Сибирский математический журнал
Март—апрель, 2005. Том 46, № 2

УДК 512.543.72

УРАВНЕНИЕ $[x, y] = g$ В ЧАСТИЧНО КОММУТАТИВНЫХ ГРУППАХ

С. Л. Шестаков

Аннотация: Частично коммутативная группа — это группа, заданная при помощи образующих и определяющих соотношений, причем все соотношения имеют вид: коммутатор некоторых образующих равен единице. Рассмотрен алгоритм, позволяющий по данному элементу группы определить, является ли он коммутатором. Тем самым обобщается результат Уикса для свободных групп.

Ключевые слова: уравнения в группах, частично коммутативные группы.

Алфавит — это непустое множество Σ, его элементы называются *буквами.* Σ^{-1} — *дизъюнктная* копия алфавита Σ, состоящая из букв вида x^{-1}, где $x \in \Sigma$. Алфавит $\Sigma^{\pm 1} = \Sigma \cup \Sigma^{-1}$ называется *групповым алфавитом.* Конечная последовательность W букв из $\Sigma^{\pm 1}$ называется (групповым) *словом* над Σ, ее длина называется длиной слова и обозначается через $|W|$. Пустое слово обозначается цифрой 1, графическое (побуквенное) равенство слов — знаком $\equiv$. *Коммутатором слов* X, Y называется слово $[X, Y] \equiv X^{-1}Y^{-1}XY$.

Частично коммутативная группа — это группа, заданная копредставлением вида $\mathscr{P} = \langle \Sigma \mid \mathscr{R} \rangle$, где Σ — множество образующих, $\mathscr{R}$ — множество определяющих соотношений, причем все соотношения имеют вид $[x_i, x_j] = 1$, где x_i, x_j — различные образующие. Для этих групп используются также термины «графические группы» (graph groups) и «прямоугольные артиновы группы» (right-angled Artin groups). Для полугрупп и моноидов с аналогичным свойством термин «частично коммутативные» является общепринятым.

Любая частично коммутативная группа может быть задана при помощи (простого) графа Γ следующим образом: множеством порождающих группы будет множество всех всех вершин графа; порождающие x_i, x_j коммутируют, т. е. среди определяющих соотношений есть соотношение $[x_i, x_j] = 1$, тогда и только тогда, когда соответствующие x_i и x_j вершины соединены в графе Γ ребром. В этом случае мы вводим обозначение $x_i^{\pm 1} \leftrightarrow x_j^{\pm 1}$. Группу, заданную таким образом при помощи графа Γ, будем обозначать через $G(\Gamma)$.

Нетрудно видеть, что в классе частично коммутативных групп содержатся все свободные группы; в этом случае множество определяющих соотношений будет пустым, а в соответствующем графе не будет ребер. Свободные абелевы группы также являются частным случаем частично коммутативных групп. Соответствующий граф будет полным, т. е. в нем любые две вершины соединены ребром.

Уравнение $[x, y] = g$ в свободной группе рассматривал Уикс [1]. Он доказал, что циклически приведенное в свободной группе слово является коммутатором тогда и только тогда, когда некоторый его циклический сдвиг имеет вид $ABCA^{-1}B^{-1}C^{-1}$. Позднее результат Уикса неоднократно обобщался в различных направлениях [2–4]. Г. С. Маканин [5] указал алгоритм, позволяющий решать любые уравнения в свободных группах (см. также [6]). В настоящей работе мы даем описание коммутаторов в частично коммутативных группах (теорема 1) и основанный на нем алгоритм, проверяющий разрешимость коммутаторных уравнений вида $[x, y] = g$ в этих группах (следствие 2). Как уже отмечалось, свободные группы являются частным случаем частично коммутативных групп, и поэтому результат данной работы можно считать обобщением результата Уикса. Мы считаем, что могут быть предприняты попытки распространить использованные здесь идеи для решения уравнения $[x, y] = g$ в группе Томпсона F и в более широком классе групп диаграмм, которые тесно связаны с частично коммутативными группами [7, 8].

Зафиксируем некоторую частично коммутативную группу G, заданную при помощи простого графа Γ.

Далее мы рассматриваем некоторые элементарные факты о частично коммутативных группах, необходимые нам для доказательства основного результата. Похожие утверждения содержатся в статье [9].

Введем понятие элементарного преобразования. Пусть $W \equiv W_1abW_2$, где $a, b \in \Sigma^{\pm 1}$, причем $a \leftrightarrow b$. Тогда *элементарным преобразованием* назовем переход от слова W к слову $W' \equiv W_1baW_2$. Будем говорить, что $W \sim V$, если V может быть получено из W при помощи элементарных преобразований. Очевидно, что $\sim$ есть отношение эквивалентности на множестве всех групповых слов. Слова, находящиеся в данном отношении, будут в дальнейшем называться *эквивалентными* (в группе G). Через $[W]$ обозначим класс эквивалентности слова W. Очевидно, все слова из $[W]$ равны W в группе G.

Слово W называется *приведенным* в частично коммутативной группе G, если всякое слово V, эквивалентное W, приведено в свободной группе, т. е. никакое $V \in [W]$ не имеет вида $V_1aa^{-1}V_2$ ($a \in \Sigma^{\pm 1}$). Если $V \equiv V_1aa^{-1}V_2$, то мы можем произвести сокращение, перейдя к слову V_1V_2. Любое слово в частично коммутативной группе можно *привести* (вообще говоря, многими способами), т. е. для любого слова W существует последовательность слов $W \equiv W_1, W_2, \ldots, W_n \equiv V$, где V приведено в G, и каждое W_{i+1} получено из W_i ($1 \leq i < n$) при помощи элементарных преобразований или сокращений. При этом, очевидно, V равно W в группе G. Всякое приведенное слово V, равное W в G, будем называть *приведенной формой* слова W в группе G.

