Доклады Академии наук СССР
1974. Том 218, № 2

УДК 517.11

МАТЕМАТИКА

М. И. КАНОВИЧ

«СЛОЖНЫЕ» И «ПРОСТЫЕ» ЧИСЛА

(Представлено академиком А. Н. Колмогоровым 4 III 1974)

В заметке приводится алгорифмическая характеристика множества чисел, «простых» при заданном способе программирования, близком к оптимальному.

1. Всякий алгорифм над алфавитом натуральных чисел $0|$ можно рассматривать как способ программирования (кодирования) (см. [1]). Пусть $\mathfrak{A}$ — алгорифм над алфавитом $0|$. Слово P в алфавите $0|$ назовем $\mathfrak{A}$-кодом натурального числа x, если

$$\mathfrak{A}(P) \overline{\circ} x.$$

Сложность числа x (при данном способе программирования $\mathfrak{A}$) измеряется длиной «минимального» $\mathfrak{A}$-кода числа x. Будем говорить, что $\mathfrak{A}$-сложность числа x не превосходит числа k, если существует $\mathfrak{A}$-код числа x длины не больше чем k.

Пусть h — общерекурсивная функция. Число x назовем h-простым (для данного алгорифма $\mathfrak{A}$), если $\mathfrak{A}$-сложность числа x не превосходит $h(x)$. Число x назовем h-сложным (для данного алгорифма $\mathfrak{A}$), если оно не является h-простым. Множество всех h-простых (для данного алгорифма $\mathfrak{A}$) натуральных чисел будем обозначать $N_{\mathfrak{A}}{}^h$.

Нетрудно видеть, что множество $N_{\mathfrak{A}}{}^h$ является рекурсивно-перечислимым множеством.

Можно построить такой алгорифм $\mathfrak{A}$ над алфавитом $0|$, что для функции h_0, определяемой равенством

$$h_0(x) = [\log_2(x+1)],$$

все натуральные числа будут h_0-простыми (для этого алгорифма $\mathfrak{A}$).

Для функций, возрастающих медленнее, картина резко меняется. Каков бы ни был алгорифм $\mathfrak{A}$, если разность функций h_0 и h (функция $h_0 - h$) — неограниченная неубывающая общерекурсивная функция, то h-сложными (для данного алгорифма $\mathfrak{A}$) являются «почти» все натуральные числа: можно указать такую конструктивную функцию ε, убывающую к нулю при возрастании аргумента, что, каково бы ни было n, среди первых n натуральных чисел не может быть менее чем $n(1-\varepsilon(n))$ h-сложных (для данного $\mathfrak{A}$) натуральных чисел.

Однако оказывается, что множество h-сложных чисел «разрежено» с алгорифмической точки зрения, если алгорифм $\mathfrak{A}$ обладает «оптимальными» свойствами. Я. М. Барздинь показал, что оно иммунно, если алгорифм $\mathfrak{A}$ асимптотически оптимален (см. [2], теорема 1.6). Мы покажем, что множество h-сложных чисел строго эффективно иммунно, если алгорифм $\mathfrak{A}$ хотя бы «близок» к оптимальному. Кроме того, оказывается, что «разреженность» множества h-сложных чисел является не только необходимым, но и достаточным условием почти оптимальности алгорифма $\mathfrak{A}$.

2. В статье используются понятия и терминология работ [3, 4]. Все математические суждения понимаются конструктивно (см. [5]).

3. Общерекурсивную функцию h назовем сублогарифмической, если для всякого числа m найдется такое натуральное число x, не меньшее чем m, что выполняется неравенство

$$h(x) < [\log_2(x+1)].$$

Нетрудно видеть, что, каков бы ни был алгорифм $\mathfrak{A}$, для любой неубывающей сублогарифмической функции h множество $N_{\mathfrak{A}}{}^h$ негиперпросто.

Алгорифм $\mathfrak{A}$ называется асимптотически оптимальным, если для любого алгорифма $\mathfrak{B}$ можно указать такое число C, что каковы

бы ни были натуральные числа x и k, если $\mathfrak{B}$-сложность числа x не превосходит k, то $\mathfrak{A}$-сложность числа x не превосходит $k+C$ (см. [1, 2]).

Мы обобщим это понятие.

