Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 4916–4930
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Gröbner–Shirshov basis of the Adyan extension of the Novikov group

L.A. Bokut[a,1], V.V. Chainikov[b,1]

[a] Sobolev Institute of Mathematics, Novosibirsk 630090, Russia
[b] Novosibirsk State University, Novosibirsk 630090, Russia

Received 20 December 2004; accepted 5 September 2007
Available online 18 October 2007

Abstract

The goal of this paper is to give a comparatively short and simple analysis of the Adyan origional group constraction (S.I. Adyan, Unsolvability of some algorithmic problems in the theory of groups, Trudy MMO 6 (1957) 231–298).

Keywords: Gröbner–Shirshov basis; Non-commutative Gröbner basis; Novikov group; Word problem

1. Introduction

In the fundamental paper [20], P. S. Novikov solved the Dehn word problem for groups. He constructed the first example of a finitely presented (f. p.) group with algorithmically undecidable word problem. This group is called the (centrally-symmetric) Novikov group. Later Boone [15] published another example of a f. p. group with the same property.

Based on the Novikov group, Adyan [1] solved the Dehn isomorphism problem for an arbitrary f. p. group. More generally, he proved that many Markov's properties of f. p. groups are algorithmically undecidable (see the definition in the beginning of Section 4). Later Rabin [21] proved that each Markov's property of a f. p. group is algorithmically undecidable. These results are now known as the Adyan–Rabin theorem.

In the paper [10], the first author essentially simplified the original analysis of the Novikov group. Namely, based on the notion of a group with standard basis [3] (see also [9,11]), the first author gave a comparatively simple proof of the main technical group-theoretic result of [20]. It is Novikov's equality criterion Theorem 3.2, see ([20, Chapter 4]).

The goal of this paper is to give a comparatively short and simple analysis of the Adyan original construction [1]. For this reason we suggest the following definition of the Adyan extension of a group G. Let G be a group with four fixed elements g_1, g_2, g_3, g_4. Then

$$A(G, g_1, g_2, g_3, g_4) = \mathrm{gr}\langle G, q \mid g_1 q = q g_2, g_3 q g_4 q = q g_3\rangle$$

is called the (two-relation) Adyan extension of G.

[1] Supported by the RFBR grant and the Integration grant of the SB of the RAS (No. 1.9) (Russia).
E-mail addresses: bokut@math.nsc.ru (L.A. Bokut), chain@front.ru (V.V. Chainikov).

0012-365X/$ - see front matter
doi:10.1016/j.disc.2007.09.011

Let us call some elements of a group independent if they freely generate a free subgroup of the group. One of the main results of the paper is the following:

Theorem 1.1. *Let G be a group with four independent elements* g_i, $i=\overline{1,4}$. *Then* $A(G, g_i, i=\overline{1,4})$ *contains G as a subgroup.*

The main technical result of Adyan [1]—that his group contains the Novikov group—readily follows from the above theorem because Adyan's original construction has the form $A(G, g_i, i=\overline{1,4})$ for some independent elements g_i, $i=\overline{1,4}$. To prove the last statement, we generalize slightly Novikov's equality criterion, see Proposition 3.4. Based on this Proposition, we prove that some three elements of the Novikov group are independent (Proposition 3.5), and finally that some four elements of the original Adyan's group are independent (Proposition 4.1). It gives the desired proof that the original Adyan's group is of the form $A(G, g_i, i=\overline{1,4})$.

Let us say some words about the method of the proof of Theorem 1.1. It is a Gröbner–Shirshov bases method. The concept of the Gröbner–Shirshov bases was introduced by Shirshov [23], for the (most difficult, see below) case of Lie polynomials $\mathrm{Lie}(X)$ over a field k under the Lie bracket $[x, y]=xy-yx$. Note that Shirshov was dealing with Lie polynomials via non-commutative (associative) polynomials $k\langle X\rangle$, $\mathrm{Lie}(X)\subset k\langle X\rangle$. To be more precise, to make a composition (S-polynomial by the later Buchberger's [17] terminology) of two monic Lie polynomials f, g relative to some word w, where $w=\overline{f}v=u\overline{g}$ ($\overline{f}$, $\overline{g}$ are leading associative terms of polynomials f, g as non-commutative polynomials), he makes first an associative composition

$$(f, g)_w = fv - ug.$$

Then he puts the special Lie bracketing

$$[f, g]_w = [fv] - [ug]$$

and the result is the Lie composition of f, g. Shirshov had invented the special Lie bracketing earlier [22].

The same was with the notion of elimination of a leading word of g in f. Let f, g be monic Lie polynomials, $\overline{f}=a\overline{g}b$. Then

$$f \mapsto f - ugv$$

is the associative elimination of $\overline{g}$ in $\overline{f}$. To make the Lie elimination, Shirshov used the special Lie bracketing

$$f \mapsto f - [ugv].$$

The Composition Lemma for associative polynomials is just a simple version of the Shirshov Composition Lemma for Lie polynomials:

Lemma 1.2 (*Composition Lemma, Shirshov [23, Lemma 3]*). *Let S be a set of Lie polynomials,* S^* *be the completion of S under all possible (nontrivial) compositions, i.e.,* S^* *is obtained by adding to S all compositions of elements of S, then compositions of the result and so on. If* $f\in LieId(S)$, *then* $\overline{f}$ *contains* $\overline{s}$ *for some* $s\in S^*$.

Remark 1.3. Shirshov had further assumed that S is "stable". But this assumption was not used in his proof. Stability of S means that the degree (after eliminations of leading words) of any (nontrivial) composition $(f, g)_w$, where $f, g\in S^*$ is greater than degrees of f, g, and leading associative monomials of different elements of S^* do not contain each other. It follows that S^* is a recursive set.

Later the first author stated this lemma in the modern form.

Lemma 1.4 (*Composition Lemma, Bokut [7, the Shirshov Lemma]*). *Let S be a set of Lie polynomials that is closed under compositions (i.e., any composition is trivial, or* $S=S^*$*). If* $f\in LieId(S)$, *then* $\overline{f}$ *contains* $\overline{s}$ *for some* $s\in S$.

All in all, the Shirshov's paper [23] can be viewed as the beginning of Gröbner–Shirshov bases theory not only for Lie polynomials but also for non-commutative (associative) polynomials (see also for example [12]).

The case of associative polynomials was observed by the first author [8] and by Bergman [2].

In the case of commutative polynomials (and power series) essentially the same ideas were introduced by Hironaka [19] (standard bases) and Buchberger (Gröbner bases) [16–18]. It is well known and well recognized.

Gröbner–Shirshov basis of a group presentation $G = \mathrm{gr}\langle X|R\rangle$ is the Gröbner–Shirshov basis of the group algebra kG over a field k. Thus a Gröbner–Shirshov basis S of a group $G = \mathrm{gr}\langle X|R\rangle$ leads to the set of S-reduced group words in X such that any word is equal to one and only one S-reduced word (S-reduced normal form).

In the papers [3,4,10], the first author discovered the standard normal forms in some groups, namely in two Novikov's and Boon's groups. Recently it has become clear that the standard normal forms for Novikov's and Boon's groups are nothing but reduced normal forms in this groups relative to some Gröbner–Shirshov bases [13]. In the papers [5,6], the first author constructed the relative standard normal forms in some groups arising from the rings. These are reduced normal forms for the "relative" Gröbner–Shirshov bases [14].

We denote the graphical equality of words by $\doteq$. Letters ε, δ stand for ± 1. An order on the set of all words in a given alphabet is called a monomial order if it agrees with the concatenation of words.

After this paper had been submitted, A. Klyachko pointed out to us that Theorem 1.1 follows also from Stalling's theorem [24], that was proved with the completely different methods. Of course, our main result, Theorem 7.1, on Gröbner–Shirshov bases for Adyan extensions does not follow from the Stalling's paper.

2. Gröbner–Shirshov bases

For a set $\mathbf{X}$ and a field k, let $k\langle\mathbf{X}\rangle$ be the free associative algebra in $\mathbf{X}$ over k. On the set $\mathbf{X}^*$ of words we impose a monomial well order $>$. By $\bar{f}$ we denote the leading term of a polynomial $f \in k\langle\mathbf{X}\rangle$. We say that f is monic if $\bar{f}$ occurs in f with coefficient 1. A composition (inclusion and intersection, respectively) $(f, g)_w$ of two monic polynomials relative to some word w is the polynomial

$$(f, g)_w = \begin{cases} f - agb & \text{if } w = \overline{f} = a\overline{g}b, \\ fb - ag & \text{if } w = \overline{f}b = a\overline{g}, \ |\overline{f}| > |a|, \end{cases}$$

where $a, b \in X^*$, $|a|$ is the length of a.

