Math-Net.Ru

Общероссийский математический портал

В. Г. Дурнев, К проблеме разрешимости уравнений с одним коэффициентом, *Матем. заметки*, 1996, том 59, выпуск 6, 832–845

DOI: <https://doi.org/10.4213/mzm1782>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.82.47.9

26 апреля 2023 г., 11:58:53

К ПРОБЛЕМЕ РАЗРЕШИМОСТИ УРАВНЕНИЙ С ОДНИМ КОЭФФИЦИЕНТОМ

В. Г. Дурнев

В этой заметке рассматривается проблема разрешимости для уравнений с одним коэффициентом в группе G , т.е. для уравнений вида

$$w(x_1, \dots, x_n) = g, \quad (1)$$

где $w(x_1, \dots, x_n)$ – групповое слово в алфавите неизвестных $\{x_1, \dots, x_n, \dots\}$, а g – коэффициент, т.е. элемент группы G .

Конечно, рассматриваемая для группы G проблема – это частный случай общей проблемы разрешимости в G уравнений и их систем. Уравнения вида (1) в некоторых работах называются *уравнениями с правой частью* или *уравнениями, разрешенными относительно неизвестных*.

Проблема эндоморфной сводимости для свободной в некотором многообразии группы, состоящая в определении по двум произвольным элементам g и h группы G существует ли такой эндоморфизм φ этой группы, что $\varphi(g) = h$, очевидным образом сводится к проблеме разрешимости в группе G уравнений вида (1).

Проблема эндоморфной сводимости для свободной группы исследовалась в ряде работ К. Эдмундса, например, [1].

Проблема разрешимости уравнений с одним коэффициентом изучалась, прежде всего, для свободных групп [1]–[4], ее разрешимость, конечно, теперь следует из доказанной Г.С. Маканиным [5] алгоритмической разрешимости проблемы совместности для систем уравнений в свободных группах.

Проблема разрешимости уравнений вида (1) для свободных нильпотентных групп изучалась в работах [6]–[8], где доказана ее неразрешимость даже для нильпотентных групп небольшой степени.

В первой половине настоящей заметки доказывается, что проблема разрешимости уравнений с одним коэффициентом в свободной нециклической группе является NP-трудной, т.е. к ней полиномиально сводима любая задача из класса NP [9] и, более того, общая проблема разрешимости систем

Работа выполнена при частичной поддержке Международного научного фонда, грант MUV000.

уравнений в свободной группе F_n ранга $n \geq 2$ полиномиально сводится к проблеме разрешимости уравнений с одним коэффициентом в свободной группе F_n ранга $m = 2[(n+1)/2]$, а проблема разрешимости уравнений в группе F_n даже линейно сводится к проблеме разрешимости уравнений с одним коэффициентом в группе F_m .

Во второй половине заметки доказывается, что проблема разрешимости уравнений вида (1) в свободной полугруппе является NP-полной.

Пусть F_n — это свободная группа ранга n со свободными образующими $a_1, \dots, a_n$. Через $[u, v]$ будем обозначать коммутатор элементов u, v группы F_n , при этом $[u, v] = uvu^{-1}v^{-1}$.

Докажем ряд вспомогательных лемм, представляющих, впрочем, и определенный самостоятельный интерес.

ЛЕММА 1. *Если H — подгруппа свободной группы F_m ранга m со свободными образующими $a_1, \dots, a_m$, $m \geq 2n$, и*

$$[a_1, a_2] \cdots [a_{2n-1}, a_{2n}] \in H',$$

где H' — коммутант группы H , то $a_1, \dots, a_{2n} \in H$.

ДОКАЗАТЕЛЬСТВО. Для доказательства воспользуемся свободным дифференциальным исчислением Фокса для группового кольца $l[F_m]$ [10].

Пусть u, v — элементы группы F_m , непосредственные вычисления дают равенство

$$\frac{\partial[u, v]}{\partial a_i} = (1 - [u, v]v) \frac{\partial u}{\partial a_i} + (u - [u, v]) \frac{\partial v}{\partial a_i}.$$

Индукцией по k покажем, что при любом i для любых элементов $x_1, y_1, \dots, x_k, y_k$ группы F_m найдутся такие $\alpha_1, \dots, \alpha_{2k}$ в $l[F_m]$ и $v_1, \dots, v_{2k} \in \text{gr}(x_1, y_1, \dots, x_k, y_k)$, что

$$\frac{\partial[x_1, y_1] \cdots [x_k, y_k]}{\partial a_i} = (1 - v_1)\alpha_1 + \cdots + (1 - v_{2k})\alpha_{2k},$$

где $\text{gr}(x_1, y_1, \dots, x_k, y_k)$ — подгруппа, порожденная элементами $x_1, y_1, \dots, x_k, y_k$.

