram using techniques developed for random van Kampen diagrams in Part I. Recall how we introduced a discrete probability measure on diagrams using the random generators producing random diagrams, so the probability of a diagram was the probability of its generation.

First, recall some definitions from above. Let $\mathcal{K} = \{D_i \mid i \in \mathbb{N}\}$ be a countable (enumerable) collection of diagrams. In here we assume that diagrams from $\mathcal{K}$ are annular diagrams over some fixed presentation $\langle X; R\rangle$ equipped, perhaps, with some extra predicates. Denote by $B : \mathcal{K} \to \mathcal{K}$ a stochastic map which with probability $p_{i,j}$ maps D_i into D_j. Sometimes we write $B(D_i) = D_j$ if $p_{i,j} > 0$. The map B can be viewed as a random walk on $\mathcal{K}$ defined by the infinite stochastic matrix $(p_{i,j})$. We say that B is a *basic extension* if for every diagrams D_i, D_j such that $B(D_i) = D_j$ there exists a diagram morphism $D_i \to D_j$.

Given a basic extension B and a diagram, say $D_0 \in \mathcal{K}$, one can define the *transition tree* $\mathcal{T} = (V(\mathcal{T}), E(\mathcal{T}))$ of B as follows.

1) $V(\mathcal{T}) = \{D_{i_0}, \dots, D_{i_k} \mid D_{i_j} = B(D_{i_{j-1}})$ for each $1 \leq j \leq k$ and $D_{i_0} = D_0\}$.

2) $E(\mathcal{T}) = \{(D_{i_0}, \ldots, D_{i_k}, D_{i_0}, \ldots, D_{i_{k+1}})\}$.

3) Each edge $e = (D_{i_0}, \ldots, D_{i_k}, D_{i_0}, \ldots, D_{i_{k+1}}) \in E(\mathcal{T})$ has an associated number $p_{i_k, i_{k+1}}$.

The vertex ε (empty sequence of diagrams from $\mathcal{K}$) in the tree $\mathcal{T}$ is called a *root* of $\mathcal{T}$. Denote by $\mathcal{W}$ the random walk on $\mathcal{T}$ which starts at ε with probability 1.

For $D \in \mathcal{K}$ we denote by $\Phi = \Phi_B(D)$ the set of all diagrams C in $\mathcal{K}$ such that $C = B^n(D)$ for some $n \in \mathbb{N}$. A basic extension B is called $\mathcal{K}$-*complete* if there exists $D \in \mathcal{K}$ such that $\Phi_B(D) = \mathcal{K}$. More generally, if $\varphi : \mathcal{K} \to \mathcal{L}$ is a mapping from $\mathcal{K}$ onto a collection of diagrams $\mathcal{L}$ then we say that B is $\mathcal{L}$-*complete relative to* φ if $\varphi(\Phi) = \mathcal{L}$.

Let $D \in \mathcal{K}$ and v is a vertex in D. We say that B is *locally stable* v if the neighborhood of v eventually stabilizes, i.e., for any infinite sequence of diagrams

$$D = D_{i_1}, D_{i_2}, \ldots$$

such that $D_{i_{j+1}} = B(D_{i_j})$, there exists $k \in \mathbb{N}$ such that $N_{D_{i_j}}(v) = N_{D_{i_k}}(v)$ for every $j \geq k$. A random generator B is called *locally stable* if it is stable at every vertex v of every diagram $D \in \mathcal{K}$.

An infinite directed path in $\mathcal{T}$ starting at ε is called a *trajectory*. Let Λ is the set of all trajectories in $\mathcal{T}$. A *cone* of $\theta \in V(\mathcal{T})$ is the set of all trajectories passing through θ:

$$Cone(\theta) = \{\lambda \in \Lambda \mid \lambda \text{ is passing through } \theta\}.$$

Let $\mathcal{F}$ be a σ-algebra generated by all cones $Cone(\theta)$, where $\theta \in V(\mathcal{T})$. For each $\theta = D_{i_0}, \ldots, D_{i_k} \in V(\mathcal{T})$ the real number $P(Cone(\theta))$ is defined as the probability

to hit the vertex $\theta \in \mathcal{T}$ by the random walk W, i.e.,

$$P(Cone(\theta)) = \prod_{j=1}^{k} p_{i_{j-1},i_j}.$$

By the Kolmogorov's extension theorem the function P extends onto the σ-algebra $\mathcal{F}$ in such a way that $(\Lambda, \mathcal{F}, P)$ is a probability space, so P is a probability measure on Λ.

A random variable $Q : \Lambda \to \mathbb{N}$ is called a *termination condition*. For a termination condition Q denote by V_Q the set of all stop-vertices of $\mathcal{W}$ in $\mathcal{T}$ relative to the termination condition Q and P_Q the discrete probability measure on V_Q induced from $(\Lambda, \mathcal{F}, P)$. We say that a sequence of termination conditions $\mathcal{Q} = \{Q_i\}_{i\in\mathbb{N}}$ is *complete* for $\mathcal{W}$ if

$$V(\mathcal{T}) = \sqcup V_{Q_i}.$$

Let $\mathcal{Q}$ be a complete sequence of termination conditions for $\mathcal{W}$. Define an asymptotic density of subsets of $V(\mathcal{T})$. Namely, if $S \subseteq V(\mathcal{T})$ then the asymptotic density $\rho_{V(\mathcal{T})}(S)$ of S in $V(\mathcal{T})$ relative to B, D_0, and $\mathcal{Q}$ is equal to the following limit (if it exists)

$$\rho_{V(\mathcal{T})}(S) = \lim_{i\to\infty} P_{Q_i}(S \cap V_{Q_i}).$$

If $\mu : \mathbb{N} \to \mathbb{R}$ is a probability distribution on $\mathbb{N}$ then one can define a discrete probability measure on $V(\mathcal{T})$