Отметим, что этот факт позволяет решать в частично коммутативных группах проблему равенства слов (см. [10], а также строгое обоснование ниже). Чтобы определить, равны ли слова W и V, достаточно их привести и для полученных слов проверить, совпадают ли их классы эквивалентности. Это можно сделать, так как класс эквивалентности любого слова конечен.

Далее мы будем использовать диаграммы ван Кампена [11]. Пусть есть слово W, равное единице в группе G, заданной копредставлением $\mathscr{P} = \langle \Sigma \mid \mathscr{R} \rangle$. Тогда согласно лемме ван Кампена существует диаграмма с меткой контура W, заполненная клетками, причем метка контура каждой клетки является одним из соотношений из $\mathscr{R}$ (с точностью до циклического сдвига или взятия обратного). Следуя монографии [12], мы для удобства будем также рассматривать так называемые 0-клетки, т. е. клетки с пустыми метками контура или метками вида $1 \cdot x = x \cdot 1$, где $x \in \Sigma$ (рис. 1). Любую диаграмму ван Кампена можно преобразовать, используя 0-клетки так, что контур диаграммы и контуры всех клеток будут простыми замкнутыми кривыми; подробности см. в [12].

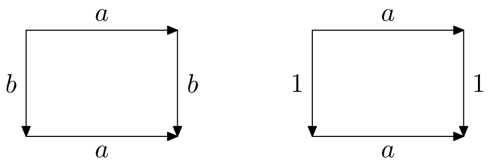

Рис. 1.

Пусть $W = 1$ в группе G, заданной при помощи $\mathscr{P}$, и пусть Δ — диаграмма над $\mathscr{P}$, осуществляющая это равенство. Если $W \equiv UV^{-1}$, то, очевидно, слова U и V равны в группе G, и мы будем также говорить, что *диаграмма* Δ *осуществляет равенство* $U = V$.

Введем понятие *полосы*, которое часто используется при работе с диаграммами. Пусть $U = V$ в частично коммутативной группе G, заданной копредставлением $\mathscr{P} = \langle \Sigma \mid \mathscr{R} \rangle$. Рассмотрим диаграмму ван Кампена над $\mathscr{P}$, осуществляющую это равенство. Рассмотрим вхождение некоторой буквы $a \in \Sigma^{\pm 1}$ в слово U. Будем строить полосу, начиная с ребра e_0, соответствующего этому вхождению. К e_0 примыкает некоторая клетка π_1. Такая клетка в диаграммах над $\mathscr{P}$ имеет метку контура $aba^{-1}b^{-1}$ при $a \leftrightarrow b$ или же является 0-клеткой с меткой контура $a \cdot 1 \cdot a^{-1} \cdot 1$.

Заметим, что в любой клетке для ребра с меткой a найдется лежащее напротив него ребро с этой же меткой. Обозначим через e_1 ребро клетки π_1, лежащее напротив e_0. Продолжим процедуру, выбирая клетку $\pi_2 \neq \pi_1$, примыкающую к e_1, и т. д., пока не получим ребро e_n, лежащее на границе. Таким образом, для любого вхождения буквы в слово U (или V) можно рассмотреть полосу, начинающуюся с этого вхождения. При этом все клетки полосы будут попарно различны, так как полоса не может иметь самопересечений из-за вида определяющих соотношений (рис. 2).

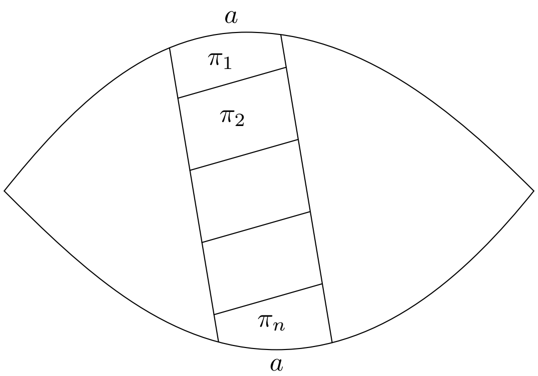

Рис. 2.

Определение. Слова U и V в частично коммутативной группе G называются *коммутирующими побуквенно* (обозначается $U \leftrightarrow V$), если любая буква из U коммутирует с любой буквой из V в силу определяющих соотношений. (В частности, если буква $x \in \Sigma^{\pm 1}$ входит в U, то $x^{\pm 1}$ не входит в V.)

Лемма 1. *Слово W в частично коммутативной группе G не является приведенным в G тогда и только тогда, когда W содержит подслово вида xUx^{-1} $(x \in \Sigma^{\pm 1})$, где $x \leftrightarrow U$.*

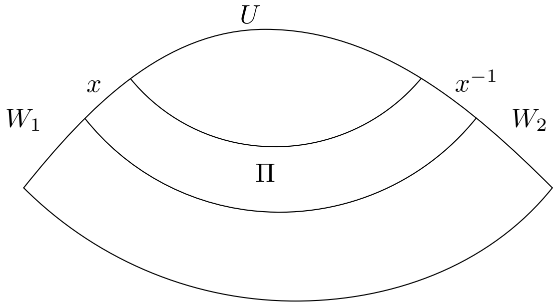

Рис. 3.

