Быстрый алгоритм вычисления коммутаторной длины в свободной группе

Данил Фиалковский (Санкт-Петербург, Россия)

Введение

Пусть $F = F(x_1, \ldots, x_N)$ — свободная группа. Коммутатором элементов $w_1, w_2 \in F$, называется элемент

$$[w_1, w_2] = w_1^{-1} w_2^{-1} w_1 w_2 \in F. \tag{0.1}$$

Так как в записи (0.1) может произойти много сокращений, вопрос о том, является ли данный элемент коммутатором, представляется неочевидным. Первым достижением в этом вопросе была теорема Викса [3].

Теорема (Wicks)**.** *Пусть W — циклически приведенное слово. Тогда W представляет некоторый коммутатор в F тогда и только тогда, когда существует такая циклическая перестановка W' слова W, что она представляется в виде произведения без сокращений*

$$W' = W_1^{-1} W_2^{-1} W_3^{-1} W_1 W_2 W_3.$$

В частности, эта теорема даёт алгоритм по проверке того, является ли элемент свободной группы коммутатором.

Множество элементов, которые можно записать в виде произведения коммутаторов образует нормальную подгруппу в F, обозначается через $[F, F]$ и называется коммутантом F. Минимальное количество коммутаторов, необходимое для того, чтобы представить элемент $w \in [F, F]$ называется **коммутаторной длиной** w и обозначается через $\mathsf{cl}(w)$. Первый неочевидный пример даёт куб коммутатора двух букв $[x, y]^3$. Очевидно, что его коммутаторная длина не больше трёх, но совершенно неочевидным фактом является то, что она равна двум:

$$[x, y]^3 = [x^{-1} yx, x^{-2} yxy^{-1}][yxy^{-1}, y^2].$$

Более того в [2] доказано, что для произвольного $n \geq 1$

$$\mathrm{cl}([x, y]^n) = \lfloor \frac{n}{2} + 1 \rfloor,$$

где $\lfloor - \rfloor$ — целая часть числа. Существует несколько подходов к вычислению коммутаторной длины [1],[2], но самым явным, и программируемым является подход Бардакова [4], которому посвящен отдельный параграф этой работы.

На основе работы Бардакова мы доказали теорему, которая даёт новый алгоритм для вычисления коммутаторной длины. Заметим, что если слово w можно представить в виде произведения

$$w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4,$$

где $a, b \in \{x_1^{\pm 1}, x_2^{\pm 1}, \ldots, x_N^{\pm 1}\}$, то выполнено следующее равенство

$$w = [w_1 w_3 a w_1^{-1}, w_1 w_3 b w_2^{-1} w_3^{-1} w_1^{-1}] w_1 w_3 w_2 w_4. \tag{0.2}$$

Это замечание вместе со следующей теоремой даёт алгоритм для вычисления коммутаторной длины в свободной группе.

Теорема 4.1. *Пусть $F = F(x_1, \ldots, x_n)$ — свободная группа и $w \in [F, F]$. Тогда существует представление w в виде произведения без сокращений*

$$w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$$

такое, что $a, b \in \{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$ и

$$\mathsf{cl}(w_1 w_3 w_2 w_4) = \mathsf{cl}(w) - 1.$$

Из этой теоремы также вытекает классификация коммутаторов альтернативная теореме Викса:

Следствие 4.2. *Пусть $w \in [F, F]$. Тогда w — коммутатор тогда и только тогда, когда w может быть представлено в виде произведения без сокращений*

$$w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$$

так, что

$$w_1 w_3 w_2 w_4 = 1.$$

В этом случае

$$w = [w_1 w_3 a w_1^{-1}, w_1 w_3 b w_2^{-1} w_3^{-1} w_1^{-1}].$$

Алгоритм проверки того, является ли слово коммутатором, основанный на Следствии 4.2, заключается в переборе представлений в виде произведения без сокращений $w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$, и проверки равенства $w_1 w_3 w_2 w_4 = 1$.