In the first case, the transformation

$$f \mapsto (f, g)_w = f - agb$$

is called the elimination of the leading word (ELW) of g in f.

In both cases, the word w is called an *ambiguity* of polynomials (relations) f, g.

A composition $(f, g)_w$ is called trivial relative to some $\mathbf{S} \subset k\langle\mathbf{X}\rangle$ ($(f, g)_w \equiv 0 \bmod (\mathbf{S}, w)$) if

$$(f, g)_w = \sum \alpha_i a_i t_i b_i,$$

where $t_i \in \mathbf{S}$, $a_i, b_i \in \mathbf{X}^*$, and $a_i \bar{t_i} b_i < w$.

In particular, if $(f, g)_w$ goes to zero by the ELW's of $\mathbf{S}$ then $(f, g)_w$ is trivial relative to $\mathbf{S}$.

We write for some polynomials f_1 and f_2 that

$$f_1 \equiv f_2 \bmod (\mathbf{S}, w)$$

if

$$f_1 - f_2 \equiv 0 \bmod (\mathbf{S}, w).$$

A subset $\mathbf{S}$ of $k\langle\mathbf{X}\rangle$ is called a Gröbner–Shirshov basis if any composition of polynomials from $\mathbf{S}$ is trivial relative to $\mathbf{S}$.

We will denote by $\langle\mathbf{X}|\mathbf{S}\rangle$ the k-algebra with generators $\mathbf{X}$ and defining relations $\mathbf{S}$, that is the quotient algebra of $k\langle\mathbf{X}\rangle$ by the ideal generated by $\mathbf{S}$.

Lemma 2.1 (*Composition-Diamond Lemma*). $\mathbf{S}$ *is a Gröbner–Shirshov basis if and only if the set*

$$\mathrm{Red}(S) = \{u \in \mathbf{X}^* \mid u \neq a\bar{s}b \text{ for any } s \in \mathbf{S}\}$$

of $\mathbf{S}$*-reduced words is a linear basis of the algebra* $\langle\mathbf{X}|\mathbf{S}\rangle$.

If a subset $\mathbf{S}$ of $k\langle\mathbf{X}\rangle$ is not a Gröbner–Shirshov basis, then one can add to $\mathbf{S}$ all nontrivial compositions of polynomials of $\mathbf{S}$, and continuing this process (infinitely) many times in order to build a Gröbner–Shirshov basis $\mathbf{S}^{\mathrm{comp}}$. This procedure is called the Buchberger–Shirshov algorithm [23,16,17].

If $\mathbf{S}$ is a set of "semigroup relations" (that is, polynomials of the form $u - v$, where $u, v \in \mathbf{X}^*$), then any nontrivial composition will have the same form. As a result the set $\mathbf{S}^{\mathrm{comp}}$ also consists of semigroup relations.

Let $A = \mathrm{smg}\langle\mathbf{X}|\mathbf{S}\rangle$ be a semigroup presentation. Then $\mathbf{S}$ is a subset of $k\langle\mathbf{S}\rangle$ and one can find a Gröbner–Shirshov basis $\mathbf{S}^{\mathrm{comp}}$. The last set does not depend on k and, as it mentioned, consists of semigroup relations. We will call $\mathbf{S}^{\mathrm{comp}}$ a Gröbner–Shirshov basis of the semigroup A. It is the same as a Gröbner–Shirshov basis of the semigroup algebra $kA = \langle\mathbf{X}|\mathbf{S}\rangle$.

The same terminology is valid for any group presentation if we include in this presentation generators X^{-1} and trivial group relations

$$xx^{-1} = 1, \quad x^{-1}x = 1, \quad x \in \mathbf{X}.$$

We will use the tower order of words. This order is naturally suited for towers of HNN-extensions (see [3,4]).

Let $X = Y \dot{\cup} Z$. We assume that Y^* and Z are well-ordered and the order on Y^* is monomial. Every word in X is of the form

$$u = u_1 z_1 \ldots u_k z_k u_{k+1}, \tag{2.1}$$

where $u_i \in Y^*$, $z_i \in Z$. By the weight of the word u we mean the vector

$$wt(u) = (k, u_1, z_1, \ldots, u_k, z_k, u_{k+1}).$$

We arrange the lexicographic order on weights using the orders on Y^* and Z. Finally, define

$$u > v \quad \Longleftrightarrow \quad wt(u) > wt(v).$$

Observe that the tower order is a well monomial order. Also note that the ordinary deg–lex order is a special case of tower order when Y is empty.

We will also need the following version of the tower order. Let X, Y, Z be as above. For any X-word (2.1) let us define

$$wt'(u) = (k, |u|, u_1, z_1, \ldots, u_k, z_k, u_{k+1}),$$

where $|u|$ is the total length of u. Let us order $wt'(u)$ lexicographically and order X-words by the rule

$$u > v \quad \Longleftrightarrow \quad wt'(u) > wt'(v).$$

We call this order by the deg–tower order. This is also a well-monomial order.

3. The (centrally symmetric) Novikov group

In 1955, Novikov [20] proved the existence of a finitely presented group with undecidable word problem. He showed that every finitely presented semigroup Π with cancellation can be effectively mapped into a finitely presented group $\mathcal{N}(\Pi)$ with respect to the equality predicate. Thus, every word $u \in \Pi$ effectively maps to $f(u) \in \mathcal{N}(\Pi)$ so that

$$u = v\,(\Pi) \quad \Longleftrightarrow \quad f(u) = f(v)\,(\mathcal{N}(\Pi)).$$

If Π is a f. p. Turing's cancellation semigroup with undecidable word problem [25], then $\mathcal{N}(\Pi)$ is a f. p. group with the same property.

The group $\mathcal{N}(\Pi)$ is called the (centrally symmetric) Novikov group. We will need some of its properties.

Let

$$\Pi = \langle \Sigma_1;\, A_i = B_i,\, i = \overline{1, m}\rangle$$

be a semigroup with cancellation. In [20], it was defined a new alphabet Σ, $\Sigma_1 \subset \Sigma$, $\tau_1, \tau_2 \in \Sigma$, and a finite set $\mathscr{F}$ of words in the alphabet Σ, $\mathscr{F} = \{(A_i, B_i),\ i = \overline{1,n}\}$, where $n > m$ (i.e., the defining relations of Π are included into $\mathscr{F}$). We will not need the explicit forms of Σ and $\mathscr{F}$.

The group $\mathscr{N}(\Pi)$ admits a presentation as a tower of groups with stable letters. Let

$$G_0 = \langle \rho_i, \tilde{\rho}_i, i = \overline{1,n} \rangle$$

be the free group of rank $2n$, and let

$$G_1 = \langle G_0, \Sigma;\ \hat{\rho}_i a = a \hat{\rho}_i^2, a \in \Sigma, i = \overline{1,n} \rangle,$$

$$G_2 = \langle G_1, l_{ai}, a \in \Sigma;\ b l_{ai} = l_{ai} b, b \in \Sigma, i = \overline{1,n} \rangle,$$

$$G_3 = \langle G_2, \mu_{ki}, \tilde{\mu}_{ki}, i = \overline{1,n}, k = 1,2;\ a\hat{\mu}_{1i} = \hat{\mu}_{1i} a l_{ai}^{-1}, a l_{ai} \hat{\mu}_{2i} = \hat{\mu}_{2i} a, a \in \Sigma, \hat{\mu}_{ki} \in \{\mu_{ki}, \tilde{\mu}_{ki}\}, i = \overline{1,n} \rangle,$$

$$G_4 = \langle G_3, d_i;\ \rho_i^{-1} \mu_{1i}^{-1} \tilde{\mu}_{1i} \tilde{\rho}_i d_i = d_i \mu_{2i} Q_i \mu_{2i}^{-1}, a d_i = d_i a, a \in \Sigma, Q_i = A_i^{-1} B_i, i = \overline{1,n} \rangle,$$

where $\hat{\rho}_{ki}$ and $\hat{\mu}_{ki}$ stand for one of the letters $\rho_{ki}, \tilde{\rho}_{ki}$ and $\mu_{ki}, \tilde{\mu}_{ki}$, respectively.

Define G_s^+ $(s = \overline{1,4})$ to be the anti-isomorphic group relative to the map $x \mapsto x^+$, where x is a letter in the alphabet of G_s.

