Сибирский математический журнал
Март—апрель, 2006. Том 47, № 2

УДК 512.543.72

УРАВНЕНИЕ $x^2y^2 = g$ 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. Мы рассматриваем алгоритм, позволяющий по данному элементу группы определить, является ли он произведением двух квадратов. Тем самым обобщается известный результат Уикса для свободных групп.

Ключевые слова: частично-коммутативные группы, уравнения в группах.

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 $\Sigma^{\pm 1} = \Sigma \cup \Sigma^{-1}$ называют *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 символом 1. Графическое (побуквенное) равенство слов обозначается через $\equiv$. *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 $[a, b] = 1$, где $a, b \in \Sigma$ — 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 вершин графа; порождающие a, b коммутируют, т. е. среди определяющих соотношений есть соотношение $[a, b] = 1$ тогда и только тогда, когда соответствующие a и b вершины соединены в графе Γ ребром. В этом случае мы вводим обозначение $a^{\pm 1} \leftrightarrow b^{\pm 1}$. 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.

Частично-коммутативные группы тесно связаны со свободными группами и обладают многими свойствами, которыми обладают и свободные группы. Так, в частично-коммутативных группах подобно тому, как в свободных группах, решаются проблема слов и проблема сопряженности, доказательства можно найти в [1] (см. также [2, 3]). В работе [4] доказано, что любые два некоммутирующих элемента в частично-коммутативной группе образуют базис свободной группы. Кроме того, как и в свободных группах, члены нижнего центрального ряда имеют тривиальное пересечение, откуда следует, что частично-коммутативные группы линейно упорядочены (см. [5]).

Эти результаты можно считать обобщениями аналогичных результатов для свободных групп. Однако следующие факты показывают, что частично-коммутативные группы обладают рядом специфических интересных свойств. В группе $F_2 \times F_2$, которая, очевидно, частично-коммутативна, может быть неразрешимой проблема вхождения в подгруппу (см. [6]). Кроме того, в работе [7] доказано, что частично-коммутативные группы могут содержать фундаментальные группы двумерных поверхностей.

Алгоритм решения уравнений вида $[x, y] = g$ и $x^2y^2 = g$ в свободных группах найден Уиксом [8]. В работе [1] автор обобщил результат Уикса для уравнения $[x, y] = g$ на случай частично-коммутативных групп. В настоящей работе продолжены исследования, начатые в [3]. Мы предлагаем алгоритм, определяющий разрешимость уравнения $x^2y^2 = g$ в частично-коммутативных группах, и тем самым, в частности, обобщаем результат Уикса для свободных групп.

В связи с этим следует упомянуть работу А. Вдовиной [9], в которой результаты Уикса распространяются на случай произведения n коммутаторов. Известно, что любое квадратичное слово в свободной группе при помощи некоторого автоморфизма переводится либо в слово вида $[x_1, y_1] \dots [x_n, y_n]$, либо в слово вида $x_1^2 \dots x_n^2$, т. е. либо в произведение коммутаторов, либо в произведение квадратов [10]. Поэтому можно предположить, что используемые здесь и в статье [1] методы могут быть применены и для описания решений квадратичных уравнений более общего вида в частично-коммутативных группах.

Далее приводится ряд определений и вспомогательных лемм. Доказательства можно найти в статье [1].

Определение. 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 писать $W \sim V$, 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, что все слова из $[W]$ равны W в группе G.

Определение. 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 $W \equiv W_1, W_2, \dots, W_n \equiv V$, где V приведено в G и каждое W_{i+1} получено из W_i ($1 \le i < n$) при помощи элементарного преобразования или сокращения в свободной группе. 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.

Определение. Слова U и V в частично-коммутативной группе G называются *коммутирующими побуквенно* (обозначается $U \leftrightarrow V$), если любая буква a из U коммутирует с любой буквой b из V в силу определяющих соотношений, т. е. $a \leftrightarrow b$. (В частности, если буква $x \in \Sigma^{\pm 1}$ входит в U, то $x^{\pm 1}$ не входит в V, так как все определяющие соотношения имеют вид $[a, b] = 1$, где $a \neq b$, $a, b \in \Sigma$.)