При $k = 1$ имеем

$$\frac{\partial[x_1, y_1]}{\partial a_i} = (1 - [x_1, y_1]y_1) \frac{\partial x_1}{\partial a_i} + (x_1 - [x_1, y_1]) \frac{\partial y_1}{\partial a_i} = (1 - v_1)\alpha_1 + (1 - v_2)\alpha_2,$$

где $v_1 = [x_1, y_1]y_1$, $v_2 = [x_1, y_1]x_1^{-1}$, $\alpha_1 = \partial x_1 / \partial a_i$, $\alpha_2 = x_1(\partial y_1 / \partial a_i)$.

Предположим, что выполняется равенство

$$\frac{\partial[x_1, y_1] \cdots [x_k, y_k]}{\partial a_i} = (1 - v_1)\alpha_1 + \cdots + (1 - v_{2k})\alpha_{2k},$$

где $v_1, \dots, v_{2k} \in \text{gr}(x_1, y_1, \dots, x_k, y_k)$, $\alpha_1, \dots, \alpha_{2k} \in \mathbb{Z}[F_m]$.

Тогда, воспользовавшись формулой Лейбница для свободных дифференцирований: для любых u, v из F_m

$$\frac{\partial uv}{\partial a_i} = \frac{\partial u}{\partial a_i} + u \frac{\partial v}{\partial a_i},$$

получим следующие равенства, в которых w — это $[x_1, y_1] \cdots [x_k, y_k]$:

$$\begin{aligned} \frac{\partial [x_1, y_1] \cdots [x_{k+1}, y_{k+1}]}{\partial a_i} &= \frac{\partial [x_1, y_1] \cdots [x_k, y_k]}{\partial a_i} + w \frac{\partial [x_{k+1}, y_{k+1}]}{\partial a_i} \\ &= (1 - v_1)\alpha_1 + \cdots + (1 - v_{2k})\alpha_{2k} + w[(1 - u)\alpha + (1 - v)\beta] \\ &= (1 - v_1)\alpha_1 + \cdots + (1 - v_{2k})\alpha_{2k} \\ &\quad + (1 - v_{2k+1})\alpha_{2k+1} + (1 - v_{2k+2})\alpha_{2k+2}, \end{aligned}$$

где $\partial[x_{k+1}, y_{k+1}]/(\partial a_i) = (1 - u)\alpha + (1 - v)\beta$; $\alpha, \beta \in l[F_m]$,

$$\begin{aligned} u, v \in \text{gr}(x_{k+1}, y_{k+1}), \quad v_{2k+1} = wuw^{-1}, \quad v_{2k+2} = wvw^{-1}, \\ \alpha_{2k+1} = w\alpha, \quad \alpha_{2k+2} = w\beta. \end{aligned}$$

Тогда нетрудно понять, что

$$v_1, \dots, v_{2k}, v_{2k+1}, v_{2k+2} \in \text{gr}(x_1, y_1, \dots, x_k, y_k, x_{k+1}, y_{k+1}).$$

Завершим доказательство леммы индукцией по n .

Если при $n = 1$ для некоторых $x_1, y_1, \dots, x_m, y_m$ из H выполняется равенство $[a_1, a_2] = [x_1, y_1] \cdots [x_m, y_m]$, то, так как

$$\frac{\partial [a_1, a_2]}{\partial a_1} = 1 - [a_1, a_2]a_2, \quad \frac{\partial [a_1, a_2]}{\partial a_2} = a_1 - [a_1, a_2],$$

получим равенства

$$\begin{aligned} 1 - [a_1, a_2]a_2 &= (1 - v_1)\alpha_1 + \cdots + (1 - v_{2m})\alpha_{2m}, \\ a_1 - [a_1, a_2] &= (1 - u_1)\beta_1 + \cdots + (1 - u_{2m})\beta_{2m}, \end{aligned}$$

где $v_1, \dots, v_{2m}, u_1, \dots, u_{2m} \in \text{gr}(x_1, y_1, \dots, x_m, y_m) \subseteq H$.

Тогда по лемме 4.1 из работы [11] из этих двух равенств следует, что

$$[a_1, a_2]a_2 \in H \quad \text{и} \quad [a_1, a_2]a_1^{-1} \in H.$$

Отсюда легко получить, что $a_1, a_2 \in H$.

Переход от n к $n + 1$ осуществляется следующим образом.

