

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 17 Выпуск 3

УДК 519.40

ТЕОРЕМА О ПЛОЩАДИ ДИСКОВОЙ ДИАГРАММЫ
НАД $C(3)$ - $T(6)$ -ГРУППОЙ

Н. В. Безверхний (г. Тула)

Аннотация

Геометрические методы широко используются в комбинаторной теории групп. Теория групп с малыми сокращениями эффективно использует метод групповых диаграмм. Это позволяет решать, в частности, различные алгоритмические проблемы. Одной из таких проблем является проблема степенной сопряжённости. Будучи решённой в классе групп с условиями малого сокращения $C(6)$ - $T(3)$, она остаётся открытой в близком классе $C(3)$ - $T(6)$ -групп.

В данной статье исследуется структура односвязных диаграмм над $C(3)$ - $T(6)$ -группами и указывается, как это исследование может быть использовано при решении проблемы степенной сопряжённости.

Основным результатом данной статьи является доказательство теоремы о нижней оценке площади дисковой диаграммы на группой с условиями $C(3)$ - $T(6)$. Известно, что для групп с условиями $C(p)$ - $T(q)$ при $(p, q) \in \{(3, 6), (4, 4), (6, 3)\}$, являющихся автоматными, изопериметрическое неравенство является квадратичным. То же самое утверждается в известной в теории групп с малыми сокращениями теореме о площади. Оба утверждения ограничивают сверху площадь односвязной приведённой диаграммы в рассматриваемом классе групп квадратичной функцией длины границы.

В данной статье доказано, что нижняя граница для площади диаграммы указанного типа тоже является квадратичной функцией длины границы. Важность этого результата видна с точки зрения оценки сложности алгоритма, решающего проблему равенства слов. Он оказывается не менее, чем квадратичной сложности от длины сравниваемых слов.

Ключевые слова: карта, диаграмма, дуальная карта, дэновская область, полоса, кольцевая диаграмма, условия малого сокращения, определяющее соотношение, образующие.

Библиография: 15 названий.

THE AREA THEOREM FOR THE DISC DIAGRAM
OVER $C(3)$ - $T(6)$ -GROUP

N. V. Bezverkhniy (Tula)

Abstract

Geometric methods are widely used in combinatorial group theory. The theory of small cancellation groups use the diagram method. In particular, it allows to approach various algorithmic problems. One of them is the power conjugacy problem. It is already solved for groups with a presentation satisfying the small cancellation conditions $C(3)$ and $T(6)$. However, it remains open for a similar class of groups, having a presentation satisfying the small cancellation conditions $C(3)$ and $T(3)$.

In this paper we investigate the structure of connected diagrams over presentations satisfying the small cancellation conditions $C(3)$ and $T(3)$ and we indicate how our results may be possible used in the power conjugacy problem.

The main result of this article is the proof of the theorem about lower bound on square of the reduced diagram on the group with small cancellation conditions $C(3)$ - $T(6)$. It is known that for groups with conditions $C(p)$ - $T(q)$ with $(p, q) \in \{(3, 6), (4, 4), (6, 3)\}$, being automatic, isoperimetric inequality is quadratic. The same stated in well-known in small cancellation theory theorem of the square. Both statements restrict the area of the simply connected diagrams in the considered class of groups by the quadratic function of the length of the boundary.

In this article it is proved that the lower bound for the area of the diagram of the specified type also is a quadratic function of the length of the border. The importance of this result is visible from the point of view of evaluation of complexity of the algorithm solves the word problem. It is not less than quadratic complexity of the length of the compared words.

Keywords: map, diagram, dual map, dehn region, band, ring diagram, small cancellation condition, defining relation, generators.

Bibliography: 15 titles.

1. Введение

Известная теорема о площади [1] ограничивает сверху число областей приведённой диаграммы M над $C(p)$ - $T(q)$ группой квадратичной функцией длины границы:

$$|M| \leq \frac{q}{p^2} \left(\sum_M^* [q - i(D)] \right)^2, (p, q) \in \{(3, 6), (4, 4), (6, 3)\}.$$

В этой статье доказывается, что площадь любой приведённой дисковой диаграммы M над $C(3)$ - $T(6)$ -группой с границей $\partial M = \sigma \cup \tau$ и $R, \bar{R}$ -несократимыми метками $\varphi(\sigma), \varphi(\tau)$ является квадратичной функцией длины границы ∂M .

Свойство квадратичности изопериметрического неравенства для автоматных групп, которыми являются и $C(3)$ - $T(6)$ -группы, усиливается, и неравенство становится квадратичным уравнением.