Let

$$\mathscr{N}(\Pi) = \langle G_4, G_4^+, p;\ E p E^+ = p, E \in \{\hat{\mu}_{2i}^{-1} l_{ai} \hat{\mu}_{2i}, \hat{\mu}_{2i}^{-1} d_i^{-1} l_{ai} d_i \hat{\mu}_{2i}, \hat{\mu}_{2i}^{-1} d_i^{-1} \hat{\rho}_i d_i \hat{\mu}_{2i}, \tilde{\mu}_{2i}^{-1} d_i^{-1} \tilde{\mu}_{1i}^{-1} \mu_{1i} d_i \mu_{2i}\},$$
$$a \in \Sigma, \hat{\mu}_{ki} \in \{\mu_{ki}, \tilde{\mu}_{ki}\}, i = \overline{1,n} \rangle,$$

where in each relation $\hat{\mu}_{ki}$ stands for one of the letters $\tilde{\mu}_{ki}$ or μ_{ki}.

In fact, the tower $N(\Pi)$ is the tower of HNN-extensions, i.e., the stable letters are regular at each step [20] (see also [10]).

Let us recall the definition of the map f mentioned above. If u is a word in Π, then

$$f(u) = X(u) p X^+(u),$$

where $X(u) = u \tau_1 \tau_2$.

The following theorem is the main technical result of [20].

Theorem 3.1. *For arbitrary $u, v \in \Pi$, we have*

$$u = v\ (\Pi) \quad \Longleftrightarrow \quad X(u) p X^+(u) = X(v) p X^+(v)\ (\mathscr{N}(\Pi)).$$

In other words, $u = v(\Pi)$ if and only if $X^{-1}(u) X(v) = \mathscr{A}_p$ (or $X^+(u)(X^+(v))^{-1} = \mathscr{B}_p$).

Here $\mathscr{A}_p := V(E)$ and $\mathscr{B}_p := V((E^+)^{-1})$, so these are elements of the subgroups generated by E and $(E^+)^{-1}$, respectively. Let us put $\mathscr{A}_{p^{-1}} := \mathscr{B}_p$ and $\mathscr{B}_{p^{-1}} := \mathscr{A}_p$. We use the same notations for any HNN-extension. For example, $\mathscr{A}_{d_i}$ in G_4 stands for any group word in $\rho_i^{-1} \mu_{1i}^{-1} \tilde{\mu}_{1i} \tilde{\rho}_i, a$, where $a \in \Sigma,\ i = \overline{1,n}$.

Let us recall the Britton Lemma for HNN-extensions using $\mathscr{N}(\Pi)$ as an example. It says that if $W \in G_4 \backslash G_3$ and $W = 1$, then W contains a subword $p^{-\varepsilon} \mathscr{A}_{p^\varepsilon} p^\varepsilon$.

In the proof of Theorem 3.1, given in [20], the following Novikov's equality criterion had been used.

Theorem 3.2 (*[20, Theorem, Chapter 4], see also [10]*). *Let $\mathscr{A}_p = W(\Sigma)$, where W is a group word in Σ. Then $\mathscr{A}_p$ belongs to the subgroup generated by $C^{-1} Q_i C$, where C's are stable group words in Σ, i.e., $\rho_i C = C \rho_i^{k(C)}$, $i = \overline{1,n}$.*

This is the main group-theoretical result of [20].

Next Proposition 3.4 is a generalization of the Novikov equality criterion. In the proof, we will use the notion of a semi-canonical word and the main technical Lemma 3 from [10] that any word $\mathscr{A}_p$ can be transformed to a semi-canonical form. Let us recall that a semi-canonical form of $\mathscr{A}_p$ is a product of words:

$$\hat{\mu}_{2i}^{-1} V(l_{ai})\hat{\mu}_{2i}, \tag{3.1}$$

$$C^{-1} Q_i^{\varepsilon} C, \tag{3.2}$$

$$\hat{\mu}_{2i}^{-1} V_1(l_{ai}) d_i^{-1} W(\rho_i, \tilde{\rho}_i, l_{ai}, C^{-1}Q_i C, A^{-1}N_i A, A^{-1}Q_i M_i A) d_i V_2(l_{ai})\hat{\mu}_{2i} \tag{3.3}$$

with some additional properties (see [10, Section 3]); here C's are stable group words in Σ.

Lemma 3.3. *Any semi-canonical word $\mathscr{A}_p$ is d_i-irreducible, i.e., it contains no subword of the form $d_i^{-\varepsilon}\mathscr{A}_{d_i^{\varepsilon}} d_i^{\varepsilon}$.*

Proof. See the proof of the Corollary in [10]. □

Proposition 3.4. *Let us have an equality*

$$\mathscr{A}_p = W(\Sigma, \rho_i, l_{ai})$$

(*thus W is a group word in this letters*). *Then there exists a group word $W_1(\Sigma)$ such that $\mathscr{A}_p = W_1$ (actually, $W_1 = W_1(C^{-1}Q_i C)$).*

Proof. By [10], Lemma 3, the word $\mathscr{A}_p$ can be assumed to be a semi-canonical in the sense of that paper. From Lemma 3.3, our assumption on W, and the Britton Lemma, it follows that $\mathscr{A}_p$ has no letters d_i at all, i.e, $\mathscr{A}_p$ has no subwords (3.3). Now by the definition of semi-canonical words, the d_i-free word $\mathscr{A}_p$ should be $\hat{\mu}_i$-irreducible. Again, our assumption on W and the Britton Lemma imply that $\mathscr{A}_p$ has no letters $\hat{\mu}_i$, i.e., it has no subwords (3.1). Finally, $\mathscr{A}_p$ is a product of subwords (3.2). □

Now we prove the following

Proposition 3.5. *Let $u \neq v(\Pi)$, $a \in \Sigma$, $i \in [1, n]$. Then the elements*

$$l_{ai}, l_{ai}^+, pX(u)pX^+(u)(X^+(v))^{-1}p^{-1}X(v)^{-1}p^{-1}$$

are independent, i.e., they generate freely a free subgroup in $\mathscr{N}(\Pi)$.

Proof. Assume that

$$V(l_{ai}, l_{ai}^+, pX(u)pX^+(u)(X^+(v))^{-1}p^{-1}X(v)^{-1}p^{-1}) = 1,$$

where $V(x_1, x_2, x_3)$ is a nontrivial freely reduced word. It is clear that x_3 appears in V since elements l_{ai}, l_{ai}^+ are independent. Then by the Britton Lemma V contains a subword $p^{-\varepsilon}Ep^{\varepsilon}$, $E = \mathscr{A}_{p^{\varepsilon}}$. We have the following options:

(1) $\varepsilon = -1$. Then $E \doteq X^+(u)(X(v)^+)^{-1} = \mathscr{B}_p$. By Novikov's Theorem 3.1 we obtain $u = v(\Pi)$, that contradicts the assumption.
(2) $\varepsilon = 1$ and $E \doteq V(l_{ai}, l_{ai}^+) = \mathscr{A}_p$, where $V \neq 1$. We have $\mathscr{A}_p \in G_4$, $V \in G_4 * G_4^+$. It follows that V does not contain l_{ai}^+. By the Proposition 3.4, V is equal to a Σ-word, that contradicts the definition of G_2.
(3) $\varepsilon = 1$ and $E \doteq X(v)^{-1}p^{-1}pX(u) = \mathscr{A}_p$. By Novikov's Theorem 3.1 we obtain $u = v(\Pi)$, that is impossible. □

4. On the Adyan original construction

In 1957, S. I. Adyan proved that there is no algorithm to decide whether a given (arbitrary) finitely presented group has a given Markov property (for "almost all" Markov's properties). Recall that a property $\wp$ is said to be a Markov property if there exist a finitely presented group with $\wp$ and a finitely presented group that cannot be embedded into any finitely presented group with $\wp$. The main idea of the proof was to construct a special extension of the Novikov group (see below). The main difficulty in Adyan's paper was to prove that the Novikov group is a subgroup in the extension. In this paper we simplify the Adyan's proof by using Gröbner–Shirshov bases.

Let us recall some definitions and properties from [1].

To construct the extension, Adyan first re-arranges the positive alphabet of $\mathscr{N}(\Pi)$ to an order $a_1, a_2, \ldots, a_n$ (this n is nothing to do with n from the previous section) and adds new letters $q_1, \ldots, q_n$. Then he adds new defining relations to the group $\mathscr{N}(\Pi)$, depending on two words u, v from the semigroup Π. Let $A_{u,v}(\mathscr{N}(\Pi))$ be the original Adyan extension [1]. We need to know some properties of $A_{u,v}(\mathscr{N}(\Pi))$.