Доказательство. Если $W \equiv W_1 x U x^{-1} W_2$ и $x \leftrightarrow U$, то W не приведено в G по определению, так как эквивалентно слову $W_1 U x x^{-1} W_2$.

Докажем обратное. Из определения следует, что если W не приведено в G, то оно равно в G более короткому слову V (при желании последнее можно считать приведенным в G). Пусть Δ — диаграмма, осуществляющая равенство $W = V$. Рассмотрим полосы, исходящие из всех букв слова W (рис. 3). Так как $|W| > |V|$, некоторые из этих полос заканчиваются на W. Каждая полоса, начинающаяся и заканчивающаяся на W, задает разбиение вида $W \equiv W_1 x U x^{-1} W_2$, где $x \in \Sigma^{\pm 1}$. Среди всех таких полос выберем полосу П, у которой значение $|U|$ минимально.

Все полосы, начинающиеся на U, пересекают П. В противном случае была бы полоса, начинающаяся и заканчивающаяся на U, что противоречило бы минимальности выбора слова U.

Итак, полоса, начинающаяся с любой буквы y слова U, пересекает полосу П. Это означает, что в П есть клетка, осуществляющая равенство $xy = yx$, т. е. $x \leftrightarrow y$. Следовательно, $x \leftrightarrow U$.

Лемма доказана.

Заметим, что лемму 1 можно было доказать проще, обращаясь лишь к определению отношения эквивалентности $\sim$ и не используя диаграмм ван Кампена. Однако в дальнейшем нам понадобится прием, примененный при доказательстве.

Лемма 2. *Приведенные в G слова U и V равны в G тогда и только тогда, когда $U \sim V$. В частности, приведенные формы одного и того же слова эквивалентны.*

Доказательство. Если $U \sim V$, то U и V равны в G. Докажем обратное индукцией по сумме длин слов U и V.

Если U и V оба пусты, то доказывать нечего. Поэтому предположим без ограничения общности, что U непусто. Рассмотрим диаграмму, осуществляющую равенство $U = V$ (рис. 4). Первую букву слова U обозначим через x. Положим $U \equiv xU'$. Рассмотрим полосу, исходящую из x, обозначая ее через П. Из доказательства леммы 1 вытекает, что эта полоса не может заканчиваться на U, следовательно, она заканчивается на V. Тогда $V \equiv YxZ$. Каждая полоса, начинающаяся на какой-либо букве слова Y, пересекает полосу П. Следовательно, $Y \leftrightarrow x$. Поэтому $V \sim xYZ$.

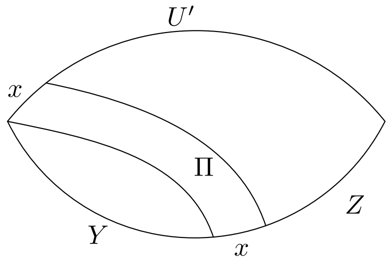

Рис. 4.

Так как $U \equiv xU'$, то $U' = YZ$ в группе G. При этом U' приведено в G как подслово приведенного в G слова U. Слово YZ приведено в G, так как в противном случае было бы не приведено также слово xYZ, а следовательно, и эквивалентное ему слово $V \equiv YxZ$. Слова U' и YZ в сумме имеют меньшую длину, чем U и V, и мы можем применить предположение индукции. Отсюда $U' \sim YZ$. Значит, $xU' \sim xYZ$, поэтому $U \sim V$.

Лемма доказана.

Определение. Пусть $U \equiv XY$, $V \equiv YX$ для некоторых слов X, Y. Тогда будем говорить, что V *получено из* U *циклическим сдвигом.*

Определение. Слово W называется *циклически приведенным* в частично-коммутативной группе G, если всякое слово V, эквивалентное W, циклически приведено в свободной группе.

Если слово W не циклически приведено в G, то мы можем его *циклически привести*, переходя к циклическим сдвигам и приводя получающиеся слова, пока это возможно. В итоге получим (вообще говоря, не единственным образом) некоторое циклически приведенное слово, сопряженное слову W в группе G. Всякое циклически приведенное слово, сопряженное W, будет называться *циклически приведенной формой* слова W.

Определение. Будем говорить, что слова V и W *циклически эквивалентны* в G (обозначается $V \overset{c}{\sim} W$), если V и W циклически приведены в G, и W может быть получено из V при помощи элементарных преобразований и циклических сдвигов. Циклически эквивалентные слова сопряжены в G. Очевидно, $\overset{c}{\sim}$ есть отношение эквивалентности на множестве циклически приведенных слов.

Лемма 3. *Пусть $W \equiv UabV$, $a, b \in \Sigma^{\pm 1}$, причем $a \leftrightarrow b$. Если все циклические сдвиги слова W приведены в G, то и все циклические сдвиги слова $W' \equiv UbaV$ приведены в G.*

Доказательство. Всякому циклическому сдвигу слова W', не разрезающему подслово ba, соответствует циклический сдвиг слова W, в котором ba заменено на ab. Оба этих циклических сдвига эквивалентны и потому оказываются приведенными.

Осталось рассмотреть циклический сдвиг слова W', который графически равен $aVUb$. Допустим, что он не приведен. Тогда по лемме 1 он содержит подслово вида xYx^{-1}, где $x \in \Sigma^{\pm 1}$, причем $x \leftrightarrow Y$. Если слово xYx^{-1} содержится в aVU, то слово aVU не приведено и потому не будет приведен циклический сдвиг слова W, графически равный $abVU$ (так как последний эквивалентен $b \cdot aVU$). Аналогично рассматривается случай, когда слово xYx^{-1} содержится в

VUb. Поэтому остается последний случай, когда xYx^{-1} совпадает с $aVUb$, что невозможно, так как a и b не взаимно обратны.

