Доклады Академии наук СССР
1973. Том 211, № 5

УДК 517.11

МАТЕМАТИКА

М. И. КАНОВИЧ

О СЛОЖНОСТИ АППРОКСИМАЦИИ АРИФМЕТИЧЕСКИХ МНОЖЕСТВ

(Представлено академиком А. Н. Колмогоровым 11 XII 1972)

В работах ([1-4]) исследовалась сложность «начальных отрезков» перечислимых множеств. Получены оценки сложности разрешимых множеств, совпадающих с данным перечислимым множеством на первых n числах. В данной статье рассматривается сложность аппроксимации некоторого арифметического множества множествами другого уровня в арифметической иерархии. Используются понятия и терминология работ ([5, 6]). Все суждения понимаются конструктивно ([7, 1]).

1. Мы будем рассматривать следующий вариант формальной арифметической системы.

Используется алфавит 0, ( ) & $\bigvee$ $\supset$ $\neg$ $\forall$ $\exists$ a f.

&, $\bigvee$, $\supset$ будем называть юнкторами, $\forall$, $\exists$ — кванторами.

Переменные — слова вида (a^n), где n — натуральное число $(n > 0)$.

Пусть $u(n, x)$ — общерекурсивная функция такая, что для любой примитивно-рекурсивной функции φ от k аргументов существует такое натуральное число n, что для любых натуральных чисел $x_1, x_2, \ldots, x_k$

$$\varphi(x_1, x_2, \ldots, x_k) = u(n, p_1^{x_1} p_2^{x_2} \ldots p_k^{x_k}),$$

где p_i — i-е простое число.

Пусть g — неограниченная неубывающая общерекурсивная функция.

Определение (индуктивное) терма t и сложности терма $[t^\lambda$.

1) 0 есть терм. $[0^\lambda = 1$.

2) Переменная есть терм. Сложность переменной равна 1.

3) Если $t_1, \ldots, t_k$ — термы, n — натуральное число, то (f^n) $(t_1 t_2 \ldots t_k)$ есть терм и $[(f^n)(t_1 \ldots t_k)^\lambda = g(n) + [t_1^\lambda + [t_2^\lambda + \ldots + [t_k^\lambda$*.

Определение значения постоянного терма.

1) Значение 0 есть 0.

2) Если $t_1, \ldots, t_k$ — постоянные термы со значениями $m_1, \ldots, m_k$ соответственно, n — натуральное число, то значение терма (f^n) $(t_1, \ldots, t_k)$ есть число $u(n, p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k})$.

Определение формулы и сложности формулы.

1) Если t и s — термы, то $(t = s)$ есть формула и $[(t = s)^\lambda = [t^\lambda + [s^\lambda + 1$.

2) Если A и B — формулы, δ — юнктор, то $(A\,\delta\,B)$ есть формула и $[(A\,\delta\,B)^\lambda = [A^\lambda + [B^\lambda + 1$.

3) Если A — формула, то $\neg A$ есть формула и $[\neg A^\lambda = [A^\lambda + 1$.

4) Если A — формула, X — переменная, Q — квантор, то $Q\,X\,A$ — формула и $[Q\,X\,A^\lambda = [A^\lambda + 1$.

---

* Число $g(n)$ можно понимать как сложность n-й операции.

Пусть h — такое натуральное число, что $u(h, 2^x) = x + 1$. Каждому натуральному числу n сопоставим терм

$$\underbrace{(f^h)((f^h)(\ldots((f^h)}_{n \text{ раз}}(0))\ldots)).$$

который будем обозначать символом $\underline{n}$. Очевидно, что значение терма $\underline{n}$ есть число n.

Пусть A — формула, X — переменная, n — натуральное число. Символом $F_n^X(A)$ будем обозначать результат подстановки вместо всех свободных вхождений переменной X в A терма $\underline{n}$.

Определение Σ_n- и Π-формулы.

1) Всякая формула, не содержащая кванторов, называется Σ_0-формулой (и Π_0-формулой).

2) Если A — Σ_n-формула и X — переменная, то $\forall XA$ называется Π_{n+1}-формулой.

3) Если A — Π_n-формула и X — переменная, то $\neg\neg\exists XA$ называется Σ_{n+1}-формулой *.