Пусть при некотором m в H найдутся такие элементы $x_1, y_1, \dots, x_m, y_m$, что

$$[a_1, a_2] \cdots [a_{2n+1}, a_{2n+2}] = [x_1, y_1] \cdots [x_m, y_m].$$

Так как при $i = 1, 2$

$$\frac{\partial[a_3, a_4] \cdots [a_{2n+1}, a_{2n+2}]}{\partial a_i} = 0,$$

то получаем равенства

$$\begin{aligned} 1 - [a_1, a_2]a_2 &= (1 - v_1)\alpha_1 + \cdots + (1 - v_{2m})\alpha_{2m}, \\ a_1 - [a_1, a_2] &= (1 - u_1)\beta_1 + \cdots + (1 - u_{2m})\beta_{2m}, \end{aligned}$$

где $v_1, u_1, \dots, v_{2m}, u_{2m} \in H$.

Выше уже было показано, что эти равенства влекут $a_1, a_2 \in H$.

Значит, $[a_3, a_4] \cdots [a_{2n+1}, a_{2n+2}] \in H'$, тогда по индуктивному предположению $a_3, a_4, \dots, a_{2n+1}, a_{2n+2} \in H$.

Это завершает доказательство леммы 1.

СЛЕДСТВИЕ 1 (А.И. Мальцев [12]). *Если в свободной группе F_2 со свободными образующими a_1, a_2 выполняется равенство $[a_1, a_2] = [x, y]$, то x, y – свободные образующие группы F_2 .*

СЛЕДСТВИЕ 2 (Г. Зайшанг [13]). *Если элементы $g_1, \dots, g_{2n}$ свободной группы F_{2n} ранга $2n$ со свободными образующими $a_1, \dots, a_{2n}$ удовлетворяют равенству*

$$[g_1, g_2] \cdots [g_{2n-1}, g_{2n}] = [a_1, a_2] \cdots [a_{2n-1}, a_{2n}],$$

то $g_1, \dots, g_{2n}$ – свободные образующие группы F_{2n} .

ЛЕММА 2. *При $m \geq 2$ в свободной группе F_k ранга k со свободными образующими $a_1, \dots, a_{2n}$ ($k \geq 2n$) уравнение*

$$([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^m = [x_1, x_2] \cdots [x_{2n-1}, x_{2n}]$$

не имеет решений.

ДОКАЗАТЕЛЬСТВО. Предположим противное. Пусть при некотором $m \geq 2$ в группе F_k найдутся такие элементы $g_1, \dots, g_{2n}$, что

$$([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^m = [g_1, g_2] \cdots [g_{2n-1}, g_{2n}].$$

Обозначим через φ гомоморфизм группы F_k на группу F_2 , заданный равенствами $\varphi(a_i) = a_1$ при нечетном i и $\varphi(a_i) = a_2$ при четном i .

Тогда в группе F_2 выполняется равенство

$$[a_1, a_2]^{nm} = [\varphi(g_1), \varphi(g_2)] \cdots [\varphi(g_{2n-1}), \varphi(g_{2n})].$$

В работе [14] доказано, что если в группе F_2 выполняется равенство

$$[a_1, a_2]^k = [h_1, h_2] \cdots [h_{2t-1}, h_{2t}],$$

то $t \geq [k/2] + 1$.

Поэтому получаем неравенство $n \geq [nm/2] + 1$.

Но при $m \geq 2$ $[nm/2] + 1 \geq n + 1$.

Полученное противоречие завершает доказательство леммы 2.

ЛЕММА 3. В группе F_{2n} имеет место эквивалентность

$$w = 1 \& [u_1, u_2] \cdots [u_{2n-1}, u_{2n}] = [a_1, a_2] \cdots [a_{2n-1}, a_{2n}] \\ \iff w^8 \cdot ([u_1, u_2] \cdots [u_{2n-1}, u_{2n}])^2 = ([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^2.$$

ДОКАЗАТЕЛЬСТВО. Если

$$w^8 ([u_1, u_2] \cdots [u_{2n-1}, u_{2n}])^2 = ([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^2,$$

то по теореме Линдона–Шенкмана–Шютценбергера–Баумелага [15]–[17] $w, [u_1, u_2] \cdots [u_{2n-1}, u_{2n}], [a_1, a_2] \cdots [a_{2n-1}, a_{2n}]$ – степени одного и того же элемента g группы F_{2n} .

Пусть

$$[a_1, a_2] \cdots [a_{2n-1}, a_{2n}] = g^t, \\ [u_1, u_2] \cdots [u_{2n-1}, u_{2n}] = g^s.$$

Легко понять, $|t| = 1$, поэтому

$$[u_1, u_2] \cdots [u_{2n-1}, u_{2n}] = ([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^p$$

для некоторого p .

В силу леммы 2 $|p| \leq 1$.

Если $p = 0$, то

$$w^8 = ([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^2, \quad w^4 = [a_1, a_2] \cdots [a_{2n-1}, a_{2n}],$$

что также невозможно.

