УДК 512.542 + 512.54.03 MSC: 20D60, 20F70, 20F10

СКОЛЬКО НАБОРОВ ЭЛЕМЕНТОВ ГРУППЫ ОБЛАДАЕТ ДАННЫМ СВОЙСТВОМ?

Антон А. Клячко Анна А. Мкртчян
Механико-математический факультет
Московского государственного университета
Москва 119991, Ленинские горы, МГУ
klyachko@mech.math.msu.su anna.mkr@gmail.com

с дополнением Дмитрия В. Трушина

Теорема Гордона–Родригеса-Виллегаса, обобщающая теорему Соломона, говорит, что в любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если ранг матрицы, составленной из сумм показателей степеней при i-м неизвестном в j-м уравнении, меньше числа неизвестных. Мы обобщаем эту теорему в двух направлениях: во-первых, мы рассматриваем уравнения с коэффициентами, а во-вторых, мы рассматриваем не только системы уравнений, но и произвольные формулы первого порядка в групповом языке (с константами). Из нашей теоремы можно вывести разные забавные факты. Например, число элементов группы, квадраты которых лежат в данной подгруппе, делится на порядок этой подгруппы.

0. Введение

Теорема Соломона [Solo69]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если уравнений меньше, чем неизвестных.*

Эта тема развивалась в разных направлениях (см., например, [Стру95], [AmV11], [Isaa70] и литературу, там цитируемую), но наиболее простое и естественное обобщение теоремы Соломона было получено совсем недавно.

Теорема Гордона–Родригеса-Виллегаса [GRV12]. *В любой группе число решений системы уравнений без коэффициентов делится на порядок этой группы, если ранг матрицы, составленной из сумм показателей степеней при i-м неизвестном в j-м уравнении, меньше числа неизвестных.*

Например, к системе уравнений $x^2y^3[x,y]y^{-1} = 1 = (yx)^2$ теорема Соломона неприменима, но по теореме Гордона–Родригеса-Виллегаса число решений всё же делится на порядок группы, так как ранг соответствующей матрицы $\left(\begin{smallmatrix}2&2\\2&2\end{smallmatrix}\right)$ равен единице, а неизвестных два.

Напрашивается гипотеза, что если ранг матрицы сильно меньше числа неизвестных, то число решений должно делиться на высокую степень порядка группы. Однако ни эта гипотеза, ни её естественное ослабление не верны. В параграфе 2 мы приводим соответствующий пример.

Мы обобщаем теорему Гордона–Родригеса-Виллегаса в других направлениях. Мы изучаем уравнения с коэффициентами, причём не только системы уравнений, но и произвольные формулы первого порядка. Основная теорема позволяет заключить, что имеет место множество фактов, подобных тому, что упомянут в аннотации. В параграфе 1 читатель может найти формулировку основной теоремы, в параграфе 2 — несколько примеров, а в параграфе 3 — доказательство, которое для случая систем уравнений без коэффициентов превращается в доказательство теоремы Гордона–Родригеса-Виллегаса, немного более простое по сравнению с оригинальным, на наш взгляд, но основанное на тех же идеях. В параграфе 4 мы даём прямое доказательство забавного факта, сформулированного в аннотации. Нам не удалось найти этот факт в литературе,*) хотя он легко мог бы быть выведен из одной теоремы Ф. Холла (смотрите параграф 1), обобщающей известную теорему Фробениуса [Frob03] (смотрите также [Hall59]), которая утверждает, что *число решений уравнения $x^n = g$ делится на* НОД$(n, |C(g)|)$. Теорема Фробениуса обобщалась в разных направлениях (смотрите, например, [Hall36], [Kula38], [Sehg62], [BrTh88], [AsTa01] и литературу там цитируемую).

В дополнении, написанном Д. В. Трушиным, содержится доказательство чисто логического утверждения, которое позволяет несколько упростить формулировку одного из следствий основной теоремы за счёт предварительного преобразования логической формулы.

Обозначения, которые мы используем, в целом стандартны. Отметим только, что если $k \in \mathbb{Z}$, а x и y — элементы некоторой группы, то x^y, x^{ky} и x^{-y} обозначают $y^{-1}xy$, $y^{-1}x^ky$ и $y^{-1}x^{-1}y$, соответственно. Коммутатор $[x,y]$ мы понимаем как $x^{-1}y^{-1}xy$. Если X — подмножество некоторой группы, то $|X|$, $\langle X\rangle$ и $C(X)$ означают, соответственно, мощность множества X, подгруппу, порождённую множеством X, и централизатор множества X. Буква $\mathbb{Z}$ обозначает множество целых чисел.

Авторы благодарят анонимного рецензента, А. В. Васильева и И. М. Айзекса за полезные замечания.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант №11-01-00945.

*) В 2017 году мы узнали, что этот факт был установлен в [Iwa82].

1. Основная теорема

Рассмотрим групповой язык L над группой G, в нём имеется два функциональных символа: $\cdot$ и $^{-1}$, кроме того, для каждого элемента группы G имеется константный символ g. Мы не предполагаем, что группа конечна (хотя это так в большинстве интересных случаев); результаты о делимости следует понимать в смысле кардинальной арифметики: любой бесконечный кардинал делится на любой не превосходящий его ненулевой кардинал (а ноль делится на любой кардинал).

Рассмотрим произвольную формулу φ первого порядка в языке L. Каждая атомарная подформула может быть записана в виде

$$u = 1,$$

где слова $u \in G * F$, а F — свободная группа, порождённая всеми (свободными и связанными) переменными формулы φ. Таким образом, слова u (возможно, разные для разных подформул) могут содержать свободные и связанные переменные и элементы группы G (называемые *коэффициентами* формулы φ).