Таким образом, диаграммы указанного типа не могут быть "тонкими" и должны иметь структуру вложенных матрёшек. Поясним это примером.

Рассмотрим на плоскости E^2 прямоугольник M_1 из n клеток размера 1×1 с вершинами $A_1(0, 0), B_1(0, 1), C_1(n, 1), D_1(n, 0)$. Он содержится в прямоугольнике M_2 с вершинами $A_2(-1, -1), B_2(-1, 2), C_2(n+1, 2), D_2(n+1, -1)$, который, в свою очередь, содержится в прямоугольнике M_3 с вершинами $A_3(-2, -2), B_3(-2, 3), C_3(n+2, 3), D_3(n+1, -2)$, и так далее. Прямоугольник M_m имеет вершины $A_m(-(m-1), -(m-1)), B_m(-(m-1), m), C_m(n+m-1, m), D_m(n+m-1, -(m-1))$.

Сравним площадь прямоугольника M_m с длиной его границы:

$$|M_m| = |A_mB_m||B_mC_m| = (2m-1)(2m+n-2) = 4m^2 + 2m(n-3) - n + 2;$$

$$|\partial M_m| = 2|A_mB_m| + 2|B_mC_m| = 2((2m-1) + (n+2m-2)) = 8m + 2n - 6.$$

Таким образом, площадь $|M_m|$ с ростом m растёт, как квадрат длины границы ∂M_m . Похожую структуру имеют приведённые дисковые диаграммы над $C(3)$ - $T(6)$ -группами.

Полученный результат может быть использован в исследовании разрешимости проблемы степенной сопряжённости слов в классе групп с условиями $C(3)$ - $T(6)$. Соответствующий алгоритм представляет интерес при построении односторонних функций, применяющихся в криптографии для передачи информации по открытому каналу [12, 13, 14].

2. Основные определения

Будем считать, что копредставление $G = (X; R)$ обладает следующими свойствами: $|X| < \infty, |R| < \infty$, X содержит инверсии всех своих элементов, множество R определяющих соотношений симметризовано: содержит инверсии и все циклические перестановки своих элементов.

ОПРЕДЕЛЕНИЕ 1. Обозначим через $F = F(X)$ свободную группу с базисом X . Непустое общее начало двух различных определяющих соотношений называется куском. Группа G с копредставлением $(X; R)$ удовлетворяет условию $C(p)$, если ни одно из слов множества R не представимо в виде произведения менее, чем p кусков. Группа G удовлетворяет условию $T(q)$, если для любого набора слов $r_1, \dots, r_t$ из R , $2 < t < q$, таких, что соседние элементы в последовательности $r_1, r_2, \dots, r_i, r_{i+1}, \dots, r_t, r_1$, не являются взаимно обратными в $F(X)$, по крайней мере одно из произведений $r_1 r_2, \dots, r_t r_1$ приведено в $F(X)$.

Класс групп с условиями $C(3) - T(6)$ отличается от двух названных слабостью условия $C(3)$ и спецификой условия $T(6)$. И тем не менее, работа в этом классе сильно упрощается, благодаря следующему элементарно доказываемому в статье [2] утверждению.

СВОЙСТВО КОПРЕДСТАВЛЕНИЙ С УСЛОВИЕМ $T(q)$ ПРИ $q > 4$.

Если группа G обладает копредставлением $(X; R)$ с условием $T(q)$ при $q > 4$, то длина любого куска равна единице.

ДОКАЗАТЕЛЬСТВО.

Графическое равенство слов u, v будем обозначать $u \equiv v$. Предположим, что $r_1 \equiv abr'_1$, $r_2 \equiv abr'_2$ — различные определяющие соотношения, где a, b, r'_1, r'_2 — непустые слова в алфавите X .

Рассмотрим слова из R , обратные к r_1, r_2 , и их циклические перестановки: $u_1 \equiv br'_1 a$, $u_2 \equiv a^{-1}(r'_2)^{-1}b^{-1}$, $u_3 \equiv br'_1 a$, $u_4 \equiv a^{-1}(r'_2)^{-1}b^{-1}$. Последовательность u_1, u_2, u_3, u_4, u_1 противоречит условию $T(6)$. Значит, общее начало ab двух различных определяющих соотношений из R имеет единичную длину.

□

Понятия области, карты, диаграммы, кольцевой диаграммы, граничного цикла области D (∂D) и граничного цикла связной односвязной диаграммы M (∂M), граничной метки $\varphi(p)$ пути p будем считать известными [1]. Кроме того, считаем, что граничная метка области читается по часовой стрелке, граничная метка связной односвязной диаграммы — против.

