Г. А. НАЗАРЯН

О РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ В АЛГОРИФМИЧЕСКИХ ЯЗЫКАХ ПРИ ОГРАНИЧЕНИЯХ НА ВРЕМЯ РАБОТЫ АЛГОРИФМОВ

В статье рассматриваются вопросы реализации булевых функций (б. ф.) в алгорифмических языках при общерекурсивных ограничениях на время работы алгорифмов. Объекты рассмотрения суть множества б. ф. Исследуются ограниченные функции Шеннона для этих множеств и связанные с ними понятия.

В § 1 формулируются факты общего характера. Доказывается, например, существование множеств, допускающих эффективные ускорения вычислений б. ф., им принадлежащих, за счет лишь незначительного увеличения объема программ, вычисляющих б. ф. из этих множеств. Формулируются необходимые и достаточные условия, которым должны удовлетворять множества б. ф., чтобы функции Шеннона с общерекурсивным ограничением на время были бы для этих множеств оптимальными (мощностными). Описываются некоторые свойства множеств, обуславливающие скачок оценок при введении ограничений на время вычислений, строится пример перечислимых множеств, для которых функции Шеннона при ограничении на время вычислений и без него существенно отличаются при любом ограничении.

В § 2 рассматриваются классы сложности множеств б. ф. Класс сложности R_t определяется как класс таких перечислимых множеств, для которых сохраняются оптимальные (мощностные) оценки при введении ограничения t на время вычислений.

Пользуюсь случаем выразить благодарность И. Д. Заславскому за постановку задачи и внимание к работе.

Определения и обозначения. Всюду далее чрф есть сокращение для выражения «частично рекурсивная функция», орф — «общерекурсивная функция», б. ф. — «булева функция», н. ч. — «натуральное число», рпм — «рекурсивно перечислимое множество». Определим н. ч. как слова в алфавите {0, 1} так, как это сделано, например в [3]. Булевы функции и связанные с ними понятия, здесь не определяемые, будем понимать как в [6] (в частности, понятие б. ф. рассматривается как частный случай понятия н. ч.). Размерность б. ф. будем указывать верхним индексом: так, если F есть б. ф. размерности n, то будем писать F^n наря-

ду с F. Длину н. ч. x будем обозначать через $l(x)$, через $d(A)$ — мощность конечного множества A, через M_n — множество б. ф. размерности n, принадлежащих множеству M б. ф., через D_x — множество н. ч., имеющее номер x в канонической нумерации конечных множеств [7]. Пусть P — одноместный предикат, допустимыми значениями переменной которого являются н. ч. Посредством $\forall_n^{\infty} P(n)$ будем обозначать суждение $\exists k \forall n (n > k \supset P(n))$. Символы $\succ$, $\prec$ и $\asymp$ будем использовать в следующем смысле: $a(n) \prec b(n) \equiv \exists C \forall n (a(n) \leqslant b(n+C))$, $a(n) \succ b(n) \equiv b(n) \prec a(n)$, $a(n) \asymp b(n) \equiv a(n) \prec b(n) \,\&\, a(n) \prec b(n)$. Буквы $\mathcal{T}$, t, τ, f будем использовать для обозначения одноместных орф, C, p, z, k — для н. ч., M — для множества б. ф.

