УДК 512.543

Е. В. Соколов

О ПРИМЕНИМОСТИ АЛГОРИТМА А. И. МАЛЬЦЕВА К БЕСКОНЕЧНЫМ ПРЕДСТАВЛЕНИЯМ ГРУПП

Рассматриваются группы, заданные бесконечными рекурсивными представлениями. Получены некоторые условия, достаточные для того, чтобы для решения алгоритмических проблем в таких группах можно было применить алгоритмы, основанные на идее "конечной сводимости".

Ключевые слова: финитная аппроксимируемость, финитная отделимость, отделимость относительно сопряженности, проблема равенства, проблема включения, проблема сопряженности.

Groups with infinite recursive presentations are considered. Certain conditions are obtained which are sufficient to apply algorithms based on the idea of "finite reducibility" for solving algorithmic problems in such groups.

Key words: residual finiteness, subgroup separability, conjugacy separability, word problem, generalized word problem, conjugacy problem.

1. Введение

Пусть ρ — некоторое отношение между элементами группы и подмножествами данной группы, сохраняющееся при гомоморфизмах. Говорят, что множество элементов H группы G *финитно отделимо* в этой группе *относительно отношения* ρ, если для каждого элемента $g \in G$, не находящегося в отношении ρ с множеством H, найдется гомоморфизм φ группы G на некоторую конечную группу F такой, что образы $g\varphi$ и $H\varphi$ по-прежнему не состоят в отношении ρ.

Понятие финитной отделимости было введено А. И. Мальцевым [1], заметившим, что если множество H элементов группы является финитно отделимым относительно отношения ρ, то при некоторых дополнительных ограничениях существует алгоритм, который для каждого элемента группы определяет, находится ли этот элемент в отношении ρ с множеством H. Данный алгоритм мы будем рассматривать в следующей формулировке.

Пусть G — некоторая группа, заданная представлением $\langle A; R\rangle$ с множеством образующих A и множеством соотношений R, W — множество всех слов в алфавите $A \cup A^{-1}$ и Φ_A — свободная группа с базисом A (все эти обозначения далее предполагаются фиксированными). Пусть также w и S — произвольные слово и множество слов из W. Допуская вольность речи, мы будем говорить, что слово w состоит в отношении ρ с множеством S, если в этом отношении находятся определяемые ими элемент и множество элементов группы G.

Метаалгоритм $\mathfrak{M}$, отвечающий на вопрос, состоят ли w и S в отношении ρ, включает две ветви. Ветвь $\mathfrak{A}$ последовательно перечисляет все слова из множества W, которые находятся в отношении ρ с множеством S, и останавливается, если встречает слово w. Ветвь $\mathfrak{B}$ для каждой конечной группы F и для каждого отображения $\varphi : A \to F$ (естественным образом продолжаемого до гомоморфизма группы Φ_A) проверяет, совпадает ли образ множества R с единицей (т. е. индуцирует ли это отображение гомоморфизм группы G) и находятся ли образы $w\varphi$ и $S\varphi$ в отношении ρ. Если ответ на первый вопрос положительный, а на второй — отрицательный, ветвь останавливается.

Обе ветви выполняются параллельно и остановка любой из них означает завершение работы всего метаалгоритма. Если множество элементов, определяемых словами из S, финитно отделимо в группе G относительно отношения ρ, то остановится либо ветвь $\mathfrak{A}$ (при $(w, S) \in \rho$), либо ветвь $\mathfrak{B}$ (при $(w, S) \notin \rho$). Таким образом, выполнение метаалгоритма заведомо завершится через конечное число шагов.

Далее мы будем рассматривать главным образом следующие четыре отношения:

ρ_1 — элемент принадлежит множеству;

ρ_2 — элемент принадлежит подгруппе, порожденной множеством;

ρ_3 — элемент сопряжен с некоторым элементом множества;

ρ_4 — элемент сопряжен с некоторым элементом подгруппы, порожденной множеством.

Вместе с тем приводимые ниже рассуждения могут быть легко адаптированы и к другим отношениям, в том числе и таким, которые связывают иное количество элементов и множеств элементов. Версии приведенного метаалгоритма, соответствующие отношениям $\rho_1, \ldots, \rho_4$, мы будем обозначать через $\mathfrak{M}_1, \ldots, \mathfrak{M}_4$.

Метаалгоритм $\mathfrak{M}$ превращается в настоящий алгоритм, если указан конкретный способ осуществления действий, выполняемых ветвями $\mathfrak{A}$ и $\mathfrak{B}$. Хорошо известно и легко показать, что множество слов, которые находятся с множеством S в одном из отношений $\rho_1, \ldots, \rho_4$, перечислимо, если только перечислимыми являются множества A, R и S. Очевидно также и то, что действия ветви $\mathfrak{B}$ выполнимы в случае, когда множества A, R, S конечны и отношение ρ вычислимо в любой конечной группе (разумеется, это так для отношений $\rho_1, \ldots, \rho_4$). Оказывается, однако, что если хотя бы одно из множеств R, S перечислимо, но бесконечно, то соответствующей конкретизации всего метаалгоритма может не существовать. Об этом свидетельствуют построенные В. Дайсоном [2] и С. Мескиным [3] примеры конечно порожденных рекурсивно представленных финитно аппроксимируемых групп с неразрешимой проблемой равенства слов.