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 1 [1, 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 $x \leftrightarrow Y$.*

Лемма 2 [1, лемма 5]. *Два циклически приведенных в G слова V и W сопряжены в G тогда и только тогда, когда $V \overset{c}{\sim} W$. В частности, циклические приведенные формы одного и того же слова циклически эквивалентны.*

Определение. Будем говорить, что слово A в частично-коммутативной группе G *удовлетворяет условию* $Q(m)$, если A может быть представлено в виде

$$A_m B_{m-1} A_{m-1} \ldots A_2 B_1 A_1 C A_1 B_1^{-1} A_2 \ldots A_{m-1} B_{m-1}^{-1} A_m C^{-1} \tag{1}$$

для некоторых слов $A_1, \ldots, A_m$, $B_1, \ldots, B_{m-1}$, C при $m \geq 0$, причем выполнены следующие условия:

1) $A_i \leftrightarrow A_j$ при $|j - i| > 1$;
2) $A_i \leftrightarrow B_j$ при $i \neq j, j + 1$;
3) $B_i \leftrightarrow B_j$ при $i \neq j$;
4) $B_i \leftrightarrow C$ при всех $1 \leq i < m$.

Введем обозначение $v(A_1, B_1, \ldots, B_{m-1}, A_m, C)$ для слова (1). Вхождения букв в слово (1) естественным образом можно разбить на пары. Пусть буква y входит в первую половину слова (1) и содержится в одном из подслов вида A_i ($1 \leq i \leq m$). Тогда ей соответствует вхождение буквы y в подслово A_i из второй половины. Если y содержится в подслове B_i ($1 \leq i < m$) так, что $B_i \equiv B_i' \cdot y \cdot B_i''$, то ставим ей в соответствие вхождение $(B_i'')^{-1} \cdot y^{-1} (B_i')^{-1}$ буквы y^{-1} в подслово

B_i^{-1} из второй половины. Аналогично поступаем, если y входит в C. Таким образом, можно говорить о *парных вхождениях* букв в слово (1).

Сформулируем и докажем основной результат статьи.

Теорема 1. *Слово W в частично-коммутативной группе G представимо в виде произведения двух квадратов тогда и только тогда, когда некоторая его циклически приведенная форма удовлетворяет условию $Q(m)$ для некоторого m. При этом дополнительно можно считать все слова $A_1, \dots, A_m$ в определении условия $Q(m)$ непустыми.*

Доказательство. Достаточность. Пусть

$$A \equiv v(A_1, B_1, \dots, B_{m-1}, A_m, C)$$

и для A выполнено условие $Q(m)$. Индукцией по m будем доказывать, что A является произведением двух квадратов в G. Можно считать, что $m \geq 1$.

При $m = 1$ имеем $A \equiv A_1CA_1C^{-1} = (A_1C)^2(C^{-1})^2$ в группе G.

Пусть $m > 1$. Нам потребуется два этапа. На первом мы устраняем слово B_{m-1}, на втором — A_m.

Этап 1. $A \equiv A_mB_{m-1}A_{m-1}\dots A_1CA_1\dots A_mC^{-1}$. Из условия $Q(m)$ следует, что $B_{m-1} \leftrightarrow B_i$ при $1 \leq i < m-1$, $B_{m-1} \leftrightarrow A_i$ при $1 \leq i < m-1$, а также $B_{m-1} \leftrightarrow C$. Вставим слово $B_{m-1}^{-1}B_{m-1}$ после первого из вхождений A_{m-1} в слово A. Получим, что A равно в группе G слову

$$A_mB_{m-1}A_{m-1}\big(B_{m-1}^{-1}B_{m-1}\big)B_{m-2}A_{m-2}\dots A_{m-2}B_{m-2}^{-1}A_{m-1}B_{m-1}^{-1}A_mC^{-1}.$$

Воспользуемся перестановочностью слова B_{m-1} со словами, перечисленными выше, и придем к тому, что в группе G

$$A = A_m\big(B_{m-1}A_{m-1}B_{m-1}^{-1}\big)B_{m-2}A_{m-2}\dots A_{m-2}B_{m-2}^{-1}\big(B_{m-1}A_{m-1}B_{m-1}^{-1}\big)A_mC^{-1}.$$

Теперь обозначим $B_{m-1}A_{m-1}B_{m-1}^{-1}$ через A'_{m-1}. Получим, что A равно в группе G слову $A' \equiv v(A_1, B_1, \dots, B_{m-2}, A'_{m-1}, 1, A_m, C)$.

