Доклады Академии Наук СССР
1947. Том LV, № 7

МАТЕМАТИКА

А. МАРКОВ

НЕВОЗМОЖНОСТЬ НЕКОТОРЫХ АЛГОРИФМОВ В ТЕОРИИ АССОЦИАТИВНЫХ СИСТЕМ

(Представлено академиком И. М. Виноградовым 6 XI 1946)

1. В этой заметке устанавливаются некоторые результаты, в которых существенную роль играет понятие алгорифма. Это понятие применяется здесь в точном смысле, определенном в работах Church'a (1), Turing'a (9,10), Kleen'a (3,4) и Post'a (5).

2. Ассоциативной системой называется множество, рассматриваемое совместно с определенной для его элементов операцией умножения, такой, что произведение любых двух элементов этого множества также есть его элемент, и удовлетворяющей ассоциативному закону.

3. Единицей ассоциативной системы называется такой ее элемент e, что $e \times x = x \times e = x$ для любого элемента x этой системы. Косой крестик здесь и в дальнейшем есть знак умножения в рассматриваемой ассоциативной системе. Ассоциативная система, как нетрудно видеть, имеет не более одной единицы. В дальнейшем мы будем рассматривать лишь ассоциативные системы с единицей (не оговаривая этого каждый раз), что не является существенным ограничением общности.

4. Если A — какой-либо алфавит, т. е. конечный перечень элементарных знаков (например, букв, цифр и т. п.), то под словом в A мы понимаем произвольную конечную последовательность знаков этого алфавита. Эта последовательность может быть и пустой. Предполагая, что «0» не является знаком алфавита A, условимся обозначать знаком «0» пустое слово.

5. Пусть знакам алфавита A соотнесены некоторые элементы ассоциативной системы S таким образом, что каждому знаку алфавита A соотнесен единственный элемент системы S. Условимся говорить, что этот элемент обозначен соответствующим знаком. При этом допускается, что один и тот же элемент будет обозначен разными знаками алфавита A. Если α — какой-либо знак алфавита A, то под элементом α системы S мы будем понимать элемент этой системы, обозначенный знаком α.

Словам в A можно следующим образом соотнести элементы системы S. Пустому слову соотносим единицу системы S; произвольному непустому слову $\alpha_1 \ldots \alpha_l$ в A — элемент $\alpha_1 \times \ldots \times \alpha_l$ системы S, где под α_i в произведении подразумевается элемент α_i системы S. Элемент системы S, соотнесенный таким образом слову Q в A, будем называть произведением слова Q в S и обозначать символом ΠQ. Произведение слова Q в S зависит от Q, от операции умножения в S и от того, каким образом элементы системы S соотнесены знакам алфавита A.

Будем говорить, что в S определен конечный базис, если это соотнесение сделано так, что каждый элемент системы S является произведением хотя бы одного слова в A.

6. Предполагая, что алфавит A не содержит знака «$\longleftrightarrow$», будем рассматривать последовательности знаков вида

$$Q \longleftrightarrow R, \tag{1}$$

где Q и R — слова в A. Такие последовательности будем называть соотношениями в A.

Пусть имеем конечную систему соотношений в A:

$$Q_i \longleftrightarrow R_i \qquad (i=1, \ldots, m). \tag{2}$$

Определим понятие следствия из системы (2) индуктивным образом, формулируя следующие положения.

С1. Соотношение

$$0 \longleftrightarrow 0$$

есть следствие из (2).

С2. Каждое из соотношений $Q_i \longleftrightarrow R_i$ системы (2) есть следствие из этой системы.

С3. Если какое-нибудь соотношение (1) есть следствие из (2) и α есть знак из алфавита A, то соотношения

$$\alpha Q \longleftrightarrow \alpha R, \quad Q\alpha \longleftrightarrow R\alpha$$

суть следствия из (2).

С4. Если соотношения

$$Q \longleftrightarrow R, \quad Q \longleftrightarrow T$$

суть следствия из (2), то соотношение

$$R \longleftrightarrow T$$

есть следствие из (2).

С5. Соотношение (1) есть следствие из (2) лишь в том случае, когда об этом можно заключить на основании положений С1—С4.

7. Пусть в ассоциативной системе S определен конечный базис путем соотнесения знакам из алфавита A элементов этой системы. Мы будем говорить, что при этом осуществляется соотношение (1), если

$$\Pi Q = \Pi R. \tag{3}$$

Очевидно, что если осуществляется каждое соотношение системы (2), то осуществляются и все следствия из этой системы. Если это имеет место, а, с другой стороны, оказывается, что и обратно, всякое осуществляющееся соотношение в A есть следствие из (2), то мы говорим, что (2) есть определяющая система соотношений ассоциативной системы.

Эта терминология оправдывается тем, что, как легко доказать посредством классических способов рассуждения, для любого алфавита A и любой конечной системы соотношений в этом алфавите существует ассоциативная система, определяемая этой системой соотношений, и при том существенно единственная.

8. При рассмотрении ассоциативной системы, определяемой какой-либо системой соотношений в алфавите A, возникает следующая

Проблема тождества. Указать алгорифм, посредством которого можно было бы для любых слов Q и R в A узнавать, верно ли равенство (3).

Очевидно, что эта проблема равносильна следующей: указать алгорифм, посредством которого можно было бы для любых слов Q и R в A узнавать, является ли соотношение (1) следствием из системы (2).

9. Другой интересной проблемой, возникающей при рассмотрении ассоциативной системы, определяемой системой соотношений, является проблема делимости. Мы говорим, что элемент b ассоциативной системы S делится в S на элемент a этой системы, если существует элемент x системы S такой, что $x \times a = b$.