Алгорифм $\mathfrak{A}$ назовем почти оптимальным, если для любого алгорифма $\mathfrak{B}$ можно указать такую общерекурсивную функцию f, что каковы бы ни были натуральные числа x и k, если $\mathfrak{B}$-сложность числа x не превосходит k, то $\mathfrak{A}$-сложность числа x не превосходит $f(k)$.

Очевидно, что асимптотически оптимальный алгорифм почти оптимален.

Теорема 1. *Пусть $\mathfrak{A}$ — почти оптимальный алгорифм. Тогда для любой неограниченной неубывающей сублогарифмической функции h множество $N_{\mathfrak{A}}^{h}$ строго эффективно просто* *.

Для формулировки более сильного варианта обратного предложения нам понадобятся следующие определения.

Алгорифм $\mathfrak{A}$ назовем полным способом программирования, если для любого натурального числа существует его $\mathfrak{A}$-код.

Общерекурсивные функции f и g назовем ω-эквивалентными, если

$$\neg\forall n\exists m\ (m>n\&f(m)\neq g(m)).$$

Теорема 2. *Пусть алгорифм $\mathfrak{A}$ — полный способ программирования и пусть существует такая неубывающая общерекурсивная функция h, что для всякой неубывающей общерекурсивной функции f, ω-эквивалентной функции h, множество $N_{\mathfrak{A}}^{f}$ строго эффективно просто.*

Тогда алгорифм $\mathfrak{A}$ почти оптимален.

Следствие 1. *Полный способ программирования $\mathfrak{A}$ почти оптимален тогда и только тогда, когда для любой неограниченной неубывающей сублогарифмической функции h множество $N_{\mathfrak{A}}^{h}$ строго эффективно просто.*

4. Можно построить такой полный способ программирования $\mathfrak{A}$ и указать такую сублогарифмическую функцию h, что множество $N_{\mathfrak{A}}^{h}$ будет эффективно простым, но не строго эффективно простым множеством. Такой алгорифм $\mathfrak{A}$, согласно теореме 1, не является почти оптимальным. Однако можно показать, что его область определения ** совпадает с областью определения некоторого почти оптимального алгорифма.

Теорема 3. *Пусть $\mathfrak{A}$ — алгорифм над алфавитом $0|$ и пусть существует такая сублогарифмическая функция h, что множество $N_{\mathfrak{A}}^{h}$ эффективно просто.*

Тогда область определения алгорифма $\mathfrak{A}$ эффективно нерекурсивна ***.

Согласно статье [6] получаем следствие ****.

Следствие 2. *Пусть алгорифм $\mathfrak{A}$ над алфавитом $0|$ таков, что существует такая сублогарифмическая функция h, что множество $N_{\mathfrak{A}}^{h}$ эффективно просто.*

Тогда область определения алгорифма $\mathfrak{A}$ совпадает с областью определения некоторого почти оптимального алгорифма.

Автор благодарен чл.-корр. АН СССР А. А. Маркову за внимание и советы при обсуждении данной работы.

Калининский государственный университет

Поступило 26 II 1974

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] *А. Н. Колмогоров*, Проблемы передачи информации, т. 1, в. 1, 3 (1965). [2] *А. К. Звонкин, Л. А. Левин*, УМН, т. 25, в. 6, 85 (1970). [3] *А. А. Марков*, Тр. Матем. инст. им. В. А. Стеклова АН СССР, т. 42 (1954). [4] *Х. Роджерс*, Теория рекурсивных функций и эффективная вычислимость, 1972. [5] *Н. А. Шанин*, Тр. Матем. инст. им. В. А. Стеклова АН СССР, т. 52, 226 (1958). [6] *М. И. Канович*, ДАН, т. 198, № 2, 283 (1971). [7] *М. И. Канович*, ДАН, т. 194, № 3, 500 (1970).

* Т. е. для всякого рекурсивно-перечислимого подмножества $\mathfrak{N}$ множества h-сложных (для данного $\mathfrak{A}$) чисел можно указать такое число p, что всякий элемент множества $\mathfrak{N}$ не превосходит p.

** Под областью определения алгорифма $\mathfrak{A}$ понимается множество всех слов в алфавите $0|$, к которым применим алгорифм $\mathfrak{A}$.

*** Определение эффективной нерекурсивности см. в [6, 7].

**** В статье [6] почти оптимальные алгорифмы назывались оптимальными.