В связи с этим мы будем говорить, что метаалгоритм $\mathfrak{M}_i$ применим к тройке перечислимых множеств (A, R, S), если существует эффективный способ выполнения действий, осуществляемых ветвью $\mathfrak{B}$. Целью настоя-

щей статьи является отыскание условий, которые достаточно наложить на множества A, R и S для того, чтобы метаалгоритмы $\mathfrak{M}_1, \ldots, \mathfrak{M}_4$ оказались применимы к тройке (A, R, S).

2. Представления с конечным числом образующих

Пусть множество A образующих группы G является конечным. Подмножество $S \subseteq W$ назовем *конечно сводимым*, если существует алгоритм, позволяющий для каждой конечной группы F и для каждого эффективно заданного отображения $\varphi : A \to F$ (естественным образом продолжаемого до гомоморфизма группы Φ_A) вычислить множество $S\varphi$ (здесь и далее выражение "вычислить множество" означает перечислить все его элементы за конечное, заранее известное число шагов).

Очевидно, что если множества R и S конечно сводимы, то любой из метаалгоритмов $\mathfrak{M}_1, \ldots, \mathfrak{M}_4$ применим к тройке (A, R, S). Некоторые простейшие свойства конечно сводимых множеств содержит

Предложение 1. (i) *Множество W и любое эффективно заданное конечное множество конечно сводимы.* (ii) *Объединение конечного числа конечно сводимых множеств конечно сводимо.* (iii) *Если $w(x_1, x_2, \ldots, x_n)$ — некоторое слово и $S_1, S_2, \ldots, S_n$ — конечно сводимые множества, то множество $w(S_1, S_2, \ldots, S_n)$ конечно сводимо.* (iv) *Если S — конечно сводимое множество, то порожденная им подгруппа группы Φ_A также является конечно сводимым множеством.*

Пусть далее $\Omega^{(n)}$, $n \in \mathbb{N}$, обозначает множество всех функций, отображающих $\mathbb{Z}^n$ в W (здесь и далее рассматриваются только всюду определенные вычислимые функции). Очевидно, что любое слово из множества W можно рассматривать как функцию-константу, принадлежащую $\Omega^{(n)}$. Пусть также $\Lambda^{(n)}$, $n \in \mathbb{N}$, есть множество всех функций $\lambda : \mathbb{Z}^n \to \mathbb{Z}$, удовлетворяющих условию

$$\begin{aligned}\forall x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in \mathbb{Z} \quad \forall q > 1 \\ x_1 \equiv y_1, x_2 \equiv y_2, \ldots, x_n \equiv y_n \pmod{\chi_\lambda(q)} \Rightarrow \\ \lambda(x_1, x_2, \ldots, x_n) \equiv \lambda(y_1, y_2, \ldots, y_n) \pmod{q},\end{aligned}$$

где $\chi_\lambda : \mathbb{N} \to \mathbb{N}$ — некоторая функция, зависящая от функции λ.

Пользуясь тем, что множество W является полугруппой относительно операции конкатенации, определим на множестве $\Omega^{(n)}$ операции произведения и возведения в Λ-степень. Если $\omega, \omega_1, \omega_2 \in \Omega^{(n)}$ и $\lambda \in \Lambda^{(n)}$, положим

$$\begin{aligned}(\omega_1 \circ \omega_2)(x_1, x_2, \ldots, x_n) &= \omega_1(x_1, x_2, \ldots, x_n)\omega_2(x_1, x_2, \ldots, x_n); \\ (\omega^\lambda)(x_1, x_2, \ldots, x_n) &= \omega(x_1, x_2, \ldots, x_n)^{\lambda(x_1, x_2, \ldots, x_n)}.\end{aligned}$$

Первым из основных результатов работы является

Теорема 1. *Пусть функция $\omega : \mathbb{Z}^n \to W$ получается из некоторых слов $w_1, w_2, \ldots, w_m \in W$ конечным числом операций произведения и возведения в Λ-степень. Тогда множество значений функции ω является конечно сводимым.*

3. Представления со счетным множеством образующих

Если множество A образующих группы G является счетным, то перечислить за конечное число шагов все его отображения в конечную группу оказывается невозможным. Но это и не требуется, поскольку нас интересуют не сами отображения, а лишь совокупности образов множеств A, R, S и элемента g. Ясно, что число таких совокупностей конечно, и это подсказывает введение следующего определения.

Систему $\mathfrak{S} = (S_1, S_2, \ldots, S_n)$ подмножеств множества W назовем *конечно сводимой*, если существует алгоритм, позволяющий для любой конечной группы F вычислить системы $\mathfrak{S}_1 = (S_{11}, S_{12}, \ldots, S_{1n}), \ldots, \mathfrak{S}_k = (S_{k1}, S_{k2}, \ldots, S_{kn})$, $k = k(F)$, подмножеств множества F такие, что для любого гомоморфизма $\varphi : \Phi_A \to F$ множества $S_1\varphi, S_2\varphi, \ldots, S_n\varphi$ совпадают с множествами $S_{i1}, S_{i2}, \ldots, S_{in}$ соответственно, при подходящем выборе числа i.

Как и ранее, очевидно, что если для каждого слова $w \in W$ система $(R, S, \{w\})$ является конечно сводимой, то метаалгоритмы $\mathfrak{M}_1$ и $\mathfrak{M}_2$ применимы к тройке (A, R, S). Если же конечно сводимой является система $(W, R, S, \{w\})$, то к тройке (A, R, S) применимы и метаалгоритмы $\mathfrak{M}_3$, $\mathfrak{M}_4$.