Алгоритм вычисления коммутаторной длины при помощи Теоремы 4.1 выглядит следующим образом. Надо перебрать все представления элемента w в виде произведения $w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$ и рассмотреть множество $C_1(w)$, которое состоит из элементов $w_1 w_3 w_2 w_4$ по всем этим представлениям. Далее нужно рассмотреть множество $C_2(w) = \bigcup_{u \in C_1(w)} C_1(u)$ и так далее $C_{i+1}(w) = \bigcup_{u \in C_i(w)} C_1(u)$, пока множество $C_l(w)$ не будет содержать элемент 1. Тогда $\mathsf{cl}(w) = l$.

Практика показывает, что эти алгоритмы гораздо быстрее, чем алгоритмы, которые дают теорема Викса и теорема Бардакова. Более того, наш алгоритм вычисления коммутаторной длины позволяет не только вычислить её, но и предъявить явно минимальное представление в виде произведения коммутаторов.

1 Основные определения и обозначения

- **Алфавитом** мы называем произвольное фиксированное N-элементное множество $\{x_1, \ldots, x_N\}$, элементы которого мы называем **буквами**. Каждой букве x_i мы сопоставляем некоторый элемент x_i^{-1} так, что все элементы $x_1, \ldots, x_N, x_1^{-1}, \ldots, x_N^{-1}$ различны. Тогда на множестве $\{x_1^{\pm 1}, \ldots, x_N^{\pm 1}\} = \{x_1, \ldots, x_N, x_1^{-1}, \ldots, x_N^{-1}\}$ определено отображение $(-)^{-1}$, которое посылает $x_i \mapsto x_i^{-1}$ и $x_i^{-1} \mapsto x_i$.

- **Словом** назовём произвольную последовательность

$$W = a_1 \dots a_n,$$

где $a_i \in \{x_1^{\pm 1}, \dots, x_N^{\pm 1}\}$. Множество всех слов, включая пустое, образует моноид относительно приписывания, который мы будем обозначать через

$$FM = FM(x_1, \dots, x_N, x_1^{-1}, \dots, x_N^{-1}).$$

- Слово W называется **приведённым**, если $a_i \neq a_{i+1}^{-1}$ для любого $1 \leq i \leq n-1$. Приведённое слово W называется **циклически приведённым**, если $a_1 \neq a_n^{-1}$.

- Слова W_1 и W_2 называются **элементарно эквивалентными**, если $W_1 = Waa^{-1}W'$ и $W_2 = WW'$ для некоторых слов W, W' и символа $a \in \{x_1^{\pm 1}, \dots, x_N^{\pm 1}\}$. Обозначим через $\sim$ наименьшее отношение эквивалентности на множестве слов, содержащее отношение элементарной эквивалентности. Тогда слова W_1 и W_2 называются **эквивалентными**, если $W_1 \sim W_2$. Класс эквивалентности слова W мы обозначаем через

$$w = [W].$$

Для каждого слова W, существует единственное приведённое слово $\mathsf{red}(W)$ эквивалентное W.

- Фактор множество $FM/\sim$ является группой относительно умножения, которое индуцировано операцией приписывания. Эта группа называется **свободной группой** на алфавите $x_1, \dots, x_N$ и обозначается через $F = F(x_1, \dots, x_N)$.

- Для каждого элемента $w \in F$ существует единственное приведённое слово W такое, что $w = [W]$. Мы будем обозначать его

$$\mathsf{red}(w) = W.$$

Замечание 1.1. Так как нам будет полезно работать не только с приведёнными словами, мы будем чётко различать слова $W \in FM$ и соответствующие элементы свободной группы $w = [W] \in F$.

- Слово W представляется в виде **произведения слов** $W_1, W_2, \dots, W_k$ **без сокращений**, если W_i — непустые слова,

$$W = W_1 W_2 \dots W_k$$

и последняя буква W_i не совпадает с обратной к первой букве W_{i+1} для всех i.

- Элемент $w \in F$ представляется в виде **произведения элементов** $w_1, w_2, \dots, w_k \in F$ **без сокращений**, если слово $\mathsf{red}(w)$, представляется в виде произведения без сокращений слов $\mathsf{red}(w_1), \dots, \mathsf{red}(w_k)$.

- Если $n \in \mathbb{N}$, мы полагаем $\underline{n} = \{1, \dots, n\}$.

- Если X — конечное множество, количество элементов X обозначается через $\#X$.