Рассмотрение обобщенной «примитивно-рекурсивной» арифметики (см. ([6]), § 48) связано со стремлением расширить класс Σ_0-формул.

Равнозначность замкнутых формул A и B будем обозначать $A \sim B$.

2. Под множествами понимаются однопараметрические формулы.

Если множество $\mathfrak{M}$ определяется формулой A с параметром X и n — натуральное число, то формулу $F_n^X(A)$ будем обозначать $n \in \mathfrak{M}$. Если A — Σ_n-формула, то множество $\mathfrak{M}$ будем называть Σ_n-множеством. Если A — Π_n-формула, то $\mathfrak{M}$ будем называть Π_n-множеством.

3. Будем говорить, что множество $\mathfrak{M}$ n-аппроксимируется формулой B с параметром X, если для любого натурального числа q, не превосходящего числа n, $F_q^X(B) \sim q \in \mathfrak{M}$.

Пусть имеется класс Δ-формул.

Функция β называется верхней оценкой Δ-аппроксимации множества $\mathfrak{M}$, если для любого натурального числа m квазиосуществима ([1]) Δ-формула B, m-аппроксимирующая множество $\mathfrak{M}$ и такая, что

$$[B^\lambda \leqslant \beta(m).$$

Функция α называется нижней оценкой Δ-аппроксимации множества $\mathfrak{M}$, если для любого натурального числа m сложность любой Δ-формулы, m-аппроксимирующей множество $\mathfrak{M}$, не меньше, чем $\alpha(m)$.

4. Следующая теорема очевидна.

Теорема 1. *Осуществимо такое число C, что функция β, определяемая равенством $\beta(m) = Cm$, является верхней оценкой Σ_0-аппроксимации (и Π_0-аппроксимации) любого множества $\mathfrak{M}$.*

При аппроксимации Σ_n-множества «параллельными» Π_n-множествами имеет место логарифмическая оценка.

Теорема 2. *Осуществимы такие положительные числа C_0 и C_1, что, каково бы ни было натуральное число n,*

а) *для любого Σ_n-множества $\mathfrak{M}$ функция β, определяемая равенством*

$$\beta(m) = C_0 \log_2(m+1) + C_1[A^\lambda,$$

где A — Σ_n-формула, определяющая множество $\mathfrak{M}$, является верхней оценкой Π_n-аппроксимации множества $\mathfrak{M}$;

в) *для любого Π_n-множества $\mathfrak{N}$ функция β', определяемая равенством*

$$\beta'(m) = C_0 \log_2(m+1) + C_1[B^\lambda,$$

где B — Π_n-формула, определяющая множество $\mathfrak{N}$, является верхней оценкой Σ_n-аппроксимации множества $\mathfrak{N}$.

* Детальное рассмотрение конструктивной арифметической иерархии проведено в ([8]).

Теорема 3. *Осуществимо такое положительное число C_2, что для любого положительного целого числа n можно указать Σ_n-множество $\mathfrak{M}$ и Π_n-множество $\mathfrak{N}$ такие, что функция α, определяемая равенством*

$$\alpha(m) = C_2 \log_2(m+1),$$

является нижней оценкой Π_n-аппроксимации множества $\mathfrak{M}$ и нижней оценкой Σ_n-аппроксимации множества $\mathfrak{N}$.

Однако логарифмическая оценка имеет место только для «пары» $\Sigma_n - \Pi_n$. Для «пары» $\Sigma_n - \Sigma_{n-1}$ это не так. Более того, для любого $n \geqslant 1$ можно указать такое множество $\mathfrak{M}$ типа $\Sigma_n \cap \Pi_n$, что сложность аппроксимации его пропозициональными комбинациями Σ_{n-1}- и Π_{n-1}-формул растет линейно.

Определение $(\Sigma_n \cup \Pi_n)^\beta$-формулы.

1) Всякая Σ_n-формула считается $(\Sigma_n \cup \Pi_n)^\beta$-формулой.

2) Всякая Π_n-формула считается $(\Sigma_n \cup \Pi_n)^\beta$-формулой.

3) Если A и B — $(\Sigma_n \cup \Pi_n)^\beta$-формулы, δ — юнктор, то $(A\,\delta\,B)$ считается $(\Sigma_n \cup \Pi_n)^\beta$-формулой.