Лемма доказана.

Доказанная лемма, по сути, утверждает, что свойство слова иметь все циклические сдвиги приведенными в G не меняется при замене слова эквивалентным ему в группе.

Лемма 4. *Слово W циклически приведено в G тогда и только тогда, когда все его циклические сдвиги приведены в G.*

Доказательство. Пусть W циклически приведено в G, а некоторый его циклический сдвиг не приведен. Тогда по лемме 1 он содержит подслово вида xYx^{-1}, где $x \leftrightarrow Y$. Следовательно, W содержит циклическое подслово вида xYx^{-1}. Поскольку W приведено, то W не может содержать это подслово. Следовательно, W можно представить в виде $Y_2x^{-1}W'xY_1$, где $Y \equiv Y_1Y_2$. Поскольку $x \leftrightarrow Y_1$, $x \leftrightarrow Y_2$, имеем $W \sim x^{-1}Y_2W'Y_1x$, т. е. W не является циклически приведенным, что противоречит условию леммы.

Пусть W не циклически приведено. Тогда оно эквивалентно слову, не циклически приведенному в свободной группе, т. е. слову, у которого есть циклический сдвиг, не приведенный в свободной группе. Тогда по лемме 3 у эквивалентного ему слова W есть не приведенный в G циклический сдвиг.

Лемма доказана.

Следствие 1. *Слово W в частично коммутативной группе G не является циклически приведенным в G тогда и только тогда, когда существует его циклический сдвиг W', содержащий подслово вида xYx^{-1} ($x \in \Sigma^{\pm 1}$), причем $x \leftrightarrow Y$.*

Это прямо следует из лемм 1 и 4.

Определение. Пусть $U \equiv U_1 \cdot x \cdot U_2$, где $x \in \Sigma^{\pm 1}$. Тогда $U^{-1} \equiv U_2^{-1} \cdot x^{-1} \cdot U_1^{-1}$. В этом случае указанные вхождения x в U и x^{-1} в U^{-1} будем называть *согласованными.*

Лемма 5. *Два циклически приведенных в G слова V и W сопряжены в G тогда и только тогда, когда $V \stackrel{c}{\sim} W$. В частности, циклические приведенные формы одного и того же слова циклически эквивалентны.*

Доказательство. Если $V \stackrel{c}{\sim} W$, то, очевидно, V и W сопряжены в G.

Докажем обратное. Пусть V сопряжено W в G. Тогда V сопряжено в G любому слову, которое циклически эквивалентно W. Выберем самое короткое слово U такое, что $V = U^{-1}W'U$ в группе G для некоторого $W' \stackrel{c}{\sim} W$. Очевидно, U должно быть приведенным в G. Положим $Z \equiv U^{-1}W'U$. Докажем, что Z приведено в G. Пусть это не так. Тогда по лемме 1 в Z содержится подслово вида $x^{-1}Yx$, где $x \in \Sigma^{\pm 1}$, причем $x \leftrightarrow Y$. Так как W' приведено в G, то $x^{-1}Yx$ не содержится в W'. Поэтому либо x^{-1} содержится в U^{-1}, либо x содержится в U. В силу симметрии можно считать, что x^{-1} содержится в U^{-1}.

Поскольку слово U приведено, то x не содержится в U^{-1}. Предположим, что x содержится в W'. Тогда $U^{-1} \equiv U_2^{-1}x^{-1}U_1^{-1}$, $W' \equiv W_1xW_2$, причем $x \leftrightarrow U_1^{-1}W_1$. Подставим выражения для $U^{\pm 1}$ и W' в Z. Получим

$$Z \equiv \bigl(U_2^{-1}x^{-1}U_1^{-1}\bigr)(W_1xW_2)(U_1xU_2).$$

Теперь воспользуемся коммутативностью x с $U_1^{\pm 1}$ и с W_1 в G. Тогда Z равно в G слову $U_2^{-1}U_1^{-1}W_1W_2xU_1U_2$. Итак, Z равно в G слову $(U_1U_2)^{-1}W_1W_2x(U_1U_2)$.

Очевидно, W' циклически эквивалентно W_1W_2x (с учетом того, что x коммутирует с W_1), а U_1U_2 имеет меньшую длину, чем U. Получили противоречие с выбором U.

Предположим теперь, что x содержится в U, причем это его вхождение согласовано с рассмотренным выше вхождением x^{-1} в U^{-1}. Тогда $U \equiv U_1xU_2$, причем $x \leftrightarrow U_1^{-1}W'U_1$. Подставим выражение для $U^{\pm1}$ в Z. Получим $Z \equiv U_2^{-1}x^{-1}U_1^{-1}W'U_1xU_2$. Теперь мы снова сокращаем x^{-1} с x, пользуясь коммутативностью, получая, что Z равно в G слову $(U_1U_2)^{-1}W'(U_1U_2)$. Очевидно, длина U_1U_2 меньше, чем длина U, поэтому мы опять получили противоречие с выбором U.

Остался последний случай: x содержится в U, причем вхождения x^{-1} в U^{-1} и x в U не согласованы. В силу симметрии можно считать, что согласованное с первой буквой слова $x^{-1}Yx$ вхождение x в слово U расположено левее, чем последняя буква слова $x^{-1}Yx$, т. е. входит в слово Y. Тогда мы можем сократить эти два согласованных вхождения, как в предыдущем случае, ибо содержащееся между ними подслово слова Y по-прежнему побуквенно коммутирует с x. Вновь приходим к противоречию с выбором U.