- Если X — конечное множество, то биекция $\sigma : X \to X$ называется перестановкой на X. Группа всех перестановок на X обозначается через $S(X)$. Тогда $S_n = S(\underline{n})$. Перестановки записываются в циклической записи .

- **Орбитой** элемента $x \in X$ относительно перестановки $\sigma \in S(X)$ мы называем множество $\{\sigma^i(x) \in i \in \mathbb{Z}\}$. **Множество орбит** всех элементов X относительно перестановки σ обозначим через $\mathcal{O}(\sigma)$. **Количество орбит** всех элементов X относительно перестановки σ оозначим через $o(\sigma)$.

- Перестановка $\pi \in S_n$ называется **инволюцией**, если $\pi^2 = 1$.

- Для инволюции $\pi \in S_n$ мы через σ_π мы обозначаем следующую перестановку из S_n :
$$\sigma_\pi = (1, 2, \ldots, n)\pi.$$

- Количество орбит перестановки σ_π мы обозначаем через
$$v(\pi) = o(\sigma_\pi).$$

2 Теорема Бардакова

В этом пункте мы опишем алгоритм Бардакова для вычисления коммутаторной длины в свободной группе [4].

Пусть
$$W = a_1 \ldots a_n \in F$$
— (необзательно приведенное) слово, которое представляет элемент из коммутанта, где $a_i \in \{x_1^{\pm 1}, \ldots, x_N^{\pm 1}\}$. **Спариванием** на слове W назовём инволюцию $\pi \in S_n$ такую, что
$$a_{\pi(i)} = a_i^{-1}.$$

Множество спариваний на слове W обозначим через $P(W)$. Так как W представляет элемент из коммутанта, количество вхождений каждой буквы в W в первой степени равно количеству вхождений в минус первой степени, и следовательно, множество $P(W)$ не пусто. Для каждого $\pi \in P(W)$ обозначим через $v(\pi)$ количество орбит перестановки $\sigma_\pi = (1, \ldots, n)\pi$, где $(1, \ldots, n) \in S_n$ — это длинный цикл. Спаривание назовём **минимальным**, если $v(\pi)$ максимально среди всех $\pi \in P(w)$.

Теорема 2.1 (Бардаков)**.** *Пусть слово W представляет элемент $w \in [F, F]$ и π — минимальное спаривание на слове W. Тогда*
$$\mathsf{cl}(w) = \frac{1 - v(\pi)}{2} + \frac{n}{4}.$$

Замечание 2.2. В статье Бардакова предполагается, что W — циклически приведенное слово, но в доказательстве это не используется. Это предположение сделано потому, что в вопросах, связанный с коммутаторной длиной, от произвольного слова W всегда можно перейти к соответствующему циклически редуцированному слову, но нам будет удобно пользоваться этой теоремой в полной общности.

3 Леммы о перестановках

Пусть X, Y — конечные множества и $\alpha : X \to Y$ — инъективное отображение. Рассмотрим отображение

$$\alpha^* : S(Y) \longrightarrow S(X),$$

которое задаётся следующим образом. Для $\sigma \in S(Y)$ и $x \in X$ обозначим через $m = m(x, \sigma) \geq 1$ наименьшее число такое, что $\sigma^m(\alpha(x)) \in \alpha(X)$. Тогда

$$\alpha^*(\sigma)(x) = \alpha^{-1}(\sigma^m(\alpha(x))).$$

Легко видеть, что $\alpha^*(\sigma)$ — корректно определённая перестановка. Так как α инъективно, отождествив X и $\alpha(X)$, мы всегда можем считать, что $X \subseteq Y$ и α — тождественное вложение. Тогда $m = m(x, \sigma)$ — это наименьшее число такое, что $\sigma^m(x) \in X$.