Проблема делимости для ассоциативной системы, определяемой системой соотношений (2) в алфавите A, состоит в следующем. Указать алгорифм, посредством которого можно было бы для любых слов Q и R в A узнавать, делится ли ΠR на ΠQ.

Нетрудно видеть, что эта проблема равносильна следующей. Указать алгорифм, посредством которого можно было бы для любых слов Q и R в A узнавать, существует ли слово X в A такое, что соотношение

$$XQ \longleftrightarrow R$$

является следствием из (2).

10. Имеют место следующие результаты:

Теорема 1. *Можно указать такой алфавит и такую конечную систему соотношений в этом алфавите, что соответствующая проблема тождества будет неразрешимой, т. е. что требуемого в этой проблеме алгорифма не будет существовать.*

Иначе говоря, может быть построена ассоциативная система, определяемая конечной системой соотношений в некотором алфавите и такая, что для нее проблема тождества будет неразрешимой.

Теорема 2. *Можно указать такой алфавит и такую конечную систему соотношений в этом алфавите, что соответствующая проблема тождества будет разрешима, а соответствующая проблема делимости не будет разрешима, т. е. что будет существовать алгорифм, требуемый в первой проблеме, и не будет существовать алгорифма, требуемого во второй проблеме.*

Иначе говоря, может быть построена ассоциативная система, определяемая конечной системой соотношений в некотором алфавите и такая, что для нее проблема тождества будет разрешима, а проблема делимости — нет.

11. Доказательство теоремы 1 основано на теореме Church'а о несуществовании алгорифма для распознавания λ-конвертируемости ([1]). После ряда приведений, в которых существенную роль играют, с одной стороны, комбинаторный эквивалент λ-конверсии, установленный Rosser'ом ([8])*, а с другой — разработанные Post'ом методы приведения логических систем ([6]), проблема λ-конвертируемости приводится к проблеме следующего типа.

Дан некоторый алфавит A и фиксированы некоторые слова G_i, G_i' ($i = 1, \ldots, m$) в этом алфавите, где m — натуральное число. Каждому i от 1 до m соотносим две операции над словами в A. Первая из них применима лишь к словам, начинающимся с G_i, т. е. к словам вида G_iP. Она состоит в переводе слова G_iP (с произвольным P) в слово PG_i'. Вторая операция, обратная первой, применима лишь к словам вида PG_i' и состоит в переводе всякого такого слова в слово G_iP. Требуется указать алгорифм, посредством которого можно было бы для любых слов Q и R в A узнавать, переводимо ли Q в R конечной последовательностью этих операций.

Эта проблема оказывается неразрешимой в силу цитированной теоремы Church'а. Система соотношений, определяющая ассоциативную систему с неразрешимой проблемой тождества, строится затем следующим образом. Алфавит A дополняется новыми знаками

---

* См. также Church ([2]).

d, e_i $(i = 1, \ldots, m)$, что дает новый алфавит A'. Пишутся следующие соотношения в A':

$$\left.\begin{array}{r} dG_i \longleftrightarrow de_i G_i, \\ e_i G_i \alpha \longleftrightarrow \alpha e_i G_i, \\ e_i G_i d \longleftrightarrow G_i' d. \end{array}\right\} \quad i = 1, \ldots, m; \ \alpha \in A.$$

Эта система соотношений и будет искомой.

12. Доказательство теоремы 2 основано на следующем результате Post'а.

Может быть построена неразрешимая проблема следующего типа. Дан алфавит A и фиксированы слова G_i, G_i' $(i = 1, \ldots, m)$ в этом алфавите. Каждому i от 1 до m соотносим операцию над словами в A, применимую лишь к словам вида $G_i P$ и состоящую в переводе всякого такого слова в слово PG_i'. Требуется указать алгорифм, посредством которого можно было бы для любых слов Q и R в A узнавать, переводимо ли Q в R конечной последовательностью этих операций.

Выбрав алфавит A и слова G_i, G_i' $(i = 1, \ldots, m)$, согласно Post'у, таким образом, чтобы требуемого алгорифма не существовало, мы следующим образом строим систему соотношений, определяющую ассоциативную систему с разрешимой проблемой тождества, но неразрешимой проблемой делимости. Дополняем A новыми знаками: d, f, e_i $(i = 1, \ldots, m)$, что дает новый алфавит A', и пишем следующие соотношения в A':

$$\left.\begin{array}{r} e_i f \longleftrightarrow f e_i, \\ e_i G_i \alpha \longleftrightarrow \alpha e_i G_i, \\ e_i G_i d \longleftrightarrow G_i' d \end{array}\right\} \quad i = 1, \ldots, m; \ \alpha \in A.$$

Эта система соотношений и будет искомой.

Поступило
6 XI 1946

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] A. Church, Am. J. Math., 58, 345 (1936). [2] A. Church, Ann. Math. Studies, 6 (1941). [3] S. C. Kleene, Math. Ann., 112, 727 (1936). [4] S. C. Kleene, Trans. Am. Math. Soc., 53, 41 (1943). [5] E. L. Post, J. Symb. Logic, 1, 103 (1936). [6] E. L. Post, Am. J. Math., 65, 2, 197 (1943). [7] E. L. Post, Bull. Am. Math. Soc., 50, 5, 284 (1944). [8] J. B. Posser, Ann. Math., 36, 194 (1935); Duke Math. J., 1, 328 (1945). [9] A. M. Turing, Proc., London Math. Soc. (2), 42, 230 (1936); (2), 43, 544 (1937). [10] A. M. Turing, J. Symb. Logic, 2, 153 (1937).