The sub-extension G of $\mathscr{N}(\Pi)$ formed by letters $q_1, \ldots, q_{n-1}$ and the corresponding relations is a tower of HNN-extensions of $\mathscr{N}(\Pi)$. Thus the group $\mathscr{N}(\Pi)$ is a subgroup in this sub-extension G (see [1, Lemma 1, Chapter 2]). So we only need to prove that this sub-extension is a subgroup in the whole extension.

We state here some explicit definitions from [1] related to the letter q_n. For two words $u, v \in \Pi$, let

$$a(u, v) := pX(u)pX^+(u)(X^+(v))^{-1}p^{-1}(X(v))^{-1}p^{-1}.$$

Now $a_{n-2} := p$, $a_{n-1} := l_{ai}$, $a_n := l_{ai}^+$, and

$$q_{n-2}q_{n-1} = q_{n-1}a_{n-2} \tag{4.1}$$

is the relation corresponding to the letter q_{n-1};

$$q_{n-1}q_n = q_n a_{n-1}, \quad a_n q_n a(u, v) q_n = q_n a_n \tag{4.2}$$

are the relations corresponding to the letter q_n.

We can prove the following

Proposition 4.1. *Elements $a_n, a_{n-1}, a(u, v), q_{n-1} (u \neq v$ in $\Pi)$ freely generate a free subgroup in the sub-extension G.*

Proof. Assume that there exists a freely reduced word $V(x_1, x_2, x_3, x_4)$ and $V(a_n, a_{n-1}, a(u, v), q_{n-1}) = 1$ in the sub-extension. By Proposition 3.5, V contains entries of the letter q_{n-1}. So by the Britton Lemma, V has a subword

$$q_{n-1}^{-\delta} W(a_n, a_{n-1}, a(u, v)) q_{n-1}^{\delta},$$

where $W = \mathscr{A}_{q_{n-1}^{\delta}}$. We have to check the following cases:

(1) $\delta = 1$. Then $W(a_n, a_{n-1}, a(u, v))$ is equal to $\mathscr{A}_{q_{n-1}} = q_{n-2}^t$, that contradicts the Britton Lemma ($W \in \mathscr{N}(\Pi)$ and G is the tower of HNN-extensions of $\mathscr{N}(\Pi)$).

(2) $\delta = -1$, then $W = a_{n-2}^{-t} = p^{-t}$. So

$$p^t W(l_{ai}^+, l_{ai}, pX(u)pX^+(u)(X^+(v))^{-1}p^{-1}(X(v))^{-1}p^{-1}) = 1. \tag{4.3}$$

By the Britton Lemma, this word has a subword $p^{-\delta}Ep^{\delta}$ with $E = \mathscr{A}_{p^\delta}$. We have the following cases:

(a) $\delta = -1$ and $E \doteq X^+(u)(X^+(v))^{-1} = \mathscr{B}_p$ (i.e., $p^{-\delta}Ep^{\delta}$ is a subword of $a(u, v)$);

(b) $\delta = 1$ and $E \doteq (X(v))^{-1}p^{-1}pX(u) = \mathscr{A}_p$ (i.e., $p^{-\delta}Ep^{\delta}$ is a subword of $a(u, v)a(u, v)$);

(c) $\delta = 1$ and $E \doteq W_1(l_{ai}, l_{ai}^+) = \mathscr{A}_p$, where $W_1 \neq 1$ (i.e., $p^{-\delta}Ep^{\delta}$ is a subword of $p^t W_1(l_{ai}, l_{ai}^+)a(u, v)$, $t < 0$, and it is not the next case (d));

(d) $\delta = 1$ and $E \doteq X(u) = \mathscr{A}_p$ (i.e., $p^{-\delta}Ep^{\delta}$ is a subword of $p^t a(u, v) = p^{t+1}X(u)pX^+(u)(X^+(v))^{-1} p^{-1}(X(v))^{-1}p^{-1}, t < -1$).

Cases (2a), (2b) are impossible by Novikov's Theorem 3.1 (otherwise $u = v$ in Π, it is a contradiction).

Case (2c) is impossible by Proposition 3.4 (otherwise, the word $W_1(l_{ai}, l_{ai}^+)$ is equal to a Σ-word, so W_1 is empty; it is a contradiction).

Case (2d) is impossible by Novikov's Theorem 2 ([20, Chapter 6, Section 2]) and Lemma 2 ([20, Chapter 6, Section 1]). Let us give some details. From $X(u) = \mathscr{A}_p$ it follows $X(u)pX^+(u) = p$. Then by Novikov's Theorem 2 ([20, Chapter 6, Section 2]), $X(u)$ is equal to 1 in a Novikov's system **B**. By Novikov's Lemma 2 ([20, Chapter 6, Section 1]), a non-empty positive word in Σ cannot be equal to 1 in **B**. But $X(u) = u\tau_1\tau_2$ is non-empty. $\square$

Since Proposition 4.1, it is sufficient to prove that every group G with four independent elements can be embedded into the extension corresponding to the adjunction of the letter q_n in the Adyan original construction. Thus we focus our attention on this extension.

5. The Adyan (two-relation) extension

Let G be an arbitrary group that contains four independent letters $\Sigma = \{q_0, a_0, a, a_1\}$. Let $F_4 = \mathrm{gr}\langle q_0, a_0, a, a_1\rangle$. By the Adyan extension of G with respect to the fixed free subgroup F_4 we mean the following group (in a semigroup presentation):

$$A(G, F_4) = \langle G, q, q^{-1}; q_0 q = q a_0, a_1 q a q = q a_1, q^{\varepsilon} q^{-\varepsilon} = 1, \varepsilon = \pm 1\rangle.$$

We have already proved that the original Adyan group from [1] is of such form.

Now we define a presentation of $A(G, F_4)$ by generators and defining relations. First we define a partition of G as

$$G = F_4 \dot{\cup} \{u_i; i \in I\},$$

where I is a well-ordered index set and $u_i < u_j$ if $i < j$.

Then we define G by generators

$$Y = (\Sigma \cup \Sigma^{-1}) \dot{\cup} U, \quad U = \{u_i, i \in I\}$$

and relations

$$u_i u_j = w, \quad w \in F_4 \cup U, \ \ i, j \in I; \tag{5.1}$$

$$u_i c = u_j; \quad c u_i = u_k, \ \ i, j, k \in I, \ \ c \in \Sigma \cup \Sigma^{-1}; \tag{5.2}$$

$$c c^{-1} = 1, \quad c \in \Sigma \cup \Sigma^{-1}. \tag{5.3}$$

Note that, for example, $u_i c \notin F_4$, otherwise, $u_i \in F_4$ that is impossible.

We obtain a semigroup presentation of $A(G, F_4)$ in the set of generators $X = Y \cup \{q, q^{-1}\}$.

Let us impose the deg–tower order on the set of Y-words starting with the deg–lex order of words in $\Sigma \cup \Sigma^{-1}$. Then leading words of relations (5.1), (5.2), (5.3) occupy the left-hand side of these relations. For example, we have

$$wt'(u_i c) = (1, 2, u_i, c) > wt'(u_j) = (1, 1, u_j, 1).$$

We define the tower order of words in $X = Y \dot{\cup} Z$ starting with the deg–tower order of words in $Y = (\Sigma \cup \Sigma^{-1}) \dot{\cup} U$.

Denote the elements w, u_j, u_k from the right-hand sides of the defining relations of G, (5.1), (5.2) by $\overline{u_i u_j}$, $\overline{u_i c}$, $\overline{c u_i}$, respectively.

Also we use the following notation:

$$\mathscr{A}_q := q_0^n =: \mathscr{B}_{q^{-1}}, \quad \mathscr{B}_q := a_0^n =: \mathscr{A}_{q^{-1}}.$$

For all words $\mathscr{A}_{q^{\varepsilon}}, \mathscr{B}_{q^{\varepsilon}}$ appearing in one relation, the number n is a fixed integer. Similarly, we define

$$a_q := q_0^{\delta} =: b_{q^{-1}}, \quad b_q := a_0^{\delta} =: a_{q^{-1}}, \quad \delta = \pm 1.$$

We write $f \vee g$ for $(f, g)_w$. It is especially convenient when the composition $(f, g)_w$ is unique and there is no need to specify w.

6. Gröbner–Shirshov Basis of $A(F_4)$

Recall that we fix the deg–lex order in F_4 and the tower order in $A(F_4)$.