Лемма 3.1. *Пусть $\sigma \in S(X)$ и $A \in \mathcal{O}(\sigma)$. Тогда или $\alpha^{-1}(A) = \emptyset$, или $\alpha^{-1}(A) \in \mathcal{O}(\alpha^*(\sigma))$.*

Доказательство. Не уменьшая общности, будем считать, что $X \subseteq Y$ и α — тождественное вложение. Тогда нужно доказать, что или $A \cap X = \emptyset$, или $A \cap X \in \mathcal{O}(\alpha^*(\sigma))$. Пусть $A \cap X \neq \emptyset$. Рассмотрим $x \in A \cap X$. Тогда $A = \{\sigma^i(x) \mid i \geq 1\}$. Рассмотрим возрастающую последовательность всех тех чисел $1 \leq m_1 < m_2 < m_3 < \dots$ для которых $\sigma^{m_i}(x) \in X$. Тогда, с одной стороны, $A \cap X = \{\sigma^{m_i}(x) \mid i \geq 1\}$, с другой стороны $\sigma^{m_i}(x) = \alpha^*(\sigma)^i(x)$. Отсюда получаем, что $A \cap X = \{\alpha^*(\sigma)^i(x) \mid i \geq 1\}$ — орбита элемента x относительно перестановки $\alpha^*(\sigma)$. □

Следствие 3.2. *Пусть $\sigma \in S(X)$ такая, что $A \cap \alpha(X) \neq \emptyset$ для любого $A \in O(\sigma)$. Тогда для любого $A \in \mathcal{O}(\sigma)$ имеем $\alpha^{-1}(A) \in \mathcal{O}(\alpha^*(\sigma))$ и соответствующее отображение*

$$\alpha^{-1} : \mathcal{O}(\sigma) \longrightarrow \mathcal{O}(\alpha^*(\sigma))$$

является биекцией. В частности, $o(\sigma) = o(\alpha^*(\sigma))$.

Доказательство. Не уменьшая общности, будем считать, что $X \subseteq Y$ и α — тождественное вложение. Отображение $\alpha^{-1} : \mathcal{O}(\sigma) \longrightarrow \mathcal{O}(\alpha^*(\sigma))$ инъективно, так как любая орбита A относительно σ определяется однозначно любым своим элементом, и в частности, любым элементом из непустого множества $A \cap X$. Орбиты относительно σ покрывают Y, и следовательно, пересечения $A \cap X$ покрывают X, где $A \in \mathcal{O}(\sigma)$. Из этого следует, что множество пересечений $\{A \cap X \mid A \in \mathcal{O}(\sigma)\}$ совпадает с множеством орбит $\mathcal{O}(\alpha^*(\sigma))$, и следовательно, отображениие $\alpha^{-1} : \mathcal{O}(\sigma) \longrightarrow \mathcal{O}(\alpha^*(\sigma))$ сюръективно. □

Рассмотрим n и $1 \leq i < j < j+1 < k \leq n$. Далее будем обозначать через

$$\alpha : \underline{n-4} \longrightarrow \underline{n}$$

единственное инъективное монотонное отображение, образ которого не содержит $i, j, j+1, k$. Тогда α задаётся по формуле:

$$\alpha(x) = \begin{cases} x, & \text{если } x < i \\ x+1, & \text{если } i \leq x < j-1 \\ x+3, & \text{если } j-1 \leq x < k-3 \\ x+4, & \text{если } k-3 \leq x \leq n-4. \end{cases} \tag{3.1}$$

Далее рассмотрим перестановку $\tau \in S_{n-4}$, которая задаётся по формуле:

$$\tau(x) = \begin{cases} x, & \text{если } x < i \\ x+k-j-2, & \text{если } i \le x < j-1 \\ x+i-j+1, & \text{если } j-1 \le x < k-3 \\ x, & \text{если } k-3 \le x \le n-4. \end{cases}$$

Лемма 3.3. *Пусть $n \ge 5$ и $\pi \in S_n$ — инволюция такая, что $\pi(i) = j+1$ и $\pi(j) = k$, и пусть $\pi' \in S_{n-4}$ — единственная инволюция такая, что $\alpha\pi' = \pi\alpha$. Тогда*

$$\alpha^*(\sigma_\pi) = \tau^{-1}(1, \dots, n-4)\tau\pi'.$$

Доказательство. Если $n = 4$, то это утверждение тривиально. Поэтому будем считать, что $n \ge 5$. Пусть $\sigma := \sigma_\pi$. Множество $\underline{n}$ мы отождествляем с циклической группой $\mathbb{Z}/n$, и аналогичо, множество $\underline{n-4}$ с циклической группой $\mathbb{Z}/(n-4)$. В том смысле, что элементы из $\underline{n}$ мы складываем по модулю n, а элементы из $\underline{n-4}$ по модулю $n-4$. Таким образом, для $y \in \underline{n}$ имеет место равенство $y+1 = (1, \dots, n)(y)$ и для $x \in \underline{n-4}$ имеет место $x+1 = (1, \dots, n-4)(x)$. Тогда $\sigma(y) = \pi(y) + 1$ для любого $y \in \underline{n}$. В этих обозначенных необходимо доказать, что для любого $x \in \underline{n-4}$ выполняется