Формуле φ мы сопоставляем ориентированный *граф* $\Gamma(\varphi)$ *формулы* φ следующим образом. Вершинами графа $\Gamma(\varphi)$ служат связанные переменные формулы φ. Каждая атомарная подформула, содержащая связанные переменные, имеет вид

$$v_1(y_1)w_1(x_1\ldots,x_n)\ldots v_r(y_r)w_r(x_1\ldots,x_n) = h,$$

где y_i — связанные переменные формулы φ (необязательно различные), $x_1\ldots,x_n$ — все (различные) свободные переменные формулы φ, слова $v_i(y_i)$ являются элементами свободного произведения $G * \langle y_i\rangle_\infty$ группы G и бесконечной циклической группы, порождённой буквой y_i, слова $w_i(x_1\ldots,x_n)$ являются элементами свободного произведения $G * F(x_1\ldots,x_n)$ группы G и свободной группы с базисом $x_1\ldots,x_n$, а $h \in G$. Соединим вершины y_i и y_{i+1} (индексы по модулю r) ориентированным ребром и пометим это ребро целочисленной строкой $(\alpha_1,\ldots,\alpha_n)$, где α_j — это сумма показателей степеней при переменной x_j в слове w_i; причём петли с нулевыми метками мы не проводим. Проделаем это с каждой атомарной подформулой, содержащей связанные переменные.

Например, если формула $\varphi(x_1,x_2)$ имеет вид *)

$$\forall y\exists z\ \left(\left([ygy,x_1gx_2]x_1z^{-1}azx_2^{-3}x_1^3hx_2^7 = 1\right) \wedge \neg\left(z^{-1}bz(x_2x_1)^2 = 1\right) \vee \left((x_1^2x_2^2)^5 = 1\right)\right), \tag{1}$$

где $g,h,a,b \in G$ — фиксированные элементы (необязательно различные), то граф $\Gamma(\varphi)$ имеет выглядит так:

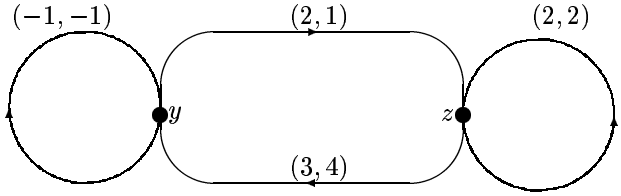

Рис. 1

Далее выберем в графе $\Gamma(\varphi)$ циклы $c_1,c_2,\ldots$, порождающие его первую группу гомологий (например, порождающие фундаментальных групп всех компонент), и составим *матрицу* $A(\varphi)$ *формулы* φ следующим образом: для каждого из порождающих циклов c_i напишем строку, являющуюся суммой меток рёбер этого цикла (взятых со знаком плюс или минус в зависимости от ориентации), после чего добавим ещё строки, состоящие из сумм показателей степеней в атомарных подформулах, не содержащих связанных переменных.

Эта матрица зависит от выбора порождающих циклов, но целочисленная линейная оболочка её строк определяется однозначно формулой φ. В приведённом выше примере матрица $A(\varphi)$ будет иметь вид

$$A(\varphi) = \begin{pmatrix} -1 & -1 \\ 5 & 5 \\ 2 & 2 \\ 10 & 10 \end{pmatrix} \quad \text{(при очевидном выборе трёх порождающих циклов).} \tag{2}$$

Связанную переменную t назовём *изолирующей*, если она входит в атомарные подформулы только в составе подслов вида $t^{-1}g_it$, где $g_i \in G$. Соответствующие коэффициенты g_i мы будем называть *изолированными*. Более точно, элемент g группы G называется *изолированным*, если он встречается в формуле φ только в подсловах вида $t_i^{-1}gt_i$, где все t_i — изолирующие переменные. В рассматриваемом примере z является изолирующей переменной, а a и b — изолированными коэффициентами.

*) Мы не предполагаем, что в формуле всегда кванторы вынесены наружу, как в этом примере.

Основная теорема. *Если ранг матрицы $A(\varphi)$ формулы φ меньше числа свободных переменных в этой формуле, то число наборов элементов группы, удовлетворяющих формуле φ делится на порядок централизатора множества всех неизолированных коэффициентов формулы φ. В частности, это число делится на порядок группы, если все неизолированные коэффициенты равны единице.*

В приведённом выше примере ранг матрицы равен единице, а свободных переменных две, поэтому можно утверждать, что мощность множества

$$\left\{(x_1,x_2)\in G^2\ ;\ \forall y\exists z\ \left(\left([ygy,x_1gx_2]x_1z^{-1}azx_2^{-3}x_1^3hx_2^7=1\right)\wedge\neg\left(z^{-1}bz(x_2x_1)^2=1\right)\vee\left((x_1^2x_2^2)^5=1\right)\right)\right\}$$

делится на $|C(g,h)|$ (даже если $g=a$, мы должны считать коэффициент g неизолированным). В следующем параграфе мы приведём более содержательные примеры.

Следствие 1. *Число решений системы уравнений в группе делится на порядок централизатора множества всех коэффициентов, если ранг матрицы этой системы меньше числа неизвестных.*

Это следствие превращается в теорему Гордона–Родригеса-Виллегаса в случае, когда все коэффициенты равны единице.

Теорема Гордона–Родригеса-Виллегаса о сопряжённости ([GRV12], следствие 3.5*)).
Пусть $\{w_j(x_1,\dots,x_n)\}\subset F(x_1,\dots,x_n)$ — произвольное множество слов (элементов свободной группы) такое, что ранг матрицы, составленной из сумм показателей степеней при x_i в w_j меньше n. Тогда для любой группы G и любых элементов $h_j\in G$ число наборов, удовлетворяющих формуле

$$\bigwedge_j\left(\exists q_j\ w_j(x_1,\dots,x_n)=q_j^{-1}h_jq_j\right),$$

делится на порядок группы G.

Это утверждение (обобщающее теорему о сопряжённости из работы [Solo69]) очевидно сильнее, чем теорема Гордона–Родригеса-Виллегаса, сформулированная во введении. Наша теорема даёт ещё более сильное утверждение: поточечная сопряжённость заменяется на сопряжённость одним элементом.