$$P_{V(\mathcal{T})} : V(\mathcal{T}) \to \mathbb{R}$$

(relative to B, D_0, $\mathcal{Q}$ and μ) as follows. For $\theta \in V(\mathcal{T})$ such that $\theta \in V_{Q_i}$ for some $i \in \mathbb{N}$ put

$$P_{V(\mathcal{T})}(\theta) = \mu(i) P_{Q_i}(\theta). \tag{28}$$

Using the discrete probability and asymptotic density defined on $V(\mathcal{T})$ one can induce the discrete probability measure on $\mathcal{K}$ and asymptotic density on subsets of $\mathcal{K}$. For $\theta = D_{i_0}, \ldots, D_{i_k} \in \mathcal{T}$ denote by $D(\theta)$ the diagram D_{i_k}. Now, for $D \in \mathcal{K}$ we define a function

$$P_{\mathcal{K}}(D) = \sum_{\theta \in V(\mathcal{T}),\ D(\theta)=D} P_{V(\mathcal{T})}(\theta).$$

It is easy to see that $P_{\mathcal{K}}$ is a discrete probability measure on $\mathcal{K}$. To define asymptotic density on $\mathcal{K}$, define auxiliary sets

$$\mathcal{K}_i = D(V_{Q_i}) = \{D(\theta) \mid \theta \in V_{Q_i}\}$$

with functions $P_{\mathcal{K}_i} : \mathcal{K}_i \to \mathbb{R}$ such for $D \in \mathcal{K}_i$:

$$P_{\mathcal{K}_i}(D) = \sum_{\theta \in V_{Q_i} \text{ and } D(\theta)=D} P_{Q_i}(\theta).$$

The function $P_{\mathcal{K}_i}$ is a discrete probability measure on $\mathcal{K}_i$. Moreover, if the sets $\mathcal{K}_i$ form a partition of $\mathcal{K}$ then one can define an *asymptotic density* of diagrams from $\mathcal{K}$ as follows. If $S \subseteq \mathcal{K}$ then

$$\rho_{\mathcal{K}}(S) = \lim_{i \to \infty} P_{\mathcal{K}_i}(\mathcal{K}_i \cap S)$$

(if it exists) is an asymptotic density of S in $\mathcal{K}$.

In a similar way one can induce a discrete probability measure $P_{\mathcal{L}}$ on $\mathcal{L}$. Define a partition of $\mathcal{L}$ into the sets $\mathcal{L}_i$, define a discrete probability measure on $\mathcal{L}_i$, and, finally, if $\mathcal{L}_i$ is a partition of $\mathcal{L}$, introduce an asymptotic density $\rho_{\mathcal{L}}$ on sets from $\mathcal{L}$.

Finally, define two particular complete series of termination conditions. The first function Q_n simply counts the number of applications of a basic extension. For

$\lambda \in \Lambda$ and $n \in \mathbb{N}$ put

$$Q_n(\lambda) = n. \tag{29}$$

The termination conditions of the second type measure the size of a constructed diagram. To introduce it we need the following auxiliary random variable. For $\lambda \in \Lambda$ and $n \in \mathbb{N}$ put

$$X_n(\lambda) = \min\{i \in \mathbb{N} \mid \chi(D(\lambda_i)) = n\}.$$

The second series of termination conditions is defined by

$$\widehat{Q}_n(\lambda) = \max\{i \in \mathbb{N} \mid \chi(D(\lambda_i)) = n\} = X_{n+1}(\lambda) - 1. \tag{30}$$

The last series $\{\widehat{Q}_n\}$ of termination conditions defines partitions of $\mathcal{K}$ and $\mathcal{L}$. We will analyze properties of random diagrams relative to $\{\widehat{Q}_n\}$.

18.1 Basic random extension of annular diagrams

Let $\langle X; R\rangle$ be a finite presentation, $G = \langle X; R\rangle$, and $w = w(X)$. Denote by $\mathcal{L}_w = \mathcal{L}_w(X, R)$ a set of representatives (up to isomorphism) of all annular diagrams D over $\langle X; R\rangle$ in which there exists a loop without self-intersections labelled with w. Any loop π in D with defined above properties will be called a *base loop* in D. Since $\langle X; R\rangle$ is finite $\mathcal{L}_w$ is a countable set. So, let $\mathcal{L}_w = \{D_0, D_1, \ldots\}$ be a numeration of diagrams from $\mathcal{L}_w$. We will always denote by D_0 an annular diagram $Loop(w)$, which is a loop labelled with w. When the index of a diagram $D_i \in \mathcal{L}_w$ is irrelevant it will be omitted, we will refer to D_i simply as to $D \in \mathcal{L}_w$.

Proposition 18.1. Let $D \in \mathcal{L}_w$ and $w_1 = \mu(\partial_{in} D)$ and $w_2 = \mu(\partial_{out} D)$. Then $w \simeq_G w_1 \simeq_G w_2$.

Proof. Obvious. □

Proposition 18.2. Let $D_i \in \mathcal{L}_w$. There exist annular diagrams $D_i^{(1)}$ and $D_i^{(2)}$ over $\langle X; R\rangle$ such that $\mu(\partial_{in} D_i^{(1)}) = \mu(\partial_{in} D_i^{(2)}) = w$ and

$$D_i = D_i^{(1)} \bigvee_{\partial_{in} D_i^{(1)} = \partial_{in} D_i^{(2)}} D_i^{(2)}. \tag{31}$$

Moreover, for any pair of diagrams $D_i^{(1)}$ and $D_i^{(2)}$ such that $\mu(\partial_{in} D_i^{(1)}) = \mu(\partial_{in} D_i^{(2)}) = w$ (31) belongs to $\mathcal{L}_w$.

Proof. Let π_{D_i} be a base loop in D_i. Cut D_i along π_{D_i}. Let D_{in} and D_{out} be two obtained annular diagrams (inner and outer, respectively). By turning D_{in} inside out we can make $\mu(\partial_{in} D_{in}) = \mu(\partial_{in} D_{out}) = w$. Clearly, D_{in} and D_{out} are the required diagrams.