$$\alpha^*(\sigma)(x) = \tau^{-1}(\tau\pi'(x) + 1). \tag{3.2}$$

Легко проверить, что если $y \in \underline{n}$, то

$$y, y+1 \notin \{i, j, j+1, k\} \quad \Rightarrow \quad \alpha^{-1}(y+1) = \alpha^{-1}(y) + 1. \tag{3.3}$$

Кроме того, для $x \in \underline{n-4}$ выполняется

$$x \notin \{i-1, j-2, k-4\} \quad \Leftrightarrow \quad \tau(x+1) = \tau(x)+1 \quad \Leftrightarrow \quad \tau^{-1}(\tau(x)+1) = x+1. \tag{3.4}$$

Докажем равенство (3.2) для произвольного $x \in \underline{n-4}$. Рассмотрим случаи.

Случай 1. Пусть $\pi'(x) \notin \{i-1, j-2, k-4\}$. Легко видеть, что это эквивалентно тому, что $\pi\alpha(x) + 1 \notin \{i, j, j+1, k\}$. Так как $\pi\alpha(x)$ всегда не лежит в $\{i, j, j+1, k\}$ и $\sigma\alpha(x) = \pi\alpha(x) + 1$ лежит в образе α, используя (3.3) и (3.4), получаем

$$\alpha^*(\sigma)(x) = \alpha^{-1}(\sigma\alpha(x)) = \alpha^{-1}(\pi\alpha(x)+1) = \alpha^{-1}(\pi\alpha(x)) + 1 = \pi'(x) + 1 = \tau^{-1}(\tau\pi'(x) + 1).$$

Случай 2. Пусть $\pi'(x) \in \{i-1, j-2, k-4\}$ и $|\{i-1, j-2, k-4\}| = 3$. То есть $i \ne j-1$, $j+2 \ne k$ и $i-1 \ne k-4 \pmod{n-4}$. В частности, $(i,k) \ne (1,n)$.

Случай 2.1. Пусть $\pi'(x) = i-1$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(i-1)+1 = i$ не лежит в образе α. Тогда $\sigma^2\alpha(x) = \sigma(i) = \pi(i)+1 = j+2 < k$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^2\alpha(x) = \alpha^{-1}(j+2) = j-1 = \tau^{-1}(i) = \tau^{-1}(\tau(i-1)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 2.2. Пусть $\pi'(x) = j-2$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(j-2)+1 = j$ не лежит в образе α. Тогда $\sigma^2\alpha(x) = \sigma(j) = k+1 \ne i$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^2\alpha(x) = k-3 = \tau^{-1}(k-3) = \tau^{-1}(\tau(j-1)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 2.3. Пусть $\pi'(x) = k-4$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(k-4)+1 = k$ не лежит в образе α. Тогда $\sigma^2\alpha(x) = \sigma(k) = j+1$ не лежит в образе α, но $\sigma^3\alpha(x) = \sigma(j+1) = i+1 < j$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^3\alpha(x) = i = \tau^{-1}(i+k-j-2) = \tau^{-1}(\tau(k-4)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 3. Пусть $\pi'(x) \in \{i-1, j-2, k-4\}$ и $i-1 = j-2$, но $i-1 \neq k-4 \neq j-2$. В таком случае, $\pi'(x) \in \{i-1, k-4\}$ и $(i,k) \neq (1,n), j+2 < k, i+1 = j$. Кроме того, $\tau = 1$.