Следствие 2. *В условиях теоремы Гордона–Родригеса-Виллегаса о сопряжённости число наборов, удовлетворяющих формуле*

$$\exists q\ \left(\bigwedge_j\left(w_j(x_1,\dots,x_n)=q^{-1}h_jq\right)\right),$$

делится на порядок группы G.
(А если $w_j(x_1,\dots,x_n)\in G*F(x_1,\dots,x_n)$, то число удовлетворяющих наборов делится на порядок централизатора множества всех коэффициентов слов w_j.)

Доказательство. В этом случае граф имеет единственную вершину, соответствующую изолирующей переменной q, коэффициенты h_j изолированы и матрица формулы совпадает с матрицей из теоремы Гордона–Родригеса-Виллегаса о сопряжённости. Таким образом, это следствие немедленно вытекает из основной теоремы.

Следующее утверждение обобщает теорему Гордона–Родригеса-Виллегаса о сопряжённости в другом направлении.

Теорема об инвариантных множествах. *Пусть U_j,V_j — подмножества конечной группы G, инвариантные относительно сопряжённости (то есть объединения некоторых классов сопряжённости) и $\{w_j(x_1,\dots,x_n)\}\subset F(x_1,\dots,x_n)*G$ — произвольное множество слов такое, что ранг матрицы, составленной из сумм показателей степеней при x_i в w_j меньше n. Тогда число наборов элементов группы G, удовлетворяющих формуле*

$$\bigwedge_j\left(w_jU_j\subseteq V_j\right),$$

делится на порядок централизатора множества всех коэффициентов слов w_j. В частности, это число делится на порядок группы G, если $\{w_j(x_1,\dots,x_n)\}\subset F(x_1,\dots,x_n)$.

Доказательство. Рассмотрим одно из включений $wU\subseteq V$. Разложим множества U и V в объединения классов сопряжённости:

$$U=a_1^G\cup a_2^G\cup\dots,\quad V=b_1^G\cup b_2^G\cup\dots.$$

*) которое мы переформулировали на удобном для нас языке.

Тогда включение $wU \subseteq V$ эквивалентно следующей формуле первого порядка:

$$\forall y_1 \forall y_2 \ldots \exists z_1 \exists z_2 \ldots \bigwedge_k \bigvee_l w y_k^{-1} a_k y_k = z_l^{-1} b_l z_l.$$

Таким образом исходная конъюнкция включений превращается в формулу первого порядка, в которой все связанные переменные являются изолирующими, а все коэффициенты a_i и b_i — изолированными. Матрица этой формулы отличается от матрицы, составленной из сумм показателей степеней при x_i в w_j, только повторением строчек и утверждение вытекает теперь из основной теоремы.

Доказанное утверждение превращается в теорему Гордона–Родригеса-Виллегаса о сопряжённости, если $U_j = \{1\}$ и все $w_j \in F(x_1, \ldots, x_n)$. Отметим, что теорема об инвариантных множествах останется верной, если конъюнкцию включений заменить на конъюнкцию произвольных (возможно различных) теоретико-множественных отношений, «логически выражающихся» через включения. Например, $\subseteq$ можно заменить на $\subset$, $\supseteq$, $\supset$, $=$, $\neq$, $\not\subset$, «*пересекается с*»,... Саму конъюнкцию тоже можно заменить на любую бескванторную формулу первого порядка. Например, *если* $A = a^G$ *и* $B = b^G$ *— какие-то классы сопряжённости в группе* G*, то число пар элементов* $(x, y) \in G^2$ *таких, что*

$$x^2 y^3 [x, y] y^{-1} AB = A \quad \textit{или} \quad (yx)^2 A \textit{ не пересекается с } B,$$

делится на $|G|$. Это следует из основной теоремы. (Второе утверждение дизъюнкции эквивалентно формуле $\forall z \forall t\ (yx)^2 z^{-1} az \neq t^{-1} bt$.)

Следующее утверждение является аналогом теоремы Соломона (и превращается в неё в случае, когда все коэффициенты равны единице, формула является бескванторной и имеет вид конъюнкции равенств).

Следствие 3. *Число наборов элементов группы, удовлетворяющих формуле* φ*, делится на порядок централизатора множества всех неизолированных коэффициентов формулы* φ *(в частности, это число делится на порядок группы при условии, что все неизолированные коэффициенты равны единице), если в формуле* φ

$$\begin{gathered}(\textit{число собственных вхождений связанных переменных}) + \\ + (\textit{число компонент связности графа } \Gamma(\varphi)) + \\ + (\textit{число атомарных подформул, не содержащих связанных переменных}) < (\textit{число всех переменных}).\end{gathered} \qquad (*)$$

Под *вхождением переменной* y здесь понимается максимальное подслово в левой части уравнения, рассматриваемой как циклическое слово, содержащее переменную y и не содержащее других переменных; вхождение называем *собственным*, если оно не совпадает со всей левой частью равенства. В приведённом выше примере имеется два вхождения переменной y и два вхождения переменной z, всего четыре вхождения связанных переменных, все эти вхождения собственные. Число вхождений особой переменной q всегда равно числу неоднородных уравнений (из-за того, что мы рассматриваем левые части уравнений как циклические слова).

Доказательство. Ранг первой группы гомологий графа, как известно, равен числу рёбер минус число вершин плюс число компонент связности. Число вершин равно числу связанных переменных, а число рёбер равно числу вхождений связанных переменных, причём несобственные вхождения дадут петли с нулевой меткой. Поэтому ранг матрицы $A(\varphi)$ не больше чем величина, стоящая в левой части неравенства $(*)$, минус число связанных переменных. Остаётся сослаться на теорему.

Интересно, что на самом деле граф $\Gamma(\varphi)$ всегда можно считать связным в том смысле, что граф формулы, записанной экономно, то есть с минимально возможным числом связанных переменных (среди формул, эквивалентных данной), всегда связен. Например, всякая формула с двумя связанными переменными, которые не входят вместе ни в одну атомарную подформулу, эквивалентна формуле с одной связанной переменной. Этот факт доказывает Дима Трушин в дополнении к этой статье.

