Л.22

3.4. Алгоритмические проблемы

Копредставления групп — вещь полезная, но очень неконструктивная. Пусть, например, дано копредставление $G = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1\rangle$ и слово v в алфавите $\{x_1^{\pm1}, \dots, x_n^{\pm1}\}$. Как выяснить, представляет ли слово v единичный элемент группы G? Или, другими словами, следует ли соотношение $v = 1$ из определяющих соотношений $r_1 = 1, \dots, r_m = 1$? Эта задача называется *проблемой равенства**) для данного копредставления. Вообще говоря, не существует способа решить проблему равенства.

Теорема Новикова–Буна. *Существует конечное копредставление с алгоритмически неразрешимой проблемой равенства.*

Вот явный пример (заимствованный из статьи [КоЦи90]) такого копредставления:

$$\left\langle \begin{array}{l} a, b, \\ c, d, \\ e, p, \\ q, r, \\ t, k \end{array} \middle| \begin{array}{c} p = p^{10a} = p^{10b} = p^{10c} = p^{10d} = p^{10e},\ q^{10} = q^a = q^b = q^c = q^d = q^e, \\ [r,a] = [r,b] = [r,c] = [r,d] = [r,e] = 1, \\ (pacq)^r = pcaq,\ (p^2adq^2)^r = p^2daq^2,\ (p^3bcq^3)^r = p^3cbq^3, (p^3bcq^4)^r = p^4cbq^4,\ (p^5ceq^5)^r = p^5ecaq^5, \\ (p^6deq^6)^r = p^6edbq^6,\ (p^7cdcq^7)^r = p^7cdceq^7,\ (p^8ca^3q^8)^r = p^8a^3q^8,\ (p^9da^3q^9)^r = p^9a^3q^9, \\ [p,t] = [q,t] = [p,k] = [q,k] = [k, t^{a^3}] = 1 \end{array} \right\rangle .$$

Не существует алгоритма, решающего проблему равенства в этой группе. Обратите внимание, что утверждается не то, что такого алгоритма никто не смог придумать, а то, что такой алгоритм нельзя придумать.

Мы не будем доказывать теорему Новикова–Буна, мы даже не будем пытаться дать строгое определение того, что мы понимаем под словом «алгоритм» (смотрите по этому поводу, например, [ВеШе99]). Интуитивно алгоритм можно понимать как очень чётко указанный универсальный способ, позволяющий решить данный класс задач «не думая». Не будет ошибкой, если под словом алгоритм понимать компьютерную программу. Обратите внимание, что для доказательства существования алгоритма, решающего ту или иную задачу, достаточно иметь интуитивное представление об алгоритмах, но если вы хотите доказать алгоритмическую неразрешимость некоторой проблемы, вы должны иметь строгое определение понятия *алгоритм*.

Следующее утверждение показывает, что свойство группы иметь разрешимую (или неразрешимую) проблему равенства является *алгебраическим свойством*, то есть не зависит от выбора конечного копредставления.

Утверждение 3.4.1. *Если конечные копредставления*

$$G = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1\rangle \quad \text{и} \quad H = \langle y_1, \dots, y_l \,|\, s_1 = 1, \dots, s_k = 1\rangle$$

задают изоморфные группы, то проблема равенства для этих копредставлений разрешима или неразрешима одновременно.

Доказательство. Пусть $\varphi\colon G \to H$ — изоморфизм и копредставление H имеет разрешимую проблему равенства. Тогда алгоритм, решающий проблему равенства для копредставления G, выглядит следующим образом: Чтобы узнать, представляет ли слово $v = \prod x_i^{\varepsilon_i}$ единицу группы G, запишем слово $\varphi(v) = \prod \varphi(x_i)^{\varepsilon_i}$ и применим к нему алгоритм, решающий проблему равенства в группе H. Ясно, что $\varphi(v) = 1$ в H тогда и только тогда, когда $v = 1$ в G.

Имеется простой алгоритм, решающий проблему равенства «наполовину». Действительно, легко написать алгоритм, который выписывает все следствия из определяющих соотношений $r_1, \dots, r_n$, то есть все слова вида $\prod r_{i_j}^{\pm u_j}$, где u_j — произвольные слова. Если слово v равно единице в группе $G = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1\rangle$, то оно рано или поздно окажется выписанным и алгоритм нам скажет: «Да, это слово равно единице»; если же v не равно единице в группе G, то алгоритм никогда не остановится.

Итак, для любого конечного копредставления G существует алгоритм, назовём его $\mathsf{РАВНО}_G$, который ведёт себя следующим образом:

$$\mathsf{РАВНО}_G(v) = \begin{cases} \texttt{"Да"}, & \text{если } v = 1 \text{ в } G; \\ \text{не останавливается}, & \text{если } v \neq 1 \text{ в } G. \end{cases}$$

Утверждение 3.4.2. *Проблема равенства для копредставления $G = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1\rangle$ разрешима тогда и только тогда, когда существует алгоритм $\mathsf{НЕ\_РАВНО}_G$, который ведёт себя следующим образом:*

$$\mathsf{НЕ\_РАВНО}_G(v) = \begin{cases} \texttt{"Нет"}, & \textit{если } v \neq 1 \textit{ в } G; \\ \textit{не останавливается}, & \textit{если } v = 1 \textit{ в } G. \end{cases}$$

*) Употребляются также термины *проблема слов* и *проблема равенства слов*.