Если $p = -1$, то

$$w^8 = ([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^4, \quad w^2 = [a_1, a_2] \cdots [a_{2n-1}, a_{2n}],$$

что невозможно.

Поэтому $p = 1$, а значит

$$[u_1, u_2] \cdots [u_{2n-1}, u_{2n}] = [a_1, a_2] \cdots [a_{2n-1}, a_{2n}]$$

и $w = 1$.

Обратное очевидно.

Естественно считать *размером входа* в задаче разрешимости систем уравнений в свободной группе F_n общее число букв, входящих в запись этой системы.

ТЕОРЕМА 1. Проблема разрешимости уравнений в группе F_n ($n \geq 2$) линейно сводится к проблеме разрешимости уравнений с одним коэффициентом в этой группе, а проблема разрешимости систем уравнений в группе F_n полиномиально сводима к проблеме разрешимости уравнений с одним коэффициентом в этой группе.

ДОКАЗАТЕЛЬСТВО. Рассмотрим уравнение

$$w(x_1, \dots, x_m, a_1, \dots, a_k) = 1 \quad (2)$$

в группе F_k .

Переходя, в случае необходимости, от группы F_k к группе F_{k+1} , мы можем считать, что $k = 2n$.

Покажем, что уравнение (2) имеет решение в группе F_{2n} тогда и только тогда, когда в этой группе имеет решение система уравнений

$$\begin{aligned} w(x_1, \dots, x_m, u_1, \dots, u_{2n}) &= 1 \& [u_1, u_2] \cdots [u_{2n-1}, u_{2n}] \\ &= [a_1, a_2] \cdots [a_{2n-1}, a_{2n}]. \end{aligned} \quad (3)$$

В самом деле, если уравнение (2) имеет решение $g_1, \dots, g_m$, то система уравнений (3) имеет решение $g_1, \dots, g_m, a_1, \dots, a_{2n}$.

Обратно, пусть $g_1, \dots, g_m, u_1, \dots, u_{2n}$ — решение системы уравнений (3).

Тогда по следствию 2 леммы 1 $u_1, \dots, u_{2n}$ — свободные образующие группы F_{2n} , поэтому существует такой автоморфизм φ группы F_n , что $\varphi(u_i) = a_i$ ($i = 1, \dots, 2n$).

Применяя к равенству $w(g_1, \dots, g_m, u_1, \dots, u_{2n}) = 1$ автоморфизм φ , мы получим равенство

$$w(\varphi(g_1), \dots, \varphi(g_m), a_1, \dots, a_{2n}) = 1,$$

т.е. уравнение (2) имеет решение.

По лемме 3 система (3) равносильна уравнению

$$w^8(\bar{x}, \bar{u})([u_1, u_2] \cdots [u_{2n-1}, u_{2n}])^2 = ([a_1, a_2] \cdots [a_{2n-1}, a_{2n}])^2,$$

что завершает доказательство первой части теоремы 1.

Покажем, что проблема разрешимости систем уравнений в группе F_n ($n \geq 2$) полиномиально сводима к вопросу о разрешимости одного уравнения.

Рассмотрим произвольную систему уравнений в группе F_n

$$\&_{i=1}^m w_i = 1. \quad (4)$$

Воспользуемся эквивалентностью А. И. Мальцева [12]

$$u_1 = 1 \& u_2 = 1 \iff u_1^2 a_1 u_1^2 a_1^{-1} (a_2 u_2 a_2^{-1} u_2)^2 = 1.$$

Через $|w|$ будем обозначать длину слова w , т.е. число букв в w , а через $|\&_{i=1}^m w_i = 1|$ — число $L = \sum_{i=1}^m |w_i|$ и называть это число размером системы (4).

Заметим, что

$$|u_1^2 a_1 u_1^2 a_1^{-1} (a_2 u_2 a_2^{-1} u_2)^2| = 4(|u_1| + |u_2|) + 6.$$

При замене конъюнкции $u_1 = 1 \& u_2 = 1 \& u_3 = 1$ одним ей равносильным равенством $u = 1$ можем считать, что

$$|u| \leq 2^5(|u_1| + |u_2| + |u_3|).$$

Сворачивая уравнения системы (4) парами или тройками (при нечетном m), мы по системе (4) получим систему (5)

$$\bigg\&_{i=1}^{k_1} w_i^{(1)} = 1, \quad (5)$$

причем

$$L_1 = \sum_{i=1}^{k_1} |w_i^{(1)}| \leq 2^5 \sum_{i=1}^m |w_i| = 2^5 L$$

и $k_1 \leq m/2$.

Поступая аналогичным образом, мы, не более чем за $\log_2 m$ шагов, получим одно уравнение $w = 1$, равносильное исходной системе (4), и при этом $|w| \leq 2^{5 \log_2 m} L$, т.е. $|w| \leq m^5 L \leq L^6$.