Следствие 4. *Число элементов группы,* k*-е степени которых лежат в данной подгруппе, делится на порядок этой подгруппы.*[*)]

Доказательство. Пусть H — подгруппа группы G. Нас интересуют элементы x, для которых $x^k \in H$. Предположим сперва, что подгруппа H является централизатором некоторой подгруппы A. Тогда включение $x \in H$ равносильно системе уравнений $\{[x^k, a] = 1\ ;\ a \in A\}$, удовлетворяющей основной теореме (здесь связанных переменных нет и матрица нулевая). Поэтому число решений делится на порядок централизатора множества коэффициентов, то есть на $|H|$, что и требовалось.

[*)] В 2017 году мы узнали, что этот факт был установлен в [Iwa82].

Пусть теперь H — произвольная подгруппа. Можно применить следующий трюк. Вложим группу G в бóльшую группу $\widehat{G}$ так, что H станет централизатором некоторой подгруппы A группы $\widehat{G}$. Ещё надо позаботиться о том, чтобы все решения нашей системы уравнений над $\widehat{G}$ лежали в G. Для этого мы сделаем G централизатором некоторой другой подгруппы $B \subset \widehat{G}$ и рассмотрим систему уравнений

$$\left(\bigwedge_{a\in A} ([x^k, a] = 1)\right) \wedge \left(\bigwedge_{b\in B} ([x, b] = 1)\right).$$

Это докажет следствие 4 в общем случае.

В качестве $\widehat{G}$ можно взять свободное произведение с объединёнными подгруппами $\widehat{G} = (B \times G) \underset{H}{*} (H \times A)$, где A и B — произвольные нетривиальные группы с тривиальными центрами. Ясно, что $C(A) = H$ и $C(B) = G$, то есть решениями нашей системы уравнений являются в точности элементы группы G, k-е степени которых лежат в H. Согласно основной теореме число решений делится на $|C(A) \cap C(B)| = |H \cap G| = |H|$, что и требовалось.

Это доказательство следствия 4 использует лишь очень частный случай основной теоремы, когда формула φ представляет собой систему уравнений с одним неизвестным. В этом случае наша теорема немедленно вытекает из старого результата Ф. Холла (обобщающего теорему Фробениуса).

Теорема Холла ([Hall36], Теорема II)**.** *В любой группе число решений системы уравнений с одним неизвестным делится на* НОД$(|C|, n_1, n_2, \ldots)$*, где C — это централизатор множества всех коэффициентов, а n_i — сумма показателей степеней при неизвестном в i-м уравнении.*

Трюк (но другой) с превращением произвольной подгруппы в централизатор также можно найти в [Hall36]. В параграфе 4 мы приведём прямое доказательство следствия 4, иллюстрирующее часть доказательства основной теоремы.

Аналогичным образом доказывается более общий факт.

Следствие 5. *Пусть H — подгруппа группы G и W — подгруппа (или подмножество) конечно порождённой группы F с бесконечным индексом коммутанта. Тогда число гомоморфизмов $f\colon F \to G$ таких, что $f(W) \subseteq H$, делится на $|H|$.*

Доказательство. Пусть группа F задаётся копредставлением $F = \langle X \mid R\rangle$. Тогда число интересующих нас гомоморфизмов равно числу решений системы уравнений

$$\left(\bigwedge_{r\in R} (r = 1)\right) \wedge \left(\bigwedge_{a\in A,\ w\in W} ([w, a] = 1)\right) \wedge \left(\bigwedge_{b\in B\ x\in X} ([x, b] = 1)\right) \quad \text{с множеством неизвестных } X$$

в группе $\widehat{G} = (B \times G) \underset{H}{*} (H \times A)$, где A и B — произвольные нетривиальные группы с тривиальными центрами. Ранг матрицы этой системы совпадает с рангом матрицы системы $\{r = 1\ ;\ r \in R\}$ (так как остальные уравнения коммутаторные) и меньше числа неизвестных X, поскольку индекс коммутанта группы $F = \langle X \mid R\rangle$ бесконечен. Согласно следствию 1 число решений делится на $|C(A) \cap C(B)| = |H \cap G| = |H|$, что и требовалось.

Отметим, что следствие 5 превращается в следствие 4 в случае $F = \mathbb{Z}$ и в теорему Гордона–Родригеса-Виллегаса в случае $H = G$.

2. Примеры

Начнём с любопытного примера применения теоремы Соломона.

Пример 1. Скажем, что два элемента группы принадлежат одному *племени*, если их квадраты равны. Ясно, что суммарная численность всех племён равна порядку группы. Менее очевидно, что

сумма 2017-х степеней численностей племён всегда делится на порядок группы.

Для доказательства этого факта достаточно рассмотреть систему уравнений $x_1^2 = \ldots = x_{2017}^2$. Число решений, очевидно, равно сумме 2017-х степеней численностей племён, а уравнений меньше чем неизвестных. Остаётся сослаться на теорему Соломона. Утверждение останется справедливым, если 2017 заменить на любое натуральное число; квадраты в определении племени тоже можно заменить на любые (одинаковые) натуральные степени.

Пример 2. *Число пар элементов группы, произведение квадратов которых является кубом, делится на порядок группы.* Это вытекает из следствия 3, поскольку в формуле $\exists z\, x^2y^2 = z^3$ одна связанная переменная, она входит один раз, равенств без связанных переменных нет, граф связный, свободных переменных две: $1 + 0 + 1 < 2 + 1$.

Правда, этот факт легко вывести из теоремы Гордона–Родригеса-Виллегаса о сопряжённости. Действительно, эта теорема, в частности, означает, что на порядок группы делится число пар элементов группы, произведение квадратов которых сопряжено любому заданному элементу. По тем же причинам *на порядок группы делятся, например, следующие числа:*

- *число пар некоммутирующих элементов группы, произведение квадратов которых является кубом нецентрального элемента;*
- *число пар некоммутирующих элементов группы, произведение квадратов которых является кубом тогда и только тогда, когда куб их произведения лежит в центре;*
- *число пар элементов группы, у которых либо произведение квадратов является кубом, либо коммутатор не является квадратом;*
- ...