The second part of the statement is obvious.

□

An *extended diagram* D over $\langle X; R\rangle$ is a quintuple $(D^{(1)}, D^{(2)}, M(D^{(1)}), M(D^{(2)}), A)$ where:

- D_1 and D_2 are annular diagrams over $\langle X; R\rangle$ such that $\mu(\partial_{in} D_1) = \mu(\partial_{in} D_2)$;
- $M(D^{(i)}) \subseteq V(D^{(i)})$ (where $i = 1, 2$) is called a set of *marked vertices* (worked out vertices);
- A set
$$A \subseteq (\partial_{out} D_1 \cup \partial_{out} D_2) \setminus (M(D_1) \cup M(D_2))$$
is such that $|A| \leq 1$. We refer to vertices from A as to "active vertices" (vertices in the working).

For an extended diagram $D = (D^{(1)}, D^{(2)}, M(D^{(1)}), M(D^{(2)}), A)$ over $\langle X; R\rangle$

denote by $\overline{D}$ the diagram

$$\overline{D} = D^{(1)} \vee_{\partial_{in} D^{(1)} = \partial_{in} D^{(2)}} D^{(2)}.$$

Clearly, $\overline{D}$ is an annular diagram over $\langle X; R\rangle$. Denote by $\mathcal{K}_w = \mathcal{K}_w(X; R)$ the set of all extended annular diagrams D over $\langle X; R\rangle$ such that $\mu(\partial_{in} D_1) = \mu(\partial_{in} D_2) = w$. Clearly, for any $D \in \mathcal{K}_w$ $\overline{D} \in \mathcal{L}_w$. Conversely, for any $D' \in \mathcal{L}_w$ there exists $D \in \mathcal{K}_w$ such that D' and $\overline{D}$ are isomorphic. Morphisms of extended diagrams D are morphisms of annular diagrams $\overline{D}$ that preserve the marked vertices.

Let $S = (s_1, s_2, s_3, s_4)$ be a sequence of reals such that $s_i \in [0, 1], s_1 + s_2 + s_3 = 1$. The following procedure provides the basic extension B_S of extended annular diagrams.

Algorithm 18.3. (*Basic Extension* B_S)

INPUT: Let D be an extended annular diagram over $\langle X; R\rangle$ such that either $A(D) \neq \emptyset$ or $(\partial_{out} D^{(1)} \setminus M(D^{(1)})) \cup (\partial_{out} D^{(2)} \setminus M(D^{(2)})) \neq \emptyset$.

OUTPUT: Diagram $D' = B_S(D)$.

COMPUTATIONS:

1) If $|A(D)| = 1$ then take the only vertex $v \in A(D)$. If $|A(D)| = 0$ then, choose randomly and uniformly an unmarked vertex

$$v \in (\partial_{out} D^{(1)} \setminus M(D^{(1)})) \cup (\partial_{out} D^{(2)} \setminus M(D^{(2)})),$$

and put $A(D) = \{v\}$.

2) If $|(\partial_{out} D^{(1)} \setminus M(D^{(1)})) \cup (\partial_{out} D^{(2)} \setminus M(D^{(2)}))| > 1$ then with probability s_1 do a), with probability s_2 do b), and with probability $s_3 = 1 - s_1 - s_2$ do c) below:

   a) Take randomly and uniformly a relator $r \in R$. Make a cell N with the

boundary label r starting at some vertex $u \in \partial N$. Attach N at v from the outer side by identifying the vertices u and v. Go to 5).

b) Take randomly and uniformly a letter $y \in X^{\pm 1}$. Make a free edge $e = (u_1, u_2)$ with the label y. Attach e at v from the outer side by identifying the vertices v and u_1. Go to 5).

c) Do not attach anything to v and go to 4).

3) If $|(\partial_{out} D^{(1)} \setminus M(D^{(1)})) \cup (\partial_{out} D^{(2)} \setminus M(D^{(2)}))| = 1$ and $s_1 + s_2 \neq 0$ then with probability $\frac{s_1}{s_1+s_2}$ do a) below, otherwise do b):

a) Take randomly and uniformly a relator $r \in R$. Make a cell N with the boundary label r starting at some vertex $u \in \partial N$. Attach N at v from the outer side by identifying the vertices u and v. Go to 5).

b) Take randomly and uniformly a letter $y \in X^{\pm 1}$. Make a free edge $e = (u_1, u_2)$ with the label y. Attach e at v from the outer side by identifying the vertices v and u_1. Go to 5).

4) a) Let $(e_1, h_1), \ldots, (e_k, h_k)$ be all pairs of edges incident to v and such that for each i the following conditions hold:

- the path $e_i h_i$ belongs to the outer boundary of the diagram (with respect to a fixed orientation);
- all endpoints of e_i and f_i are unmarked;
- e_i and h_i^{-1} have the same labels (potential fold);
- edges e_i and h_i are not free.

Then for each $i = 1, \ldots, k$ with a fixed probability s_4 fold e_i and h_i^{-1}.

b) add v to $M(D^{(i)})$,

c) remove v from $A(D)$. Go to 5).

5) Denote the resulting diagram by $B_S(D)$. Output $B_S(D)$.

The basic extension B_S presented here is similar to the basic extension B_S (Algorithm 7.1) from the Part I. It is straightforward to check that B_S has the following basic properties (they are all similar to the properties of B_S in Algorithm 7.1).

Lemma 18.4. (Properties of B_S) *Let $D^* = B_S(D)$ and $i = 1, 2$. Then:*

1) if a vertex $v \in D^{(i)}$ is marked then $N_{D^{(i)}}(v) = N_{D^{(i)*}}(v)$.