Под алгорифмическим языком будем понимать некоторую допустимую в смысле [7] нумерацию чрф φ (иногда будем предполагать, что φ — аддитивно оптимальная нумерация чрф [2], [4]). Предполагаем, что для нумерации φ фиксирована последовательность сигнализирующих Φ [9]. С последовательностью сигнализирующих ассоциируем последовательность чрф $\widehat{\Phi}$ такую, что $\forall i \forall n (\widehat{\Phi}_i(n) = \max\limits_{l(x)=n} \Phi_i(x)$. В дальнейшем, рассматривая поведение сигнализирующей, мы будем для краткости называть ее „время вычислений“ или просто „время“; под „объемом программы φ_p“ будем понимать длину индекса p. Будем говорить, что чрф φ_p вычисляет б. ф. F^n, и писать $\varphi_p \Rightarrow F^n$ (соответственно t вычисляет F^n), если $\forall x (l(x) = n \supset \varphi_p(x) = F^n(x))$ $(\forall x (l(x) = n \supset \varphi_p(x) = F^n(x)) \,\&\, \widehat{\Phi}_p(n) < t(n))$. Под сложностью $L(F)$ б. ф. F (t ограниченной сложностью $L^t(F)$ б. ф. F) будем понимать соответственно объем минимальной программы из программ вычисляющих F (t вычисляющих F). Наконец, посредством L_M и L_M^t будем обозначать функции Шеннона (не ограниченную и t ограниченную) множества M б. ф., определяемые как $\forall n (L_M(n) = \max\limits_{F \in M_n} L(F))$ и $\forall n (L_M^t(n) = \max\limits_{F \in M_n} L^t(F)$.

Нетрудно убедится, что если рассматриваемая нумерация φ аддитивно оптимальна, то для любого рпм M выполнено: $L_M(n) \asymp l(d(M_n))$ (т. е. оценки функций Шеннона для этих множеств оптимальные, „мощностные“). Определение T-мощностных множеств ниже предполагает, что нумерация φ аддитивно оптимальна (соответственно в формулировках утверждений, использующих это определение, нумерация предполагается таковой, хотя эти утверждения естественным образом могут быть обобщены на языки более общего типа). Множество M будем называть T-мощностным, если

$$\exists t (L_M^t(n) \asymp L_M(n) \asymp l(d(M_n))).$$

§ 1. Время—ограниченная реализация булевых функций в универсальном алгорифмическом языке

1. Говоря, что время работы алгорифмов ограничено некоторой орф t (фиксирован ограничитель t), будем иметь в виду, что рассматриваются те алгорифмы φ_z алгорифмического языка φ, для которых выполнено: $\Phi_z(n) < t(n)$ (для фиксированного n). Ясно, что от выбора ограничителя могут существенно зависеть объемы программ, вычисляющих б. ф. и работающих не дольше времени, заданного ограничителем, или, в терминах множеств б. ф., можно указать t_1, t_2 и M такие, что $L_M^{t_1} \ll L_M^{t_2}$. Но, с другой стороны, для ограничителей имеет место некоторый аналог теоремы о пробелах ([8], [10]): можно указывать ограничители, «идентичные» с точки зрения объемов программ. Точной формулировке этого факта предпошлем одно определение. Программу φ_z будем называть (n, C)-минимальной, если для некоторой б. ф. F^n от n аргументов выполнено: $((\varphi_z \Rightarrow F^n) \& (\widehat{\Phi}_z(n) < C))$ и для всех $z' < z$ неверно, что $((\varphi_{z'} \Rightarrow F^n) \& (\widehat{\Phi}_{z'}(n) < C))$.

1.1 *Для любых орф s и t можно указать $T > t$ такую, что всякая $(n, T(n))$ — минимальная программа является также $(n, s(T(n)))$ — минимальной.*

Доказательство. Пусть β есть орф, удовлетворяющая условию: $\forall n \forall F^n (\varphi_{\beta(F^n)} \Rightarrow F^n)$ и пусть орф α связана с β соотношением $\forall n (\alpha(n) = \max \beta(F^n))$, где max берется по всем б. ф. размерности n. Определим орф T, удовлетворяющую условиям утверждения. Для любого n значение $T(n)$ положим равным наименьшему н. ч. m такому, что $m > t(n)$ и $\forall i \leqslant \alpha(n) (\neg (m < \widehat{\Phi}_i(n) < T(m))$. Такое m всегда найдется, так как квазиосуществимо н. ч. k такое, что для всех i, для которых $! \Phi_i(n)$, выполнено $k > \widehat{\Phi}_i(n)$. Так определенная орф T — искомая.