Этап 2. Рассмотрим слово A'. Из условия $Q(m)$ следует, что $A_m \leftrightarrow A_i$ при $1 \leq i < m-1$, $A_m \leftrightarrow B_i$ при $1 \leq i < m-1$. Вставим слово $A_mA_m^{-1}$ после первого из вхождений A'_{m-1} в слово A'. Получим, что A' равно в группе G слову

$$A_mA'_{m-1}\big(A_mA_m^{-1}\big)B_{m-2}\dots A_1CA_1\dots A'_{m-1}A_mC^{-1}.$$

Воспользуемся перестановочностью слова A_m^{-1} со словами, перечисленными выше; затем применим циклический сдвиг, перемещая A_m из начала в конец слова. Получим, что A' сопряжено в G слову

$$A'_{m-1}A_mB_{m-2}\dots A_1A_m^{-1}CA_1\dots B_{m-2}^{-1}A'_{m-1}A_mC^{-1}A_m.$$

Теперь обозначим слово $A'_{m-1}A_m$ через A''_{m-1}, слово $A_m^{-1}C$ — через C'' и получим, что A сопряжено в G слову $A'' \equiv v(A_1, B_1, \dots, B_{m-2}, A''_{m-1}, C'')$.

Убедимся, что A'' удовлетворяет условию $Q(m-1)$. Для этого достаточно проверить условия побуквенной коммутативности для слова A''_{m-1} и для слова C'', так как для остальных слов выполнение этих условий следует из того, что слово A удовлетворяет условию $Q(m)$.

Поскольку как C, так и A_m побуквенно коммутируют с B_i при $1 \leq i < m-1$, условия побуквенной коммутативности для слова $C'' \equiv A_m^{-1}C$ выполнены.

Каждое из слов A_m, A_{m-1}, B_{m-1} побуквенно коммутирует с каждым из слов A_i, B_i при $1 \le i < m-2$, поэтому слово

$$A''_{m-1} \equiv A'_{m-1}A_m \equiv B_{m-1}A_{m-1}B_{m-1}^{-1}A_m$$

будет побуквенно коммутировать с каждым из слов $A_1, \dots, A_{m-3}$, $B_1, \dots, B_{m-3}$, что и требуется для выполнения условия $Q(m-1)$.

Итак, слово A'' удовлетворяет условию $Q(m-1)$. Тогда по предположению индукции A'' является произведением двух квадратов в G. Следовательно, сопряженное ему в группе G слово A также будет произведением двух квадратов.

Необходимость. Пусть слово W равно произведению двух квадратов в группе G. Тогда для некоторых слов X, Y выполняется равенство $W = X^2Y^2$ в G. Следовательно, слово $YXXY$ сопряжено W в группе G. Слово $YXXY$, очевидно, удовлетворяет условию $Q(2)$ при $A_1 \equiv X$, $A_2 \equiv Y$, $B_1 \equiv 1$, $C \equiv 1$. Рассмотрим все слова, сопряженные W или W^{-1}, удовлетворяющие условию $Q(m)$ при каком-либо m. Выберем среди них слово наименьшей длины и обозначим его через A. Тогда для некоторого m имеем $A \equiv v(A_1, B_1, \dots, B_{m-1}, A_m, C)$. Наша цель — доказать, что слово 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 лемме 1 существует циклическое подслово слова A вида xUx^{-1}, где $x \leftrightarrow U$, $x \in \Sigma^{\pm 1}$. Заметим, что условие $Q(m)$ инвариантно относительно циклического сдвига, начинающегося со второго вхождения слова A_1 в слово A (т. е. ровно с середины слова A). Поэтому можно считать, что x входит в первую половину слова A, т. е. содержится в подслове $A_mB_{m-1}\dots B_1A_1C$.

Из условия $x \leftrightarrow U$ следует, что $x^{\pm 1}$ не содержится в U. Поэтому U не может содержать вторую половину слова A, т. е. подслово $A_1B_1^{-1}\dots B_{m-1}^{-1}A_mC^{-1}$. Значит, xUx^{-1} — подслово в A.

I. Сначала разберем случай, когда x^{-1} содержится во второй половине слова A. Рассмотрим три подслучая.

Случай 1.1. Буква x содержится в одном из слов A_i, $1 \le i \le m$. Тогда из условия $x \leftrightarrow U$ следует, что x^{-1} содержится во втором вхождении слова A_i в слово A, так как в противном случае слово U будет содержать хотя бы одну букву $x^{\pm 1}$. Действительно, если последняя буква слова xUx^{-1} расположена левее второго вхождения A_i в A, то парная ей буква содержится в U. Аналогично если x^{-1} расположена правее второго вхождения A_i, то U содержит букву, парную первой букве слова xUx^{-1}.