2) if every vertex $v \in D^{(i)} \setminus \partial_{out} D^{(i)}$ is marked then every vertex $v \in D^{(i)*} \setminus \partial_{out} D^{(i)*}$ is marked.

3) if every cut vertex in $D^{(i)} \setminus \partial_{in} D^{(i)}$ is either marked or active then every cut vertex in $D^{(i)*} \setminus \partial_{in} D^{(i)*}$ is either marked or active;

4) Given a diagram D there are only finitely many possible outcomes for D^*.

5) If $(\partial_{out} D^{(1)} \setminus M(D^{(1)})) \cup (\partial_{out} D^{(2)} \setminus M(D^{(2)})) \neq \emptyset$ then $(\partial_{out} D^{(1)*} \setminus M(D^{(1)*})) \cup (\partial_{out} D^{(2)*} \setminus M(D^{(2)*})) \neq \emptyset$

Proof. Follows from the description of B_S. □

Let D be a diagram. The following notation

$$D^* = B_S^n(D)$$

means that D^* is a result of n applications of B_S to the diagram D.

Proposition 18.5. Let $D = (D^{(1)}, D^{(2)}, M(D^{(1)}), M(D^{(2)}), \emptyset)$, $D' = B_S^n(D) = (E^{(1)}, E^{(2)}, M(E^{(1)}), M(E^{(2)}), \emptyset)$. There exists n_1, n_2 such that $n_1 + n_2 = n$ and

$$D'' = B_S^{n_1}(D) = (E^{(1)}, D^{(2)}, M(E^{(1)}), M(D^{(2)}), \emptyset),$$

$$(D^{(1)}, D^{(2)}, M(D^{(1)}), M(D^{(2)}), \emptyset) = B_S^{n_2}(D'').$$

Proof. The basic extension B_S treats parts $D^{(1)}$ and $D^{(2)}$ of D separately, i.e., changing the part $D^{(i)}$ (where $i = 1, 2$) does not affect the part $D^{(1-i)}$. Therefore, processing a vertex from $D^{(i)}$ and processing a vertex from $D^{(1-i)}$ are commuting operations. □

Remark 18.6. Let $D^* = B_S^n(D_0)$ where

$$D_0 = (Loop(w), Loop(w), \emptyset, \emptyset, \emptyset).$$

The following holds:

1) if $s_2 = 1$ then $\overline{D^*}$ is a "forest on a loop";

2) if $s_1 = 1$ then $\overline{D^*}$ is a "forest of cells on a loop", i.e., diagram without free edges and such that the dual graph is a tree with one cycle;

3) if $s_1 + s_2 = 1$ then $\overline{D^*}$ is a "forest of cells and free edges on a loop".

Let $\mathcal{W}_S$ be the random walk on $\mathcal{K}_w$ relative to B_S which starts with probability 1 at $D_0 = Loop(w)$ and $\mathcal{T}$ be the corresponding transition tree. In the following lemma we collect some basic properties of $\mathcal{W}_S$. By D_∞ we denote an infinite path in $\mathcal{T}$ which defines a sequence of extended annular diagrams from $\mathcal{K}_w$:

$$D_0 = D_{i_0} \to D_{i_1} \to \ldots \to D_{i_k} \to \ldots.$$

Lemma 18.7. *(*Properties of $\mathcal{T}$*) Let* $D_{i_j} = (D_{i_j}^{(1)}, D_{i_j}^{(2)}, M(D_{i_j}^{(1)}), M(D_{i_j}^{(2)}), A_{i_j})$. *The following hold:*

1) every vertex $v \in (D_{i_j}^{(k)} - \partial_{out} D_{i_j}^{(k)})$ *(*$k = 1, 2$*) is marked, i.e.,*

$$D_{i_j}^{(k)} - \partial_{out} D_{i_j}^{(k)} \subseteq M(D_{i_j}^{(k)});$$

2) for every marked vertex $v \in D_{i_j}^{(k)}$ the neighborhood of v does not change in $D_{i_m}^{(k)}$ for $m \geq j$, i.e.,

$$N_{D_{i_m}^{(k)}}(v) = N_{D_{i_j}^{(k)}}(v);$$

3) every unmarked vertex $v \in D_{i_j}^{(k)}$ either stays unmarked in all $D_{i_m}^{(k)}$ for $m \geq j$ or eventually becomes active;

4) every active vertex $v \in D_{i_j}^{(k)}$ either stays active in all $D_{i_m}^{(k)}$ for $m \geq j$ (and in this event the case 4) in the description of B_S does not occur) or eventually it becomes marked;

Corollary 18.8. The random basic extension B_S is locally stable at every marked vertex v.

18.2 Completeness of B_S

Let $\langle X; R\rangle$ be a finite symmetrized presentation and $w = w(X)$. In this section we show that the basic extension B_S is $\mathcal{L}_w$-complete. More precisely, we show that for any annular diagram $D \in \mathcal{L}_w$ (satisfying certain simple properties) there exists $n \in \mathbb{N}$ such that $D = \overline{B_S^n(D_0)}$, where

$$D_0 = (Loop(w), Loop(w), \emptyset, \emptyset, \emptyset).$$

Let $D \in \mathcal{L}_w$ and π_D be a base loop in D. Assume that D contains no loops of length 1 and there is no cell c such that ∂c is not vertex-simple. We cut D along π_D to obtain two annular diagrams D_{in} and D_{out}. As before, turn D_{in} inside out. Clearly,

$$\mu(\partial_{in} D_{in}) = w, \quad \mu(\partial_{out} D_{in}) = \mu(\partial_{in} D), \text{ and}$$
$$\mu(\partial_{in} D_{out}) = w, \quad \mu(\partial_{out} D_{out}) = \mu(\partial_{out} D).$$

Proposition 18.9. Let $\langle X; R\rangle$ be a finite symmetrized presentation, D an annular diagram over $\langle X; R\rangle$ which does not contain cycles of length 1 and cells c such that ∂c is not vertex-simple. Assume that none of the probabilities in S is trivial. Then there exist n_1 and n_2 such that

$$(Loop(w), D_{out}, \emptyset, M(D_{out}), \emptyset) = B_S^{n_1}(D_0),$$

$$D' = (D_{in}, D_{out}, M(D_{in}), M(D_{out}), \emptyset) = B_S^{n_1+n_2}(D_0)$$

and $D = \overline{D}'$, for some $M(D_{in}) \subseteq V(D_{in})$ and $M(D_{out}) \subseteq V(D_{out})$.