Из 1.1 следует, что если орф s и T выбраны таким образом, чтобы удовлетворялись условия 1.1, то для любого множества M б. ф. выполнено $\forall n (L_M^T(n) = L_M^{S \circ T}(n))$.

Время вычисления б. ф. (множеств б. ф.) связано с объемом программ, вычисляющих эти б. ф., нетрудно строить примеры множеств, функции из которых вычислимы программами малого объема, но за большое время, и, в то же время, программами большого объема, но за малое время (любая б. ф. F может быть «быстро» вычислена программой, запоминающей вектор значений F). Очевидно следующее утверждение.

1.2. $\forall t \exists M \exists C \exists t_1 ((L_M^{t_1}(n) < C) \& (L_M^t(n) \geqslant 2^n))$.

Таким образом (это утверждается в 1.2), «ускорения» вычислений могут быть связаны с существенным увеличением объемов программ. Воз-

никает вопрос: неизбежно ли «ускорения» вычислений обуславливают рост объемов программ. Следующее утверждение дает отрицательный ответ на вопрос, оно показывает существование множеств, допускающих эффективные ускорения вычислений б. ф., им принадлежащих, за счет лишь незначительного увеличения объемов программ.

1.3. *Существует орф t такая, что для любой орф T можно указать множество M б. ф. и н. ч. C_1, C_2 и m, удовлетворяющие условиям*

а) *множество M вычислимо программами с объемом, не превосходящим C_1, но за время, большее чем T* (т. е. $((\exists T' > T)\ \forall n (L^{T'}_M(n) < C_1)) \& (\forall T' ((L^{T'}_M(n) < C_1) \supset (\forall n > m (T'(n) > T(n)))))$),

б) *множество M вычислимо программами с объемом, не превосходящим C_2, но за время t* (т. е. $\forall n (L^t_M(n) < C_2)$).

Доказательство. Посредством $Q^{c,k}_n$ будем обозначать множество, состоящее из б. ф. F размерности n, для которых выполнено: $\exists i \leqslant k ((\varphi_i \Rightarrow F) \& (\widehat{\Phi}_i(n) < C))$. Пусть орф δ удовлетворяет условию: для всех n, для всех $i \leqslant 2^{2^n}$ $\varphi_{\delta(i)}$ вычисляет i-тию в лексикографической упорядоченности б. ф. размерности n (для фиксированного i $\varphi_{\delta(i)}$ вычисляет б. ф. разных размерностей — F^n_i, F^{n+1}_i, ...).

Определим орф $t - \forall n (t(n) = \max\limits_{i \leqslant 2^{2^n}} \widehat{\Phi}_{\delta(i)}(n))$. Пусть фиксировано некоторое z. Рассмотрим произвольное n больше m_z такого, что $2^{2^{m_z}} \geqslant (z+2)$. Рассмотрим множества $Q^{T(n),\, z+1}_n$ и $Q^{t(n),\, \delta(z+2)}_n$. Пусть орф α удовлетворяет условию: для всех $n > m_z$ $\varphi_{\alpha(z)}$ вычисляет б. ф. F^n, принадлежащую $Q^{t(n),\, \delta(z+2)}_n$ и не принадлежащую $Q^{T(n),\, z+1}_n$ (выбор такой F^n возможен, потому, что $d(Q^{t(n),\, \delta(z+2)}_n) \geqslant z+2$ и $d(Q^{T(n),\, z+1}_n) \leqslant z+1$). По теореме о рекурсии существует z такое, что $\varphi_{\alpha(z)} = \varphi_z$. Искомое множество M определим как множество всех б. ф., вычислимых орф φ_z. Пусть $C_1 = l(z+1)$, $C_2 = l(\delta(z+2))$ и $m = m_z$. Убедимся, что для так определенных M, C_1, C_2 и m условия утверждения выполнены. Действительно, так как б. ф. из M принадлежат $Q^{t(n),\, \delta(z+2)}_n$, то условие б) выполнено, условие а) выполнено в силу того, что если $F^n \in M$, то $F^n \overline{\in} Q^{T(n),\, z+1}_n$. Утверждение доказано.