В итоге мы получили, что слово Z приведено в G. Так как $V = Z$ в группе G, а V и Z приведены в G, то $V \sim Z$ по лемме 2. Поскольку V циклически приведено в G, то и Z циклически приведено в G по определению. Поэтому U должно быть пустым. Следовательно, $V = W'$ в G. Тогда $V \sim W'$ в силу леммы 2. Из $W' \overset{c}{\sim} W$ вытекает $V \overset{c}{\sim} W$, что и требовалось доказать.

Лемма доказана.

Заметим, что лемма 5 позволяет решать в частично коммутативных группах проблему сопряженности. Чтобы определить, сопряжены или нет слова V и W, достаточно их циклически привести (каким-либо способом) и определить, будут ли полученные слова циклически эквивалентны. Последнее можно сделать эффективно, так как для каждого слова класс циклически эквивалентных ему слов конечен.

Проблема сопряженности в частично коммутативных группах была решена в [8].

Рассмотрим выпуклый m-угольник. Проведем в нем диагонали так, чтобы они образовывали триангуляцию этого m-угольника. Полученный граф назовем *триангуляционным*. Триангуляционный граф, у которого каждой вершине сопоставлено некоторое слово A_i $(1 \leq i \leq m)$, называется *размеченным триангуляционным графом*.

Заметим, что при $m = 3$ размеченный триангуляционный граф (для данного набора слов) единственный, при $m = 4$ имеется два различных размеченных триангуляционных графа, так как в четырехугольнике диагональ можно провести двумя различными способами (рис. 5).

Определение. Будем говорить, что слово A в частично коммутативной группе G *удовлетворяет условию* $\mathscr{C}(m)$ $(m \geq 3)$, если A может быть представлено как $A_1A_2\ldots A_mA_1^{-1}A_2^{-1}\ldots A_m^{-1}$ для некоторых (возможно, пустых) слов $A_1,\ldots,A_m$ и существует размеченный триангуляционный граф с m вершинами, имеющими метки $A_1,\ldots,A_m$ (при чтении по часовой стрелке), удовлетворяющий следующему условию: если две различные вершины, помеченные словами A_i и A_j, не соединены в триангуляционном графе, то $A_i \leftrightarrow A_j$.

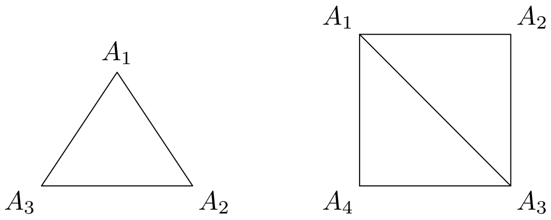

Рис. 5.

Для дальнейшего удобства введем обозначение

$$v(A_1, \ldots, A_m) \equiv A_1 \ldots A_m A_1^{-1} \ldots A_m^{-1}.$$

Будем считать, что слово $v(A_1, \ldots, A_m)$ автоматически удовлетворяет условию $\mathscr{C}(m)$ при $0 \leq m \leq 2$.

Из определения ясно, что слово, представимое в виде $v(A_1, A_2, A_3)$, всегда удовлетворяет условию $\mathscr{C}(3)$. Для того чтобы слово, представимое в виде $v(A_1, A_2, A_3, A_4)$, удовлетворяло условию $\mathscr{C}(4)$, достаточно, чтобы A_2 побуквенно коммутировало с A_4 (как на рис. 5) или A_1 побуквенно коммутировало с A_3, если проведена другая диагональ.

Очевидно, что условие $\mathscr{C}(m)$ инвариантно относительно циклических сдвигов слова A, начинающихся с любого из слов $A_i^{\pm 1}$ ($1 \leq i \leq m$).

В дальнейшем будем часто говорить, что слово имеет вид $\mathscr{C}(m)$, если оно удовлетворяет условию $\mathscr{C}(m)$. В формулировке основного результата будем использовать некоторое другое условие, более удобное для проверки и эквивалентное $\mathscr{C}(m)$.

Теорема 1. *Слово W в частично коммутативной группе G является коммутатором тогда и только тогда, когда некоторая его циклически приведенная форма A представима в виде $A_1 A_2 \ldots A_m A_1^{-1} A_2^{-1} \ldots A_m^{-1}$ и для любых чисел α, β, γ, δ таких, что $1 \leq \alpha < \beta < \gamma < \delta \leq m$, выполняется хотя бы одно из условий: $A_\alpha \leftrightarrow A_\gamma$ или $A_\beta \leftrightarrow A_\delta$.*

Следствие 2. *Для любой частично коммутативной группы G, заданной конечным копредставлением, алгоритмически разрешимо свойство данного элемента быть коммутатором. Иными словами, существует алгоритм, проверяющий разрешимость уравнений вида $[x, y] = g$ в группе G.*

Доказательство. Для данного элемента группы можно эффективно найти некоторую его циклически приведенную форму, а затем выписать все такие формы, так как они циклически эквивалентны по лемме 5.

Для каждого из слов списка нужно проверить, имеет ли оно вид $\mathscr{C}(m)$ для какого-либо m. Достаточно заметить, что в условии теоремы можно считать все слова $A_1, \ldots, A_m$ непустыми, поэтому значения m ограничены сверху.