Proof. By Proposition 18.5 it is enough to show the existence of n_1 only. Let $\partial_{in} D_{out} = e_1, \ldots, e_k$, where $e_i = v_i \stackrel{x_i}{\to} v_{i+1}$ $(i = 1, \ldots, k)$ and $v_1 = v_{k+1}$. Construct a van Kampen diagram D' over some presentation $\langle X'; R'\rangle$ (it will be defined later) as follows. First, add a vertex v_0 into the inner hole of D_{out}. Then, for each v_i add an edge $v_0 \stackrel{x'_i}{\to} v_i$ in such a way to not spoil the planarity of the diagram and add a triangular cell v_0, v_i, v_{i+1} labelled with $x'_i x_i {x'}_{i+1}^{-1}$ (where each x'_i is a new symbol, i.e., $x'_i \notin X$). See Figure 24 for example. The presentation $\langle X'; R'\rangle$ is obtained from $\langle X; R\rangle$ by adding all new symbols x'_i to the set X and all relators corresponding to new cells in D' to the set R'.

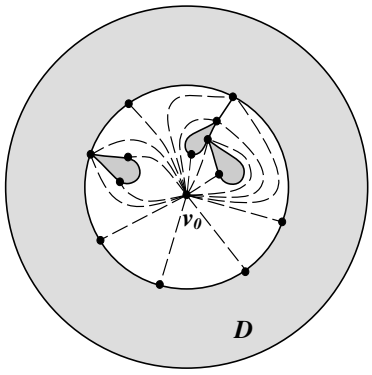

Figure 24: Annular hole triangulation.

By construction, the diagram D' does not contain loops of length 1 and does

not have cells c such that ∂c is non vertex-simple. Hence, D' can be obtained in a number of applications of B_S for van Kampen diagrams to the trivial diagram D'_0 which consists of exactly one vertex. Moreover, from the proof of Completeness Theorem for van Kampen diagrams (Theorem 7.6), it follows that we may assume that the only vertex in D'_0 corresponds to the vertex $v_0 \in D'$. Let

$$D'_0 \stackrel{B_S}{\to} D'_1 \stackrel{B_S}{\to} \dots \stackrel{B_S}{\to} D'_k = D'$$

be the corresponding sequence of extended van Kampen diagrams. Let D'_j be the first diagram in which the initial vertex v_0 is marked. Clearly, $\mu(\partial D'_j) = w$ and each vertex in $\partial D'_j$ is unmarked. This is exactly the initial configuration we have in D_0 (except the internal cells, of course). Now, since the basic extension B_S for annular diagrams can perform the same operations as its counterpart for van Kampen diagrams, the proof is done.

□

Theorem 18.10. (Completeness of B_S.) *Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation and $w = w(X)$ such that w does not belong to the conjugacy class of a word of length less or equal to* 1. *Let $D \in \mathcal{L}_w$. Then there exists a number n such that*

$$D = \overline{B_S^n(D_0)},$$

i.e., B_S is $\mathcal{L}_w$ complete.

Proof. Observe, that the assumptions on a presentation $\langle X; R\rangle$ and a word w imply that D does not contain loops of length 1. Also, the assumption on $\langle X; R\rangle$ implies that D contains no loops such that ∂c is not vertex-simple. Now, the theorem follows from Proposition 18.9.

□

19 Asymptotic properties of random annular diagrams

In this section we describe several asymptotic properties of diagrams relative to the basic extension B_S and the complete series of termination conditions $\{\widehat{Q}_i\}_{i\in\mathbb{N}}$. In particular, we discuss asymptotic behavior of the length of the perimeter and the depth of diagrams relative to their size.

All results in this section can be proved by arguments similar to those in Part I (we leave them to the reader). Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation and $w = w(X)$ such that w does not belong to the conjugacy class of a word of length less or equal to 1. Let $\mathcal{L}_{w,n}$ be a set of all annular diagrams from $\mathcal{L}_w$ of size n, i.e.,

$$\mathcal{L}_{w,n} = \{D \in \mathcal{L}_w \mid \chi(D) = n\}.$$

Let $\mathcal{K}_{w,n}$ be a set of all extended annular diagrams from $\mathcal{K}_w$ of size n, i.e.,

$$\mathcal{K}_{w,n} = \{D \in \mathcal{K}_w \mid \chi(D) = n\}.$$

Clearly, the sets $\{\mathcal{L}_{w,n}\}$ is a partition of $\mathcal{L}_w$ and the sets $\{\mathcal{K}_{w,n}\}$ is a partition of $\mathcal{K}_w$.