Доказательство. В одну сторону это утверждение очевидно: если имеется алгоритм, решающий проблему равенства, то сделать из него алгоритм $\mathsf{HE\_PABHO}_G$ не составляет труда.

Если же у нас есть алгоритм $\mathsf{HE\_PABHO}_G$, то алгоритм, решающий проблему равенства, строится следующим образом: запускаем на слове v параллельно алгоритмы PABHO_G и $\mathsf{HE\_PABHO}_G$; рано или поздно один из этих алгоритмов выдаст правильный ответ.

Будучи алгебраическим свойством, разрешимость проблемы равенства оказывается связанной с другими свойствами группы.

Теорема 3.4.1. *Проблема равенства разрешима в каждой простой конечно представленной группе.*

Доказательство. Пусть простая группа задана копредставлением $G = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1\rangle$. В силу утверждения 3.4.2 достаточно построить алгоритм $\mathsf{HE\_PABHO}_G$. Пусть v – произвольное слово в алфавите $\{x_1^{\pm 1}, \dots, x_n^{\pm 1}\}$. Рассмотрим копредставление $\widetilde{G} = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1, v = 1\rangle$ и определим алгоритм $\mathsf{HE\_PABHO}_G$ так:

$$\mathsf{HE\_PABHO}_G(v) = \texttt{"Нет"}, \text{ если для всех } i \;\; \mathsf{PABHO}_{\widetilde{G}}(x_i)=\texttt{"Да"}.$$

Если этот алгоритм останавливается, то он даёт правильный ответ, поскольку группа $\widetilde{G}$ тривиальна при $v \neq 1$ в G.

Очевидно, что проблема равенства разрешима также в каждой конечной группе. Следующая теорема представляет собой обобщение этого факта.

Теорема 3.4.2. *Проблема равенства разрешима в каждой финитно аппроксимируемой конечно представленной группе.*

Доказательство. Пусть $G = \langle x_1, \dots, x_n \,|\, r_1 = 1, \dots, r_m = 1\rangle$ — финитно аппроксимируемая группа. В силу утверждения 3.4.2 достаточно построить алгоритм $\mathsf{HE\_PABHO}_G$. Пусть $v(x_1, \dots, x_n)$ – произвольное слово в алфавите $\{x_1^{\pm 1}, \dots, x_n^{\pm 1}\}$. Определим алгоритм $\mathsf{HE\_PABHO}_G$ так: будем перебирать все отображения

$$\varphi\colon \{x_1, \dots, x_n\} \to S_k, \quad k = 1, 2, \dots,$$

множества образующих в симметрические группы и остановимся с ответом "Нет" в случае если

$$r_i(\varphi(x_1), \dots, \varphi(x_n)) = 1$$

для всех i (то есть отображение φ продолжается до гомоморфизма), а $v(\varphi(x_1), \dots, \varphi(x_n)) \neq 1$.

В силу финитной аппроксимируемости группы G и теоремы Кэли о вложимости всякой конечной группы в симметрическую наш алгоритм отвечает правильно для всех слов v, не равных единице в группе G.

Теорема 3.4.2 является основным приложением финитной аппроксимируемости и одним из самых мощных средств доказательства разрешимости проблемы равенства.

Упомянем некоторые другие алгоритмические проблемы.

Проблема сопряжённости. *По данным двум элементам требуется определить, сопряжены ли они в группе G.*

Проблема вхождения. *По данным элементам v, $u_1, \dots, u_k$ требуется определить, лежит ли v в подгруппе группы G, порождённой элементами $u_1, \dots, u_k$.*

Легко сообразить, что эти проблемы являются более трудными, чем проблема равенства: разрешимость любой из этих проблем влечёт разрешимость проблемы равенства. (Докажите!) Обратное неверно — имеются примеры конечно определённых групп с разрешимой проблемой равенства, но неразрешимой проблемой сопряжённости. А проблема вхождения неразрешима даже в такой безобидной группе как $F_2 \times F_2$ — прямое произведение двух свободных групп ранга 2 (теорема К. А. Михайловой).

Несколько особняком стоит ещё одна классическая алгоритмическая проблема.

Проблема изоморфизма. *По данным двум конечным копредставлениям требуется определить, изоморфны ли соответствующие группы.*

Обратите внимание, что в проблемах равенства, сопряжённости и вхождения копредставление фиксировано, а на вход алгоритма поступают слова от образующих и требуется определить те или иные свойства элементов группы, представленных данными словами. В проблеме изоморфизма на вход поступают сами копредставления.