Доказательство теоремы 1. Для начала убедимся в том, что условие из формулировки теоремы, относящееся к слову A, эквивалентно условию $\mathscr{C}(m)$. В самом деле, пусть слово A имеет вид $\mathscr{C}(m)$. Пусть числа α, β, γ, δ удовлетворяют условию $1 \leq \alpha < \beta < \gamma < \delta \leq m$. Тогда $m \geq 4$ и вершины A_α, A_γ не являются соседними в m-угольнике. То же самое верно для вершин A_β и A_δ. Поскольку в триангуляционном графе никакие две диагонали не пересекаются, то либо не соединены вершины с метками A_α и A_γ, либо не соединены вершины с метками A_β и A_δ. Поэтому либо $A_\alpha \leftrightarrow A_\gamma$, либо $A_\beta \leftrightarrow A_\delta$.

Обратно, пусть слово A удовлетворяет условию из формулировки. Если $m \le 2$, то условие $\mathscr{C}(m)$ выполнено. При $m \ge 3$ рассмотрим контур выпуклого m-угольника, вершины которого помечены словами $A_1, \ldots, A_m$. Проведем все те диагонали, концы которых помечены словами, не коммутирующими побуквенно. По условию никакие две из проведенных диагоналей не пересекаются во внутренних точках. Остается дополнить полученный граф до триангуляционного.

Достаточность. Пусть $A \equiv v(A_1, \ldots, A_m)$ и для A выполнено условие $\mathscr{C}(m)$. Будем доказывать индукцией по m, что A является коммутатором. При $m \le 2$ это очевидно. Пусть $m \ge 3$. Рассмотрим размеченный триангуляционный граф. Легко видеть, что в любой триангуляции выпуклого m-угольника есть вершина валентности 2. С учетом сделанного перед теоремой замечания об инвариантности A относительно подходящих циклических сдвигов можно считать, что это вершина с меткой A_m. Из определения размеченного триангуляционного графа и условия $\mathscr{C}(m)$ для A следует, что $A_m \leftrightarrow A_i$ при всех i, удовлетворяющих условию $2 \le i \le m-2$. В частности, A_m коммутирует с $A_2 \ldots A_{m-2}$. (Все равенства далее рассматриваются в группе G.) Вставим $A_m^{-1} A_m$ после A_1 в слове A. Тогда

$$A = A_1 \bigl(A_m^{-1} A_m\bigr) A_2 \ldots A_{m-1} A_m A_1^{-1} \ldots A_{m-1}^{-1} A_m^{-1}.$$

Воспользуемся указанной выше коммутативностью и получим, что

$$A = A_1 A_m^{-1} A_2 \ldots A_m A_{m-1} A_m A_1^{-1} \ldots A_{m-1}^{-1} A_m^{-1}.$$

Теперь обозначим $A_1 A_m^{-1}$ через A_1', $A_m A_{m-1}$ через A_{m-1}'. В результате получим, что A равно в G слову $A' \equiv v(A_1', A_2, \ldots, A_{m-1}')$.

Проверим, что A' удовлетворяет условию $\mathscr{C}(m-1)$. Из исходного триангуляционного графа исключим вершину A_m с двумя исходящими из нее ребрами. Получим $(m-1)$-угольник, в котором метку A_1 заменим на A_1', а метку A_{m-1} — на A_{m-1}'. Если в исходном графе не было ребра между вершиной A_1 и вершиной A_i $(3 \le i \le m-2)$, то $A_1 \leftrightarrow A_i$. Так как и A_m побуквенно коммутирует с A_i, то для слова $A_1' \equiv A_1 A_m^{-1}$ также будет выполняться условие $A_1' \leftrightarrow A_i$. Те же рассуждения можно провести и для слова A_{m-1}'. Следовательно, A' имеет вид $\mathscr{C}(m-1)$. По предположению индукции A' является коммутатором. Поскольку $A = A'$ в G, то и A является коммутатором. Достаточность доказана.

Необходимость. Поскольку W является коммутатором, для некоторых слов X, Y выполняется $W = [X, Y] = X^{-1} Y^{-1} X Y$ в G. В частности, $X^{-1} Y^{-1} X Y$ удовлетворяет условию $\mathscr{C}(2)$ и сопряжено W в G. Рассмотрим все слова, сопряженные W и удовлетворяющие условию $\mathscr{C}(m)$ при каком-либо m. Выберем среди них слово наименьшей длины и обозначим его через A. Тогда $A \equiv v(A_1, \ldots, A_m)$ для некоторого m. Наша цель — доказать, что A циклически приведено в G. Тогда A будет циклически приведенной формой слова W.

Будем вести доказательство от противного. Пусть A не является циклически приведенным. Тогда по следствию 1 существует циклическое подслово слова A вида xUx^{-1}, где $x \leftrightarrow U$, $x \in \Sigma^{\pm 1}$. В силу инвариантности условия $\mathscr{C}(m)$ относительно подходящих циклических сдвигов можно считать, что x входит в A_1.

Предположим сначала, что слово, расположенное между некоторым вхождением буквы x в A_1 и согласованным вхождением буквы x^{-1} в A_1^{-1}, коммутирует с x в группе G. Тогда данные вхождения букв x, x^{-1} можно вычеркнуть из слова A, в результате чего слово A заменится более коротким и равным ему в группе словом $A' \equiv v(A_1', A_2, \ldots, A_m)$, где A_1' получено из A_1 вычеркиванием буквы x. Поскольку состав букв, входящих в рассматриваемые слова, мог только уменьшиться, все побуквенно коммутирующие слова таковыми и остались и потому A' имеет вид $\mathscr{C}(m)$, что противоречит выбору слова A.