Предложение 2.. *Пусть система $\mathfrak{S} = (S_1, S_2, \ldots, S_n)$ конечно сводима. Тогда:*

(i) *любая подсистема системы $\mathfrak{S}$ конечно сводима;*
(ii) *системы $\mathfrak{S} \cup \{S_i \cup S_j\}$, $\mathfrak{S} \cup \{sgp(S_i)\}$, $1 \leqslant i, j \leqslant n$, конечно сводимы;*
(iii) *если $w(x_1, x_2, \ldots, x_n)$ — некоторое слово, то система $\mathfrak{S} \cup \{w(S_1, S_2, \ldots, S_n)\}$ конечно сводима.*

Пусть B — некоторое подмножество множества A и пусть Σ_B — множество всех автоморфизмов полугруппы W, индуцированных биекциями множества B, продолженными естественным образом до биекций множества A. Определим на множестве W отношение *Σ_B-эквивалентности*, считая слова v и w эквивалентными, если $v = w\sigma$ для некоторого $\sigma \in \Sigma_B$. Очевидно, что введенное таким образом отношение действительно является эквивалентностью.

Будем говорить также, что система $\mathfrak{B} = (B_1, B_2, \ldots, B_r)$ подмножеств множества A *эффективно почти дизъюнктна*, если при $i \neq j$ пересечение $B_i \cap B_j$ конечно и вычислимо.

Теорема 2. *Пусть $\mathfrak{B} = (B_1, B_2, \ldots, B_r)$ — эффективно почти дизъюнктная система разрешимых подмножеств множества A,*

$w_1, w_2, \ldots, w_t \in W$ — заданные слова и V_{ik}, $1 \leqslant i \leqslant r$, $1 \leqslant k \leqslant t$, — класс Σ_{B_i}-эквивалентности с представителем w_k. Если мощности множеств $B_1, B_2, \ldots, B_r$ вычислимы, то система $\mathfrak{S}$, включающая все классы V_{ik} и эффективно заданные конечные подмножества $U_1, U_2, \ldots, U_s$ множества W, является конечно сводимой. Если вдобавок к этому вычислима мощность множества $B_0 = A \setminus \bigcup_{i=1}^{r} B_i$, то конечно сводимой является и система $\mathfrak{S} \cup \{W\}$.

Сформулируем теперь расширенный аналог теоремы 1. Для этого нам потребуется ввести еще несколько вспомогательных определений.

Всюду определенную вычислимую функцию $\alpha : \mathbb{Z}^n \to A$ назовем *допустимой*, если она либо является константой, либо удовлетворяет следующим условиям:

(i) функция α почти инъективна (т. е. инъективна всюду, за исключением конечного множества точек);

(ii) множество значений, принимаемых функцией α более чем в одной точке, вычислимо;

(iii) функция $\overleftarrow{\alpha}$, отображающая множество A в множество всех подмножеств множества $\mathbb{Z}^n$ и определенная по правилу

$$\overleftarrow{\alpha}(a) = \{(x_1, x_2, \ldots, x_n) \mid \alpha(x_1, x_2, \ldots, x_n) = a\},$$

вычислима (ввиду условия (i) ее значением в каждой точке является либо пустое множество, либо конечное подмножество множества $\mathbb{Z}^n$).

Также по аналогии с системой подмножеств систему функций $(\alpha_1, \alpha_2, \ldots, \alpha_m)$, отображающих $\mathbb{Z}^n$ в A, будем называть *эффективно почти дизъюнктной*, если для любых i, j, $1 \leqslant i \neq j \leqslant m$, пересечение множеств значений $V(\alpha_i)$ и $V(\alpha_j)$ функций α_i и α_j конечно и вычислимо.

Теорема 3. *Пусть $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ — эффективно почти дизъюнктная совокупность допустимых функций, отображающих $\mathbb{Z}^n$ в A, и пусть для каждого j, $1 \leqslant j \leqslant r$, функция $\omega_j \in \Omega^{(n)}$ получается из функций $\alpha_1, \alpha_2, \ldots, \alpha_m$ (необязательно всех) конечным числом операций произведения и возведения в Λ-степень. Тогда система $\mathfrak{S}$, включающая множества значений функций ω_j и произвольные эффективно заданные конечные подмножества $U_1, U_2, \ldots, U_s$ множества W, является конечно сводимой. Если в дополнение к этому вычислима мощность множества $B = A \setminus \bigcup_{i=1}^{m} V(\alpha_i)$, то конечная сводимость сохраняется при добавлении к системе $\mathfrak{S}$ множества W.*

4. Замечание об отделимости подмножеств в других классах групп

Вернемся к обозначениям из п. 1 и предположим, что подмножество H элементов группы G, определяемых словами из S, является отделимым относительно отношения ρ в классе конечных π-групп для некоторого множества простых чисел π, отличного от множества всех простых

чисел. Это означает, что для каждого элемента $g \in G$, не находящегося в отношении ρ с множеством H, найдется гомоморфизм φ группы G на конечную π-группу, при котором образы $g\varphi$ и $H\varphi$ также не состоят в отношении ρ. Очевидно, что в этом случае в определениях метаалгоритма $\mathfrak{M}$ и понятий конечной сводимости подмножества и системы подмножеств достаточно рассматривать лишь отображения множества A на конечные π-группы.