Пусть G есть некоторый класс орф. Множество M б. ф. будем называть G — множеством, если характеристическая функция M принадлежит G. Нетрудно убедиться в справедливости следующего утверждения.

1.4. *Для всякого перечислимого класса G орф можно указать орф t такую, что для любого G-множества M б. ф. выполнено $L^t_M \asymp L_M$.*

Если к примеру в качестве класса G в условии 1.4 рассмотрим класс примитивно рекурсивных функций, то, как следует из 1.4, найдется орф t

такая, что для любого примитивно рекурсивного множества M будет выполнено: $L^t_M \succeq L_M$. Из 1.4 также следует (этот факт нетрудно усмотреть и непосредственно), что любое рекурсивное множество является T-мощностным, т. е. для него можно указать t такую, что $L^t_M \succeq L_M$.

2. В этом пункте мы сформулируем необходимые и достаточные условия для того, чтобы оценки ограниченных функций Шеннона (L^t_M) для множеств M б. ф. были бы оптимальными (мощностными) в аддитивно оптимальных языках.

Замечание. Для множеств M, сохраняющих мощностные оценки при введении ограничений на время работы алгорифмов в аддитивно оптимальных языках, оценки мощностные и в языках более общего типа, таких, в которых мощностными являются неограниченные функции Шеннона этих множеств (L_M).

В то время как рекурсивные множества оказываются T-мощностными, перечислимые множества «ведут» себя иначе (в этом мы убедимся в п. 3 этого §): для них L_M и L^t_M могут существенно отличаться. Но сложность множества — L^t_M определяется сложностью сечений — M_n $(n = 1, 2, \ldots)$. Одной из возможных характеристик сложности сечений является сложность характеристических функций. Через λ_{M_n} будем обозначать характеристический вектор (н. ч.) множества M_n — вектор $\sigma_1\sigma_2\cdots\sigma_{2^{2^n}}$ i-ая буква которого есть I (σ_i суть 0 или 1) в том и только в том случае, если F^n_i (i-ая б. ф. в лексикографической упорядоченности среди б. ф. размерности n) принадлежит M. Будем рассматривать условную сложность [4] $K^t(\lambda_{M_n}|n) = l(\mu p[\varphi_p(n) = \lambda_{M_n} \& \Phi_p(n) < t(n)])$. Справедливость следующего утверждения легко проверить

2.1. $\forall t_1 \exists t_2 \forall M\,(L^{t_2}_M(n) \prec 2K^{t_1}(\lambda_{M_n}|n) + l(d(M_n)))$.

Из этого утверждения следует, что если для рпм M выполнено $\exists t(K^t(\lambda_{M_n}|n) \prec C)$, то M T-мощностное.

Введем некоторые определения. Множества M и M' будем называть аддитивно равномощными, если $l(d(M_n)) \succeq l(d(M'_n))$. Множество M будем называть (n, l) — восстанавливаемым, если

$$\exists t \exists C(K^t(\lambda_{M_n}| < n,\ l(d(M_n))>) < C).$$

Пусть D_x обозначает конечное множество н. ч. с каноническим номером x [7]. Орф g будем называть правильной, если для всех n и m $D_{g(n,m)}$ суть множества б. ф. и выполнено $(m_1 < m_2 \supset D_{g(n,m_1)} \subseteq D_{g(n,m_2)})$. Пусть α-орф, удовлетворяющая условию $\forall n(\alpha(n) \geqslant 2^{2^n})$. Правильную орф g будем называть функцией покрытия для M, если $\forall n \neg\neg \exists m \leqslant \alpha(n)[D_{g(n,m)} \supseteq M_n]$. Множество M' будем называть покрытием M по g, если $\forall n \neg\neg \exists m (D_{g(n,m)} = M'_n \supseteq M_n)$. M' будем называть покрытием M, если M' есть покрытие M по некоторой орф g.