Теорема Адяна–Рабина утверждает, что проблема изоморфизма алгоритмически неразрешима; более того, *не существует алгоритма, распознающего, задёт ли данное конечное копредставление тривиальную группу!*

3.5. Философское отступление: алгоритмические проблемы и доказуемость.

Теоремы об алгоритмической неразрешимости тех или иных проблем могут показаться на первый взгляд менее страшными, чем они есть на самом деле. Действительно, можно подумать, что в этих теоремах говорится о том, что компьютер неспособен решать некоторые задачи. В этом, конечно, нет ничего удивительного. Компьютер не обладает никакими талантами. Хочется верить, что если нам с вами очень нужно будет решить какую-нибудь задачу, например, выяснить, равно ли данное слово единице в данной группе, то мы проявим смекалку и уж как-нибудь получим ответ. К сожалению, для такого оптимизма нет оснований.

Метатеорема 3.5.1. *Для каждого конечного копредставления G с неразрешимой проблемой равенства существует слово w (такие слова будем называть плохими), про которое нельзя доказать ни то, что $w = 1$ в G, ни то, что $w \neq 1$ в G.*

Доказательство. Чтобы доказать это удивительное утверждение, надо, конечно, строго определить, что мы понимаем под словом «доказательство». Мы не будем здесь приводить соответствующее определение (смотрите по этому поводу, например, [СКМЛ83]). Отметим только, что любое разумное определение понятия *доказательство* обладает следующим свойством:

Всякое математическое доказательство может быть написано на некотором фиксированном формальном языке. Причём существует алгоритм ПРОВЕРКА, *который по данному тексту на этом языке и данному утверждению (также записанному на этом языке) говорит, является ли данный текст доказательством данного утверждения.*

Грубо говоря, этот тезис утверждает, что для проверки правильности максимально подробно записанного доказательства не надо думать, надо лишь проверить правильность всех переходов, и эту задачу вполне может решить компьютер.

Предположим теперь, что плохих слов для данного копредставления нет. Тогда мы можем легко построить алгоритм, решающий проблему равенства: получив на вход слово v, мы будем просто перебирать все тексты и давать их алгоритму ПРОВЕРКА, пока не наткнёмся на текст, который является либо доказательством того, что $v = 1$ в группе G, либо доказательством того, что $v \neq 1$ в G.*)

Замечание. Всякое слово, равное плохому в группе G, само является плохим, т.к. равенство двух слов v и w всегда можно доказать: для этого достаточно представить частное vw^{-1} в виде

$$vw^{-1} = \prod_j r_{i_j}^{\varepsilon_j u_j}, \quad \text{где } r_{i_j} \text{ — определяющие соотношения, } \varepsilon_j \in \{\pm 1\} \text{ и } u_j \text{ — произвольные слова.}$$

Значит, можно говорить о плохих или хороших элементах группы.**) Единица, очевидно, является хорошим элементом (поскольку задаётся пустым словом), то есть имеет место следующий странный факт:

Метатеорема 3.5.2. *Всякое плохое слово на самом деле не равно единице.*

В параграфе 3.4 мы привели пример группы с неразрешимой проблемой равенства. Можно ли привести конкретный пример плохого слова для этого копредставления? Нет. Хотя плохие слова существуют, предъявить конкретный пример в принципе невозможно!

Метатеорема 3.5.3. *Ни про один плохой элемент нельзя доказать, что он плохой.*

Доказательство. Действительно, доказательство плохости элемента g доказывало бы, в частности, что $g \neq 1$ (в силу метатеоремы 3.5.2), что противоречит определению плохого элемента.

Проблема равенства, о которой шла речь в этом параграфе, взята просто в качестве примера. Аналогичные метатеоремы можно сформулировать и для проблем сопряжённости и вхождения. Можно рассматривать и другие задачи, не обязательно даже алгебраические. Метатеорема 3.5.1 является одним из проявлений следующего общего принципа:

Во всякой достаточно сложной теории имеются верные, но недоказуемые утверждения.

Этот факт и его уточнения называют *теоремой Гёделя о неполноте.* Подробнее об этом можно прочитать в книгах по математической логике, например, [Успе82], [ВеШе99] или [СКМЛ83].

*) Разумеется, это чисто теоретическое рассуждение. Сколько времени понадобится компьютеру, чтобы таким способом найти правильное доказательство? Это время может оказаться больше чем время существования Солнца. А длина найденного доказательства может превзойти количество элементарных частиц во Вселенной.

**) Строго говоря, мы объяснили, что можно говорить о плохости элементов группы, заданной фиксированным копредставлением. Однако легко проверить, что если элемент группы G плох относительно некоторого конечного копредставления, то он плох и относительно любого другого конечного копредставления группы G (т.к. то, что два конечных копредставления задают изоморфные группы и при этом изоморфизме один конкретный элемент переходит в другой всегда можно доказать).