Эти же соображения показывают, что последняя буква слова xUx^{-1}, входящая в A_i, расположена левее вхождения, парного первой букве слова xUx^{-1}. Таким образом, A_i имеет вид $A_i \equiv A'_ix^{-1}A''_ixA'''_i$. При этом

$$U \equiv A'''_iB_{i-1}\dots B_1A_1CA_1B_1^{-1}\dots B_{i-1}^{-1}A'_i.$$

Подставим слово A_i в слово A:

$$A \equiv A_m \dots B_iA'_ix^{-1}A''_ixA'''_i \dots A_1CA_1 \dots A'_ix^{-1}A''_ixA'''_iB_i^{-1}\dots A_mC^{-1}.$$

Теперь заменим в слове A подслово xUx^{-1} на U и воспользуемся коммутативностью x^{-1} с A'_i и x с A'''_i (последнее вытекает из того, что A'''_i, A'_i входят в U). Получим, что A равно в G слову

$$A_m \dots B_ix^{-1}A'_iA''_iA'''_i \dots A_1CA_1 \dots A'_iA''_iA'''_ixB_i^{-1}\dots A_mC^{-1}.$$

Обозначим $B_i x^{-1}$ через $\overline{B_i}$, а $A'_i A''_i A'''_i$ — через $\overline{A_i}$. Получим, что в группе G слово A равно $\overline{A} \equiv v(A_1, B_1, \ldots, \overline{A_i}, \overline{B_i}, \ldots, A_m, C)$. Докажем, что $\overline{A}$ удовлетворяет условию $Q(m)$. Достаточно проверить условия побуквенной коммутативности для $\overline{B_i}$, так как состав букв в слове $\overline{A_i}$ не увеличился по сравнению со словом A_i, а остальные слова не изменились. Поскольку $\overline{B_i} \equiv B_i x$, достаточно проверить несколько условий коммутативности, относящихся к x. Во-первых, $x \leftrightarrow C$, так как C входит в U; во-вторых, $x \leftrightarrow A_j$ и $x \leftrightarrow B_j$ при $j < i$, так как слова A_j и B_j входят в U при $j < i$; в-третьих, $x \leftrightarrow A_j$ при $j > i+1$ и $x \leftrightarrow B_j$ при $j > i$, так как x входит в слово A_i.

В итоге видим, что $\overline{A}$ удовлетворяет условию $Q(m)$ и имеет меньшую длину, чем A, что противоречит условию выбора слова A.

Случай 1.2. Буква x содержится в одном из слов B_i, $1 \leq i < m$. Тогда из условия $x \leftrightarrow U$ следует, что x^{-1} содержится в слове B_i^{-1}, причем вхождения x в B_i и x^{-1} в B_i^{-1} являются парными (см. рассуждения, проведенные при рассмотрении предыдущего случая). Следовательно, $B_i \equiv B'_i x B''_i$, а $U \equiv B''_i A_i \ldots A_1 C A_1 \ldots A_i (B''_i)^{-1}$. Теперь подставим выражение для B_i в A, сократим через слово U пару букв x, x^{-1} и обозначим $B'_i B''_i$ через $\overline{B}_i$. Тогда получим, что A равно в группе G слову $\overline{A} \equiv v(A_1, B_1, \ldots, A_i, \overline{B_i}, \ldots, A_m, C)$. Поскольку в $\overline{B_i}$ состав букв не увеличился по сравнению с B_i, а остальные слова не изменились, то $\overline{A}$ удовлетворяет условию $Q(m)$. Так как $\overline{A}$ короче, чем A, мы опять получили противоречие с выбором слова A.

Случай 1.3. Буква x содержится в слове C. Пусть x^{-1} содержится в одном из слов вида A_i или B_i^{-1} во второй половине слова A. Заметим, что условие $Q(m)$ инвариантно относительно операции, заключающейся в переносе слова C^{-1} из конца в начало и последующей замене получившегося слова обратным. Если мы применим эту операцию в данном случае, то получим слово, в котором подслово xUx^{-1} находится целиком в первой половине. Этот случай будет рассмотрен ниже.

Пусть теперь x^{-1} содержится в слове C^{-1}. Тогда, как и выше, из условия $x \leftrightarrow U$ вытекает, что вхождения x в C и x^{-1} в C^{-1} являются парными. Поэтому $C \equiv C'xC''$, $U \equiv C''A_1 \ldots A_m (C'')^{-1}$. Теперь мы можем подставить выражение для C в слово A, сократить буквы x и x^{-1} через слово U, обозначить $C'C''$ через $\overline{C}$ и получить противоречие с выбором A.