Подпуть $\partial D \cap \partial M = p$ в граничных циклах области D и диаграммы M , либо в граничных циклах двух областей, называется *последовательной частью границы* как области D , так и карты M , или двух областей, соответственно [1].

Граничной вершиной в карте M называется любая вершина, принадлежащая граничному циклу карты M . Вершины, не являющиеся граничными, называются внутренними. *Внутренним ребром* в карте будем считать общую часть граничных циклов двух областей, гомеоморфную отрезку и являющуюся последовательной частью границы обеих областей. Область D называется *граничной* в карте M , если в её граничном цикле ∂D есть граничные вершины карты M , то есть $\partial D \cap \partial M \neq \emptyset$. *Граничные ребра диаграммы M* взаимно однозначно сопоставим множеству букв в слове $\varphi(\partial M)$.

ОПРЕДЕЛЕНИЕ 2. Пара областей (D_1, D_2) с общим ребром e в диаграмме M называется *сократимой*, если граничная метка односвязной поддиаграммы $D_1 \cup D_2$ равна единице в свободной группе $F(X)$. Если в диаграмме M нет сократимых пар областей, то диаграмма M называется *приведённой*. (Можно определить сократимую пару и в случае многосвязной диаграммы $D_1 \cup D_2$ — см. [1].)

Очевидно, что в приведённой диаграмме метка внутреннего ребра всегда является куском, а в $C(3) - T(6)$ -диаграмме — буквой.

Скажем несколько слов о геометрической интерпретации условий малого сокращения $C(3)$ и $T(6)$. Рассмотрим произвольную группу $G = (X; R)$ с копредставлением, удовлетворяющим условиям $C(3) - T(6)$. Пусть M — приведённая диаграмма над группой G с данным копредставлением. Тогда условие $C(3)$ означает, что если область $D \subset M$ не имеет рёбер на границе ∂M диаграммы M , то степень области $D : d(D)$ (число рёбер в её граничном цикле ∂D) не может быть меньше 3. Число внутренних рёбер области D обозначим через $i(D)$.

Условие $T(6)$ означает, что степень $d(v)$ (число инцидентных ей рёбер) любой *внутренней* вершины v диаграммы M не может быть меньше 6.

Циклические перестановки слова w обозначаются w^* . Символом $|w|$ обозначают длину слова w .

Связную односвязную диаграмму (карту) M над группой $G = (X; R)$ будем называть *дисковой*, если её граничный цикл ∂M является простым замкнутым путём.

В этой статье нас будут интересовать дисковые карты с граничными циклами вида $\partial M = \sigma \cup \tau$, где простые пути σ, τ имеют ровно две общие вершины A и B : $\sigma \cap \tau = \{A, B\}$.

3. Понятия $R, \bar{R}$ -сокращений

ОПРЕДЕЛЕНИЕ 3. Рассмотрим диаграмму M над $C(3) - T(6)$ -группой. Область $D \subset M$ называется *дэновской*, если

- 1) $\partial D \cap \partial M$ — последовательная часть границы ∂M (то есть $\partial D \cap \partial M = p$ — подпуть в граничных циклах области D и диаграммы M [1]);
- 2) $i(D) \in \{0, 1\}$. Понятие дэновской области аналогично определяется и для карты M , в которой любая внутренняя область имеет не менее трёх рёбер и любое внутреннее ребро имеет степень не менее 6.

ОПРЕДЕЛЕНИЕ 4. Будем говорить, что в слове w есть R -сокращение, если существует элемент $r \in R$ такой, что:

1. $r \equiv r_1 r_2$,
2. $w \equiv w_1 w_2 w_3$,
3. $r_1 \equiv w_2$,
4. слово r_2 либо пусто, либо является куском,
5. слова $w_1 r_2^{-1}, r_2^{-1} w_3$ несократимы в свободной группе;
6. в случае замены слова w равным ему в группе G словом $w_1 r_2^{-1} w_3$ будем говорить, что в w выполнено R -сокращение.

7. R -сокращение в слове w , являющемся степенью некоторого слова $v : w = v^s$, называется *длинным*, если $|w_2| \geq |v|$ для w_2 из пункта 2 определения 4. Если же $|w_2| < |v|$, то R -сокращение называется *коротким*.

Если в любой циклической перестановке слова w нет R -сокращений, то слово w называется *циклически R -несократимым*.