Следующее утверждение устанавливает необходимые и достаточные условия для того, чтобы M было T-мощностным.

2.2. *Условия* (а), (б) *и* (в) *эквивалентны для* M:

(а) M *является* T*-мощностным,*

(б) *существует аддитивно равномощное ему* (n, l)*-восстанавливаемое надмножество* M',

(в) *существует аддитивно равномощное ему покрытие* M'.

Доказательство. (а)$\rightarrow$(в). Пусть M T-мощностное, то есть $\exists t\, C\, \forall n\, (L^t_M(n) \leqslant ld(M_n) + C)$. Пусть g-орф такая, что $\forall n\, \forall m\, (D_{g(n,m)} = \{F^n \mid L^t(F^n) \leqslant m + C\})$ и пусть M' есть множество, определяемое как: для всех n $M'_n = D_{g(n, ld(M_n))}$. Нетрудно убедится, что M' искомое. (в)$\rightarrow$(б). Пусть для M существует аддитивно равномощное ему покрытие M' и пусть g есть орф такая, что M' есть покрытие M по g. Через δ будем обозначать двухместную орф такую, что $\forall u\, \forall \overline{l}\, (\delta(n, l)\overline{)}$ есть максимальное из чисел $m \leqslant \alpha(n)$ таких, что $\overline{l} = l(d(D_{g(n,m)}))$, если таковое имеется. По определению δ, если $\overline{l}$ есть одно из чисел $l(d(D_{g(n,m)}))$ $(m = 1, \ldots, \alpha(n))$, то выполнено: $\overline{l} = l(d(D_{g(n, \delta(n, \overline{l}))}))$. Пусть $l^n_1, \ldots, l^n_k$ суть различные н. ч. из чисел $l(d(D_{g(n,m)}))$ $(m = 1, \ldots, \alpha(n))$. Пусть далее g' — правильная орф, такая, что $\forall n\, (D_{g'(n, l^n_i)} = D_{g(n, \delta(n, l^n_i))})$. Рассмотрим множество M'', определенное как $\forall n\, (M''_n = D_{g(n, l(d(M'_n)))})$. Нетрудно убедится, что $M''(n, l)$ — восстанавливаемое (б)$\rightarrow$(а). Пусть для M существует равномощное ему (n, l) — восстанавливаемое надмножество M' и орф t и константа C такие, что $\forall n\, (K^t(\lambda_{M'_n} \mid \langle n, ld(M'_n)\rangle) \leqslant C)$. Через $w(\lambda)$ будем обозначать „вес“ н. ч. λ — число единиц в слове λ. Пусть $\lambda_1, \ldots, \lambda_k$ суть н. ч. длины 2^{2^n} (рассматриваемые как характеристические функции множеств б. ф. размерности n), удовлетворяющие условию — $K^t(\lambda_l \mid \langle n, l(w(\lambda_l))\rangle) \leqslant C$. Ясно, что таких λ может быть не более $2^n \cdot C$. Пусть R^n_i $(i = 1, \ldots, k)$ есть множество б. ф. размерности n для которого λ_l является характеристическим вектором. Упорядочим множества R^n_i по возрастанию их мощности, i-тое множество в этой новой упорядоченности обозначим через $(R^n_i)'$. Пусть g — двухместная орф, перечисляющая при всяком n $(g(n, i)$, $i = 1, 2, \ldots)$ б. ф. из $(R^n_1)'$, затем из $(R^n_2)'$ и так далее. По орф g нетрудно построить орф β такую, что $l(\beta(i)) \prec l(i)$ и для каждого n $\varphi_{\beta(i)}$ вычисляет б. ф., перечисленную $g(n, i)$. В силу эффективности β можно указать t такую, что $L^t_M(n) \prec l(dM'_n) \prec l(d(M_n))$.