Это завершает доказательство теоремы 1.

ТЕОРЕМА 2. *Проблема разрешимости уровней с одним коэффициентом в группе F_2 является NP-трудной.*

ДОКАЗАТЕЛЬСТВО. Покажем, что к проблеме разрешимости уравнений с одним коэффициентом в группе F_2 полиномиально сводима задача 3-выполнимости (3-ВЫП-задача), являющаяся NP-полной задачей [19], [9].

Напомним, что 3-ВЫП-задача состоит в определении по формуле логики высказываний, находящейся в конъюнктивной нормальной форме, содержащей в каждом дизъюнкте ровно 3 литерала, является ли эта формула выполнимой.

Пусть формула Φ логики высказываний имеет вид

$$\bigg\&_{i=1}^m \bigvee_{j=1}^n X_j^{\varepsilon_{ij}},$$

где $\varepsilon_{ij} \in \{-1, 0, 1\}$, причем $X_j^1 \rightleftharpoons X_j$, X_j^0 — пустое слово, т.е. в этом случае литерал $X_j^{\varepsilon_{ij}}$ просто отсутствует, $X_j^{-1} \rightleftharpoons \overline{X_j}$.

Кроме того, при любом i ($1 \leq i \leq m$)

$$\sum_{j=1}^m |\varepsilon_{ij}| = 3.$$

По формуле Φ построим формулу Φ^*

$$\bigg\&_{i=1}^m \bigvee_{\varepsilon=1,2,3} \left(\prod_{j=1}^n v_{ij} = a_1^\varepsilon \right) \& \bigg\&_{j=1}^n (x_j = 1 \vee x_j = a_1),$$

где $v_{ij} \rightleftharpoons a_1 x_j^{-1}$ при $\varepsilon_{ij} = -1$, $v_{ij} \rightleftharpoons 1$ при $\varepsilon_{ij} = 0$, $v_{ij} \rightleftharpoons x_j$ при $\varepsilon_{ij} = 1$.

Нетрудно понять, что формула Φ выполнима тогда и только тогда, когда формула Φ^* истинна на группе F_2 .

Для удаления из формулы Φ^* знаков дизъюнкции и конъюнкции воспользуемся эквивалентностью Г. А. Гуревича [18]

$$(w_1 = 1 \vee w_2 = 1) \iff \&_{\varepsilon, \delta = \pm 1} [w_1 a_1^\varepsilon w_1 a_1^{-\varepsilon}, w_2 a_2^\delta w_2 a_2^{-\delta}] = 1$$

и уже использовавшейся нами в ходе доказательства теоремы 1 эквивалентностью А. И. Мальцева [16]

$$(u_1 = 1 \& u_2 = 1) \iff u_1^2 a_1 u_1^2 a_1^{-1} (a_2 u_2 a_2^{-1} u_2)^2 = 1.$$

Заметим, что

$$|u_1^2 a_1 u_1^2 a_1^{-1} (a_2 u_2 a_2^{-1} u_2)^2| = 4(|u_1| + |u_2|) + 6.$$

Поэтому, заменяя конъюнкцию равенств $u_1 = 1 \& u_2 = 1$ одним, ей равносильным, равенством $u = 1$, мы можем считать, что

$$|u| = 4(|u_1| + |u_2|) + 6 \leq 8(|u_1| + |u_2|).$$

Конъюнкцию

$$\&_{\varepsilon, \delta = \pm 1} [w_1 a_1^\varepsilon w_1 a_1^{-\varepsilon}, w_2 a_2^\delta w_2 a_2^{-\delta}] = 1$$

мы можем свернуть за два шага в одно, ей равносильное, равенство $w = 1$, при этом можно считать, что $|w| \leq 2^9(|w_1| + |w_2|)$.

Дизъюнкцию вида

$$(u_1 = 1 \vee u_2 = 1 \vee u_3 = 1)$$

мы можем заменить одним, ей равносильным, равенством $u = 1$, причем

$$|u| \leq 2^{18}(|u_1| + |u_2| + |u_3|).$$

В итоге по формуле Φ^* мы можем построить формулу Φ^{**} вида

$$\&_{i=1}^m w_i = 1 \& \&_{j=1}^n u_j = 1,$$

причем длина $|\Phi^{**}|$ записи формулы Φ^{**} удовлетворяет неравенству

$$|\Phi^{**}| \leq 2^{18} |\Phi^*|.$$

Для сворачивания конъюнкции

$$\&_{i=1}^m w_i = 1 \& \&_{j=1}^n u_j = 1$$

в одно равенство $w = 1$ поступаем как в доказательстве теоремы 1, при этом нам потребуется не более чем $\log_2(n + m)$ шагов, значит можно считать, что

$$|w| \leq 2^{5 \log_2(n+m)} L, \quad \text{где } L = \sum_{i=1}^m |w_i| + \sum_{j=1}^n |u_j|.$$

Окончательно получаем, что

$$|w| \leq 2^{18} (n + m)^5 |\Phi^*| \leq 2^{18} |\Phi^*|^6.$$

В итоге, применяя лемму 3, получаем, что формула Φ выполнима тогда и только тогда, когда уравнение

$$w^8(x_1, \dots, x_n, u_1, u_2)[u_1, u_2]^2 = [a_1, a_2]^2$$

имеет решение в группе F_2 .