ОПРЕДЕЛЕНИЕ 5. Полосой в диаграмме M над $C(3) - T(6)$ -группой называется поддиаграмма $\Pi = \bigcup_{i=1}^k D_i$ со свойствами:

- 1) $\partial D_i \cap \partial M = p$ — последовательная часть границы ∂M ;
- 2) $\partial \Pi \cap \partial M$ — последовательная часть границы ∂M ;
- 3) при $k = 3$ $i(D_1) = i(D_2) = i(D_3) = 2$, причём соседние области имеют общее ребро, а все три области полосы имеют общую вершину;
- при $k > 3, k = 2l + 1$ $i(D_1) = i(D_2) = i(D_{2l}) = i(D_{2l+1}) = 2, i(D_3) = i(D_5) = \dots = i(D_{2l-3}) = i(D_{2l-1}) = 3, i(D_4) = i(D_6) = i(D_{2l-4}) = i(D_{2l-2}) = 2$;
- 4) $\partial D_i \cap \partial D_{i+1}$ — ребро ($i = 1, \dots, k - 1$).

Понятие полосы аналогично определяется и для карты M .

ЗАМЕЧАНИЕ 1. Любая полоса в диаграмме M с циклически несократимой в свободной группе, циклически R -несократимой граничной меткой $\varphi(\partial M)$ является приведённой диаграммой.

Действительно, предположив, что две соседние области в полосе образуют сократимую пару, приходим к выводу о свободной сократимости слова $\varphi(\partial M)$, либо к выводу о том, что в слове $\varphi(\partial M)$ есть R -сокращение. Достаточно рассмотреть два случая: 1) сократимые области D_1, D_2 имеют внутренние степени $i(D_1) = 2, i(D_2) = 2$; 2) $i(D_1) = 2, i(D_2) = 3$.

В первом случае из сократимости пары (D_1, D_2) следует свободная сократимость слова $\varphi(\partial M)$. Во втором случае рассмотрим три соседние области в полосе: D_1, D_2, D_3 . Ясно, что $i(D_3) = i(D_1) = 2, i(D_2) = 3$. Из сократимости пары D_1, D_2 и из того, что кусок в $T(6)$ -группе имеет длину 1 следует, что в слове $\varphi(\partial M)$ есть R -сокращение: метка ребра $\partial D_2 \cap \partial D_3$ является подсловом в метке пути $\partial D_1 \cap \partial M$, и область D_3 можно наклеить по указанному ребру на границу ∂M , в результате чего будет получена область, реализующая R -сокращение в граничной метке диаграммы M .

Понятие $\bar{R}$ -сокращения можно определять в рассматриваемом классе групп аналогично тому, как это сделано для R -сокращения (см. также [3, 4] — $\bar{R}$ -сокращение для групп с условием $C(6)$ и $C(4) - T(4)$). Но из-за громоздкости такого определения в группах, удовлетворяющих условию $T(6)$, будем пользоваться другим, эквивалентным определением.

ОПРЕДЕЛЕНИЕ 6. Пусть Π — полоса в диаграмме M . Граничным словом области $D_i \subset \Pi$ называется метка пути $\partial D_i \cap \partial M$, прочитанная в соответствии с ориентацией области D_i . Граничным словом полосы Π называется метка пути $\partial \Pi \cap \partial M$, прочитанная в направлении, противоположном ориентации границы ∂M . Аналогично определяется граничное слово дэновской области.

Понятиям R -, $\bar{R}$ -сокращений дадим определения, использующие только язык диаграмм.

ОПРЕДЕЛЕНИЕ 7. Будем говорить, что в слове v есть R -сокращение, если существует связная односвязная диаграмма M над копредставлением $G = (X; R)$, в которой существует дэновская область, граничное слово которой является подсловом в v . В слове v есть $\bar{R}$ -сокращение, если существует связная односвязная диаграмма M над копредставлением $G = (X; R)$, в которой существует полоса Π , граничное слово которой является подсловом в v .

СЛЕДСТВИЕ (из определения 7.) Для любого циклически несократимого в $F(X)$ слова w , не равного единице в группе G , существует циклически $R, \bar{R}$ -несократимое слово w_0 , сопряжённое с w в G .

ДОКАЗАТЕЛЬСТВО. Действительно, из определения 7 следует, что в результате $R, \bar{R}$ -сокращения длина слова строго уменьшается. Записав произвольное слово w на окружности S и выполняя в его циклических перестановках $R, \bar{R}$ -сокращения, получим либо пустое слово, что невозможно, поскольку $w \neq 1$ в G , либо непустое слово w_0 , в циклических перестановках которого нет $R, \bar{R}$ -сокращений. $\square$

Так же просто доказывается утверждение о существовании $R, \bar{R}$ -несократимого слова, равного данному.