Расширим теперь множество $\Lambda^{(n)}$, включив в него все функции $\lambda : \mathbb{Z}^n \to \mathbb{Z}$, удовлетворяющие условию

$$\forall x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n \in \mathbb{Z} \quad \forall q > 1, q \text{ — } \pi\text{-число},$$
$$x_1 \equiv y_1, x_2 \equiv y_2, \ldots, x_n \equiv y_n \pmod{\chi_\lambda(q)} \Rightarrow$$
$$\lambda(x_1, x_2, \ldots, x_n) \equiv \lambda(y_1, y_2, \ldots, y_n) \pmod{q}.$$

Легко проверить, что утверждения теорем 1 и 3 остаются при этом справедливыми без каких-либо исправлений. Заметим также, что в множестве $\Lambda^{(n)}$ действительно появляются новые элементы. Конкретным примером может служить функция $g(x_1, x_2, \ldots, x_n) = a^{c_1 x_1^2 + c_2 x_2^2 + \ldots + c_n x_n^2}$, где $a, c_1, c_2, \ldots, c_n \in \mathbb{N}$ и все простые делители числа a не принадлежат множеству π (в качестве χ_g здесь следует взять функцию Эйлера).

5. Доказательство теоремы 2

Обозначим через C подмножество множества A, состоящее:

(i) из всех символов, входящих в слова $w_1, w_2, \ldots, w_t$;

(ii) всех символов, входящих в слова из подмножеств $U_1, U_2, \ldots, U_s$;

(iii) элементов всех пересечений вида $B_i \cap B_j$, где $i \neq j$.

Поскольку система $\mathfrak{B}$ эффективно почти дизъюнктна и множества $U_1, U_2, \ldots, U_s$ конечны и вычислимы, множество C также является конечным и вычислимым.

Пусть далее F — конечная группа и $f_1, f_2, \ldots, f_q$ — все ее элементы. Если отображение θ переводит некоторое подмножество множества A в группу F, то через $\mathfrak{p}_{ij}^{\theta}$, $0 \leqslant i \leqslant r$, $1 \leqslant j \leqslant q$, мы будем обозначать мощность множества $B_i \cap \theta^{-1}(f_j)$.

Пусть $\varphi : A \to F$ — произвольное отображение и ψ — его ограничение на множество C. Очевидно, что тогда $\mathfrak{p}_{ij}^{\psi} \leqslant \mathfrak{p}_{ij}^{\varphi}$ для всех допустимых i, j, причем если отображение ψ вычислимо, то и числа $\mathfrak{p}_{ij}^{\psi}$ являются вычислимыми (это следует из разрешимости множеств $B_1, B_2, \ldots, B_r$ и вычислимости множества C). Очевидно также, что $\sum_{j=1}^{q} \mathfrak{p}_{ij}^{\varphi} = \operatorname{card}(B_i)$ для каждого $i \in \{0, 1, \ldots, r\}$ (здесь и далее $\operatorname{card}(B)$ обозначает мощность множества B). В действительности перечисленные условия являются в определенном смысле характеристическими.

Лемма 1. *Пусть $\psi : C \to F$ — некоторое отображение, $\mathfrak{I} \subseteq \{0, 1, \ldots, r\}$ и $\mathfrak{p}_{\mathfrak{I}} = (\mathfrak{p}_{ij}, i \in \mathfrak{I}, 1 \leqslant j \leqslant q)$ — такой набор кардинальных чисел, что*

(i) $\forall i \in \mathfrak{I} \quad \forall j \in \{1, 2, \ldots, q\} \quad \mathfrak{p}_{ij}^{\psi} \leqslant \mathfrak{p}_{ij}$;
(ii) $\forall i \in \mathfrak{I} \quad \sum_{j=1}^{q} \mathfrak{p}_{ij} = \operatorname{card}(B_i)$.

Тогда существует такое отображение $\varphi : A \to F$, *что* $\psi = \varphi|_C$ *и* $\mathfrak{p}_{ij}^{\varphi} = \mathfrak{p}_{ij}$ *для всех* $i \in \mathfrak{I}$, $1 \leqslant j \leqslant q$.

Доказательство. Если $i \notin \mathfrak{I}$, определим отображение φ на множестве B_i, полагая $x\varphi = f_j$ при $x \in B_i \cap \psi^{-1}(f_j)$ и $x\varphi = 1$ при $x \in B_i \backslash C$. Если же $i \in \mathfrak{I}$, то ввиду условий (i), (ii) и очевидного соотношения $\sum_{j=1}^{q} \mathfrak{p}_{ij}^{\psi} = \operatorname{card}(B_i \cap C)$ существует разбиение множества B_i на подмножества $B_{i1}, B_{i2}, \ldots, B_{iq}$ такие, что $\operatorname{card}(B_{ij}) = \mathfrak{p}_{ij}$ и $B_{ij} \cap C = B_i \cap \psi^{-1}(f_j)$. Положим $x\varphi = f_j$ для всех $x \in B_{ij}$, $1 \leqslant j \leqslant q$.

Поскольку при таком определении φ продолжает ψ, а пересечение любых двух различных множеств из системы $\mathfrak{B}$ содержится в множестве C, отображение φ задано корректно. Кроме того, по построению $\mathfrak{p}_{ij}^{\varphi} = \mathfrak{p}_{ij}$ для всех $i \in \mathfrak{I}$, $1 \leqslant j \leqslant q$, что и требовалось.

Для каждого подмножества $\mathfrak{I}$ множества $\{0, 1, \ldots, r\}$ $\mathfrak{I}$-*сигнатурой* отображения $\varphi : A \to F$ мы будем называть совокупность, состоящую из отображения $\psi = \varphi|_C$ и набора кардинальных чисел $\mathfrak{p}_{\mathfrak{I}}^{\varphi} = (\mathfrak{p}_{ij}^{\varphi}, i \in \mathfrak{I}, 1 \leqslant j \leqslant q)$. Очевидно, что любая сигнатура однозначно определяет образы относительно φ множеств $U_1, U_2, \ldots, U_s$.