Пример 3. *На порядок группы делится число пар элементов этой группы, произведение квадратов которых является кубом коммутатора* ($x_1^2x_2^2 = [z,t]^3$), *а квадрат произведения — коммутатором кубов тех же элементов* ($(x_1x_2)^2 = [z^3,t^3]$). Этот факт уже затруднительно вывести из теоремы Гордона–Родригеса-Виллегаса о сопряжённости, но он немедленно вытекает из нашей основной теоремы. В силу следствие 2 верен более общий факт: *на порядок группы делится число пар элементов, квадрат произведения которых и произведение квадратов которых одновременным сопряжением могут быть превращены в любую фиксированную пару элементов.*

Аналогия между теоремой Гордона–Родригеса-Виллегаса и всем известными свойствами решений систем линейных уравнений (скажем, над конечными полями) может навести на мысль, что если ранг матрицы намного меньше числа неизвестных, то число решений должно делиться на более высокую степень порядка группы. Более реалистичный вопрос следующий:

если конечно порождённая группа H допускает эпиморфизм на свободную группу ранга m, то верно ли, что число гомоморфизмов $H \to G$ делится на $|G|^m$?

Дело в том, что число решений системы уравнений $\{u(x_1,\dots,x_n) = v(x_1,\dots,x_n) = \dots = 1\}$ без коэффициентов равно числу гомоморфизмов из группы $H = \langle x_1,\dots,x_n \,|\, u(x_1,\dots,x_n) = v(x_1,\dots,x_n) = \dots = 1\rangle$ в группу G. Матрица системы имеет ранг не больше r тогда и только тогда, когда группа H обладает эпиморфизмом на свободную абелеву группу ранга $n-r$. Наличие эпиморфизма на абсолютно свободную группу такого ранга является гораздо более сильным свойством, но тем не менее гипотеза, о которой мы говорим, неверна при $m > 1$, как показывает следующий пример.

Пример 4. Группа $\langle x,y,z \,|\, z = z^xz^y\rangle$ обладает эпиморфизмом на свободную группу ранга два (посылающим z в единицу), но число решений уравнения $z = z^xz^y$ в симметрической группе S_3 не делится на $|S_3|^2 = 36$. Действительно, при $z = 1$ мы имеем 36 решений (x и y могут принимать любые значения). При $z = (123)$ мы имеем $3\cdot 3 = 9$ решений (x и y — любые транспозиции). При $z = (321)$ аналогично имеем ещё 9 решений. А если z — транспозиция, то решений нет (по соображениям чётности). Всего получается $36 + 2\cdot 9$ решений.

3. Доказательство основной теоремы

Лемма 1. *В условиях теоремы обратимой заменой свободных переменных можно добиться того, что первый столбец матрицы $A(\varphi)$ станет нулевым. В частности, в каждый цикл графа $\Gamma(\varphi)$ переменная x_1 будет входить в нулевой суммарной степени.*

Доказательство. Ранг матрицы $A(\varphi)$ меньше чем число её столбцов, поэтому, как известно, целочисленными (обратимыми) элементарными преобразованиями столбцов её можно превратить в матрицу с нулевым первым столбцом. Элементарные преобразования столбцов происходят при очевидных заменах переменных, например, замена $x_i \to x_ix_j^k$ даёт прибавление к j-му столбцу i-го столбца, умноженного на k. Лемма 1 доказана.

Например, чтобы обнулить первый столбец матрицы (2) из параграфа 1, достаточно из первого столбца вычесть второй, то есть в формуле (1) надо сделать замену переменных $x_2 \to x_2x_1^{-1}$. Формула (1) примет вид

$$\forall y \exists z \ \left(\left([ygy, x_1gx_2x_1^{-1}]x_1a^z(x_2x_1^{-1})^{-3}x_1^3h(x_2x_1^{-1})^7 = 1\right) \wedge \neg\left(b^zx_2^2 = 1\right) \vee \left(x_1^2(x_2x_1^{-1})^2)^5 = 1\right)\right), \qquad (3)$$

её граф изображён на рисунке 2

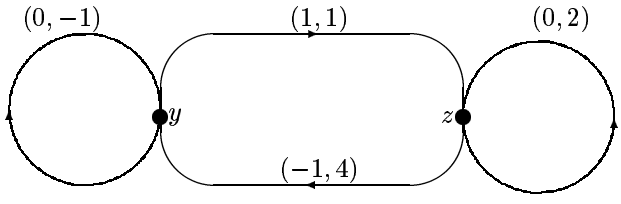

Рис. 2

и её матрица имеет вид

$$\begin{pmatrix} 0 & -1 \\ 0 & 5 \\ 0 & 2 \\ 0 & 10 \end{pmatrix}.$$

Далее считаем, что в каждый цикл графа $\Gamma(\varphi)$ переменная x_1 входит в нулевой суммарной степени.

Для каждой переменной t (свободной или связанной) введем новые символы $t^{(i)}$, где $i \in \mathbb{Z}$ (смысл их будет состоять в том, что $t^{(i)} = t^{x_1^i} = x_1^{-i} t x_1^i$, если переменная t неизолирующая, и $t^{(i)} = t x_1^i$, если переменная t изолирующая, но мы пока действуем чисто формально). Аналогично для каждого неизолированного коэффициента g введём новые символы $g^{(i)}$, где $i \in \mathbb{Z}$. Преобразуем формулу φ следующим образом:

1) заменим в атомарных подформулах каждый символ t на $t^{(0)}$, где t — переменная, отличная от x_1, или коэффициент;
2) каждое подслово вида $(t^{(i)})x_1^l$, где t — неизолирующая переменная или коэффициент, заменим на слово $x_1^l(t^{(i+l)})$; каждое подслово вида $(g^{t^{(i)}})x_1^l$, где t — изолирующая переменная и $g \in G$, заменим на слово $x_1^l(g^{t^{(i+l)}})$;
3) повторим шаг 2) до тех пор, пока это возможно.