Понятия дэновской области, полосы были введены в работе [5] на языке групповых диаграмм. Независимо аналогичные понятия использовались в работе [1] при исследовании кусочно евклидовых комплексов. Работая с диаграммами, мы будем придерживаться терминологии, использованной в [1, 5].

4. Свойства дисковых диаграмм

ОПРЕДЕЛЕНИЕ 8. Пусть M — дисковая $(6,3)$ -карта, то есть M — односвязная карта с граничным циклом ∂M без самопересечений. Кроме того, все внутренние вершины в M имеют степень не меньше 6, а все внутренние области имеют степень не меньше 3.

ОПРЕДЕЛЕНИЕ 9. Пусть граничный цикл карты M является объединением двух путей: $\partial M = \sigma \cup \tau$, причём $\sigma \cap \tau = \{A, B\}$ — две вершины. Определим граничные слои K_σ и K_τ карты M как подкарты, состоящие из всех областей вместе с границами, имеющих вершины на σ и τ , соответственно.

В этой статье считаем, что слои K_σ, K_τ не содержат полос и дэновских областей карты M .

ОПРЕДЕЛЕНИЕ 10. Пару областей в слое K_σ (K_τ) карты M внутренней степени i , имеющих общее внутреннее ребро, будем называть i -парой. При различных i, j i -пару и j -пару будем называть разноимёнными. Область внутренней степени i будем называть i -областью.

ОПРЕДЕЛЕНИЕ 11. Область $D \subset M$ называется простой, если множество $\partial D \cap \partial M$ связно и является последовательной частью границы области D .

Связная односвязная карта M с границей $\partial M = \sigma \cup \tau$ называется простым диском, если $\sigma \cap \tau = \{A, B\}$ — две вершины, и все области в M простые.

ОПРЕДЕЛЕНИЕ 12. Связная односвязная подкарта M_1 карты M называется островом в M , если $M = M_1 \cup M_2 \cup p$, где p — простой подпуть в ∂M , возможно нулевой длины, не имеющий рёбер в граничных циклах областей карт M_1 и M_2 и имеющий по одной вершине в циклах ∂M_1 и в ∂M_2 , $|M_1| > 0, |M_2| > 0$. Будем говорить, что M_1 — остров на участке s границы карты M , если граничный цикл ∂M_1 является подпутём в s .

ОПРЕДЕЛЕНИЕ 13. Связная односвязная подкарта M_1 карты M называется полуостровом в M , если существует область $D_0 \subset M$: $M = M_0 \cup D_0 \cup M_1$, $|M_1| > 0, |M_2| > 0$, причём карта $M_1 \cup M_0$ не является связной. Будем говорить, что M_1 — полуостров на участке s границы карты M , если граничный цикл ∂M_1 является подпутём в s .

ЛЕММА 1 (5). (О полосах.) Пусть M — связная односвязная $(6,3)$ -карта, не содержащая дэновских областей, $|M| > 0$. Тогда в ней есть две полосы, не имеющие общих областей.

ЛЕММА 2 (6). (Об островах и полуостровах.) Пусть M — связная односвязная или кольцевая карта. Пусть s — подпуть в граничном цикле ∂M для односвязной карты M или в одном из граничных циклов σ, τ для кольцевой карты M с границей $\partial M = \sigma \cup \tau$. Тогда если в карте M нет полос Π и дэновских областей D , для которых $\partial \Pi \cap \partial M$ — подпуть в s , $\partial D \cap \partial M$ — подпуть в s , то в M нет островов и полуостровов на участке границы s .

ЛЕММА 3 (6). (О строении граничных слоёв дисковой карты.) Пусть M — дисковая карта типа $(6,3)$, и граничные слои K_σ, K_τ не содержат полос и дэновских областей, то верно следующее:

- 1) для каждой из вершин $\{A, B\}$ в карте M существует единственная область D_A, D_B , соответственно, такая, что $A \in \partial D_A, B \in \partial D_B$;
- 2) $i(D_A) = i(D_B) = 2$;
- 3) слои K_σ, K_τ содержат только области внутренней степени 2 и 3, причём, в каждой из подкарт $K_\sigma \setminus (D_B \cup D_A), K_\tau \setminus (D_B \cup D_A)$ областей первого типа на две больше, чем второго.
- 4) в слоях K_σ, K_τ могут встречаться только 2-пары и 3-пары и нет 2-троек, 3-троек, и т. д., причём, в каждом из слоёв число 2-пар на 1 больше, чем 3-пар, а разноимённые пары чередуются в каждом из слоёв K_σ, K_τ . То же верно и для областей: в K_σ, K_τ могут встречаться только 2- и 3-области.