Заметим далее, что, поскольку множество B_i разрешимо в A, каждое слово w_k эффективно представимо в виде

$$w_k = w_k(a_{ik1}, a_{ik2}, \ldots, a_{ikm_{ik}}, b_{ik1}, b_{ik2}, \ldots, b_{ikn_{ik}}),$$

где $a_{ik1}, a_{ik2}, \ldots, a_{ikm_{ik}} \in A \backslash B_i$ и $b_{ik1}, b_{ik2}, \ldots, b_{ikn_{ik}} \in B_i$. Будучи классом Σ_{B_i}-эквивалентности, множество V_{ik} состоит из всевозможных слов, которые получаются из w_k подстановкой вместо символов $b_{ik1}, b_{ik2}, \ldots, b_{ikn_{ik}}$ произвольных элементов множества B_i, различных между собой. Следовательно, множество $V_{ik}\varphi$ в свою очередь состоит из элементов вида

$$w_k(a_{ik1}\psi, a_{ik2}\psi, \ldots, a_{ikm_{ik}}\psi, x_1, x_2, \ldots, x_{n_{ik}}),$$

где $x_1, x_2, \ldots, x_{n_{ik}} \in F$, причем количество переменных, равных f_j, не превосходит $\mathfrak{p}_{ij}^{\varphi}$.

Таким образом, зная $\{1, 2, \ldots, r\}$-сигнатуру отображения φ, т. е. умея вычислять образы элементов множества C и числа $\mathfrak{p}_{ij}^{\varphi}$, мы можем найти образ системы $\mathfrak{S}$ относительно этого отображения. Если же известна $\{0, 1, \ldots, r\}$-сигнатура, то определен и образ системы $\mathfrak{S} \cup \{W\}$: множество W переходит на подгруппу, порожденную теми элементами f_j, для которых $\mathfrak{p}_{ij}^{\varphi} > 0$ хотя бы для одного $i \in \{0, 1, \ldots, r\}$. Из сказанного вытекает также

Лемма 2. *Пусть* $\varphi_1, \varphi_2 : A \to F$ — *такие отображения, что* $\varphi_1|_C = \varphi_2|_C$ *и для всех* i, j, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant q$, *если хотя бы одно*

из двух чисел $\mathfrak{p}_{ij}^{\varphi_1}$, $\mathfrak{p}_{ij}^{\varphi_2}$ *не превосходит* $n = \max\{n_{ik}\}$, *то* $\mathfrak{p}_{ij}^{\varphi_1} = \mathfrak{p}_{ij}^{\varphi_2}$. *Тогда образы системы* $\mathfrak{S}$ *относительно отображений* φ_1 *и* φ_2 *совпадают. Если в дополнение к этому для каждого* j *числа* $\mathfrak{p}_{0j}^{\varphi_1}$, $\mathfrak{p}_{0j}^{\varphi_2}$ *равны или не равны нулю одновременно, то совпадают и системы* $(\mathfrak{S} \cup \{W\})\varphi_1$, $(\mathfrak{S} \cup \{W\})\varphi_2$.

Итак, для того чтобы вычислить всевозможные образы системы $\mathfrak{S}$ (системы $\mathfrak{S} \cup \{W\}$), нам достаточно перебрать конечное множество пар, состоящих из произвольного отображения ψ множества C в группу F и набора кардинальных чисел $\mathfrak{p} = (\mathfrak{p}_{ij}, i \in \mathfrak{I}, 1 \leqslant j \leqslant q)$, где $\mathfrak{I} = \{1, 2, \ldots, r\}$ (соответственно $\mathfrak{I} = \{0, 1, \ldots, r\}$), удовлетворяющего условиям (i), (ii) из формулировки леммы 1 и условию

(iii) если множество B_i бесконечно, то для всех j $\mathfrak{p}_{ij} \in \{0, 1, \ldots, n, \mathrm{card}(B_i)\}$ (здесь, как и в лемме 2, $n = \max\{n_{ik}\}$).

С одной стороны, каждая такая пара $(\psi, \mathfrak{p})$ согласно лемме 1 является сигнатурой некоторого отображения $\theta_{\psi,\mathfrak{p}} : A \to F$. С другой, если $\varphi : A \to F$ — произвольное отображение, то образ системы $\mathfrak{S}$ (системы $\mathfrak{S} \cup \{W\}$) относительно φ совпадает в силу леммы 2 с образом $\mathfrak{S}$ (соответственно $\mathfrak{S} \cup \{W\}$) относительно подходящего отображения $\theta_{\psi,\mathfrak{p}}$. Тем самым теорема доказана.

6. Доказательство теорем 1 и 3

Пусть $T = \{t_1, t_2, \ldots, t_m\}$ — некоторое конечное множество символов. *Шаблоном функции с параметрами* m *и* n будем называть формальное выражение, определяемое индуктивно следующим образом:

(i) каждый символ t_i является шаблоном;
(ii) если τ_1 и τ_2 — шаблоны, то $\tau_1 \circ \tau_2$ также шаблон;
(iii) если τ — шаблон и $\lambda \in \Lambda^{(n)}$, то $(\tau)^\lambda$ — шаблон;
(iv) выражение является шаблоном тогда и только тогда, когда это следует из правил (i) — (iii).

Если мы зафиксируем некоторое множество U с бинарной ассоциативной операцией $\circ$ и будем подставлять его элементы вместо символов $t_1, t_2, \ldots, t_m$, применяя затем операцию $\circ$ в соответствии с порядком построения шаблона, то в результате получим функцию $\tau_U : U^m \times \mathbb{Z}^n \to U$ — *конкретизацию шаблона* τ.