После такого сдвига влево символов x_1 мы получим формулу, не содержащую x_1 (из того, что сумма степеней при x_1 равна нулю и в каждом цикле графа, и в каждой атомарной подформуле без связанных переменных следует, что сумма степеней при x_1 равна нулю во всех атомарных подформулах). Например, формула (3) после этих преобразований будет иметь следующие атомарные подформулы:

$$\begin{aligned} [y^{(0)} g^{(0)} y^{(0)}, g^{(-1)} x_2^{(-1)}] a^{z^{(-1)}} \left(x_2^{(-4)} x_2^{(-3)} x_2^{(-2)}\right)^{-1} h^{(-7)} x_2^{(-7)} x_2^{(-6)} x_2^{(-5)} x_2^{(-4)} x_2^{(-3)} x_2^{(-2)} x_2^{(-1)} &= 1, \\ b^{z^{(0)}} (x_2^{(0)})^2 &= 1, \\ (x_2^{(-2)} x_2^{(-1)})^5 &= 1. \end{aligned} \tag{4}$$

Теперь продолжим преобразование формулы:

4) В каждой атомарной подформуле α заменим все входящие в неё символы $t^{(i)}$ на $t^{(i+j_\alpha)}$, где целые числа j_α подберём таким образом, чтобы для каждой связанной переменной t символы $t^{(i)}$ встречались во всей формуле не более чем при одном значении i; это возможно из-за того, что сумма степеней при x_1 равна нулю в каждом цикле графа.

   В рассматриваемом примере (4) достаточно уменьшить на единицу верхние индексы во втором равенстве. В общем случае следует действовать так. В каждой компоненте связности K графа Γ выберем вершину (переменную) y_K. В каждой атомарной подформуле α, содержащем связанные переменные, выберем одну из таких переменных y_α. Соединим каждую вершину y_α путём p_α с вершиной y_K такой, что $y_\alpha \in K$. Сумма s_α первых координат меток рёбер пути p_α не зависит от выбора пути по условию. Положим $j_\alpha = -i_\alpha - s_\alpha$, где i_α — такое единственное число, что $y_\alpha^{(i_\alpha)}$ входит в уравнение α. То, что сумма первых координат меток рёбер в каждом цикле равна нулю, означает, что $s_\alpha = s_\beta$, если $y_\alpha = y_\beta$, величина j_α не зависит от выбора переменных y_α, входящих в уравнение α, и после замен $t^{(i)}$ на $t^{(i+j_\alpha)}$ в каждом уравнении α каждая связанная переменная t будет входить во всю формулу только с одним индексом (i), где i есть сумма первых координат меток рёбер пути, соединяющего y_K с t.
5) Заменим в каждой кванторной приставке $\forall y$ и $\exists y$ на $\forall y^{(p)}$ и $\exists y^{(p)}$, где $p \in \mathbb{Z}$ — такое единственное число, что $y^{(p)}$ встречается в атомарных подформулах;
6) добавим к полученной формуле $\widehat{\varphi}$ равенства, определяющие новые символы, то есть заменим $\widehat{\varphi}$ на бесконечную формулу

$$\varphi' = \widehat{\varphi} \wedge \underbrace{\left(\bigwedge_g \left(g^{(0)} = g\right)\right) \wedge \left(\bigwedge_{t,i} \left(t^{(i)} = x_1^{-1} t^{(i-1)} x_1\right)\right)}_{\delta}, \tag{**}$$

   где t пробегает все свободные переменные и все коэффициенты исходной формулы, i пробегает все целые числа, а g пробегает все коэффициенты. Символы $g^{(i)}$, где $g \in G$, мы тоже считаем свободными переменными формулы φ'.

Полученной формуле φ' удовлетворяет столько же наборов элементов группы, сколько удовлетворяет исходной формуле φ. Действительно, формуле $\varphi' = \widehat{\varphi} \wedge \delta$ удовлетворяет, очевидно, столько же наборов, сколько формуле $\overline{\varphi} = \widehat{\varphi}\big|_{t^{(i)} = t^{x_1^i}}$ (то есть формуле $\widehat{\varphi}$, в которую вместо каждого символа $t^{(i)}$, где t — свободная переменная исходной формулы или коэффициент, подставлено выражение $x_1^{-i} t x_1^i$). Формула $\overline{\varphi}$ эквивалентна формуле φ (то

есть этим формулам удовлетворяют одни и те же наборы). Действительно, формула $\overline{\varphi}$ отличается от формулы φ двумя моментами:

а) в кванторных приставках вместо символов y стоят символы $y^{(p)}$;

б) в атомарных подформулах вместо связанных переменных y стоят выражения $(y^{(p)})x_1^{-p}$ или $(y^{(p)})^{x_1^{-p}}$, в зависимости от того, является ли переменная y изолирующей, где p одно и то же для всех вхождений переменной y.

Но формулы, отличающиеся только этим, очевидно эквивалентны: например, $(\forall y\,\alpha(y,z,\ldots)) \equiv (\forall t\,\alpha(t^{z^2},z,\ldots))$, так как для любого $g \in G$ верно, что если y пробегает всё группу, то y^g пробегает всю группу.

Таким образом, нам достаточно показать, что число наборов, удовлетворяющих формуле φ' (такие наборы мы будем называть *решениями*), делится на $|C|$, где буквой C мы обозначили централизатор множества всех коэффициентов формулы φ (или φ', что то же самое).

Рассмотрим одно решение $X = \left(\widetilde{x}_1,\, \widetilde{x}_i^{(j)},\, \widetilde{g}^{(j)}\ i=2,\ldots,n,\ j\in\mathbb{Z}\right)$. Набор $\left(\widetilde{x}_i^{(j)},\, \widetilde{g}^{(j)}\right)$, то есть всё, кроме $\widetilde{x}_1$, будем называть *хвостом* решения X. Буквой B_X мы обозначим централизатор хвоста решения X. Заметим, что $B_X \subseteq C$ (из-за уравнений $g^{(0)} = g$ в формуле $(**)$).

Будем говорить, что два решения *похожи*, если их хвосты сопряжены при помощи какого-то элемента из C. Ясно, что это отношение эквивалентности. Теорема очевидным образом вытекает из следующего утверждения.