Случай 3.1. Пусть $\pi'(x) = i-1 = j-2$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(i-1)+1 = i$ не лежит в образе α, но $\sigma^2\alpha(x) = \sigma(i) = j+2 < k$ в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^2\alpha(x) = \alpha^{-1}(j+2) = j-1 = \tau^{-1}(i) = \tau^{-1}(\tau(i-1)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 3.2. Пусть $\pi'(x) = k-4$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(k-4)+1 = k$ не лежит в образе α, и $\sigma^2\alpha(x) = \sigma(k) = j+1$ не лежит в образе α, и $\sigma^3\alpha(x) = \sigma(j+1) = i+1 = j$ не лежит в образе α. Но $\sigma^4\alpha(x) = \sigma(j) = k+1 \neq i$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^4\alpha(x) = \alpha^{-1}(k+1) = k-3 = \tau^{-1}(k-3) = \tau^{-1}(\tau(k-4)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 4. Пусть $\pi'(x) \in \{i-1, j-2, k-4\}$ и $j-2 = k-4$, но $j-2 \neq i-1 \neq k-4$. В таком случае, $\pi'(x) \in \{i-1, j-2\}$ и $(i,k) \neq (1,n), i+1 < j, j+2 = k$. Кроме того, $\tau = 1$.

Случай 4.1. Пусть $\pi'(x) = i-1$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(i-1)+1 = i$ не лежит в образе α, и $\sigma^2\alpha(x) = \sigma(i) = j+2 = k$ не лежит в образе α, и $\sigma^3\alpha(x) = \sigma(k) = j+1$ не лежит в образе α. Но $\sigma^4\alpha(x) = \sigma(j+1) = i+1 < j$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^4\alpha(x) = \alpha^{-1}(i+1) = i = \tau^{-1}(i) = \tau^{-1}(\tau(i-1)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 4.2. Пусть $\pi'(x) = j-2 = k-4$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(j-2)+1 = j$ не лежит в образе α, но $\sigma^2\alpha(x) = \sigma(j) = k+1$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^2\alpha(x) = \alpha^{-1}(k+1) = k-3 = \tau^{-1}(k-3) = \tau^{-1}(\tau(k-4)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 5. Пусть $\pi'(x) \in \{i-1, j-2, k-4\}$ и $i-1 = k-4$, но $i-1 \neq j-2 \neq k-4$. В таком случае, $\pi'(x) \in \{n-4, j-2\}$ и $(i,k) = (1,n), i+1 < j, j+2 < k$.

Случай 5.1. Пусть $\pi'(x) = n-4$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(n-4)+1 = n = k$ не лежит в образе α, и $\sigma^2\alpha(x) = \sigma(k) = j+1$ не лежит в образе α, но $\sigma^3\alpha(x) = \sigma(j+1) = 2$ не лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^3\alpha(x) = \alpha^{-1}(2) = 1 = \tau^{-1}(n-j-1) = \tau^{-1}(\tau(n-4)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 5.2. Пусть $\pi'(x) = j-2$. Тогда $\sigma\alpha(x) = \pi\alpha(x)+1 = \alpha(j-2)+1 = j$ не лежит в образе α, и $\sigma^2\alpha(x) = \sigma(j) = 1$ не лежит в образе α. Но $\sigma^3\alpha(x) = \sigma(1) = j+2$ лежит в образе α. Следовательно,

$$\alpha^*(\sigma)(x) = \alpha^{-1}\sigma^2\alpha(x) = \alpha^{-1}(j+2) = j-1 = \tau^{-1}(1) = \tau^{-1}(\tau(j-2)+1) = \tau^{-1}(\tau\pi'(x)+1).$$

Случай 6. Пусть $i-1 = j-2 = k-4$. Тогда $i = 1, j = 2, j+1 = 3, k = 4$, и следовательно, $n = 4$. Но это противоречит условию.

□

Рассмотрим пример, в котором работает Лемма 3.3.