Из замечания предыдущего абзаца сразу следует, что слово xUx^{-1} не содержит вхождения буквы x^{-1} в слово A_1^{-1}, согласованного с вхождением начальной буквы x в A_1. Более того, слово xUx^{-1} обязано содержаться в $A_1 \ldots A_m$. Действительно, в противном случае последняя буква слова xUx^{-1} входит в A^{-1} и расположена левее вхождения буквы x^{-1} в то же слово, согласованного с вхождением начальной буквы слова xUx^{-1} в A_1. Но тогда вхождение буквы x в A_1, согласованное с вхождением последней буквы x^{-1} слова xUx^{-1}, расположено правее первой буквы подслова xUx^{-1} и потому между некоторыми двумя согласованными вхождениями $x^{\pm 1}$, как и выше, находится коммутирующее с x слово, что невозможно.

Если слово xUx^{-1} содержится в A_1, то можно заменить слово A_1 более коротким равным ему в группе словом A_1', заменяя подслово xUx^{-1} на U. Слово $A' \equiv v(A_1', A_2, \ldots, A_m)$, очевидно, будет равно A в G и будет удовлетворять условию $\mathscr{C}(m)$, поскольку в A_1 набор букв не увеличился, а остальные слова не изменились. В результате мы вновь получим противоречие с выбором A.

Итак, xUx^{-1} не содержится в A_1. Последняя буква слова xUx^{-1} входит в некоторое слово A_k при $2 \le k \le m$. Тогда $A_1 \equiv A_1' x A_1''$, $A_k \equiv A_k' x^{-1} A_k''$, причем $x \leftrightarrow A_1''$ и $x \leftrightarrow A_k'$. Мы можем заменить в $v(A_1, \ldots, A_m)$ слово A_1 на слово $A_1' A_1'' x$, а A_k заменить на $x^{-1} A_k' A_k''$. Новое слово будет иметь такую же длину и также будет удовлетворять условию $\mathscr{C}(m)$ ввиду неизменности состава букв. Поэтому можно фактически считать, что первая буква слова xUx^{-1} является последней буквой слова A_1, последняя буква слова xUx^{-1} — первой буквой слова A_k, причем x побуквенно коммутирует с $U \equiv A_2 \ldots A_{k-1}$.

Теперь рассмотрим два случая.

Случай 1. Пусть $k = m$, т. е. x^{-1} — первая буква слова A_m. Тогда $A_1 \equiv A_1' x$, $A_m \equiv x^{-1} A_m'$, причем $x \leftrightarrow A_i$ при всех $2 \le i < m$. Тем самым

$$A \equiv A_1' x A_2 \ldots A_{m-1} x^{-1} A_m' x^{-1} (A_1')^{-1} A_2^{-1} \ldots A_{m-1}^{-1} (A_m')^{-1} x.$$

Теперь сократим пару вхождений x и x^{-1} в первой половине слова A, пользуясь коммутативностью, и положим $A_{m+1} \equiv x^{-1}$. Получим, что A равно в G слову

$$A' \equiv A_1' A_2 \ldots A_{m-1} A_m' A_{m+1} (A_1')^{-1} A_2^{-1} \ldots A_{m-1}^{-1} (A_m')^{-1} A_{m+1}^{-1}.$$

Докажем, что слово A' удовлетворяет условию $\mathscr{C}(m+1)$. Добавим к размеченному триангуляционному графу для слова A вершину A_{m+1} и соединим ее с вершинами A_1, A_m. При этом вершины A_1 и A_m будут соединены друг с другом диагональю. Очевидно, новый граф также будет размеченным триангуляционным графом. Поскольку в слове A_1' состав букв не увеличился по сравнению с A_1, то A_1' будет побуквенно коммутировать со всеми словами A_i, с которыми побуквенно коммутирует A_1. Аналогичный вывод справедлив и для слова A_m'. Со словом A_{m+1}, равным x^{-1}, побуквенно коммутируют слова A_i при всех $2 \le i < m$, что нам и требуется, поскольку в новом размеченном триангуляционном графе вершина A_{m+1} не соединена ни с одной вершиной, кроме A_1 и A_m. В итоге мы получили, что A равно в G слову A', которое имеет меньшую длину, чем A, и удовлетворяет условию $\mathscr{C}(m+1)$, что противоречит выбору A.

Можно заметить, что этот этап доказательства является в некотором смысле обращением доказательства достаточности в данной теореме.

Случай 2. Пусть $k < m$, т. е. x^{-1} — первая буква слова A_k, где $2 \leq k < m$. Тогда $A_1 \equiv A_1' x$, $A_k \equiv x^{-1} A_k'$, причем $x \leftrightarrow A_i$ при всех $2 \leq i < k$. Тем самым

$$A \equiv v(A_1' x, A_2, \ldots, A_{k-1}, x^{-1} A_k', A_{k+1}, \ldots, A_m).$$

Теперь сократим пару вхождений x и x^{-1} в первой половине слова A, пользуясь коммутативностью. Получим, что A равно в G слову

$$A' \equiv A_1' \ldots A_k' \ldots A_m x^{-1} (A_1')^{-1} \ldots (A_k')^{-1} x A_{k+1}^{-1} \ldots A_m^{-1}.$$

Заметим, что, как и в предыдущем случае, слово A_1' побуквенно коммутирует со всеми словами A_i, с которыми побуквенно коммутировало слово A_1, и аналогичное утверждение верно для слова A_k'.