Theorem 6.1. *The Gröbner–Shirshov bases of* $A(F_4)$
($F_4 = gr\langle q_0, a_0, a, a_1\rangle$) *consists of the trivial relations and Eqs.* (6.1)–(6.13):

$$a_{q^\varepsilon} q^\varepsilon = q^\varepsilon b_{q^\varepsilon}, \tag{6.1}$$

$$q^\varepsilon \mathscr{B}_{q^\varepsilon} a_1 q^{-\varepsilon} = \mathscr{A}_{q^\varepsilon} a_1 q^\varepsilon a^\varepsilon; \tag{6.2}$$

$$q^\varepsilon \mathscr{B}_{q^\varepsilon} a_1^{-1} q^{-\varepsilon} = \mathscr{A}_{q^\varepsilon} a^{-\varepsilon} q^{-\varepsilon} a_1^{-1}; \tag{6.3}$$

$$q^\varepsilon \mathscr{B}_{q^\varepsilon} a^\varepsilon q^\varepsilon = \mathscr{A}_{q^\varepsilon} a_1^{-1} q^\varepsilon a_1, \tag{6.4}$$

$$(2\vee 3) \quad a_1 q^\varepsilon a^\varepsilon \mathscr{B}_{q^{-\varepsilon}} a_1^{-1} q^\varepsilon = q^\varepsilon a_1 \mathscr{A}_{q^{-\varepsilon}} a^\varepsilon q^\varepsilon a_1^{-1}, \tag{6.5}$$

$$(2\vee 4) \quad a_1 q^\varepsilon a^\varepsilon \mathscr{B}_{q^{-\varepsilon}} a^{-\varepsilon} q^{-\varepsilon} = q^\varepsilon a_1 \mathscr{A}_{q^{-\varepsilon}} a_1^{-1} q^{-\varepsilon} a_1, \tag{6.6}$$

$$(2\vee 2) \quad a_1 q^\varepsilon a^\varepsilon \mathscr{B}_{q^{-\varepsilon}} a_1 q^\varepsilon = q^\varepsilon a_1 \mathscr{A}_{q^{-\varepsilon}} a_1 q^{-\varepsilon} a^{-\varepsilon}, \tag{6.7}$$

$$(3\vee 2) \quad a^{-\varepsilon} q^{-\varepsilon} a_1^{-1} \mathscr{B}_{q^{-\varepsilon}} a_1 q^\varepsilon = q^\varepsilon a_1^{-1} \mathscr{A}_{q^{-\varepsilon}} a_1 q^{-\varepsilon} a^{-\varepsilon}, \tag{6.8}$$

$$(3\vee 3) \quad a^{-\varepsilon} q^{-\varepsilon} a_1^{-1} \mathscr{B}_{q^{-\varepsilon}} a_1^{-1} q^\varepsilon = q^\varepsilon a_1^{-1} \mathscr{A}_{q^{-\varepsilon}} a^\varepsilon q^\varepsilon a_1^{-1}, \tag{6.9}$$

$$(3\vee 4) \quad a^{-\varepsilon} q^{-\varepsilon} a_1^{-1} \mathscr{B}_{q^{-\varepsilon}} a^{-\varepsilon} q^{-\varepsilon} = q^\varepsilon a_1^{-1} \mathscr{A}_{q^{-\varepsilon}} a_1^{-1} q^{-\varepsilon} a_1, \tag{6.10}$$

$$(4\vee 2) \quad a_1^{-1} q^\varepsilon a_1 \mathscr{B}_{q^\varepsilon} a_1 q^{-\varepsilon} = q^\varepsilon a^\varepsilon \mathscr{A}_{q^\varepsilon} a_1 q^\varepsilon a^\varepsilon, \tag{6.11}$$

$$(4\vee 3) \quad a_1^{-1} q^\varepsilon a_1 \mathscr{B}_{q^\varepsilon} a_1^{-1} q^{-\varepsilon} = q^\varepsilon a^\varepsilon \mathscr{A}_{q^\varepsilon} a^{-\varepsilon} q^{-\varepsilon} a_1^{-1}, \tag{6.12}$$

$$(4\vee 4) \quad a_1^{-1} q^\varepsilon a_1 \mathscr{B}_{q^\varepsilon} a^\varepsilon q^\varepsilon = q^\varepsilon a^\varepsilon \mathscr{A}_{q^\varepsilon} a_1^{-1} q^\varepsilon a_1. \tag{6.13}$$

We write $(i \vee j)$ meaning $(6.i \vee 6.j)$. In each relation, the leading word stands in the left-hand side. To apply a relation to another one means to eliminate the leading word of the first relation in the leading word of the second one.

Proof. The proof consists of checking compositions. Observe that the compositions of (6.2)–(6.4) with each other are relations (6.5)–(6.13), and that the compositions of (6.2)–(6.4) with (6.1) are trivial. We have to check the compositions of the following types:

- $(i \vee j) \vee k$,
- $2 \vee (2 \vee i), 3 \vee (4 \vee i), 4 \vee (3 \vee i)$,
- $(i \vee 2) \vee (2 \vee j), (i \vee 3) \vee (4 \vee j), (i \vee 4) \vee (3 \vee j)$, where $2 \leqslant i, j, k \leqslant 4$,
- compositions of (6.1)–(6.13) with trivial relations.

We denote left- and right-hand sides of relation (i), $2 \leqslant i \leqslant 13$, by $\mathscr{L}_i$ and $\Re_i$, respectively. If S is a word of length n and $k \leqslant n$, then ${}^{(k)}S(S^{(k)})$ is a suffix (prefix) of S of the length $n-k$.

Observe that the composition $(i \vee j)$, $2 \leqslant i, j \leqslant 4$, has the following form:

$$\Re_i({}^{(1)}\mathscr{L}_j) = (\mathscr{L}_i^{(1)})\Re_j, \tag{6.14}$$

where

$$w_1 \doteq \mathscr{L}_i({}^{(1)}\mathscr{L}_j) \doteq (\mathscr{L}_i^{(1)})\mathscr{L}_j,$$

(a) Let us check the compositions of type $(i \vee j) \vee k$, $2 \leqslant i, j, k \leqslant 4$. The ambiguity is

$$w \doteq \Re_i({}^{(1)}\mathscr{L}_j)({}^{(1)}\mathscr{L}_k) \doteq \Re_i({}^{(1)}\mathscr{L}_j^{(1)})\mathscr{L}_k$$

and the composition is

$$(\mathscr{L}_i^{(1)})\Re_j({}^{(1)}\mathscr{L}_k) = \Re_i({}^{(1)}\mathscr{L}_j^{(1)})\Re_k. \tag{6.15}$$

Now apply the relation $(j \vee k)$ to (6.15) and obtain

$$(\mathscr{L}_i^{(1)})(\mathscr{L}_j^{(1)})\Re_k = \Re_i({}^{(1)}\mathscr{L}_j^{(1)})\Re_k. \tag{6.16}$$

It follows from the form of $w_1(i \vee j)$ that

$$(\mathscr{L}_i^{(1)})(\mathscr{L}_j^{(1)}) \doteq \mathscr{L}_i({}^{(1)}\mathscr{L}_j^{(1)}). \tag{6.17}$$

Finally, we apply (i) to (6.16) and obtain

$$\Re_i({}^{(1)}\mathscr{L}_j^{(1)})\Re_k \doteq \Re_i({}^{(1)}\mathscr{L}_j^{(1)})\Re_k.$$

We have checked the triviality of composition (6.15).

(b) Let us check the compositions $2 \vee (2 \vee i)$, $2 \leqslant i \leqslant 4$. The ambiguity and the composition are given by

$$w \doteq q^{-\varepsilon}\mathscr{B}_{q^{-\varepsilon}}a_1q^{\varepsilon}a^{\varepsilon}({}^{(1)}\mathscr{L}_i),$$

$$\mathscr{A}_{q^{-\varepsilon}}a_1q^{-\varepsilon}a^{-\varepsilon}a^{\varepsilon}({}^{(1)}\mathscr{L}_i) = q^{-\varepsilon}\mathscr{B}_{q^{-\varepsilon}}q^{\varepsilon}a_1\Re_i,$$

$$\mathscr{A}_{q^{-\varepsilon}}a_1q^{-\varepsilon}({}^{(1)}\mathscr{L}_i) = \mathscr{B}_{q^{\varepsilon}}a_1\Re_i \tag{6.18}$$

for $\mathscr{B}_{q^{-\varepsilon}} = \mathscr{A}_{q^{\varepsilon}}$. The ambiguity $(2 \vee i)$ has the form

$$w_1 \doteq q^{\varepsilon}\mathscr{B}_{q^{\varepsilon}}a_1q^{-\varepsilon}({}^{(1)}\mathscr{L}_i) \doteq q^{\varepsilon}\mathscr{B}_{q^{\varepsilon}}a_1\mathscr{L}_i$$

so we have

$$q^{-\varepsilon}({}^{(1)}\mathscr{L}_i) \doteq \mathscr{L}_i. \tag{6.19}$$

Now apply the relations (i) and (6.19)–(6.18) and obtain

$$B_{q^{\varepsilon}}a_1\Re_i \doteq \mathscr{B}_{q^{\varepsilon}}a_1\Re_i.$$

Triviality of the composition (6.18) is now checked.
Compositions

$$3 \vee (4 \vee i), \quad 4 \vee (3 \vee i)$$

can be processed similarly.