Если τ — некоторый шаблон с параметрами m, n и $\lambda_1, \lambda_2, \ldots, \lambda_t \in \Lambda^{(n)}$ — все функции, входящие в его запись, то через χ_τ будем обозначать функцию натурального аргумента, значение которой в точке q равно наименьшему общему кратному чисел $\chi_{\lambda_1}(q), \chi_{\lambda_2}(q), \ldots, \chi_{\lambda_t}(q)$.

Лемма 1. *Пусть* F *— конечная группа порядка* q *и* τ *— шаблон функции с параметрами* m, n. *Тогда для любых целых чисел* $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_n$ *и для любых элементов* $f_1, f_2, \ldots, f_m$ *группы* F *из соотношений* $x_1 \equiv y_1, x_2 \equiv y_2, \ldots, x_n \equiv y_n \pmod{\chi_\tau(q)}$ *следует, что*

$$\tau_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) = \tau_F(f_1, f_2, \ldots, f_m, y_1, y_2, \ldots, y_n).$$

Доказательство осуществляется индукцией по построению шаблона τ.

База очевидна.

Если $\tau = \tau' \circ \tau''$, то $\chi_{\tau'}(q), \chi_{\tau''}(q) \mid \chi_\tau(q)$ и по индуктивному предположению

$$\tau'_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) = \tau'_F(f_1, f_2, \ldots, f_m, y_1, y_2, \ldots, y_n),$$
$$\tau''_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) = \tau''_F(f_1, f_2, \ldots, f_m, y_1, y_2, \ldots, y_n).$$

Отсюда

$$\tau_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) =$$
$$= \tau'_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n)\tau''_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) =$$
$$= \tau_F(f_1, f_2, \ldots, f_m, y_1, y_2, \ldots, y_n).$$

Если $\tau = (\tau')^\lambda$, то снова $\chi_{\tau'}(q) \mid \chi_\tau(q)$ и по индуктивному предположению

$$\tau'_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) = \tau'_F(f_1, f_2, \ldots, f_m, y_1, y_2, \ldots, y_n).$$

Кроме того, $\chi_\lambda(q) \mid \chi_\tau(q)$, поэтому $\lambda(x_1, x_2, \ldots, x_n) \equiv \lambda(y_1, y_2, \ldots, y_n) \pmod q$ в силу определения множества $\Lambda^{(n)}$ и

$$(\tau'_F(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n))^{\lambda(x_1, x_2, \ldots, x_n)} =$$
$$= (\tau'_F(f_1, f_2, \ldots, f_m, y_1, y_2, \ldots, y_n))^{\lambda(y_1, y_2, \ldots, y_n)},$$

так как q — порядок группы F.

Из доказанной леммы сразу же вытекает теорема 1.

В самом деле очевидно, что для подходящего шаблона τ, параметрами которого являются числа m, n из формулировки теоремы,

$$\omega(x_1, x_2, \ldots, x_n) = \tau_W(w_1, w_2, \ldots, w_m, x_1, x_2, \ldots, x_n)$$

при всех $x_1, x_2, \ldots, x_n$.

Индукцией по построению шаблона τ легко показать, что для любого гомоморфизма φ группы Φ_A в конечную группу F

$$\tau_W(w_1, w_2, \ldots, w_m, x_1, x_2, \ldots, x_n)\varphi =$$
$$\tau_F(w_1\varphi, w_2\varphi, \ldots, w_m\varphi, x_1, x_2, \ldots, x_n).$$

Поэтому множество значений функции ω переходит под действием φ на множество

$$\{\tau_F(w_1\varphi, w_2\varphi, \ldots, w_m\varphi, x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{Z}, 1 \leqslant i \leqslant n\},$$

совпадающее согласно лемме 1 с конечным вычислимым множеством

$$\{\tau_F(w_1\varphi, w_2\varphi, \ldots, w_m\varphi, x_1, x_2, \ldots, x_n) \mid 0 \leqslant x_i < \chi_\tau(q), 1 \leqslant i \leqslant n\},$$

где q — как и выше, порядок группы F.

Перейдем теперь к доказательству теоремы 3. Пусть C обозначает подмножество множества A, состоящее:

(i) из всех символов, входящих в слова из множеств $U_1, U_2, \ldots, U_s$;

(ii) для каждого $i \in \{1, 2, \ldots, m\}$: всех значений функции α_i, принимаемых ею более чем в одной точке, либо единственного значения функции α_i, если она является константой;

(iii) элементов всех пересечений $V(\alpha_i) \cap V(\alpha_j)$, где $1 \leqslant i \neq j \leqslant m$.

Обозначим также через D дополнение (в A) множества $(\bigcup_{i=1}^{m} V(\alpha_i)) \cup C$ и через $\overleftarrow{C}$ объединение

$$\bigcup_{\alpha_i \neq \text{const}} \alpha_i^{-1}(C).$$

Поскольку система $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ эффективно почти дизъюнктна и функции α_i допустимы, множество C, а вместе с ним и $\overleftarrow{C}$ является конечным и вычислимым. Очевидно также, что D — это в точности множество B за вычетом тех символов, которые входят в некоторое слово из объединения $U_1 \cup U_2 \cup \ldots \cup U_s$, но не принадлежат ни одному из множеств $V(\alpha_i)$. Перебирая все символы в словах из указанного объединения (их конечное число) и проверяя, принадлежат ли они хотя бы одному из множеств $V(\alpha_i)$ (что возможно благодаря допустимости функций α_i), мы можем вычислить разность $B \backslash D$. В частности, если известна мощность множества B, то известна и мощность множества D.