ЛЕММА 4 (6). (О длине граничных слоёв дисковой карты.) Пусть в граничных слоях K_σ, K_τ дисковой $(6, 3)$ -карты M нет полос и дэновских областей. Тогда в карте M число областей с рёбрами на σ не превышает числа областей с рёбрами на τ , умноженного на 5, и наоборот.

5. Доказательство основной теоремы

ЛЕММА 5. Пусть M — приведённая дисковая диаграмма над $C(3) - T(6)$ -группой с границей $\partial M = \sigma \cup \tau$ и $R, \bar{R}$ -несократимыми метками $\varphi(\sigma), \varphi(\tau)$. Тогда диаграмма $M_1 = M \setminus K_\sigma$ тоже является дисковой.

ДОКАЗАТЕЛЬСТВО.

Предположим, что диаграмма M_1 не является дисковой. Значит, она является объединением нескольких дисков $N_1, \dots, N_s$, соединённых простыми путями $p_0, \dots, p_s$, причём концы пути p_i принадлежат границам дисков N_i, N_{i+1} , а пути p_0, p_i являются в диаграмме M_1 шипами, то есть в граничном цикле ∂M_1 они проходятся дважды в противоположных направлениях. Не исключено, что некоторые или даже все пути p_i имеют нулевую длину.

Из $R, \bar{R}$ -несократимости слов $\varphi(\sigma), \varphi(\tau)$ следует отсутствие полос и дэновских областей в слое K_σ . Значит, их нет в дисках N_i на участках границ $\partial N_i \cap \sigma$ при $i \in \{1, \dots, s\}$.

Те же рассуждения позволяют сделать вывод об отсутствии полос и дэновских областей в дисках N_i на участках границ $\partial N_i \cap \tau$ при $i \in \{1, \dots, s\}$. Значит, диски N_i удовлетворяют условию леммы 3.

Пусть граница диска N_i состоит из двух путей σ_i, τ_i . По доказанному метки этих путей $R, \bar{R}$ -несократимы. В соответствии с леммой 3 пунктом 1 в диске N_i существуют области D_A, D_B , внутренней степени 2.

Обозначим путь $\partial D_A \cap \sigma_i$ как AC . Концевая вершина C этого пути является внутренней в карте M . Значит, по условию $T(6)$ её степень $d(C)$ не меньше 6. Но в карте N_i она инцидентна лишь трём рёбрам (по лемме 3). Значит, три другие ребра, исходящие из C , определяют в слое K_σ 2-пару областей (D_1, D_2) .

Ближайшей в карте N_i к вершине C вдоль пути σ_i является не 3-пара областей, а 2-пара, что также гарантирует лемма 3. Этой 2-паре соответствует 2-пара (D_3, D_4) в слое K_σ .

Таким образом, в слое K_σ , а значит, и в карте M на участке границы σ есть полоса состоящая из всех областей слоя K_σ , расположенных между парами $(D_1, D_2), (D_3, D_4)$, включая эти пары. Этот вывод противоречит $\bar{R}$ -несократимости граничных меток исходной диаграммы M .

В этом рассуждении мы никак не использовали соседние с N_i диски. Поэтому оно применимо и к случаю, когда после удаления из M слоя K_σ остаётся один диск N_1 с одним или двумя шипами.

Лемма 5 доказана. $\square$

ЛЕММА 6. Пусть M_0 — приведённая дисковая диаграмма над $C(3) - T(6)$ -группой с границей $\partial M_0 = \sigma_0 \cup \tau_0$ и $R, \bar{R}$ -несократимыми метками $\varphi(\sigma_0), \varphi(\tau_0)$. Тогда диаграмма M_1 , полученная из M удалением граничных слоёв K_{σ_0}, K_{τ_0} , тоже является дисковой, а граничные метки $\varphi(\sigma_1), \varphi(\tau_1)$ $R, \bar{R}$ -несократимы (здесь $\sigma_1 = \partial(M \setminus K_{\sigma_0}) \cap \partial K_{\sigma_0}$, $\tau_1 = \partial(M \setminus K_{\tau_0}) \cap \partial K_{\tau_0}$).

ДОКАЗАТЕЛЬСТВО.

Несократимость граничных меток $\varphi(\sigma_1), \varphi(\tau_1)$ следует из отсутствия полос и дэновских областей в слоях K_{σ_0}, K_{τ_0} .

Остальное является следствием леммы 5.