Это завершает доказательство теоремы 2.

ЗАМЕЧАНИЕ. Очевидно, что утверждение теоремы 2 справедливо и для любой свободной группы F_n ранга $n \geq 2$.

В оставшейся части заметки рассмотрим вопрос о разрешимости в свободной полугруппе $\Pi_2 = \langle a, b \rangle$ уравнений вида

$$w(x_1, \dots, x_n) = g(a, b), \quad (6)$$

где $w(x_1, \dots, x_n)$ – слово в алфавите неизвестных $\{x_1, \dots, x_n, \dots\}$, а $g(a, b)$ – коэффициент, т.е. элемент полугруппы Π_2 .

Естественно считать *размером входа* в задаче разрешимости уравнения вида

$$w(x_1, \dots, x_n) = g(a, b)$$

число

$$L = |w(x_1, \dots, x_n)| + |g(a, b)|,$$

где $|A|$ – длина слова A .

Покажем, что рассматриваемая задача является NP-полной.

Начнем с доказательства некоторого аналога (по применению) леммы 3.

ЛЕММА 4. Если x, y, z – слова полугруппы $\Pi_2 = \langle a, b \rangle$, причем z – непустое слово и b^2 не является подсловом слова z^2 , то имеет место эквивалентность

$$x^2 y^2 \bar{z}^2 b^2 \iff x \bar{z} z y \bar{z} b.$$

ДОКАЗАТЕЛЬСТВО. Если $x\bar{z}$ и $y\bar{b}$, то $x^2y^2\bar{z}^2b^2$. Пусть $x^2y^2\bar{z}^2b^2$.

Слово y не может быть пустым, так как в противном случае $x^2\bar{z}^2b^2$, $|x| = |z| + |b| \geq 2$, поэтому для некоторого слова u выполнялось бы равенство $x\bar{u}ub^2$, а значит, равенство $z^2\bar{u}ub^2u$, которое противоречит условию леммы.

Предположение о том, что длина y не меньше 2 также ведет к противоречию, так как неравенство $|y| \geq 2$ влечет существование такого слова u , что $y\bar{u}ub^2$, а это, в свою очередь, привело бы к равенству $z^2\bar{x}^2ub^2u$, также противоречащему условию леммы.

Значит, $|y| = 1$, поэтому $y\bar{b}$, $x\bar{z}$.

ТЕОРЕМА 3. Проблема разрешимости уравнений вида (1) в свободной полугруппе Π_2 является NP-полной.

ДОКАЗАТЕЛЬСТВО. Если $x_1^0, \dots, x_n^0$ – решение уравнения (1), то

$$|w(x_1^0, \dots, x_n^0)| = |g(a, b)| \leq L,$$

более того,

$$\sum_{i=1}^n |x_i^0| \leq L,$$

поэтому за линейное от L время мы можем убедиться в справедливости равенства $w(x_1^0, \dots, x_n^0)\bar{u}g(a, b)$, значит рассматриваемая задача лежит в классе NP.

Для доказательства ее NP-трудности покажем, как и в доказательстве теоремы 2, что к ней полиномиально сводима задача 3-выполнимости (3-ВЫП-задача).

Пусть формула Φ логики высказываний имеет вид

$$\&_{i=1}^m \bigvee_{j=1}^n X_j^{\varepsilon_{ij}},$$

где $\varepsilon_{ij} \in \{-1, 0, 1\}$, причем $X_j^1 \Rightarrow X_j$, X_j^0 – пустое слово, т.е. в этом случае литерал $X_j^{\varepsilon_{ij}}$ просто отсутствует, $X_j^{-1} \Rightarrow \bar{X}_j$. Кроме того, при любом i ($1 \leq i \leq m$)

$$\sum_{j=1}^n |\varepsilon_{ij}| = 3.$$

По формуле Φ построим систему Φ^* уравнений и неравенств

$$\&_{i=1}^m \sum_{j=1}^n |\varepsilon_{ij}| x_j^{\varepsilon_{ij}} \geq 1 \&_{j=1}^n x_j + x_j^{-1} = 1.$$

Заметим, что каждая сумма $\sum_{j=1}^n |\varepsilon_{ij}| x_j^{\varepsilon_{ij}}$ содержит ровно три слагаемых.