(c) Consider the compositions $(2 \vee 2) \vee (2 \vee i)$, $2 \leqslant i \leqslant 4$. The ambiguity and the composition are

$$w \doteq a_1q^{\varepsilon}a^{\varepsilon}\mathscr{B}_{q^{-\varepsilon}}a_1q^{\varepsilon}a^{\varepsilon}({}^{(1)}\mathscr{L}_i),$$

$$q^{\varepsilon}a_1\mathscr{A}_{q^{-\varepsilon}}a_1q^{-\varepsilon}({}^{(1)}\mathscr{L}_i) = a_1q^{\varepsilon}a^{\varepsilon}q^{\varepsilon}\mathscr{B}_{q^{\varepsilon}}a_1\Re_i. \tag{6.20}$$

Apply the relation (6.4) to the right-hand side of the last equality to obtain:

$$q^{\varepsilon}a_1\mathscr{A}_{q^{-\varepsilon}a_1q^{-\varepsilon}}(^{(1)}\mathscr{L}_i) = a_1a_1^{-1}q^{\varepsilon}a_1\mathscr{B}_{q^{\varepsilon}a_1}\mathfrak{R}_i,$$

$$q^{\varepsilon}a_1\mathscr{A}_{q^{-\varepsilon}a_1q^{-\varepsilon}}(^{(1)}\mathscr{L}_i) = q^{\varepsilon}a_1\mathscr{B}_{q^{\varepsilon}a_1}\mathfrak{R}_i.$$

Upon applying equality (6.19), we obtain

$$q^{\varepsilon}a_1\mathscr{B}_{q^{\varepsilon}a_1}\mathfrak{R}_i \doteq q^{\varepsilon}a_1\mathscr{B}_{q^{\varepsilon}a_1}\mathfrak{R}_i.$$

Triviality of the composition (6.20) is now checked.
Compositions

$$(i \vee 2) \vee (2 \vee j), \quad (i \vee 3) \vee (4 \vee j), \quad (i \vee 4) \vee (3 \vee j)$$

can be processed similarly.

(d) Now we will check the compositions $(i \vee (q^{-\delta}q^{\delta} = 1))$. We have the following ambiguity and the composition, respectively:

$$w \doteq \mathscr{L}_i q^{\delta}, \quad \mathfrak{R}_i q^{\delta} = \mathscr{L}_i^{(1)}. \tag{6.21}$$

Here δ is chosen in such a way that $\mathscr{L}_i q^{\delta}$ is an ambiguity. It is easy to see that there exist k, $2 \leqslant k \leqslant 4$, and $\mathscr{L}_k$ with $\mathscr{B} \doteq 1$ such that

$$\mathfrak{R}_i q^{\delta} \doteq (\mathfrak{R}_i^{(2)})\mathscr{L}_k.$$

Let us cancel $(\mathfrak{R}_i^{(2)})\mathfrak{R}_k = (\mathfrak{R}_i^{(3)})(^{(1)}\mathfrak{R}_k)$ and apply (6.1). We obtain the desired graphical equality.

(e) Now we will check the compositions $(i \vee j) \vee (q^{\varepsilon}q^{-\varepsilon} = 1)$,

$$w \doteq \mathfrak{R}_i(^{(1)}\mathscr{L}_j)q^{\delta},$$

where δ is chosen in such a way that $\mathscr{L}_{(i\vee j)}q^{\delta}$ is an ambiguity (in other words, $\mathscr{L}_j q^{\delta}$ is an ambiguity). The corresponding composition is

$$(\mathscr{L}_i^{(1)})\mathfrak{R}_j q^{\delta} = \mathfrak{R}_i(^{(1)}\mathscr{L}_j^{(1)}). \tag{6.22}$$

But $\mathfrak{R}_j q^{\delta} = \mathscr{L}_j^{(1)}$ is a composition $(j \vee (q^{\varepsilon}q^{-\varepsilon} = 1)$, see (6.21). To check the triviality of (6.22), we use the last relation together with (i) and (6.17).

(f) Finally, we have to check a composition

$$(v^{-1}v = 1) \vee (i \vee j).$$

We have the ambiguity

$$w \doteq v^{-1}\mathscr{L}_{i\vee j},$$

where v is the first letter of the word $\mathscr{L}_{i\vee j}$, and the composition

$$v^{-1}\mathfrak{R}_{i\vee j} = (^{(1)}\mathscr{L}_{i\vee j}).$$

It is enough to observe that there exist k and l such that

$$v^{-1}\mathfrak{R}_{i\vee j} \doteq \mathscr{L}_{k\vee l}, (^{(1)}\mathscr{L}_{i\vee j}) \doteq \mathfrak{R}_{k\vee l}.$$

Theorem 6.1 is proved. □

7. Gröbner–Shirshov basis for the group $A(G, F_4)$

Now we proceed to the general case defined in Section 5. Let us construct a Gröbner–Shirshov basis of $A(G)$.

First, we have to include the defining relations of G and the Gröbner–Shirshov basis of $A(F_4)$ (Theorem 6.1) into a Gröbner–Shirshov basis of $A(G, F_4)$.

Let us fix the following notation: u with indices will denote an element of U, c is any element of $\Sigma \cup \Sigma^{-1}$.

From (6.1) it follows

$$\mathscr{A}_{q^\varepsilon} q^\varepsilon = q^\varepsilon \mathscr{B}_{q^\varepsilon}. \tag{7.1}$$

For any u we have in G

$$u\mathscr{A}_{q^\varepsilon} = \overline{u\mathscr{A}_{q^\varepsilon}}, \tag{7.2}$$

where $\overline{u\mathscr{A}_{q^\varepsilon}} \in U$. Multiplying (7.1) by u from the left, we get new relations in G

$$\overline{u\mathscr{A}_{q^\varepsilon}} q^\varepsilon = uq^\varepsilon \mathscr{B}_{q^\varepsilon}, \textit{ if } \overline{u\mathscr{A}_{q^\varepsilon}} > u; \tag{7.3}$$

$$uq^\varepsilon = \overline{u\mathscr{A}_{q^\varepsilon}} q^\varepsilon \mathscr{B}_{q^\varepsilon}^{-1}, \textit{ if } u > \overline{u\mathscr{A}_{q^\varepsilon}}. \tag{7.4}$$

We can reduce the second relation to the first one by assuming that $u_1 = \overline{u\mathscr{A}_{q^\varepsilon}} < \overline{u_1\mathscr{A}_{q^\varepsilon}^{-1}} = u$. So we only need to keep relations of the form (7.3).

Let us include (7.3) into a Gröbner–Shirshov basis of $A(G)$.

It easy to see that compositions $(f, g)_w$ of intersection of (7.3) with defining relations of G are trivial:

$$\begin{aligned} w &= u_1\overline{u\mathscr{A}_{q^\varepsilon}}q^\varepsilon, \quad u_1\overline{u\mathscr{A}_{q^\varepsilon}} = u_2, \quad (f,g)_w = u_1uq^\varepsilon\mathscr{B}_{q^\varepsilon} - u_2q^\varepsilon \equiv \overline{\overline{u_1u}\mathscr{A}_{q^\varepsilon}}q^\varepsilon \\ &\quad - \overline{u_1u}q^\varepsilon\mathscr{B}_{q^\varepsilon} \equiv 0 (u_1u \in F_4 \cup U); \end{aligned}$$

$$w = c\overline{u\mathscr{A}_{q^\varepsilon}}q^\varepsilon, \quad c\overline{u\mathscr{A}_{q^\varepsilon}} = u_1, \quad (f,g)_w = -u_1q^\varepsilon + \overline{cu}q^\varepsilon\mathscr{B}_{q^\varepsilon} \equiv 0 (cu \in U),$$

$$w = \overline{u\mathscr{A}_{q^\varepsilon}}q^\varepsilon q^{-\varepsilon}, \quad q^\varepsilon q^{-\varepsilon} = 1, \quad (f,g)_w = \overline{u\mathscr{A}_{q^\varepsilon}} - uq^\varepsilon\mathscr{B}_{q^\varepsilon}q^{-\varepsilon} \equiv 0.$$

Now consider the compositions of inclusion of relations (7.3).