$\square$

ТЕОРЕМА 1. *(о площади дисковой диаграммы). Пусть M — приведённая дисковая диаграмма над $C(3) - T(6)$ -группой $G = (X; R)$. Пусть граница $\partial M = \sigma_0 \cup \tau_0$ имеет $R, \bar{R}$ -несократимые метки $\varphi(\sigma_0), \varphi(\tau_0)$. Тогда площадь диаграммы M_0 является квадратичной функцией длины границы ∂M_0 .*

ДОКАЗАТЕЛЬСТВО.

Рассмотрим последовательность вложенных диаграмм: $M \supset M_1 \supset M_2 \dots \supset M_k$, полученных из дисковой диаграммы M удалением граничных слоёв:

$$M_1 = M \setminus (K_{\sigma_0} \cup K_{\tau_0}), M_2 = M_1 \setminus (K_{\sigma_1} \cup K_{\tau_1}), \dots, M_k = M_{k-1} \setminus (K_{\sigma_{k-1}} \cup K_{\tau_{k-1}}).$$

При этом последняя диаграмма в этой последовательности либо 1-слойная, либо 2-слойная, то есть на следующем шаге после удаления граничных слоёв остаётся пустое множество.

В соответствии с леммой 6 все эти диаграммы являются дисковыми, а метки $\varphi(\sigma_i), \varphi(\tau_i), i = 1, \dots, k$ $\bar{R}, R$ -несократимы.

Кроме того, из леммы 3, описывающей строение граничных слоёв дисковой диаграммы, следует, что число областей в $K_{\sigma_0} \cup K_{\tau_0}$ на 6 больше, чем в $K_{\sigma_1} \cup K_{\tau_1}$, и так далее.

Найдём площадь диаграммы M , предполагая, что в диаграмме M_{k-1} число граничных областей равно s .

$$|M| = |M_k| + s + (s + 6) + \dots + (s + (k - 1)6) = |M_k| + ks + 3k(k - 1).$$

Для завершения доказательства теоремы остаётся связать число слоёв k с длиной границы ∂M . Пусть N — число граничных областей в диаграмме M . Тогда выполняется равенство $N = s + 6(k - 1)$, и $k = 1 + (N - s)/6$. Подставляя это выражение вместо k в формулу для площади диаграммы M , получаем:

$$|M| = |M_k| + s(1 + (N - s)/6) + 3(1 + (N - s)/6)((N - s)/6).$$

Нетрудно оценить число областей, имеющих рёбра на границе ∂M через длину границы $|\varphi(\partial M)|$: $N \geq |\varphi(\partial M)|/|r_0|$, где r_0 — самое длинное определяющее соотношение в копредставлении группы $G = (X; R)$. Эта оценка вместе с предыдущей формулой для площади $|M|$ даёт нижнюю оценку площади диаграммы M , из чего следует квадратичная зависимость последней от длины границы.

□

6. Заключение

Доказанная теорема о площади дисковой диаграммы в рассматриваемом классе групп интересна тем, при рассмотрении кольцевых диаграмм сопряжённости слов в $C(3)$ - $T(6)$ -группах такие дисковые диаграммы могут быть выделены как поддиаграммы кольцевых.

В случае, когда граничные метки кольцевой диаграммы являются степенями фиксированных слов, из выделенных дисковых диаграмм удаётся склеивать односвязную диаграмму с быстро растущей площадью. Всё это может быть использовано для исследования проблемы степенной сопряжённости в данном классе групп.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Линдон Р., Шупп П., 1980, "Комбинаторная теория групп". М.: Мир.
2. Gersten S.M., Short H., 1990, "Small cancellation theory and automatic groups". *Inventiones mathematicae* 102, pp. 305–334.