Theorem 19.1. *Let $0 < \alpha < 1$. Then the following holds:*

1) *Let $\mathcal{K}'_{w,n,\alpha} = \{D \in \mathcal{K}_{w,n} \mid l(D) < (1-\alpha)n+|w|\} \subseteq \mathcal{K}_{w,n}$. Then $P_{\mathcal{K}_{w,n}}(\mathcal{K}'_{w,n,\alpha}) \to 0$ exponentially fast as $n \to \infty$.*

2) *Let $\mathcal{L}'_{w,n,\alpha} = \{D \in \mathcal{L}_{w,n} \mid l(D) < (1-\alpha)n+|w|\} \subseteq \mathcal{L}_{w,n}$. Then $P_{\mathcal{L}_{w,n}}(\mathcal{L}'_{w,n,\alpha}) \to 0$ exponentially fast as $n \to \infty$.*

Corollary 19.2. Let $\langle X; R\rangle$ be a finite symmetrized presentation and $w = w(X)$ such that w does not belong to the conjugacy class of a word of length less or equal

to 1. Put

$$\mathcal{L}'_w = \{D \mid l(D) \geq \tfrac{1}{2}\chi(D)\}.$$

Then

$$\rho_{\mathcal{L}_w}(\mathcal{L}'_w) = \lim_{i\to\infty} P_{\mathcal{L}_{w,i}}(\mathcal{L}_{w,i} \cap \mathcal{L}'_w) = 1.$$

Moreover, $P_{\mathcal{L}_{w,i}}(\mathcal{L}_{w,i} \cap \mathcal{L}'_w) \to 1$ exponentially fast. Thus the set of all diagrams over $\langle X; R\rangle$ with linear isoperimetric function (with coefficient $\frac{1}{2}$) is strongly generic with respect to the asymptotic density.

Theorem 19.3. *The following holds:*

1) *Let* $\mathcal{K}''_{w,n} = \{D \in \mathcal{K}_{w,n} \mid \delta(D) < 2\log n\} \subseteq \mathcal{K}_{w,n}$. *Then* $P_{\mathcal{K}_{w,n}}(\mathcal{K}''_n) \to 1$ *as* $n \to \infty$.

2) *Let* $\mathcal{L}''_{w,n} = \{D \in \mathcal{L}_{w,n} \mid \delta(D) < 2\log n\} \subseteq \mathcal{L}_{w,n}$. *Then* $P_{\mathcal{L}_{w,n}}(\mathcal{L}''_{w,n}) \to 1$ *as* $n \to \infty$.

Theorem 19.4. *Let* $\langle X; R\rangle$ *be a symmetrized* R*-reduced presentation,* $w = w(X)$ *such that* w *does not belong to the conjugacy class of a word of length less or equal to* 1, *and* $0 < \alpha < 1$. *The following holds:*

1) *Let* $\mathcal{K}'''_{w,n,\alpha} = \{D \in \mathcal{K}_{w,n} \mid \delta(D) < 2\log n \ \&\ l(D) \geq (1-\alpha)n\} \subseteq \mathcal{K}_{w,n}$. *Then* $P_{\mathcal{K}_{w,n}}(\mathcal{K}'''_{w,n,\alpha}) \to 1$ *as* $n \to \infty$.

2) *Let* $\mathcal{L}'''_{w,n,\alpha} = \{D \in \mathcal{L}_{w,n} \mid \delta(D) < 2\log n \ \&\ l(D) \geq (1-\alpha)n\} \subseteq \mathcal{L}_{w,n}$. *Then* $P_{\mathcal{L}_{w,n}}(\mathcal{L}'''_{w,n,\alpha}) \to 1$ *as* $n \to \infty$.

Corollary 19.5. Let $\langle X; R\rangle$ be a symmetrized R-reduced presentation, $w = w(X)$ such that w does not belong to the conjugacy class of a word of length less or equal to 1. Let

$$\mathcal{L}''_w = \{D \in \mathcal{L}_w \mid \delta(D) \leq 2\log(2l(D))\}.$$

Then

$$\rho_{\mathcal{L}_w}(\mathcal{L}''_w) = \lim_{i\to\infty} P_{\mathcal{L}_{w,i}}(\mathcal{L}_{w,i} \cap \mathcal{L}''_w) = 1.$$

Proof. Follows from Theorem 19.4 when $\alpha = \frac{1}{2}$. □

20 Asymptotic properties of conjugated words

20.1 Random conjugated words

Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation and $w = w(X)$ be a word such that the shortest element in its conjugacy class is of length at least 2. Denote by $CP_w(X; R)$ the set of all pairs of cyclic words (w_1, w_2) such that $w_1 \sim_G w \sim_G w_2$. In this section we define a discrete probability measure on $CP_w(X; R)$.

Recall that $\mathcal{L}_{w,i}$ is a set of all annular diagrams from $\mathcal{L}_w$ of size i and $P_{\mathcal{L}_{w,i}}$ is a discrete probability measure on $\mathcal{L}_{w,i}$. Denote by $CW_{w,i}$ (for each $i \in \mathbb{N}$) the set of boundary labels (as cyclic words) of diagrams from $\mathcal{L}_{w,i}$ and by $\overline{CW}_{w,n}$ the union

$$\overline{CW}_{w,n} = \cup_{i=1}^{n} CW_{w,i}.$$

It follows from Proposition 16.1 that

$$CP_w(X; R) \;=\; \cup_{i=1}^{\infty} CW_{w,i} \;=\; \cup_{i=1}^{\infty} \overline{CW}_{w,i}.$$

Clearly,

$$\overline{CW}_{w,1} \subseteq \overline{CW}_{w,2} \subseteq \overline{CW}_{w,3} \subseteq \ldots.$$

One can induce probability measures from $(\mathcal{L}_{w,n}, P_{\mathcal{L}_{w,n}})$ onto the sets $CW_{w,n}$ and $\overline{CW}_{w,n}$ as follows. For $S \subseteq CW_{w,n}$ and $S' \subseteq \overline{CW}_{w,n}$ put

$$P_{CW_{w,n}}(S) = P_{\mathcal{L}_{w,n}}(\{D \in \mathcal{L}_{w,n} \mid \text{ the boundary labels of } D \text{ belong to } S\}),$$

$$P_{\overline{CW}_{w,n}}(S') = \frac{\sum_{i=1}^{n} P_{CW_{w,i}}(S' \cap CW_{w,i})}{n}.$$

It is easy to check that $P_{CW_{w,n}}$ and $P_{\overline{CW}_{w,n}}$ are discrete probability measures on $CW_{w,n}$ and $\overline{CW}_{w,n}$.