Все три подслучая рассмотрены.

II. Перейдем к рассмотрению случаев, когда xUx^{-1} целиком содержится в первой половине слова A.

Легко видеть, что слово xUx^{-1} не может содержаться целиком ни в одном из слов вида A_i, B_i или C. В противном случае мы можем заменить в нем подслово xUx^{-1} на U, не увеличивая состава букв, и перейти от $A \equiv v(A_1, B_1, \ldots, B_{m-1}, A_m, C)$ к более короткому слову вида $Q(m)$, равному A в G.

Итак, можно считать, что буквы x и x^{-1} содержатся в разных словах-сомножителях, составляющих A. Возможны следующие ситуации.

1. Буква x содержится в слове A_k, буква x^{-1} содержится в слове A_j, причем $k > j$.

2. Буква x содержится в слове A_k, буква x^{-1} содержится в слове B_j, причем $k > j$.

3. Буква x содержится в слове A_m, буква x^{-1} содержится в слове C.

4. Буква x содержится в слове A_k при $1 \le k < m$, буква x^{-1} содержится в слове C.

5. Буква x содержится в слове B_k, буква x^{-1} содержится в слове A_j, причем $k \ge j$.

6. Буква x содержится в слове B_k, буква x^{-1} содержится в слове B_j, причем $k > j$.

7. Буква x содержится в слове B_k, буква x^{-1} содержится в слове C.

В каждом из этих случаев получим противоречие с выбором A и в итоге придем к выводу, что слово A циклически приведено.

Случай 2.1. Пусть x содержится в A_k, x^{-1} содержится в A_j, причем $1 \le j < k \le m$. Поскольку из условия $Q(m)$ следует, что $A_j \leftrightarrow A_k$ при $|k-j| \ge 2$, остается единственный возможный случай, когда $k = j+1$. Положим $A_j \equiv A'_j x^{-1} A''_j$, $A_{j+1} \equiv A'_{j+1} x A''_{j+1}$, $U \equiv A''_{j+1} B_j A'_j$. В частности, $A''_{j+1} \leftrightarrow x^{-1}$, $A'_j \leftrightarrow x$. Тогда мы можем заменить в слове $v(A_1, B_1, \ldots, B_{m-1}, A_m, C)$ слово A_{j+1} на $A'_{j+1} A''_{j+1} x$, а слово A_j — на $x^{-1} A'_j A''_j$. Новые слова будут иметь такую же длину и будут удовлетворять условию $Q(m)$ ввиду неизменности состава букв. Поэтому можно считать, что первая буква слова xUx^{-1} является последней буквой слова A_{j+1}, а последняя буква слова xUx^{-1} — первой буквой слова A_j, причем x побуквенно коммутирует с $U \equiv B_j$. Аналогичный прием мы будем использовать и при рассмотрении оставшихся случаев.

С учетом вышеизложенного можно ввести переобозначения и считать, что $A_j \equiv x^{-1} A'_j$, $A_{j+1} \equiv A'_{j+1} x$, $U \equiv B_j$. Тогда

$$A \equiv A_m \ldots A'_{j+1} x B_j x^{-1} A'_j \ldots A_1 C A_1 \ldots B_{j-1}^{-1} x^{-1} A'_j B_j^{-1} A'_{j+1} x B_{j+1}^{-1} \ldots A_m C^{-1}.$$

Сократим вхождения букв x и x^{-1} (через слово U) в первой половине слова A. Заметим, что $x \leftrightarrow A_i$ и $x \leftrightarrow B_i$ при $1 \le i < j$, так как x входит в слово A_{j+1}; $x \leftrightarrow A_i$ при $j+1 < i \le m$ и $x \leftrightarrow B_i$ при $j+1 \le i < m$, так как x^{-1} входит в слово A_j; $x \leftrightarrow B_j$, так как $B_j \equiv U$. Теперь воспользуемся перестановочностью буквы x со словами, перечисленными выше, и получим, что A равно в G слову

$$A_m \ldots A'_{j+1} B_j A'_j \ldots A_1 C x^{-1} A_1 \ldots A'_j B_j^{-1} A'_{j+1} \ldots A_m x C^{-1}.$$

Обозначим Cx^{-1} через C'. Тогда A равно в G слову

$$A' \equiv v(A_1, \ldots, A'_j, B_j, A'_{j+1}, \ldots, A_m, C').$$

Докажем, что A' удовлетворяет условию $Q(m)$. Поскольку в словах A'_j и A'_{j+1} набор букв не увеличился по сравнению с A_j и A_{j+1}, а остальные слова, кроме C', не изменились, условия побуквенной коммутативности достаточно проверить только для слова C'. Но $C' \equiv Cx^{-1}$ и каждое из слов C и x^{-1} побуквенно коммутирует с каждым из слов B_i, $1 \le i < m$. Поэтому и для слова C' условия побуквенной коммутативности выполнены. Следовательно, A' удовлетворяет условию $Q(m)$ и имеет меньшую длину, чем A, что противоречит выбору A.