Поскольку x входит в A_1, а x^{-1} входит в A_k, то A_1 не коммутирует с A_k побуквенно. Тогда они соединены диагональю в размеченном триангуляционном графе. Многоугольник, образованный вершинами A_1, A_k, A_{k+1},…,A_m, также триангулирован. Ребро, соединяющее A_1 и A_k, входит в некоторый из треугольников разбиения. Поэтому существует единственная вершина A_l, где $k < l \leq m$, которая соединена ребром и с A_1, и с A_k. Поскольку в триангуляционном графе никакие две диагонали не пересекаются, $x \leftrightarrow A_i$ при всех i таких, что $k < i < l$. Докажем это от противного. Допустим, что существует A_i ($k < i < l$) такое, что x не коммутирует побуквенно с A_i. Тогда и A_1 как слово, содержащее x, не коммутирует побуквенно с A_i. Это означает, что диагонали, соединяющие A_k с A_l и A_1 с A_i, пересекаются, что противоречит определению триангуляции. Поэтому $x \leftrightarrow A_i$ при $k < i < l$. Аналогично доказывается, что x побуквенно коммутирует с A_i при $l < i \leq m$. В частности, $x \leftrightarrow A_{k+1}^{-1} \ldots A_{l-1}^{-1}$, $A_{l+1} \ldots A_m \leftrightarrow x$. Соответствующие вхождения в слово A' можно переставить. Преобразуем в соответствии с этим слово A'. Оно равно в G слову

$$A_1' \ldots A_k' \ldots A_l x^{-1} A_{l+1} \ldots A_m \bigl(A_1^{-1}\bigr)' \ldots (A_k')^{-1} \ldots A_{l-1}^{-1} x A_l^{-1} \ldots A_m^{-1}.$$

Теперь положим $A_l' \equiv A_l x^{-1}$ и получим, что A равно в G слову

$$A'' \equiv v(A_1', A_2, \ldots, A_{k-1}, A_k', A_{k+1}, \ldots, A_{l-1}, A_l', A_{l+1}, \ldots, A_m).$$

Докажем, что A'' удовлетворяет условию $\mathscr{C}(m)$. В размеченном триангуляционном графе для A заменим метки слов A_1, A_k, A_l на A_1', A_k', A_l' соответственно. Как уже отмечалось, A_1' побуквенно коммутирует со всеми словами A_i, с которыми побуквенно коммутирует A_1; аналогичное утверждение верно для A_k'. Буква x коммутирует побуквенно со всеми словами A_i при $i \neq 1$, $i \neq k$, $i \neq l$. Отсюда вытекает, что слово $A_l' \equiv A_l x^{-1}$ коммутирует побуквенно со всеми словами A_i, с которыми A_l не была соединена диагональю. В итоге мы нашли слово A'', которое удовлетворяет условию $\mathscr{C}(m)$, равно A в группе G и имеет меньшую длину. Это вновь противоречит выбору A.

Все случаи рассмотрены. Теорема доказана.

Замечание. Пусть G — частично коммутативная группа с k порождающими. Тогда без ограничения общности можно считать, что число m в формулировке теоремы не превышает числа Рамсея $R(4, k+1)$. Более тонкий анализ показывает, что m можно считать не превосходящим $3k$.

Заметим, что прямое применение алгоритма, проверяющего слово на свойство быть коммутатором в группе G, потребует времени, как минимум экспоненциально зависящего от длины слова. Вопрос о существовании более быстрых, в частности полиномиальных, алгоритмов требует отдельного исследования.

Автор выражает признательность своему научному руководителю, доктору физико-математических наук, профессору В. С. Губе за постановку задачи и помощь при проведении исследований. Автор также благодарит А. Ю. Ольшанского, высказавшего ряд полезных замечаний.

ЛИТЕРАТУРА

1. *Wicks M. J.* Commutators in free products // J. London Math. Soc. 1962. N 37. P. 433–444.

2. *Vdovina A.* Constructing orientable Wicks forms and estimation of their numbers // Comm. Algebra. 1995. N 23. P. 3205–3222.

3. *Wicks M. J.* The equation $x^2y^2 = g$ over free products // Proc. Cong. Singapore Nat. Acad. Sci. 1971. P. 238–248.

4. *Wicks M. J.* A general solution of binary homogeneous equations over free groups // Pacific J. Math. 1972. V. 41, N 2. P. 543–561.

5. *Маканин Г. С.* Уравнения в свободной группе // Изв. АН СССР. Сер. мат. 1982. Т. 46, № 6. С. 1199–1273.

6. *Разборов А. А.* О системах уравнений в свободной группе // Изв. АН СССР. Сер. мат. 1982. Т. 48, № 4. С. 779–832.

7. *Guba V., Sapir M.* Diagram groups. Providence RI: Amer. Math. Soc., 1997. (Mem. Amer. Math. Soc.; 620).

8. *Guba V., Sapir M.* Diagram groups are totally orderable. Доступно на сайте http://www.arxiv.org/math.GR/0305153.

9. *Servatius H.* Automorphisms of graph groups // J. Algebra. 1989. N 126. P. 34–60.

10. *Cartier P., Foata D.* Problémes combinatoires de commutation et de réarrangements. Berlin; Heidelberg; New York: Springer-Verl., 1969. (Lect. Notes in Math.; 85).

11. *Линдон Р., Шупп П.* Комбинаторная теория групп. М.: Наука, 1980.

12. *Ольшанский А. Ю.* Геометрия определяющих соотношений в группах. М.: Наука, 1989.

Статья поступила 1 сентября 2004 г.

Шестаков Сергей Леонидович
Вологодский гос. педагогический университет, ул. С. Орлова, 6, Вологда 160600
slashinc@mail.ru