Нетрудно понять, что формула Φ выполнима тогда и только тогда, когда система Φ^* имеет решение в числах 0, 1 (значению *истинно* переменной X_j соответствует значение 1 переменной x_j , а значению *ложно* — значение 0).

Неравенство

$$\sum_{j=1}^n |\varepsilon_{ij}| x_j^{\varepsilon_{ij}} \geq 1$$

равносильно неравенству

$$3 - \sum_{j=1}^n |\varepsilon_{ij}| x_j^{\varepsilon_{ij}} \leq 2.$$

В свою очередь, последнее неравенство равносильно неравенству

$$\sum_{j=1}^n |\varepsilon_{ij}| (1 - x_j^{\varepsilon_{ij}}) \leq 2.$$

Поэтому система Φ^* имеет решение в числах 0, 1 тогда и только тогда, когда имеет решение в числах 0, 1 система Φ^{**}

$$\&_{i=1}^m \sum_{j=1}^n |\varepsilon_{ij}| x_j^{-\varepsilon_{ij}} \leq 2 \&_{j=1}^n x_j + x_j^{-1} = 1.$$

По системе Φ^{**} построим систему уравнений Ψ в полугруппе Π_2

$$\&_{i=1}^m \left(\prod_{j=1}^n (x_j^{-\varepsilon_{ij}})^{|\varepsilon_{ij}|} y_i = a^2 \right) \&_{j=1}^n x_j x_j^{-1} = a.$$

Нетрудно понять, что формула Φ выполнима тогда и только тогда, когда система Ψ имеет решение в Π_2 .

Заметим, что система Ψ равносильна в Π_2 уравнению

$$\begin{aligned} x_1 x_1^{-1} b \cdots b x_n x_n^{-1} b \prod_{j=1}^n (x_j^{-\varepsilon_{ij}})^{|\varepsilon_{ij}|} y_1 b \cdots b \prod_{j=1}^n (x_j^{-\varepsilon_{ij}})^{|\varepsilon_{ij}|} y_m \\ = ab \cdots b a b a^2 b \cdots b a^2, \end{aligned}$$

где слева и справа буква b имеет по $n + m - 1$ вхождений.

Обозначим левую часть последнего уравнения через $w(x_1, \dots, x_n, b)$, а правую — через $g(a, b)$.

Уравнение

$$w(x_1, \dots, x_n, b) = g(a, b)$$

имеет решение в Π_2 тогда и только тогда, когда в Π_2 разрешима система уравнений

$$w(x_1, \dots, x_n, y) = g(a, b) \& y = b,$$

а последняя система, в свою очередь, в силу леммы 4 равносильна уравнению

$$w^2(x_1, \dots, x_n, y)y^2 = g^2(a, b)b^2.$$

Итак, проблема 3-выполнимости для логики высказываний полиномиально сводима к проблеме разрешимости в Π_2 уравнений вида (6).

Это и завершает доказательство теоремы 3.

ЗАМЕЧАНИЕ 1. Конечно, теорема 3 справедлива и для любой полугруппы Π_n при $n \geq 2$.

ЗАМЕЧАНИЕ 2. Естественно рассмотреть и для полугруппы $\Pi_1 = \langle a \rangle$ вопрос о разрешимости уравнений вида

$$w(x_1, \dots, x_n) = g(a). \quad (7)$$

Легко понять, что вопрос о разрешимости в Π_1 уравнений вида (7) полиномиально сводится к решению в неотрицательных числах уравнения вида $c_1x_1 + \dots + c_nx_n = b$, где $c_1, \dots, c_n, b$ — неотрицательные целые числа, но размером последней задачи следует считать число

$$L = \sum_{i=1}^n c_i + b,$$

а не число

$$L_1 = \sum_{i=1}^n \lceil \log c_i \rceil + \lceil \log b \rceil,$$

как это обычно делается при исследовании вопросов о разрешимости в натуральных или целых числах линейных уравнений и их систем.

При этом естественно считать, что при любом i $0 < c_i \leq b$.

В [9] доказано, что при этих предположениях вопрос о разрешимости в неотрицательных целых числах уравнений вида

$$c_1x_1 + \dots + c_nx_n = b$$

можно решить за время $O(nb)$.

Значит, вопрос о существовании в Π_1 решения уравнения

$$w(x_1, \dots, x_n, a) = g(a)$$

решается за полиномиальное время от

$$|w(x_1, \dots, x_n, a)| + |g(a)|.$$

В связи с этим интересно отметить, что задача о разрешимости в Π_1 систем вида

$$\bigotimes_{i=1}^m w_i(x_1, \dots, x_n) = g_i(a)$$

также является NP-полной задачей.