Пусть теперь F — некоторая конечная группа порядка q, $\varphi : A \to F$ — произвольное отображение и $\chi(q)$ — наименьшее общее кратное чисел $\chi_{\lambda_1}(q), \chi_{\lambda_2}(q), \ldots, \chi_{\lambda_t}(q)$, где $\lambda_1, \lambda_2, \ldots, \lambda_t \in \Lambda^{(n)}$ — все функции, используемые при построении функций ω_j, $1 \leqslant j \leqslant r$. Обозначим через S подмножество множества $F^m \times \mathbb{Z}^n$, состоящее из элементов вида

$$(\alpha_1(x_1, x_2, \ldots, x_n)\varphi, \alpha_2(x_1, x_2, \ldots, x_n)\varphi, \ldots, \alpha_m(x_1, x_2, \ldots, x_n)\varphi, \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n),$$

где $x_1, x_2, \ldots, x_n$ — произвольные целые числа и $\bar{x}$ — представитель числа x из наименьшей неотрицательной системы вычетов по модулю $\chi(q)$. Систему, состоящую из множества S и ограничения ψ отображения φ на множество C, будем называть *сигнатурой* φ. Определим также *расширенную сигнатуру* φ как тройку $(\psi, S, D\varphi)$.

Лемма 2. *Существует алгоритм, который по сигнатуре отображения φ вычисляет образ системы $\mathfrak{S}$ относительно φ, а по расширенной сигнатуре — образ системы $\mathfrak{S} \cup \{W\}$.*

Доказательство. Поскольку множество C содержит все символы, входящие в слова из множеств $U_1, U_2, \ldots, U_s$, образы последних определяются отображением ψ.

Далее, как и при доказательстве теоремы 1, легко заметить, что для подходящего шаблона $\tau^{(j)}$, параметрами которого являются числа m и n из формулировки теоремы 3,

$$\omega_j(x_1, x_2, \ldots, x_n) = \tau_W^{(j)}(\alpha_1(x_1, x_2, \ldots, x_n), \alpha_2(x_1, x_2, \ldots, x_n), \ldots, \alpha_m(x_1, x_2, \ldots, x_n), x_1, x_2, \ldots, x_n)$$

при всех $x_1, x_2, \ldots, x_n$. Поскольку, очевидно, $\chi_{\tau^{(j)}}(q) \mid \chi(q)$, из леммы 1 следует, что для любого набора целых чисел $x = (x_1, x_2, \ldots, x_n)$

$$\begin{aligned}\omega_j(x)\varphi &= \tau_W^{(j)}(\alpha_1(x), \alpha_2(x), \ldots, \alpha_m(x), x_1, x_2, \ldots, x_n)\varphi = \\ &= \tau_F^{(j)}(\alpha_1(x)\varphi, \alpha_2(x)\varphi, \ldots, \alpha_m(x)\varphi, x_1, x_2, \ldots, x_n) = \\ &= \tau_F^{(j)}(\alpha_1(x)\varphi, \alpha_2(x)\varphi, \ldots, \alpha_m(x)\varphi, \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n).\end{aligned}$$

Стало быть, применяя ко всевозможным кортежам из S функцию $\tau_F^{(j)}$, мы перечислим образы всех слов из множества значений функции ω_j.

Заметим, наконец, что множество A полностью покрывается множествами C, D и $V(\alpha_i)$, $1 \leqslant i \leqslant m$, поэтому его образ относительно отображения φ совпадает с объединением множеств $C\psi$, $D\varphi$ и

$$\{\alpha_i(x_1, x_2, \ldots, x_n)\varphi, 1 \leqslant i \leqslant m, x_1, x_2, \ldots, x_n \in \mathbb{Z}\}.$$

Последнее из них легко вычислить, перебирая компоненты кортежей из множества S. Рассматривая затем подгруппу группы F, порожденную всеми элементами из $A\varphi$, мы получаем образ множества W.

Перечислим теперь некоторые очевидные условия, которым удовлетворяет сигнатура любого отображения $\varphi : A \to F$:

(i) для любых чисел $x_1, x_2, \ldots, x_n \in \{0, 1, \ldots, \chi(q) - 1\}$ множество S содержит хотя бы один кортеж вида $(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n)$;

(ii) если $(x_1, x_2, \ldots, x_n) \in \overleftarrow{C}$, то существует кортеж

$$(f_1, f_2, \ldots, f_m, \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) \in S$$

такой, что $f_i = \alpha_i(x_1, x_2, \ldots, x_n)\psi$, если только

$$\alpha_i(x_1, x_2, \ldots, x_n) \in C;$$

(iii) если функция α_i является константой и ее значение равно a, то для любого кортежа $(f_1, f_2, \ldots, f_m, x_1, x_2, \ldots, x_n) \in S$ $f_i = a\psi$.

Расширенная сигнатура отображения φ удовлетворяет также условию

(iv) мощность множества $E = D\varphi$ не превосходит мощности множества D.