Случай 2.2. Пусть буква x содержится в A_k, а буква x^{-1} содержится в B_j, причем $1 \le j < k \le m$.

Из условия $Q(m)$ следует, что $A_k \leftrightarrow B_j$ при $k \ne j$ и $k \ne j+1$, тем самым остается единственный возможный случай, когда $k = j+1$. Без ограничения общности можно считать, что $A_{j+1} \equiv A'_{j+1} x$, $B_j \equiv x^{-1} B'_j$, $U \equiv 1$ (см. прием, примененный при разборе предыдущего случая). Заметим, что x как подслово

B_j побуквенно коммутирует со словами A_i при $i \neq j, j+1$, B_i при $i \neq j$, а также со словом C. Подставив выражения для A_{j+1} и B_j, получим, что

$$A \equiv A_m \dots A'_{j+1}xx^{-1}B'_j \dots A_1CA_1 \dots A_j(B'_j)^{-1}xA'_{j+1}xB^{-1}_{j+1} \dots A_mC^{-1}.$$

Теперь сократим пару x и x^{-1} в первой половине слова. Далее, пользуясь коммутативностью для x, переместим букву x, находящуюся в правой половине слова после A'_{j+1} в конец слова. Затем, применяя циклический сдвиг, перенесем x в начало слова и, снова пользуясь коммутативностью, переставим x со словом $A_m \dots B_{j+1}$. Тогда A сопряжено в G слову

$$A_m \dots B_{j+1}xA'_{j+1}B'_j \dots A_1CA_1 \dots (B'_j)^{-1}xA'_{j+1} \dots A_mC^{-1}.$$

Обозначим xA'_{j+1} через A''_{j+1} и получим, что A сопряжено в G слову $A' \equiv v(A_1, \dots, B'_j, A''_{j+1}, \dots, A_m, C)$. Слово A', очевидно, удовлетворяет условию $Q(m)$ и имеет меньшую длину, чем A, что противоречит выбору A.

Случай 2.3. Пусть буква x содержится в A_m, а буква x^{-1} содержится в C. Тогда, как и выше, полагаем $A_m \equiv A'_mx$, $C \equiv x^{-1}C'$. При этом U будет подсловом в A, начинающимся словом B_{m-1} и оканчивающимся словом A_1. Подставив выражения для A_m и C в слово A, получим

$$A \equiv A'_mxB_{m-1} \dots A_1x^{-1}C'A_1 \dots B^{-1}_{m-1}A'_mx(C')^{-1}x.$$

Сократим вхождения букв x и x^{-1} (через слово U) в первой половине слова A. Теперь применим циклический сдвиг и перенесем букву x из конца в начало слова. Обозначив x через A_{m+1}, получим, что A сопряжено в G слову $A' \equiv v(A_1, B_1, \dots, B_{m-1}, A'_m, 1, A_{m+1}, C')$. Докажем, что A' удовлетворяет условию $Q(m+1)$. Для всех слов, кроме A_{m+1}, требуемые условия побуквенной коммутативности выполняются очевидным образом. Поскольку все слова A_i, B_i при $1 \leq i < m$ входят в U, они побуквенно коммутируют со словом $A_{m+1} \equiv x$. Это означает, что необходимые условия побуквенной коммутативности выполнены и для слова A_{m+1}. Поэтому слово A' удовлетворяет условию $Q(m+1)$ и имеет меньшую длину, чем A, что противоречит выбору A.

Случай 2.4. Пусть буква x содержится в A_k, $1 \leq k < m$, а буква x^{-1} — в C. Без ограничения общности можно считать, что $A_k \equiv A'_kx$, $C \equiv x^{-1}C'$, $U \equiv B_{k-1} \dots A_1$. Заметим, что x^{-1} входит в C, поэтому $x \leftrightarrow B_i$ при всех $1 \leq i < m$. Так как x входит в A_k, то $x \leftrightarrow A_i$ при $i \neq k-1, k, k+1$. Поскольку A_{k-1} входит в U, то x побуквенно коммутирует и с A_{k-1}.