Using the probability on the sets $\overline{CW}_{w,n}$ one can define an asymptotic density of the subsets of $CP_w(X;R)$ as follows. For $S \subseteq CP_w(X;R)$ put

$$\rho_{CP_w}(S) = \lim_{n\to\infty} P_{\overline{CW}_{w,n}}(S \cap \overline{CW}_{w,n}).$$

One can describe the probability measure $P_{CW_{w,n}}$ in terms of the following random generator.

Algorithm 20.1. (*Random Generator I of conjugate words*)

INPUT. A word $w = w(X)$ and a number $n \in \mathbb{N}$.

OUTPUT. A pair of words w_1, w_2 such that $w_1 \simeq_G w \simeq_G w_2$.

INITIALIZATION. Put $D_0 = (Loop(w), Loop(w), \emptyset, \emptyset, \emptyset)$ and $i = 0$.

COMPUTATIONS.

1) Let $D_{i+1} = B_S(D_i)$.

2) If $\chi(D_{i+1}) \leq n$ then increment i and goto 1).

3) Output labels of $\partial_{out} D_i^{(1)}$ and $\partial_{out} D_i^{(2)}$.

The probability measure $P_{\overline{CW}_n}$ can be described in terms of the following random generator.

Algorithm 20.2. (*Random Generator II of conjugate words*)

INPUT. A word $w = w(X)$ and a number $n \in \mathbb{N}$.

OUTPUT. A pair of words w_1, w_2 such that $w_1 \simeq_G w \simeq_G w_2$.

COMPUTATIONS.

1) Generate randomly and uniformly a number i from the set $\{1, \ldots, n\}$.

2) Run the defined above generator to generate a random extended diagram D of size i.

3) Output the boundary labels of $\overline{D}$.

In view of the random generators above the probability measures $P_{CW_{w,n}}$ and $P_{\overline{CW}_{w,n}}$ are very natural.

20.2 Generic properties of random conjugated words

In this section we study generic properties of conjugated words in $G = \langle X; R\rangle$. Fix α such that $0 < \alpha < 1$ and define

$$\overline{CW}_{w,n,\alpha} = \{(w_1, w_2) \in \overline{CW}_{w,n} \mid w_1 \text{ and } w_2 \text{ are boundary labels of some } D \in \cup_{i=1}^{n} \mathcal{L}'''_{w,i,\alpha}\}.$$

Theorem 20.3. *Let $G = \langle X; R\rangle$ be a finite symmetrized R-reduced presentation and $w = w(X)$ be a word the conjugacy class of which does not contain words of length less than 2. The following holds:*

$$P_{\overline{CW}_{w,n}}(\overline{CW}_{w,n,\alpha}) \to 1 \text{ as } n \to \infty.$$

Proof. Follows from the Theorem 19.4 and the definition of $P_{\overline{CW}_{w,n}}$.

□

For a fixed $0 < \alpha < 1$ define a set $CP_w^{(\alpha)}$ to be

$$CP_w^{(\alpha)} = \cup_{n=1}^{\infty} \overline{CW}_{w,n,\alpha}.$$

By Theorem 20.3 we have $\rho_{CP_w}(CP_w^{(\alpha)}) = 1$.

Theorem 20.4. *Let $\langle X; R\rangle$ be a finite symmetrized R-reduced presentation, $G = \langle X; R\rangle$, and $w = w(X)$ be a word the conjugacy class of which does not contain*

words of length less than 2. *Then the the time complexity function for Algorithm 17.11 (the search algorithm for the conjugacy problem in G) on the set of inputs* $(w_1, w_2) \in CP_w^{(\alpha)}$ *is bounded from above by the polynomial*

$$O((|w_1| + |w_2|)^{2+4\log L(R)}).$$

Proof. Follows from Theorem 17.12 and the definition of the set $CP_w^{(\alpha)}$.

□

Thus, the Conjugacy search problem is polynomial on a generic subset $CP_w^{(\alpha)}$ of instances of the problem CP_w.

21 Experimental results

We performed a series of experiments to test the efficiency of the algorithm $\mathcal{A}_C$. For each series we fixed a group presentation $\langle X; R\rangle$ and generated randomly 1000 pairs of conjugate words of length about 1000 in $G = \langle X; R\rangle$. We tested all the group presentations mentioned in Section 11 almost all of which are one-relator groups and there is no known algorithm for solving the conjugacy problem in this class of groups (though for each of those presentations there exists an algorithm solving the problem under consideration).

By Theorem 20.3 the generic time complexity for pairs of conjugate words (w_1, w_2) is bounded from above by the polynomial $O((|w_1| + |w_2|)^{2+2\log L(R)})$. Our experimental results are much better than that. As proved in Theorem 17.12 the amount of time required to find a conjugator for each single pair (w_1, w_2) of conjugate words in $\langle X; R\rangle$ is $O(|w_1||w_2|L(R)^{2m})$ (where $m = \delta(w_1, w_2)$) and the number of iterations the conjugacy search algorithm $\mathcal{A}_C$ performs is bounded from above by m. And in all our experiments the algorithm $\mathcal{A}_C$ performed just one iteration. So,

all randomly generated conjugate words had depth equal to one. And, therefore, the actual time complexity was $O(|w_1||w_2|L(R)^2)$ which is quadratic in terms of the lengths of words.

We would like to point out that we know a few series of inputs for which the performance of the algorithm $\mathcal{A}_C$ is slow (exponential and superexponential in terms of length of the input). But the amount of such inputs is negligible relative to all possible inputs. In fact, if $\langle X; R\rangle$ is a presentation with unsolvable Conjugacy problem then for any computable function $f(n)$ there is a sequence of pairs of conjugate words (u_n, v_n) such that $\delta(u_n, v_n)$ grows faster than $f(n)$. But to find such a sequence is extremely hard.

References

[1] I. Anshel, M. Anshel, D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Lett. **6** (1999), 287–291.