Используя 2.2 нетрудно показать, что ограниченность функции $K^t(\lambda_{M_n} \mid n)$ не является необходимым условием для того, чтобы M было T-мощностным (см. 2.3).

2.3. *Существует Т-мощностное множество M для которого выполнено* $\forall t \forall C \neg (K^t(\lambda_{M_n} | n) < C)$.

Доказательство. Через $y_{i,n}$ будем обозначать булев вектор длины 2^{2^n}, имеющий i единиц в первых i „позициях" и 0 в остальных. Пусть α-орф, такая, что $\alpha(n) \to \infty$ и $\alpha(n) \leqslant n$, и пусть r есть функция большого размаха (то есть для всякого x множество $\{n | r(n) = x\}$ бесконечно). Пусть, наконец, t — орф, удовлетворяющая условию: $\forall n \forall i (! K^t(y_{i,n} | n))$. Определим искомое множество M. Если $! \varphi_{r(n)}(n)$, то находим $m = \max(\varphi_{r(n)}(n), t(n))$, далее находим такое $y_{i,n}$, что $K^m(y_{i,n} | n) \geqslant \alpha(n)$. Положим M_n равным $\{F_k^n | \leqslant i\}$, где F_k^n — k-тая в лексикографической упорядоченности б. ф. от n аргументов. Нетрудно убедиться, что для M выполнены условия утверждения. Тот факт, что M является Т-мощностным следует из существования орф g такой, что $D_{g(n,i)}$ есть множество для которого $y_{i,n}$ является характеристической функцией, или иначе, множество M является покрытием себя самого, и, с учетом 2.2, имеем требуемое.

Нетрудно убедиться в справедливости следующих утверждений.

2.4. *Если M' есть покрытие для M, то* $\exists t (L_M^t(n) \prec ld(M_n'))$.

2.5. *Если M' есть покрытие для рпм M, то M' содержит некоторое перечислимое покрытие M''.*

3. Если любое рекурсивное множество является T-мощностным. то уже в классе перечислимых множеств можно указывать такие, для которых L и L^t существенно отличаются при любых t. Определим некоторые свойства множеств, обуславливающие скачок оценок при введении ограничений на время вычислений, с помощью которых построим множества вышеуказанного типа. Под частично рекурсивной последовательностью (чрп) б. ф. будем понимать множество значений чрф ψ, удовлетворяющей условию: если $! \psi(n)$, то $\psi(n)$ есть б. ф. размерности n. Множество M будем называть предельным, если любая чрп S б. ф. почти содержится в M, то есть множество $S — M$ не бесконечно.

3.1. *M предельно тогда и только тогда, когда* $\min\limits_{F^n \in \overline{M}} L(F^n) \to \infty$.

Доказательство. Импликация ($\min\limits_{F^n \in \overline{M}} L(F^n) \to \infty \supset M$ предельно) очевидна. Пусть M предельно, но $\neg \min\limits_{F^n \in \overline{M}} L(F^n) \to \infty$. Квазиосуществима константа C такая, что множество б. ф., принадлежащих дополнению M, для которых выполнено $L(F) < C$, бесконечно. Квазиосуществимо н. ч. z такое, что φ_z вычисляет бесконечное множество б. ф. По φ_z можно построить чрп б. ф., которая не будет почти содержаться в M, что противоречит его предельности. Утверждение доказано.

На множества б. ф. естественным образом могут быть распространены понятия простоты и иммунности (ср. [5]).