Подставим выражения для A_k и C в слово A, сокращая x и x^{-1} в первой половине слова. Тогда A равно в G слову

$$A_m \dots A_{k+1}B_kA'_k \dots A_1C'A_1 \dots A'_kxB^{-1}_kA_{k+1} \dots A_m(C')^{-1}x.$$

Пользуясь коммутативностью, переставим x и B^{-1}_k, затем перенесем последнюю букву x в начало слова и, вновь пользуясь коммутативностью, переставим x со словом $A_m \dots B_{k+1}$ (при $k < m-1$). Получим, что A сопряжено в G слову

$$A_m \dots xA_{k+1}B_kA'_k \dots A_1C'A_1 \dots A'_kB^{-1}_kxA_{k+1} \dots A_m(C')^{-1}.$$

Вводя обозначение $A'_{k+1} \equiv xA_{k+1}$, замечаем, что A сопряжено в G слову $A' \equiv v(A_1, B_1, \dots, A'_k, B_k, A'_{k+1}, \dots, A_m, C)$. Установим, что A' удовлетворяет условию $Q(m)$. Достаточно проверить условия побуквенной коммутативности, относящиеся к A'_{k+1}. Поскольку $A'_{k+1} \equiv A_{k+1}x$, достаточно воспользоваться побуквенной перестановочностью x со всеми словами A_i при $i \neq k, k+1$ и B_i

при всех $1 \le i < m$. Следовательно, A' удовлетворяет условию $Q(m)$ и имеет меньшую длину, чем A, что противоречит выбору A.

Случай 2.5. Пусть буква x содержится в B_k, а буква x^{-1} — в A_j, причем $1 \le j \le k \le m$. Перейдем от слова A к его циклическому сдвигу, начинающемуся с C, а затем полученное слово заменим обратным ему. Условие $Q(m)$ инвариантно относительно такой замены, и этот случай сводится к случаю 2.2.

Случай 2.6. Пусть буква x содержится в B_k, а буква x^{-1} содержится в B_j, причем $1 \le j < k \le m$. Поскольку $B_k \leftrightarrow B_j$ при $k \ne j$, этот случай невозможен.

Случай 2.7. Пусть буква x содержится в B_k, буква x^{-1} содержится в C, причем $1 \le k < m$. Поскольку $B_k \leftrightarrow C$, этот случай также невозможен.

Все случаи рассмотрены.

Осталось доказать, что в формулировке теоремы слова A_i $(1 \le i \le m)$ можно дополнительно считать непустыми.

Предположим, что слово $A \equiv v(A_1, B_1, \ldots, B_{m-1}, A_m, C)$ удовлетворяет условию $Q(m)$. Допустим, что A_m пусто. Тогда

$$A \equiv B_{m-1}A_{m-1}\ldots A_1CA_1\ldots A_{m-1}B_{m-1}^{-1}C^{-1}.$$

Мы можем, перейдя к сопряженному слову, перенести B_{m-1} из начала слова в конец, а далее, пользуясь тем, что $B_{m-1} \leftrightarrow C$, сократить слова B_{m-1}^{-1} и B_{m-1} (через слово C^{-1}). После этого получим, что в группе G слово A сопряжено слову $A' \equiv v(A_1, B_1, \ldots, B_{m-2}, A_{m-1}, C)$. Слово A', очевидно, удовлетворяет условию $Q(m-1)$.

Пусть теперь слово A_i пусто для некоторого $1 < i < m$. Тогда

$$A \equiv A_m \ldots B_iB_{i-1}\ldots A_1CA_1\ldots B_{i-1}^{-1}B_i^{-1}\ldots A_mC^{-1}.$$

Тем самым $A \equiv v(A_1, B_1, \ldots, A_{i-1}, B'_{i-1}, A_{i+1}, B_{i+1}, \ldots, A_m, C)$, где через B'_{i-1} обозначено B_iB_{i-1}. Значит, то же слово A удовлетворяет и условию $Q(m-1)$ (при другом разбиении на сомножители).

Пусть пусто слово A_1. Тогда $A \equiv A_m \ldots A_2B_1CB_1^{-1}A_2\ldots A_mC^{-1}$. Мы можем, пользуясь тем, что $B_1 \leftrightarrow C$, сократить слова B_1 и B_1^{-1} через слово C. После этого получим, что A равно в G слову $A' \equiv v(A_2, B_2, \ldots, B_{m-1}, A_m, C)$. Слово A', очевидно, удовлетворяет условию $Q(m-1)$.