Пример 3.4. Пусть $n = 14, i = 3, j = 6, k = 12$, и пусть

$$\pi = (1,9)(2,4)(3,7)(5,13)(6,12)(8,11)(10,14).$$

Тогда $\sigma_\pi = (1,2,3,4,5,6,7,8,9,10,11,12,13,14)(1,9)(2,4)(3,7)(5,13)(6,12)(8,11)(10,14)$. Вычисляя, получаем

$$\sigma_\pi = (1,10)(2,5,14,11,9)(3,8,12,7,4)(6,13).$$

Отображение $\alpha : \underline{10} \to \underline{14}$ действует следующим образом: $\alpha(1) = 1,\ \alpha(2) = 2,\ \alpha(3) = 4,\ \alpha(4) = 5,\ \alpha(5) = 8,\ \alpha(6) = 9,\ \alpha(7) = 10,\ \alpha(8) = 11,\ \alpha(9) = 13,\ \alpha(10) = 14$. Тогда $\alpha^*(\sigma_\pi)$ получается выкидыванием $3, 6, 7, 12$ из циклов, и замены того, что осталось на их прообразы относительно α. Следовательно,

$$\alpha^*(\sigma_\pi) = (1,7)(2,4,10,8,6)(5,3)(9).$$

Вычислим π' :

$$\pi' = (1,6)(2,3)(4,9)(5,8)(7,10).$$

Вычислим τ :

$$\tau = (1)(2)(3,7,5)(4,8,6)(9)(10).$$

Тогда получаем

$$\tau(1,2,3,4,5,6,7,8,9,10)\tau^{-1} = (1,2,5,6,7,8,3,4,9,10)$$

Следовательно,

$$\tau(1,\dots,10)\tau^{-1}\pi' = (1,7)(2,4,10,8,6)(3,5)(9) = \alpha^*(\sigma_\pi).$$

Лемма 3.5. *Пусть n, $i,j,k \in \underline{n}$ и $\pi \in S_n, \pi' \in S_{n-4}$ как в предыдущей лемме. И пусть $\tilde{\pi} = \tau^{-1}\pi'\tau$. Тогда*

$$v(\pi) = v(\tilde{\pi}).$$

Доказательство. Необходимо доказать, что $o(\sigma_\pi) = o(\sigma_{\tilde{\pi}})$. Так как перестановки $\alpha^*(\sigma) = \tau^{-1}(1,\dots,n-4)\tau\pi'$ и $\sigma_{\tilde{\pi}} = (1,\dots,n-4)\tau\pi'\tau^{-1}$ сопряжены, то достаточно доказать, что $o(\sigma_\pi) = o(\alpha^*(\sigma_\pi))$. Ввиду Следствия 3.2, достаточно доказать, что все орбиты относительно перестановки σ_π пересекаются с образом α. Другими словами, нужно показать, что обиты каждого из элементов множества $\{i,j,j+1,k\}$ не лежат в этом множестве.

Докажем, что орбита i относительно σ_π всегда выходит из множества $\{i,j,j+1,k\}$. $\sigma_\pi(i) = j{+}2$. Таким образом, если $j{+}2 < k$, то всё доказано. Пусть теперь $j{+}2 = k$. Тогда $\sigma_\pi^2(i) = j{+}1$, и следовательно, $\sigma_\pi^3(i) = i{+}1$. Тогда если $j{+}2 = k$ и $i{+}1 < j$, то всё доказано. Пусть теперь $j{+}2 = k$ и $i{+}1 = j$. Тогда $\{i,j,j{+}1,k\} = \{i,i{+}1,i{+}2,i{+}3\}$. Следовательно, $\sigma_\pi^4(i) = k+1 = i+4$. Так как $n \geq 5$, получаем, что $i+4 \neq i$, и следовательно, орбита i не включается в множестве $\{i,j,j+1,k\}$.

Докажем, что орбита j относительно σ_π не включается в множество $\{i,j,j+1,k\}$. $\sigma_\pi(j) = k{+}1$. Таким образом, если $(i,k) \neq (1,n)$, то орбита j не включается в $\{i,j,j{+}1,k\}$. Пусть теперь $i = 1, k = n$. Тогда $\sigma_\pi(j) = i$, следовательно, орбиты i и j совпадают и, как доказано выше, не лежат в множестве $\{i,j,j+1,k\}$.

Докажем, что орбита $j+1$ не включается в $\{i,j,j+1,k\}$. $\sigma_\pi(j+1) = i+1$. Тогда, если $i+1 < j$, то всё доказано. Пусть $i+1 = j$. Тогда $\sigma_\pi^2(j+1) = j$, и тогда всё следует из предыдущего пункта.