Доказательство этого факта сразу следует из доказательства теоремы, если вспомнить, что формула

$$\Phi = \bigotimes_{i=1}^m \bigvee_{j=1}^n X_j^{\varepsilon_{ij}}$$

выполнима тогда и только тогда, когда система

$$\bigotimes_{i=1}^m \left(\prod_{j=1}^n (x_j^{-\varepsilon_{ij}})^{|\varepsilon_{ij}|} y_i = a^2 \right) \bigotimes_{j=1}^n x_j x_j^{-1} = a$$

имеет решение в Π_1 .

ЗАМЕЧАНИЕ 3. Покажем, что при любом фиксированном n задача разрешимости в Π_2 уравнения вида

$$w(x_1, \dots, x_n, a, b) = g(a, b)$$

лежит в классе P. В частности, это верно для уравнений вида (6).

Пусть $x_1^0, \dots, x_n^0$ – решение указанного уравнения.

Тогда при любом i ($1 \leq i \leq n$) x_i^0 – подслово слова $g(a, b)$.

Если

$$L = |w(x_1, \dots, x_n, a, b)| + |g(a, b)|,$$

то

$$|g(a, b)| < L,$$

поэтому число подслов слова $g(a, b)$ меньше L^2 .

Пусть A – множество всех подслов слова $g(a, b)$, тогда $(x_1^0, \dots, x_n^0) \in A^n$. Так как во множестве A^n меньше, чем L^{2n} элементов, и

$$\sum_{i=1}^n |x_i^0| < L,$$

то отсюда легко получить при фиксированном n полиномиальный алгоритм даже для нахождения всех решений уравнения

$$w(x_1, \dots, x_n, a, b) = g(a, b).$$

В заключение приношу глубокую благодарность С.И. Адян и А.А. Разбору за участие в обсуждении настоящей статьи и за целый ряд полезных замечаний по поводу ее изложения.

Ярославский государственный университет

Поступило
30.06.94

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Edmunds C. C. On the endomorphisms problem for free group // Comm. Algebra. 1975. № 3. P. 7–20.
- [2] Lyndon R. C. Dependence in groups // Colloq. Math. 1966. № 4. P. 275–283.
- [3] Wicks M. J. A general solution of binary homogeneous equations over free groups // Pacif. J. Math. 1972. V. 41. № 2. P. 543–561.
- [4] Schupp P. E. On the substitution problem for free groups // Proc. Amer. Math. Soc. 1969. V. 23. № 2. P. 421–423.
- [5] Маканин Г. С. Уравнения в свободных группах // Изв. АН СССР. Сер. матем. 1982. Т. 46. № 6. С. 1199–1273.
- [6] Романьков В. А. О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16. № 4. С. 457–471.
- [7] Репин Н. Н. Некоторые просто заданные группы, для которых невозможен алгоритм, распознающий разрешимость уравнений // Вопросы кибернетики. Сложность вычислений и прикладная математическая логика. М., 1988. С. 167–174.
- [8] Шпильрайн В. Э. Об уравнениях в группах вида $F/\gamma_n(R)$ // Алгоритм. проблемы групп и полугрупп. Тула: ТГПИ, 1990. С. 164–183.
- [9] Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. Алгоритмы и сложность. М.: Мир, 1985.
- [10] Кроуэлл Р., Фокс Р. Введение в теорию узлов. М.: Мир, 1967.
- [11] Cohen D. Groups of cohomological dimension one. Lecture Notes in Math. V. 245. Berlin, New York: Springer Verlag, 1972.
- [12] Мальцев А. И. Об уравнении $xyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ в свободной группе // Алгебра и логика. 1962. V. 1. № 5. P. 45–50.
- [13] Zieschang H. Über Automorphismen ebener diskontinuierlicher Gruppen // Math. Ann. 1966. V. 166. P. 148–167.
- [14] Bavard C. Longueur stable des commutateurs // L'Enseignement Mathématique. 1991. V. 37. P. 109–150.
- [15] Lyndon R. C., Schützenberger M. P. The equation $a^M = b^N c^P$ in a free group // Mich. Math. J. 1962. № 9. P. 289–298.
- [16] Baumslag G. On a problem of Lyndon // J. London Math. Soc. 1960. № 35. P. 30–32.
- [17] Schenkman E. The equation $a^n b^n = c^n$ in a free group // Ann. Math. 1959. V. 70. P. 562–564.
- [18] Маканин Г. С. Разрешимость универсальной и позитивной теорий свободной группы // Изв. АН СССР. Сер. матем. 1984. Т. 48. № 4. С. 735–749.
- [19] Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.