В итоге, если нам дано слово, удовлетворяющее условию $Q(m)$, то мы можем найти сопряженное ему в G слово A, удовлетворяющее условию $Q(m')$ при каком-то $m' \le m$, в котором слова A_i для всех $1 \le i \le m'$ являются непустыми.

Теорема доказана.

Следствие 1. *Для любой конечно-порожденной частично-коммутативной группы G существует алгоритм, позволяющий определить, является ли данное слово в G произведением двух квадратов.*

Доказательство. Действительно, по данному слову можно эффективно найти некоторую его циклически приведенную форму. После этого можно выписать все его циклически приведенные формы в силу леммы 2. Исходное слово является произведением квадратов в G тогда и только тогда, когда хотя бы одна из полученных циклически приведенных форм удовлетворяет условию $Q(m)$ при каком-либо m. Ввиду непустоты слов $A_1, \ldots, A_m$ из условия теоремы 1 значение m ограничено сверху длиной исходного слова. Для заданных слова и значения m проверка выполнимости условия $Q(m)$ эффективна.

Покажем, как результат Уикса для свободных групп [11] вытекает из нашего описания. Заметим, что в свободной группе условие $U \leftrightarrow V$ имеет место тогда и только тогда, когда хотя бы одно из слов U, V пусто. Поэтому если слово $A \equiv v(A_1, B_1, \ldots, B_{m-1}, A_m, C)$ удовлетворяет условию $Q(m)$, то ввиду непустоты слов $A_1, \ldots, A_m$ и того, что $A_i \leftrightarrow A_j$ при $|j - i| > 1$, сразу вытекает $m \leq 2$. При $m = 2$ имеем $A \equiv A_2 B_1 A_1 C A_1 B_1^{-1} A_2 C^{-1}$. Далее, из условия $B_1 \leftrightarrow C$ следует, что $B_1 \equiv 1$ или $C \equiv 1$. В первом случае мы получаем слово $A_2 A_1 C A_1 A_2 C^{-1}$, а во втором — слово $A_2 B_1 A_1 A_1 B_1^{-1} A_2$. Таким образом, с точностью до циклического сдвига получается одна из двух форм: $XYZYXZ^{-1}$ или $XYZZY^{-1}X$. (При $m = 1$ имеем частный случай первой из форм.) Таким образом, обе формы Уикса для произведения двух квадратов в свободной группе автоматически получаются из нашего описания.

Автор выражает признательность В. С. Губе за постановку задачи и помощь при проведении исследований.

ЛИТЕРАТУРА

1. *Шестаков С. Л.* Уравнение $[x, y] = g$ в частично-коммутативных группах // Сиб. мат. журн. 2005. Т. 46, № 2. С. 466–477.
2. *Cartier P., Foata D.* Problémes combinatoires de commutation et de réarrangements. Berlin; Heidelberg; New York: Springer, 1969 (Lecture Notes in Math.; 85).
3. *Servatius H.* Automorphisms of graph groups // J. Algebra. 1989. V. 126, N 1. P. 34–60.
4. *Baudisch A.* Subgroups of semifree groups // Acta Math. Acad. Sci. Hungar. 1981. V. 38, N 1–4. P. 19–28.
5. *Duchamp G., Krob D.* The lower central ceries of the free partially commutative group // Semigroup Forum. 1992. V. 45. P. 385–394.
6. *Михайлова К. А.* Проблема вхождения для прямых произведений групп // Докл. АН СССР. 1958. Т. 119. С. 1103–1105.
7. *Servatius H., Droms C., Servatius B.* Surface subgroups of graph groups // Proc. Amer. Math. Soc. 1989. V. 106, N 3. P. 573–578.
8. *Wicks M. J.* Commutators in free products // J. London Math. Soc. 1962. V. 37. P. 433–444.
9. *Vdovina. A.* Constructing orientable Wicks forms and estimation of their numbers // Comm. Algebra. 1995. V. 23, N 9. P. 3205–3222.
10. *Линдон Р., Шупп П.* Комбинаторная теория групп. М.: Наука, 1980.
11. *Wicks M. J.* The equation $x^2 y^2 = g$ over free products // Proc. Cong. Singapore Nat. Acad. Sci. 1971. P. 238–248.

Статья поступила 13 апреля 2005 г.

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