Let

$$\overline{u\mathscr{A}_{q^\varepsilon}}q^\varepsilon = \overline{u_1\mathscr{A}_{1q^\varepsilon}}q^\varepsilon, \quad u \neq u_1, \ \ u_1 > u.$$

be the ambiguity of two corresponding relations (7.3). Then we have $u_1 = \overline{u\mathscr{A}_{2q^\varepsilon}}$, and $\mathscr{A}_{2q^\varepsilon} = \mathscr{A}_{q^\varepsilon}\mathscr{A}_{1q^\varepsilon}^{-1}$.

The composition $u_1q^\varepsilon\mathscr{B}_{1q^\varepsilon} = uq^\varepsilon\mathscr{B}_{q^\varepsilon}$ is trivial modulo the following relation of type (7.3):

$$\overline{u\mathscr{A}_{2q^\varepsilon}}q^\varepsilon = uq^\varepsilon\mathscr{B}_{2q^\varepsilon}, \quad \overline{u\mathscr{A}_{2q^\varepsilon}} > u.$$

Now consider generalizations of relations (6.6)–(6.13) that we include into a Gröbner–Shirshov basis of $A(G, F_4)$:

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}q^\varepsilon\mathscr{B}_{1q^\varepsilon}^{-1}a^\varepsilon\tilde{B}_{q^{-\varepsilon}}a_1^{-1}q^\varepsilon = uq^\varepsilon\mathscr{B}_{q^\varepsilon}a_1\tilde{A}_{q^{-\varepsilon}}a^\varepsilon q^\varepsilon a_1^{-1}, \tag{7.5}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}q^\varepsilon\mathscr{B}_{1q^\varepsilon}^{-1}a^\varepsilon\tilde{B}_{q^{-\varepsilon}}a^{-\varepsilon}q^{-\varepsilon} = uq^\varepsilon\mathscr{B}_{q^\varepsilon}a_1\tilde{A}_{q^{-\varepsilon}}a_1^{-1}q^{-\varepsilon}a_1, \tag{7.6}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}q^\varepsilon\mathscr{B}_{1q^\varepsilon}^{-1}a^\varepsilon\tilde{B}_{q^{-\varepsilon}}a_1q^\varepsilon = uq^\varepsilon\mathscr{B}_{q^\varepsilon}a_1\tilde{A}_{q^{-\varepsilon}}a_1q^{-\varepsilon}a^{-\varepsilon}, \tag{7.7}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a^{-\varepsilon}\mathscr{A}_{1q^{-\varepsilon}}}q^{-\varepsilon}\mathscr{B}_{1q^{-\varepsilon}}^{-1}a_1^{-1}\tilde{B}_{q^{-\varepsilon}}a_1q^\varepsilon = uq^\varepsilon\mathscr{B}_{q^\varepsilon}a_1^{-1}\tilde{A}_{q^{-\varepsilon}}a_1q^{-\varepsilon}a^{-\varepsilon}, \tag{7.8}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a^{-\varepsilon}\mathscr{A}_{1q^{-\varepsilon}}}q^{-\varepsilon}\mathscr{B}^{-1}_{1q^{-\varepsilon}}a_1^{-1}\tilde{B}_{q^{-\varepsilon}}a_1^{-1}q^{\varepsilon}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a_1^{-1}\tilde{A}_{q^{-\varepsilon}}a^{\varepsilon}q^{\varepsilon}a_1^{-1}, \tag{7.9}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a^{-\varepsilon}\mathscr{A}_{1q^{-\varepsilon}}}q^{-\varepsilon}\mathscr{B}^{-1}_{1q^{-\varepsilon}}a_1^{-1}\tilde{B}_{q^{-\varepsilon}}a^{-\varepsilon}q^{-\varepsilon}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a_1^{-1}\tilde{A}_{q^{-\varepsilon}}a_1^{-1}q^{-\varepsilon}a_1, \tag{7.10}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1^{-1}\mathscr{A}_{1q^{\varepsilon}}}q^{\varepsilon}\mathscr{B}^{-1}_{1q^{\varepsilon}}a_1\tilde{B}_{q^{\varepsilon}}a_1q^{-\varepsilon}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a^{\varepsilon}\tilde{A}_{q^{\varepsilon}}a_1q^{\varepsilon}a^{\varepsilon}, \tag{7.11}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1^{-1}\mathscr{A}_{1q^{\varepsilon}}}q^{\varepsilon}\mathscr{B}^{-1}_{1q^{\varepsilon}}a_1\tilde{B}_{q^{\varepsilon}}a_1^{-1}q^{-\varepsilon}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a^{\varepsilon}\tilde{A}_{q^{\varepsilon}}a^{-\varepsilon}q^{-\varepsilon}a_1^{-1}, \tag{7.12}$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1^{-1}\mathscr{A}_{1q^{\varepsilon}}}q^{\varepsilon}\mathscr{B}^{-1}_{1q^{\varepsilon}}a_1\tilde{B}_{q^{\varepsilon}}a^{\varepsilon}q^{\varepsilon}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a^{\varepsilon}\tilde{A}_{q^{\varepsilon}}a_1^{-1}q^{\varepsilon}a_1, \tag{7.13}$$

where in (7.5)

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^{\varepsilon}}}>u \tag{7.14}$$

and the same kind of inequalities holds for (7.6)–(7.13).

If, for example, (7.14) is not valid, then $\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^{\varepsilon}}}<u$, but $\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^{\varepsilon}}$ is not a unit in the free group F_4. As the result, we obtain (7.13) with the desired inequality.

It is easy to see that compositions of intersection of (7.5)–(7.13) and the relations of G are trivial.

Now we will check compositions of inclusion of generalized relations (7.5)–(7.13). Leading words of this relations may include each other only if these words are equal. Here we use that $F_4=\mathrm{gp}\langle q_0,a_0,a,a_1\rangle$ is the free group.

Consider a composition (7.5) and another relation of the same kind

$$\overline{u_1\mathscr{A}_{2q^\varepsilon}a_1\mathscr{A}_{3q^{\varepsilon}}}q^{\varepsilon}\mathscr{B}^{-1}_{3q^{\varepsilon}}a^{\varepsilon}\tilde{\mathscr{B}}_{4q^{-\varepsilon}}a_1^{-1}q^{\varepsilon}=u_1q^{\varepsilon}\mathscr{B}_{2q^\varepsilon}a_1\tilde{\mathscr{A}}_{4q^{-\varepsilon}}a^{\varepsilon}q^{\varepsilon}a_1^{-1},$$

$$\overline{u_1\mathscr{A}_{2q^\varepsilon}a_1\mathscr{A}_{3q^{\varepsilon}}}>u_1. \tag{7.15}$$

If the left-hand sides of (7.5) and (7.15) coincide, then

$$\mathscr{B}^{-1}_{1q^{\varepsilon}}=\mathscr{B}^{-1}_{3q^{\varepsilon}},\quad \tilde{\mathscr{B}}_{q^{-\varepsilon}}=\tilde{\mathscr{B}}_{4q^{-\varepsilon}},$$

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^{\varepsilon}}}=\overline{u_1\mathscr{A}_{2q^\varepsilon}a_1\mathscr{A}_{3q^{\varepsilon}}}.$$

We obtain

$$\overline{u\mathscr{A}_{q^\varepsilon}}=\overline{u_1\mathscr{A}_{2q^\varepsilon}}. \tag{7.16}$$

The composition of (7.5) and (7.15) is the relation

$$u_1q^{\varepsilon}\mathscr{B}_{2q^\varepsilon}a_1\tilde{A}_{4q^{-\varepsilon}}a^{\varepsilon}q^{\varepsilon}a_1^{-1}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a_1\tilde{\mathscr{A}}_{q^{-\varepsilon}}a^{\varepsilon}q^{\varepsilon}a_1^{-1}. \tag{7.17}$$

This relation is graphically equal to

$$u_1q^{\varepsilon}\mathscr{B}_{2q^\varepsilon}a_1\tilde{\mathscr{A}}_{q^{-\varepsilon}}a^{\varepsilon}q^{\varepsilon}a_1^{-1}=uq^{\varepsilon}\mathscr{B}_{q^\varepsilon}a_1\tilde{\mathscr{A}}_{q^{-\varepsilon}}a^{\varepsilon}q^{\varepsilon}a_1^{-1}.$$

By the composition of the type (7.5), this relation is trivial.