Теорема 4. *Осуществимо такое положительное число C_3, что для любого положительного целого числа n можно указать Σ_n-множество $\mathfrak{M}$ и эквивалентное ему Π_n-множество $\mathfrak{N}$ такие, что функция α, определяемая равенством*

$$\alpha(m) = C_3 m,$$

является нижней оценкой $(\Sigma_{n-1} \cup \Pi_{n-1})^\beta$-аппроксимации множества $\mathfrak{M}$.

Следствие очевидно.

Следствие 1. *Осуществимо такое положительное число C_3, что для любого положительного целого числа n можно указать Σ_n-множество $\mathfrak{M}$ и Π_n-множество $\mathfrak{N}$ такие, что функция α, определяемая равенством*

$$\alpha(m) = C_3 m,$$

является нижней оценкой Σ_{n-1}-аппроксимации множества $\mathfrak{M}$ и нижней оценкой Π_{n-1}-аппроксимации множества $\mathfrak{N}$.

Теоремы 2 и 3 можно рассматривать как «сложностные» варианты теорем об арифметической иерархии (см. (9)).

5. Полученным результатам можно дать следующую геометрическую интерпретацию.

Будем рассматривать арифметические множества как точки некоторого пространства (см. (9)). Пусть $\mathfrak{M}$ — арифметическое множество.

Определим предикат $\mathfrak{C}_{\mathfrak{M}}$ над натуральными числами:

$$\mathfrak{C}_{\mathfrak{M}}(i, r) \rightleftharpoons i \in \mathfrak{M} \& r = 1 \vee i \notin \mathfrak{M} \& r = 0.$$

Пусть ρ — рациональное число. Будем говорить, что множества $\mathfrak{M}$ и $\mathfrak{N}$ ρ-близки, если, каково бы ни было натуральное число n, для любых натуральных чисел $r_0, r_1, \ldots, r_n, q_0, q_1, \ldots, q_n$ таких, что

$$\forall j (j \leqslant n \supset \mathfrak{C}_{\mathfrak{M}}(j, r_j) \& \mathfrak{C}_{\mathfrak{N}}(j, q_j)),$$

выполняется неравенство

$$\sum_{j=0} \frac{|r_j - q_j|}{2^j} < \rho.$$

Следствие 3. *Осуществимы такие положительные числа C_0 и C_1, что, каково бы ни было натуральное число n, для любого Σ_n-множества $\mathfrak{M}$ и любого рационального числа ρ такого, что $0 < \rho < 1/2$, квазиосуществимо Π_n-множество $\mathfrak{N}$, ρ-близкое к множеству $\mathfrak{M}$ и сложности* не выше, чем $C_0 \log_2 \log_2 (1/\rho) + C_1 [A^\lambda]$ (A — Σ_n-формула, определяющая множество $\mathfrak{M}$).*

Следствие 4. *Осуществимо такое положительное число C_2, что для любого положительного числа n можно указать такое Σ_n-множество $\mathfrak{M}$, что, каково бы ни было рациональное число ρ такое, что $0 < \rho < 1$, сложность любого Π_n-множества, ρ-близкого к множеству $\mathfrak{M}$, не меньше, чем $C_2 \log_2 \log_2 (1/\rho)$.*

* Под сложностью множества $\mathfrak{N}$ понимается сложность определяющей его Π_n-формулы.

Следствие 5. *Осуществимо такое положительное число C, что, каково бы ни было положительное целое число n:*

а) *для любого Σ_n-множества $\mathfrak{M}$ и для любого рационального числа ρ такого, что $0<\rho<1$, квазиосуществимо Σ_0-множество $\mathfrak{N}$, ρ-близкое к множеству $\mathfrak{M}$ и сложности не выше, чем $C\log_2(1/\rho)$;*

б) *можно указать такое Σ_n-множество $\mathfrak{M}$, что, каково бы ни было положительное рациональное число ρ, сложность любого Σ_{n-1}-множества, ρ-близкого к множеству $\mathfrak{M}$, больше, чем $\log_2(1/\rho)/C$.*

Аналогичные результаты имеют место для Π_n-множеств.