Так как $\sigma_\pi(k) = j{+}1$, орбита k равна орбите $j{+}1$, и следовательно, она не включается в $\{i,j,j+1,k\}$. □

4 Основная теорема

Заметим, что есть элемент свободной группы $w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$, то выполняется соотношение

$$w = [w_1 w_3 a w_1^{-1}, w_1 w_3 b w_2^{-1} w_3^{-1} w_1^{-1}] w_1 w_3 w_2 w_4. \tag{4.1}$$

Оно является ключевым соотношением для поиска представления элемента из коммутанта $[F, F]$ в виде произведения минимального числа коммутаторов.

Теорема 4.1. *Пусть $F = F(x_1, \dots, x_n)$ — свободная группа и $w \in [F, F]$. Тогда существует представление w в виде произведения без сокращений*

$$w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$$

такое, что $a, b \in \{x_1^{\pm 1}, \dots, x_n^{\pm 1}\}$ и

$$\mathsf{cl}(w_1 w_3 w_2 w_4) = \mathsf{cl}(w) - 1.$$

Доказательство. Пусть w представляется приведенным словом $W = a_1 \dots a_n$, где $a_i \in \{x_1^{\pm 1}, \dots, x_N^{\pm 1}\}$, и $\pi \in S_n$ — минимальное спаривание на W. Рассмотрим максимальное число $j \in \{1, \dots, n\}$ такое, что $\pi(j) > j$. Обозначим $i = \pi(j+1)$, $k = \pi(j)$. Так как слово W приведенное, $k \neq j+1$, и следовательно, $k > j+1$. Так как j — максимальное число со свойством $\pi(j) > j$, получаем $i < j+1$. Но $i \neq j$, поэтому $1 \leq i < j < j+1 < k \leq n$. Обозначим $a := a_i^{-1} = a_{j+1}$ и $b := a_j^{-1} = a_k$. Следовательно, слово W представляется в виде проиведения без сокращений

$$W = W_1 a^{-1} W_2 b^{-1} a W_3 b W_4,$$

где $W_1 = a_1 \dots a_{i-1}$, $W_2 = a_{i+1} \dots a_{j-1}$, $W_3 = a_{j+2} \dots a_{k-1}$, $W_4 = a_{k+1} \dots a_n$. Пусть $\tilde{W} = W_1 W_3 W_2 W_4$ и $\tilde{w}$ — соответствующий элемент в свободной группе. Обозначим $l = \mathsf{cl}(w)$ и $\tilde{l} = \mathsf{cl}(\tilde{w})$. Тогда осталось доказать, что $\tilde{l} = l - 1$. В силу (4.1) мы получаем, что $\tilde{l} \geq l - 1$. Поэтому достаточно доказать $\tilde{l} \leq l - 1$. Пусть $\alpha : \underline{n-4} \to \underline{n}$ единственное монотонное инъективное отображение, в образе которого не содержатся $\{i, j, j+1, k\}$, которое задаётся по формуле (3.1). Тогда обозначим через $\tilde{\pi} \in S_{n-4}$ перестановку как в Лемме 3.5. Из того, что $\pi \in P(W)$, следует, что $\tilde{\pi} \in P(\tilde{W})$. По Лемме 3.5 получаем, что $v(\tilde{\pi}) = v(\pi)$. Следовательно,

$$\tilde{l} \leq \frac{1 - v(\tilde{\pi})}{2} + \frac{n-4}{4} = \frac{1 - v(\pi)}{2} + \frac{n}{4} - 1 = l - 1.$$

□

Следствие 4.2. *Пусть $w \in [F, F]$. Тогда w — коммутатор тогда и только тогда, когда w может быть представлено в виде произведения без сокращений*

$$w = w_1 a^{-1} w_2 b^{-1} a w_3 b w_4$$

так, что

$$w_1 w_3 w_2 w_4 = 1.$$

Список литературы

[1] L. Comerford, C. Edmunds, Products of commutators and products of squares in a free group, Int.J. of Algebra and Comput., v.4(3), 469–480, 1994

[2] M. Culler, Using surfaces to solve equations in free groups, Topology, v.20(2), 1981

[3] M. J. Wicks, Commutators in free products, J. London Math. Soc. 37 (1962), 433-444

[4] В. Г. Бардаков, Вычисление коммутаторной длины в свободных группах, Алгебра и логика, 39:4 (2000), 395–440