Утверждение. *В каждом классе похожих решений содержится ровно $|C|$ решений.*

Найдем число решений, похожих на X. Число возможных хвостов таких решений равно $|C|/|B_X|$, так как на множестве хвостов решений, похожих на X, группа C действует сопряжением (так как набор, сопряжённый при помощи $c \in C$ к хвосту любого решения Y также является хвостом некоторого решения, например, Y^c) и B_X — это стабилизатор хвоста решения X.

Число решений с таким же хвостом, как у X, равно $|B_X|$, поскольку если набор с тем же хвостом и первой координатой $\widetilde{x}_1'$ тоже является решением, то частное $\widetilde{x}_1'(\widetilde{x}_1)^{-1}$ должно коммутировать с хвостом, как показывают уравнения δ в формуле $(**)$, то есть $\widetilde{x}_1' \in B_X\widetilde{x}_1$. С другой стороны, любой элемент $\widetilde{x}_1' \in B_X\widetilde{x}_1$ даёт решение с тем же хвостом, так как переменная x_1 входит в формулу φ' только в подформуле δ.

Если X' — решение, похожее на X, то число решений с таким же хвостом, как у X', равно $|B_{X'}| = |B_X|$ (раз хвосты сопряжены, то их централизаторы сопряжены и имеют одинаковые порядки).

В итоге получаем, что число решений, похожих на X, равно $(|C|/|B_X|)\cdot|B_X| = |C|$, что и доказывает утверждение, а вместе с ним и теорему.

4. Корни из подгрупп

В параграфе 1 следующее утверждение было выведено из основной теоремы.

Следствие 4. *Число элементов группы, k-е степени которых лежат в данной подгруппе, делится на порядок этой подгруппы.*

Здесь мы приведём прямое доказательство с целью продемонстрировать заключительную часть доказательства основной теоремы на простом примере.

Будем для простоты предполагать, что $k = 2$. Итак, есть группа G и её подгруппа H. Нас интересуют элементы $x \in G$ такие, что $x^2 \in H$, такие элементы мы называем *решениями*. Утверждение немедленно вытекает из следующей леммы.

Лемма. *В каждом двойном смежном классе HxH содержится либо 0, либо $|H|$ решений.*

Доказательство. Пусть x — решение, его *хвостом* мы назовём смежный класс Hx.

Группа H действует (справа) на множестве хвостов решений из двойного смежного класса HxH умножением справа:

$$Hy \circ h = Hyh\ (= \textit{хвост решения } y^h).$$

Стабилизатор хвоста Hx — это $B_x \stackrel{\text{опр}}{=} H \cap H^x$:

$$Hx = Hxh \iff h \in H^x.$$

Значит, *у всевозможных решений, лежащих в HxH, ровно $|H|/|B_x|$ различных хвостов.*

Сколько решений имеет такой же хвост, как x?

$$Hx = Hy \Longrightarrow yx^{-1} \in H,$$

но если при этом y тоже является решением, то

$$(Hx)x = Hx^2 = H = Hy^2 = (Hx)y,$$

то есть

$$yx^{-1} \in H^x.$$

Таким образом, каждое решение y с таким же хвостом, как у x, лежит в $B_x x$. С другой стороны, каждый элемент из этого смежного класса является решением:

$$(bx)^2 = bxbx = bb^{x^{-1}}x^2 \in H, \quad \text{так как } b,\ b^{x^{-1}} \text{ и } x^2 \text{ лежат в } H.$$

Получается, что *число решений с таким же хвостом, как у x, равно $|B_x|$*.

Так как $|B_x| = |B_y|$, если x и y лежат в одном двойном смежном классе по H (поскольку B_x и B_y сопряжены в этом случае), всего получается $|B_x| \cdot (|H|/|B_x|) = |H|$ решений, что и завершает доказательство.

Недавно И. М. Айзекс [Isaa12] получил получил доказательство этого следствия, опирающееся на теорию характеров.

В 2017 году мы узнали, что это следствие было получено в [Iwa82].

ДОПОЛНЕНИЕ. О МИНИМИЗАЦИИ ЧИСЛА СВЯЗАННЫХ ПЕРЕМЕННЫХ В ФОРМУЛАХ ПЕРВОГО ПОРЯДКА

Дмитрий В. Трушин

Einstein Institute of Mathematics, The Hebrew University of Jerusalem,
Givat Ram, Jerusalem, 91904, Israel
trushindima@yandex.ru

Пусть φ — формула первого порядка (в некотором языке) со связанными переменными $y_1, \dots, y_k$ и свободными переменными $x_1, \dots, x_m$. Построим граф $\Delta(\varphi)$ на вершинах $y_1, \dots, y_k$ следующим образом: вершины y_i и y_j соединяются ребром если существует атомарная подформула в φ, содержащая одновременно и y_i и y_j.

Следующее утверждение показывает, что формула φ с несвязным графом $\Delta(\varphi)$ эквивалентна формуле с меньшим числом связанных переменных.

Утверждение. *Формула φ эквивалентна формуле φ' со связным графом $\Delta(\varphi')$ таким, что*

$$|\Delta(\varphi')| \leqslant \max(|\Delta_1|, \dots, |\Delta_s|), \qquad \text{где } \Delta_1, \dots, \Delta_s \text{ — компоненты связности графа } \Delta(\varphi).$$

Доказательство. Пусть Φ_i — множество формул ψ таких, что

1) все переменные формулы ψ (и свободные, и связанные) лежат в множестве $\{x_1, \dots, x_m\} \cup \{y_1, \dots, y_k\}$;
2) все связанные переменные формулы ψ лежат в множестве $\{y_1, \dots, y_k\}$;
3) если переменная y_j встречается в ψ, не зависимо от того связанная она или свободная, то $y_j \in \Delta_i$.

Заметим, что классы Φ_i замкнуты относительно логических операций и применения кванторов по y_j.