Лемма 3. *Пусть некоторые множество*

$$S \subseteq F^m \times \{0, 1, \ldots, \chi(q) - 1\}^n$$

и отображение $\psi : C \to F$ *удовлетворяют условиям* (i) — (iii). *Тогда существует отображение* $\varphi : A \to F$, *для которого пара* (ψ, S) *является сигнатурой. Если в дополнение к этому подмножество* $E \subseteq F$ *удовлетворяет условию (iv), то отображение* φ *можно определить таким образом, чтобы система* (ψ, S, E) *оказалась его расширенной сигнатурой.*

Доказательство. Пусть

$$\eta : \{0, 1, \ldots, q^m\chi(q) - 1\} \times \{0, 1, \ldots, \chi(q) - 1\}^{n-1} \to S$$

— некоторое сюръективное отображение, переводящее кортеж

$$(x_1, x_2, \ldots, x_n)$$

в элемент множества S вида $(f_1, f_2, \ldots, f_m, \bar{x}_1, x_2, \ldots, x_n)$, где $\bar{x}$ — как и выше, представитель числа x из наименьшей неотрицательной системы вычетов по модулю $\chi(q)$ (существование такого элемента обеспечивается условием (i)). Определим отображение $\xi : \mathbb{Z}^n \to S$ следующим образом.

Если $(x_1, x_2, \ldots, x_n) \in \overleftarrow{C}$, значением функции ξ в точке

$$(x_1, x_2, \ldots, x_n)$$

будет кортеж, существующий согласно условию (ii).

Если же $(x_1, x_2, \ldots, x_n) \notin \overleftarrow{C}$, положим

$$\xi(x_1, x_2, \ldots, x_n) = \eta(x_1 \bmod q^m\chi(q), \bar{x}_2, \ldots, \bar{x}_n).$$

Очевидно, что, рассматривая всевозможные не принадлежащие (конечному) множеству $\overleftarrow{C}$ кортежи $(x_1, x_2, \ldots, x_n)$ и соответствующие им кортежи $(x_1 \bmod q^m\chi(q), \bar{x}_2, \ldots, \bar{x}_n)$, мы перечислим все точки области определения функции η. Поэтому из сюръективности последней вытекает, что и функция ξ является сюръективной.

Определим теперь отображение φ на множестве $V(\alpha_i)$: если x_1, x_2, $\ldots$, x_n — произвольные целые числа, положим $\alpha_i(x_1, x_2, \ldots, x_n)\varphi =$

$\mathrm{pr}_i(\xi(x_1, x_2, \ldots, x_n))$, где pr_i — функция, возвращающая компоненту кортежа с номером i. Заметим, что при таком определении ограничение отображения φ на множество $V(\alpha_i) \cap C$ совпадает с ψ.

В самом деле, если функция α_i является константой и ее значением служит элемент $a \in C$, то согласно условию (iii) i-е компоненты всех кортежей из множества S совпадают и равны $a\psi$. Если же α_i — не константа, но $\alpha_i(x_1, x_2, \ldots, x_n) \in C$, то $(x_1, x_2, \ldots, x_n) \in \overleftarrow{C}$ и в силу выбора кортежа $\xi(x_1, x_2, \ldots, x_n)$ его i-я компонента равна $\alpha_i(x_1, x_2, \ldots, x_n)\psi$.

Из сделанного замечания сразу же вытекает корректность определения φ: если $a = \alpha_i(x_1, x_2, \ldots, x_n) = \alpha_j(y_1, y_2, \ldots, y_n)$ и либо $i \neq j$, либо $i = j$, но для некоторого k $x_k \neq y_k$, то элемент a принадлежит множеству C согласно условиям (ii) и (iii) из определения последнего, поэтому

$$\alpha_i(x_1, x_2, \ldots, x_n)\varphi = a\psi = \alpha_j(y_1, y_2, \ldots, y_n)\varphi.$$

Задавая теперь отображение φ на множестве $C \setminus \bigcup_{i=1}^{m} V(\alpha_i)$ по правилу $\varphi(a) = \psi(a)$, мы получаем, что $\varphi|_C = \psi$ и для любых целых чисел $x_1, x_2, \ldots, x_n$

$$(\alpha_1(x_1, x_2, \ldots, x_n)\varphi, \alpha_2(x_1, x_2, \ldots, x_n)\varphi, \ldots, \alpha_m(x_1, x_2, \ldots, x_n)\varphi, \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) = \xi(x_1, x_2, \ldots, x_n).$$

Отсюда и из сюръективности функции ξ следует, что при любом продолжении отображения φ на множество D пара (ψ, S) будет его сигнатурой. Если же подмножество $E \subseteq F$ удовлетворяет условию (iv), то указанное продолжение, очевидно, можно осуществить таким образом, чтобы выполнялось равенство $E = D\varphi$ и, стало быть, система (ψ, S, E) являлась расширенной сигнатурой отображения φ. Тем самым лемма доказана.

Утверждение теоремы вытекает непосредственно из лемм 2 и 3. Для получения всевозможных образов системы $\mathfrak{S}$ нам достаточно перечислить все пары, состоящие из множества $S \subseteq F^m \times \{0, 1, \ldots, \chi(q) - 1\}^n$ и отображения $\psi : C \to A$ и удовлетворяющие условиям (i) — (iii), возможность эффективной проверки которых сомнений не вызывает. Если же известна мощность множества B, а вместе с ней и мощность множества D, мы можем перечислить расширенные сигнатуры всех отображений из множества A в группу F. Таким образом, становятся известны всевозможные образы системы $\mathfrak{S} \cup \{W\}$.

Библиографический список

1. *Мальцев А. И.* О гомоморфизмах на конечные группы // Учен. зап. Иван. гос. пед. ин-та. 1958. Т. 18. С. 49—60.
2. *Dyson V. H.* A family of groups with nice word problems // J. Austral. Math. Soc. 1974. Vol. 17. P. 414—425.
3. *Meskin S.* A finitely generated residually finite group with an unsolvable word problem // Proc. Amer. Math. Soc. 1974. Vol. 43. P. 8—10.