3. Безверхний Н. В., 1999, "Разрешимость проблемы вхождения в циклическую подгруппу в группах с условием $C(6)$ ". *Фундаментальная и прикладная математика*, т. 5, N 1, с. 39–46.
4. Паршикова Е. В., 2001, "Проблема слабой степенной сопряжённости в группах с условием $C(4)$ - $T(4)$ ". *Алгоритмические проблемы теории групп и полугрупп*. Изд-во Тгпу им. Л. Н. Толстого, с. 179–185.
5. Безверхний В. Н., 1994, "О нормализаторах элементов в $C(p)$ - $T(q)$ -группах". *Алгоритмические проблемы теории групп и полугрупп*. Изд-во Тгпу им. Л. Н. Толстого, с. 4–58.
6. Безверхний Н. В., 2012, "Проблема сопряжённого вхождения в циклическую подгруппу в группах с условиями $C(3)$ - $T(6)$ ". *Дискретная математика*, т. 24, выпуск 4, с. 27–46.
7. Безверхний Н. В., 2010, "Нормальные формы для элементов бесконечного порядка в группах с условиями $C(3)$ - $T(6)$ ". *Известия Тульского государственного университета. Естественные науки*. Выпуск 1, с. 6–25.
8. Магнус Д., Каррас А., Солитэр Д., 1974, "Комбинаторная теория групп". Перевод с английского, М.: Наука.
9. Ольшанский А. Ю., 1989, "Геометрия определяющих соотношений в группах". М.: Наука.
10. Новиков П. С., 1955, "Об алгоритмической неразрешимости проблемы тождества слов в теории групп". *Труды Математического ин-та АН СССР*, т. 44, с. 1–444.
11. Kapovich I., may 1997, "Small cancellation groups and translation numbers". *Transactions of the American Mathematical Society*, V. 349, N 5, pp. 1851–1875.
12. Глухов М. М., 2010, "К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах". *Математические вопросы криптографии*, т. 1, № 4, с. 5–22.
13. Koo K. H., Lee S. J., Cheon J. H., Han J. W., Kang J., Park C., 2000, "New publickey cryptosystem using braide groups". *CRIPTO 2000, Lect. Notes Comput. Sci.*, v. 1880, pp. 166–183.
14. Paeng S. H., Ha K. C., Kim J. H., Chee S., Park C., 2001, "New public key cryptosystem using finite nonabelian groups". *CRIPTO 2001, Lect. Notes Comput. Sci.*, v. 2139, pp. 470–485.
15. Bogley W. A., Pride S. J., 1992, "Aspherical relative presentations". *Pros. of the Edinburg Mathematical Society*, v. 35, pp. 1–39.

REFERENCES

1. Lindon R., Schupp P., 1980, "Kombinatorial group theory". М.: Mir.
2. Gersten S. M., Short H., 1990, "Small cancellation theory and automatic groups". *Inventiones mathematicae* 102, pp. 305–334.
3. Bezverkhniy N. V., 1999, "The solvability of the membership problem into the cyclic subgroup of $C(6)$ -group". *Fundamentalnaya i prikladnaya matematika*, v. 5, N 1, pp. 39–46.
4. Parshikova E. V., 2001, "The solvability of the weak power conjugacy problem in $C(4)$ - $T(4)$ -group". *Algoritmicheskie problemi teorii grupp i polugrupp*. Publishing house of the Tula state pedagogical University, pp. 179–185.

5. Bezverkhniy V. N., 1994, "The normalizers of elements of $C(p)$ - $T(q)$ -group". *Algoritmicheskie problemi teorii grupp i polugrupp*. Publishing house of the Tula state pedagogical University, с.4–58.
6. Bezverkhniy N. V., 2012, "The solvability of the weak power conjugacy problem in $C(3)$ - $T(6)$ -group". *Diskretnaya matematika.*, v. 24, issue 4, pp. 27–46.
7. Bezverkhniy N. V., 2010, "Normal forms for the elements of infinite order in $C(3)$ - $T(6)$ -groups". *Izvestiya Tul'skogo gosudarstvennogo universiteta*, issue 1, pp. 6–25.
8. Magnus W., Karrass A., Solitar D., 1965, "Combinatorial group theory". *Springer-Verlag Berlin Heidelberg New York*.
9. Ol'shanskii, A. Yu., 1991, "Geometry of Defining Relations in Groups". *Kluwer Academic Publishers Group, Dordrecht*.
10. Novikov P. S., 1955, "On algorithmic unsolvability of the word problem in the group theory". *Trudi Matematicheskogo instituta AN SSSR*, v. 44. pp. 1–444.
11. Kapovich I., may 1997, "Small cancellation groups and translation numbers". *Transactions of the American Mathematical Society*, V. 349, N 5, pp. 1851 — 1875.
12. Gluhov M. M., 2010, "The analysis of some publickey criptosistemas using nonabelian groups". *Matematicheskie voprosi kriptografii.*, v.1, № 4, pp. 5–22.
13. Koo K. H., Lee S. J., Cheon J. H., Han J. W., Kang J., Park C., 2000, "New publickey criptosistem using braide groups". *CRIPTO 2000, Lect. Notes Comput Sci.*, v. 1880, pp. 166–183.
14. Paeng S. H., Ha K. C., Kim J. H., Chee S., Park C., 2001, "New public key criptosistem using finite nonabelian groups". *CRIPTO 2001, Lect. Notes Comput. Sci.*, v. 2139, pp. 470–485.
15. Bogley W. A., Pride S. J., 1992, "Aspherical relative presentations". *Pros. of the Edinburg Mathematical Society*, v. 35, pp. 1–39.