Compositions of inclusion of (7.6)–(7.13) are processed similarly. Compositions of inclusion of (7.3) and (7.5)–(7.13) are also trivial.

Theorem 7.1. *Gröbner–Shirshov basis of the Adyan* (*two-relation*) *extension* $A(G,F_4)$ *consists of relations* (5.1)–(5.3) *of* G, *Gröbner–Shirshov basis* (6.1)–(6.13) *of* $A(F_4)$, *and relations* (7.3), (7.5)–(7.13).

Proof. Let S be the set of relations from the statement of the theorem. At the beginning of the section we proved that all compositions of intersection with relations of G and all compositions of inclusion are trivial modulo S.

It remains to check compositions of intersection of generalized relations (7.5)–(7.13). There are no compositions of intersection of (7.5)–(7.13) with each other. So it remains to check compositions of intersection of (7.5)–(7.13) with (6.2)–(6.13).

For example, consider a composition of intersection of (7.5) and (6.11). We have the ambiguity and the composition, respectively:

$$w \doteq \overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}q^\varepsilon\mathscr{B}_{1q^\varepsilon}^{-1}a^\varepsilon\tilde{B}_{q^{-\varepsilon}}a_1^{-1}q^\varepsilon a_1\tilde{\tilde{\mathscr{B}}}_{q^\varepsilon}a_1q^{-\varepsilon},$$

$$uq^\varepsilon B_{q^\varepsilon}a_1\tilde{A}_{q^{-\varepsilon}}a^\varepsilon q^\varepsilon a_1^{-1}a_1\tilde{\tilde{\mathscr{B}}}_{q^\varepsilon}a_1q^{-\varepsilon} = \overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}q^\varepsilon\mathscr{B}_{1q^\varepsilon}^{-1}a^\varepsilon q^\varepsilon\tilde{B}_{q^\varepsilon}a^\varepsilon\tilde{\tilde{\mathscr{A}}}_{q^\varepsilon}a_1q^\varepsilon a^\varepsilon.$$

Apply trivial relations and (6.2), (6.4):

$$uq^\varepsilon B_{q^\varepsilon}a_1\tilde{A}_{q^{-\varepsilon}}a^\varepsilon\tilde{\tilde{\mathscr{A}}}_{q^\varepsilon}a_1q^\varepsilon a^\varepsilon = \overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}\mathscr{A}_{q^\varepsilon}^{-1}a_1^{-1}q^\varepsilon a_1\tilde{B}_{q^\varepsilon}a^\varepsilon\tilde{\tilde{\mathscr{A}}}_{q^\varepsilon}a_1q^\varepsilon a^\varepsilon.$$

Then we have

$$\overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}}\mathscr{A}_{q^\varepsilon}^{-1}a_1^{-1} = \overline{u\mathscr{A}_{q^\varepsilon}a_1\mathscr{A}_{1q^\varepsilon}\mathscr{A}_{q^\varepsilon}^{-1}a_1^{-1}} = \overline{u\mathscr{A}_{q^\varepsilon}},$$

$$uq^\varepsilon B_{q^\varepsilon}a_1\tilde{A}_{q^{-\varepsilon}}a^\varepsilon\tilde{\tilde{\mathscr{A}}}_{q^\varepsilon}a_1q^\varepsilon a^\varepsilon = \overline{u\mathscr{A}_{q^\varepsilon}}q^\varepsilon a_1\tilde{B}_{q^\varepsilon}a^\varepsilon\tilde{\tilde{\mathscr{A}}}_{q^\varepsilon}a_1q^\varepsilon a^\varepsilon.$$

After the application of a relation of type (7.3) we obtain the graphical equality. □

Now Theorem 1.1 follows from Theorem 7.1 and the Composition-Diamond Lemma.

References

[1] S.I. Adyan, Unsolvability of some algorithmic problems in the theory of groups, Trudy MMO 6 (1957) 231–298.
[2] G.M. Bergman, The diamond lemma for ring theory, Adv. in Math. 29 (1978) 178–218.
[3] L.A. Bokut, On a property of the Boone groups. II, Algebra i Logika Sem. 5 (5) (1966) 5–23;
L.A. Bokut, On a property of the Boone groups. II, Algebra i Logika Sem. 6 (1) (1967) 15–24
[4] L.A. Bokut, On the Novikov groups, Algebra i Logika Sem. 6 (1) (1967) 25–38.
[5] L.A. Bokut, Groups of fractions of multiplicative semigroups of certain rings. I, II, III, (Russian) Sibirsk. Mat. Žh. 10 (1969) 246–286;
L.A. Bokut, Groups of fractions of multiplicative semigroups of certain rings. I, II, III, (Russian) Sibirsk. Mat. Žh. 10 (1969) 744–799;
L.A. Bokut, Groups of fractions of multiplicative semigroups of certain rings. I, II, III, (Russian) Sibirsk. Mat. Žh. 10 (1969) 800–819
[6] L.A. Bokut, The problem of Malcev, Sibirsk. Mat. Zh. 10 (1969) 965–1005.
[7] L.A. Bokut, Unsolvability of the word problem, and subalgebras of finitely presented Lie algebras, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972) 1173–1219.
[8] L.A. Bokut, Imbeddings into simple associative algebras, Algebra i Logika 15 (1976) 117–142 245.
[9] L.A. Bokut, Malcev's problem and groups with a normal form, With the collaboration of D. J. Collins. Studies in Logic and Foundations of Mathematics, 95, Word problems, II (Conference on Decision Problems in Algebra, Oxford, 1976), pp. 29–53, North-Holland, Amsterdam, New York, 1980.
[10] L.A. Bokut, The centrally symmetric Novikov group, Sibirsk. Mat. Zh. 26 (2) (1985) 18–28 221.
[11] L.A. Bokut, G.P. Kukin, Algorithmic and combinatorial algebra. Mathematics and its Applications, vol. 255, Kluwer Academic Publishers, Dordrecht, 1994 pp. xvi+384.
[12] L.A. Bokut, P.S. Kolesnikov. Grobner-Shirshov bases: from their incipiency to the present. (Russian) Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 272 (2000), Vopr. Teor. Predst. Algebr i Grupp. 7, 26–67, 345; translation in J. Math. Sci. (NY) 116 (1) (2003) 2894–2916.
[13] L.A. Bokut, L.-S. Shiao, Gröbner–Shirshov bases for Novikov and Boon groups, Algebr. Anal., to appear.
[14] L.A. Bokut, K.P. Shum, Relative Gröbner–Shirshov bases for algebras and groups.
[15] W.W. Boone, The word problem, Ann. Math. 70 (1959) 207–265.
[16] B. Buchberger, An algorithm for finding a bases for the residue class ring of a zero-dimensional polynomial ideal, (German). Ph. D. Thesis, University of Insbruck, Austria, 1965.
[17] B. Buchberger, An algorithmical criteria for the solvability of algebraic systems of equations (German), Aequationes Math. 4 (1970) 374–383.
[18] B. Buchberger, A theoretical bases for the reduction of polynomials to canonical forms, ACM SIGSAM Bull. 10 (1976) 19–29.
[19] H. Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II, Ann. of Math. 79 (1964) 109–203 205–326.
[20] P. S. Novikov, On algorithmic unsolvability of the word problem in the theory of groups, in: Proceedings of the Steklov Mathematical Institute, vol. 44, 1955; Translation: Novikov, P. S. On the algorithmic insolvability of the word problem in group theory. AMS Translations, Ser 2, vol. 9, pp. 1–122. AMS, Providence, RI, 1958.

[21] M.G. Rabin, Recursive unsolvability of group theoretic problems, Ann. of Math. 67 (1) (1958) 172–194.
[22] A.I. Shirshov, On free Lie rings, (Russian) Mat. Sb. N.S. 45 (87) (1958) 113–122.
[23] A.I. Shirshov, Some algorithm problems for Lie algebras, (Russian) Sibirsk. Mat. Zh. 3 (1962) 292–296 (Translated in ACM SIGSAM Bull. 33(2) (1999) 3–9).
[24] J. Stallings, A graph-theoretic lemma and group-embeddings, Combinatorial group theory and topology (Alta, Utah, 1984), Annals of Mathematical Studies, vol. 111, Princeton University Press, Princeton, NJ, 1987 pp. 145–155.
[25] A.M. Turing, The word problem in semi-groups with cancellation, Ann. of Math. 52 (1950) 491–505.