3.2. *Если рпм M предельно, либо выполнено* $\min\limits_{F^n \in \overline{M}} L(F^n) \to \infty$, *то* $\forall t (L^t_M(n) \succ 2^n)$ *и M просто (а, следовательно $\overline{M}$ иммунно).*

Доказательство. Пусть для некоторой орф t множество $\{n \mid L^t_M(n) < 2^n\}$ не конечно. Пусть F^n_n — конструктивная последовательность б. ф. такая, что $\forall n (L(F^n_n) \geqslant 2^n)$, тогда бесконечным будет и множество таких n, что $F^n_n \in \overline{M}$, что противоречит тому, что $\min\limits_{F^n \in \overline{M}} L(F^n) \to \infty$. Далее, если бы $\overline{M}$ не было бы иммунным, то из него можно было бы выделить некоторую чрп б. ф., сложность же всякой чрп ограничена константой, что противоречит условию $\min\limits_{F^n \in \overline{M}} L(F^n) \to \infty$.

Используя 3.2, нетрудно убедиться в справедливости утверждения.

3.3 *Для любой неограниченной, неубывающей орф g можно указать простое множество M такое, что* $\forall t (L^t_M(n) \succ 2^n)$ *и* $L_M(n) \leqslant g(n)$.

Доказательство. В качестве искомого множества можно выбрать множество, удовлетворяющее условию: $\forall n (M_n = \{F^n \mid L(F^n) \leqslant g(n)\})$. Условия утверждения для M выполняются очевидным образом либо в силу его предельности, либо того, что $\min\limits_{F^n \in \overline{M}} L(F^n) \to \infty$.

Орф γ будем называть мажорантой сложности для M если выполнено $\exists t (L^t_M(n) \leqslant \gamma(n))$. Довольно очевидно, что если M имеет иммунное дополнение, и если γ есть мажоранта сложности для M, то множество $\{n \mid \gamma(n) < 2^n\}$ не бесконечно. С другой стороны, из факта существования сколь угодно „редких" простых множеств (см. [1]) следует: существует простое M такое, что $\exists t \exists C \forall n \neg\neg \exists m > n (L^t_M(m) < C)$. Таким образом, мажоранты сложности, в свою очередь, могут существенно отличаться от L^t.

3.4. *Пусть рпм M и орф α удовлетворяют условию* $\forall n (d(M_n) < \alpha(n))$, *причем множество $\{n \mid d(M_n) = \alpha(n)\}$ не конечно. Тогда можно указать орф t и последовательность н. ч. n_i такие, что* $L^t_M(n_i) \prec L_M(n_i)$.

Доказательство. Множество n таких, что $d(M_n) = \alpha(n)$, перечислимо. Из этого множества можно выделить рекурсивное подмножество n_i. Определим рекурсивное множество $\tilde{M}$ б. ф. следующим образом: $\tilde{M}_n = M_n$, если $n = n_k$ для некоторого k и $\tilde{M}_n = \varnothing$ в противном случае. В силу его рекурсивности условия утверждения выполнены.

Функция α в условии 3.4 может быть выбрана равной константе C, тогда из 3.4 следует: (а) утверждение 3.3 не может быть усилено до

такого „$\exists M((L_M(n) < C) \& \forall t(L^t_M(n) \geqslant 2^n))$“, или, иначе, функция g в условии 3.3 не может быть константной: (б) из 3.4 вкупе с фактом, что для мажорант сложности простых множеств выполнено $\forall^{\infty}_n(\gamma(n) \geqslant 2^n)$, следует, что параллельно с фактом существования сколь угодно „редких“ простых множеств, они обладают следующим любопытным свойством — (M просто $\supset \neg \exists C(d(M_n) < C)$.

§ 2. Классы сложности множеств булевых функций и вопросы их представимости

Рассмотрение классов сложности множеств б. ф. было мотивировано фактом, сформулированным в 1.4 § 1. Классом сложности R_t множеств б. ф. будем называть класс таких рпм M булевых функций, для которых сохраняются мощностные оценки при ограничении t на время работы алгорифмов, или $L^t_M \asymp L_M$ (напомним, что рассматривается аддитивно оптимальная нумерация, и для нее выполнено $\forall$ рпм M $(L_M(n) \asymp l(d(M_n)))$).