Пусть Λ — замыкание объединения $\bigcup\limits_i \Phi_i$ относительно логических операций ($\vee$, $\wedge$ и $\neg$). Ясно, что каждая формула из класса Λ может быть записана в виде

$$\psi = \bigvee_{i=1}^{l} \bigwedge_{j=1}^{s} r_{ij}, \quad \text{где } r_{ij} \in \Phi_j, \tag{D}$$

и в виде

$$\psi = \bigwedge_{i=1}^{l} \bigvee_{j=1}^{s} r_{ij}, \quad \text{где } r_{ij} \in \Phi_j, \tag{C}$$

так как конъюнкция и дизъюнкция взаимно дистрибутивны, классы Φ_i замкнуты относительно логических операций, $\neg(A \vee B) = (\neg A) \wedge (\neg B)$ и $\neg(A \wedge B) = (\neg A) \vee (\neg B)$.

Лемма. *Класс формул Λ замкнут относительно применения кванторов по переменным y_j.*

Доказательство. Заметим, что

$$\forall y(\psi_1(y) \wedge \psi_2(y)) = (\forall \psi_1(y)) \wedge (\forall y \psi_2(y)) \quad \text{и} \quad \forall y(\psi_1(y) \vee \psi_2) = (\forall y \psi_1(y)) \vee \psi_2,$$

где во втором равенстве y не является свободной переменной формулы ψ_2. Для квантора существования верны аналогичные равенства

$$\exists y(\psi_1(y) \vee \psi_2(y)) = (\exists \psi_1(y)) \vee (\exists y \psi_2(y)) \quad \text{и} \quad \exists y(\psi_1(y) \wedge \psi_2) = (\exists y \psi_1(y)) \wedge \psi_2,$$

где во втором равенстве y не является свободной переменной формулы ψ_2.

Пусть формула $\psi \in \Lambda$ записана в виде (D):

$$\psi = (r_{11} \wedge \ldots \wedge r_{1s}) \vee \ldots \vee (r_{l1} \wedge \ldots \wedge r_{ls})$$

и переменная y_j лежит в компоненте Δ_t, тогда

$$\begin{aligned}\exists y_j\,(r_{11} \wedge \ldots \wedge r_{1s}) \vee \ldots \vee (r_{l1} \wedge \ldots \wedge r_{ls}) &= (\exists y_j\,(r_{11} \wedge \ldots \wedge r_{1s})) \vee \ldots \vee (\exists y_j\,(r_{l1} \wedge \ldots \wedge r_{ls})) = \\ &= (r_{11} \wedge \ldots \wedge (\exists y_j r_{1t}) \wedge \ldots \wedge r_{1s}) \vee \ldots \vee (r_{l1} \wedge \ldots \wedge (\exists y_j) r_{lt} \wedge \ldots \wedge r_{ls})\,,\end{aligned}$$

где первое равенство справедливо всегда, а второе равенство имеет место, так как в i-й скобке только r_{it} может зависеть от переменной y_j. Аналогичные преобразования можно сделать для квантора всеобщности, если воспользоваться видом (C) формулы $\psi \in \Lambda$. Лемма доказана.

Продолжим доказательство утверждения. По условию каждая атомарная подформула формулы φ принадлежит какому-то классу Φ_i, то есть, в частности, эта подформула лежит в Λ. Так как класс Λ замкнут относительно логических операций и применения кванторов по y_j (по лемме), мы получаем, что $\varphi \in \Lambda$, то есть

$$\varphi = \bigvee_{i=1}^{l} \bigwedge_{j=1}^{s} r_{ij}.$$

Пусть для определенности максимум $|\Delta_i|$ достигается на Δ_1. Тогда в каждой формуле r_{ij} при $j \neq 1$ поменяем имена связанных переменных из Δ_j на имена переменных из Δ_1. Так как Δ_1 самая большая компонента, мы сможем приписать разные имена из Δ_1 разным переменным (в каждой конкретной формуле r_{ij}). После такого переименования получим формулу φ', эквивалентную исходной, и все ее связанные переменные будут среди переменных из Δ_1.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[Стру95] Струнков С.П. К теории уравнений на конечных группах // Изв. РАН. Сер. матем. 1995. Т.59:6. С.171–180

[Hall59] Холл М. Теория групп. - М.: ИЛ, 1962.

[AmV11] Amit A., Vishne U. Characters and solutions to equations in finite groups // J. Pure Appl. Algebra. 2011. V.10. no.4. P.675–686.

[AsTa01] Asai T., Takegahara Y. $|\mathrm{Hom}(A,G)|$, IV // J. Algebra. 2001. 246. pp. 543–563.

[BrTh88] Brown K., Thévenaz J. A generalization of Sylow's third theorem // J. Algebra. 1988. 115. P. 414–430.

[Frob03] Frobenius G. Über einen Fundamentalsatz der Gruppentheorie // Berl. Sitz. 1903. S.987–991.

[GRV12] Gordon C., Rodriguez-Villegas F. On the divisibility of $\#\mathrm{Hom}(\Gamma,G)$ by $|G|$ // J. Algebra. 2012. V.350, no.1, P. 300–307. See also arXiv:1105.6066.

[Hall36] Hall Ph. On a theorem of Frobenius // Proc. London Math. Soc. 1936. V.40. P.468–531.

[Isaa70] Isaacs I. M. Systems of equations and generalized characters in groups // Canad. J. Math. 1970. V.22. P.1040–1046.

[Isaa12] Isaacs I. M. The number of group elements whose squares lie in a given subgroup (an answer to Klyachko's question). `http://mathoverflow.net/questions/98639#98809` (2012).

[Iwa82] S. Iwasaki, A note on the nth roots ratio of a subgroup of a finite group // J. Algebra, 78:2 (1982), 460-474.

[Kula38] Kulakoff A. Einige Bemerkungen zur Arbeit: "On a theorem of Frobenius" von P. Hall // Матем. сб. 1938. 3(45):2. 403–405.

[Sehg62] Sehgal S. K. On P. Hall's generalisation of a theorem of Frobenius // Proc. Glasgow Math. Assoc. 1962. 5. P. 97–100.

[Solo69] Solomon L. The solutions of equations in groups // Arch. Math. 1969. V.20. no.3. P. 241–247.