6. Задача разрешения данного множества $\mathfrak{M}$ ставится следующим образом: требуется построить алгорифм $\mathfrak{R}$, применимый ко всякому натуральному числу n и такой, что результат $\mathfrak{R}(n)$ содержит «информацию» о принадлежности числа n множеству $\mathfrak{M}$. Пусть имеется класс Δ-формул. Будем говорить, что алгорифм $\mathfrak{R}$ Δ-разрешает множество $\mathfrak{M}$, если $\mathfrak{R}$ перерабатывает всякое натуральное число n в замкнутую Δ-формулу, равнозначную $n\in\mathfrak{M}$. Соответствующая «ограниченная» задача ставится следующим образом. Будем говорить, что алгорифм $\mathfrak{R}$ (m,Δ)-разрешает множество $\mathfrak{M}$, если $\mathfrak{R}$ перерабатывает всякое натуральное число n, не превосходящее числа m, в замкнутую Δ-формулу, равнозначную $n\in\mathfrak{M}$.

Мы рассматриваем нормальные алгоритмы в некотором стандартном расширении алфавита O ( ) & $\vee$ $\supset$ $\neg$ V $\exists$ a f. Под сложностью алгоритма понимается длина его изображения (см. [1]).

Функцию β назовем верхней оценкой Δ-разрешения множества $\mathfrak{M}$, если для любого натурального числа m квазиосуществим алгорифм сложности не больше, чем $\beta(m)$, (m,Δ)-разрешающий множество $\mathfrak{M}$.

Функцию α назовем нижней оценкой Δ-разрешения множества $\mathfrak{M}$, если, каково бы ни было натуральное число m, сложность любого алгоритма, (m,Δ)-разрешающего множество $\mathfrak{M}$, больше, чем $\alpha(m)$.

Теорема 5. *Осуществимы такие положительные числа C_0 и C_1, что, каково бы ни было натуральное число n, для любого Σ_n-множества $\mathfrak{M}$ функция β, определяемая равенством*

$$\beta(m)=C_0\log_2(m+1)+C_1[A^{\lambda},$$

где A — формула, определяющая множество $\mathfrak{M}$, является верхней оценкой Π_n-разрешения множества $\mathfrak{M}$.

Теорема 6. *Осуществимо такое положительное число C_2, что для любого положительного целого числа n можно указать такое Σ_n-множество $\mathfrak{M}$, что функция α, определяемая равенством $\alpha(m)=C_2\log_2(m+1)-n$, является нижней оценкой Π_n-разрешения множества $\mathfrak{M}$.*

Теоремы 5 и 6 сохраняются при замене Σ_n на Π_n, а Π_n на Σ_n.

Теорема 7. *Осуществимо такое положительное число C_0, что, каково бы ни было положительное целое число n:*

а) *функция β', определяемая равенством $\beta'(m)=C_0m$, является верхней оценкой Σ_0-разрешения любого Σ_n-множества;*

б) *можно указать такое Σ_n-множество $\mathfrak{M}$ и эквивалентное ему Π_n-множество $\mathfrak{N}$, что функция α', определяемая равенством $\alpha'(m)=m/C_0-n$, является нижней оценкой $(\Sigma_{n-1}\cup\Pi_{n-1})^{\beta}$-разрешения множества $\mathfrak{M}$.*

Теоремы 5—7 являются следствием теорем 2—4.

Автор глубоко благодарен А. А. Маркову за внимание и советы в период написания данной работы.

Тульский политехнический институт

Поступило
2 XII 1972

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. А. Марков, Изв. АН СССР, сер. матем., 31, 161 (1967). [2] Я. М. Барздинь, ДАН, 182, № 6, 1249 (1968). [3] Н. В. Петри, ДАН, 186, № 1, 30 (1969). [4] М. И. Канович, ДАН, 186, № 5, 1008 (1969). [5] А. А. Марков, Тр. Матем. инст. им. В. А. Стеклова АН СССР, 42 (1954). [6] С. К. Клини, Введение в математику, 1954. [7] Н. А. Шанин, Тр. Матем. инст. им. В. А. Стеклова АН СССР, 52, 226 (1958). [8] М. М. Киппнис, Зап. научн. семинаров ЛОМИ АН СССР, 8, 53 (1968). [9] H. Rogers, jr, Theory of Recursive Functions and Effective Computability, 1967.