[2] J. Alonso, T. Brady, D. Cooper, V. Ferlini, M. Lustig, M. Mihalik, M. Shapiro, H. Short, *Notes on word hyperbolic groups*, Group Theory from a geometric viewpoint, World Scientific, Singapore. Proceedings of the ICTP conference in summer 1990.

[3] S. Adian, V. Durnev, *Algorithmic problems for groups and semigroups,* Uspekhi Mat. Nauk, **55**, no. 2, 3–94, 2000; translation in Russian Math. Surveys, **55**, no. 2, 207–296, 2000.

[4] E. Artin, *Theory of Braids*, Ann. Math., **48**, no. 1, 287–291, 1947.

[5] J. Birman, K. Ko, S. Lee, *A New Approach to the Word and Conjugacy Problems in the Braid Groups*, Adv. Math., **139**, no. 2, 322-353, 1998.

[6] B. Chandler, W. Magnus, *The Hystory of Combinatorial Group Theory: A Case Study in the History of Ideas*, Springer, 1982.

[7] A. Borovik, A. Myasnikov, V. Remeslennikov, *Algorithms for Amalgamated Products*

[8] M. Dehn, *Transformation der Kurven auf zweiseitigen Flaechen*, Math. Ann., **71**, 413-421, 1912.

[9] D. Epstein, *Word Processign in Groups*, 1992.

[10] F. Garside, *The Braid Group and Other Groups*, Quart. J. Math. Oxford, **20**, 235-254, 1969.

[11] M. Greendlinger, *Dehn's Algorithm for the Word Problem*, Comm. Pure and Appl. Math., **13**, 67-83, 1960.

[12] M. Greendlinger, *On Dehn's Algorithms for the Conjugacy and Word Problems. With Applications.*, Comm. Pure and Appl. Math., **13**, 641-677, 1960.

[13] Y. Gurevich, *Average case completeness*, J. of Computer and System Science, **42**, 346–398, 1991.

[14] D. Holt, *Word-hyperbolic groups have real-time word problem,* Internat. J. Algebra Comput., **10**, 221–227, 2000.

[15] D. Holt, S. Rees, *Solving the word problem in real time*, J. London Math. Soc. (2), **63**, 623–639, 2001.

[16] I. Kapovich, *The non-amenability of Schreier graphs for infinite index quasiconvex subgroups of hyperbolic groups*, to appear in Ensign. Math.

[17] V. Klee, G. Minty, *How good is the simplex algorithm?* Inequalities, III (Proc. Third Sympos., Univ. California, Los Angeles, Calif., 1969; dedicated to the memory of Theodore S. Motzkin), 159–175. Academic Press, New York, 1972.

[18] I. Kapovich, A. Myasnikov, *Stallings foldings and subgroups of free groups*, Journal of Algebra, **248**, 608–668, 2002.

[19] I. Kapovich, A. Myasnikov, P.Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, Journal of Algebra, **264**, 665–694, 2003.

[20] I. Kapovich, A. Myasnikov, P.Schupp, V. Shpilrain, *Average-case complexity and decision problems in group theory*, to appear in Advan. Math.

[21] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, *New public-key cryptosystem using braid groups*, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), 166–183, Lecture Notes in Comput. Sci. **1880**, Springer, Berlin, 2000.

[22] L. Levin, *Average case complete problems*, SIAM Journal of Computing, **15**, 285–286, 1986.

[23] R. Lyndon, P. Schupp, *Combinatorial Group Theory*, Springer, 1977.

[24] W. Magnus, *Über Diskontinuierliche Gruppen mit Einer Definierenden Relation (Der Freiheitssatz)*, J. Reine u. Angew. Math., **163**, 141-165, 1930.

[25] W. Magnus, *Das Identitäts Problem für Gruppen mit Einer Definierenden Relation*, Math. Ann., **106**, 295-307, 1932.

[26] A. Markov, *Foundation of the Algebraic Theorey of Tresses*, Tr. Mat. Inst. Steklova, **16**, 1945.

[27] J. McCool, *On a question of Remeslennikov*, Glasgow Math. J., **43**, 123-124, 2001.

[28] C. F. Miller III, *On group-theoretic decision problems and their classification,* Ann. of Math. Studies, **68** (1971). Princeton University Press, Princeton.

[29] C. F. Miller III, *Decision problems for groups – survey and reflections*, Algorithms and Classification in Combinatorial Group Theory (G. Bamuslag and C.F. Miller III, editors), Springer, 1–60, 1992.

[30] W. Magnus, A. Karrass, D. Solitar, *Combinatorial Group Theory*, Springer-Verlag, New York, 1977.

[31] A. Myasnikov, A. Ushakov, *Generic Complexity of Diagrams*, preprint.

[32] A. Miasnikov, A. Ushakov, D. W. Won, *The Word and Conjugacy Problems for Gerstens Groups*, in preparation.

[33] P. Novikov, *Unsolvability of the Conjugacy Problem in the Theory of Groups*, Izv. Acad. Nauk SSSR, Ser. Mat., **18**, 485-524, 1954.

[34] A. Ol'shanskii, *Geometry of Defining Relations in Groups*, Kluwer, 1991.

[35] A. Ol'shanskii, *Almost every group is hyperbolic*, Internat. J. of Algebra and Comput., **2**, no. 1, 1-17, 1992.

[36] E. Rips, *Subgroups of Small Cancellation Groups*, Bull. London Math. Soc., **14**, 45–47, 1982.

[37] J. Stallings, *Topology of finite graphs*, Invent. Math., **71**, no. 3, 551–565, 1983.

[38] V. Shpilrain, A. Ushakov, *The Conjugacy Search Problem In Public Key Cryptography: Unnecessary And Insufficient*, Applicable Algebra in Engineering, Communication and Computing, to appear.

[39] C.M. Weinbaum, *On relators and diagrams for groups with one defining relator*. Illinois J.Math. **16**, 308–322, 1972.