Замечание. Можно было бы дать несколько иное определение классов сложности, которое индуцирует, вообще говоря, более тонкую иерархию классов. Пусть для орф t и н. ч. C класс сложности $R_{t,c}$ есть класс таких рпм M, для которых выполнено $\forall^{\infty}_n(L^t_M(n) \leqslant l(d(M_n)) + C)$, тогда из слегка модифицированного утверждения 1.3 § 1:

$$\exists t_0 \forall t > t_0 \forall C \exists M \exists C_1 > C \exists C_0[(L^t_M \geqslant l(d(M_n)) + C_1) \& \forall^{\infty}_n(L^t_M(n) \leqslant$$

$$\leqslant l(d(M_n)) + C_0)]$$

(оно доказывается аналогично 1.3) следуют утверждения —

а) можно указать последовательность н. ч. C_i такую, что $R_{t,c_i} \subset R_{t,c_{i+1}}$.

б) $\exists t_0 \forall t > t_0 > t_0 \forall C \neg (R_{t,c} \supset R_{t_0})$.

1. Многие факты, относящиеся к классам сложности чрф [11], легко переносятся на классы сложности множеств б. ф. Так, существует равномерная процедура получения нового класса сложности $R_{t'}$, строго включающего R_t по сигнализирующей для t (см. 1.1 ниже), в то же время, из теоремы о пробелах (1.2) следует невозможность такой процедуры равномерной относительно самой t (1.3).

1.1. *Существует орф H такая, что для любого i, если φ_i орф, то $R_{H(n,\Phi_i(n))} \supset R_{\varphi_i}$.*

(Символ $\supset$ используется для обозначения строгого включения множеств).

1.2. *Для любых орф f и T существует орф $t > T$ такая, что $R_t = R_{f \circ t}$.*

1.3. *Не существует орф s такой, что для любой орф t $R_{s \circ t} \supset R_t$.*

2. Рассмотрим вопросы, связанные с представимостью классов R_t (ср. [11], [12]).

Пусть фиксировано некоторое взаимно однозначное соответствие между множеством н. ч. и множеством б. ф. Натуральное число, соответствующее б. ф. F, в этом соответствии будем называть кодом б. ф. F.

Будем использовать следующие обозначения:

$\overline{x}$ — б. ф., имеющая код x;

$\overline{A}$ — множество б. ф., множество кодов которых суть множество н. ч. A;

$\overline{F}$ — код б. ф. F;

$\overline{M}$ — множество кодов б. ф. из M;

Θ_n — множество кодов всех б. ф. размерности n.

Множество н. ч. S будем называть представлением класса R_t множеств б. ф., если $R_t = \{\overline{W}_i \mid i \in S\}$ (через W_i обозначено множество определенности φ_i [7]). Будем говорить, что класс R_t множеств б. ф. рекурсивно (рекурсивно перечислимо) представим, если существует рекурсивное (перечислимое) представление класса R_t. Как отмечено в [11], если класс R имеет перечислимое представление, то он также и рекурсивно представим — это следует из факта, что геделевские (допустимые) нумерации являются нумерациями с эффективно бесконечными классами ([5], [7]).

Известно, что классы сложности чрф, определяемые орф $t - R_t$, рекурсивно представимы только при достаточно больших t. Оказывается, что для классов сложности множеств б. ф. они рекурсивно представимы при любых t.

2.1. *Для любой орф t класс R_t рекурсивно представим.*

Доказательство. Опишем процедуру перечисления рпм $W_{\alpha(z)}$, равномерную относительно индекса z. Посредством Q_n^k обозначим множество н. ч., принадлежащих $\Theta_n \cap W_z$ и принадлежность которых к W_z „выясняется за k шагов“. Для каждого n определим конечное рпм V_n. Множество V_n будем определять поэтапно, так, если V_n^k есть множество, полученное на этапе k ($k = 1, 2, \ldots$), $V_n^{k+1} \supseteq V_n^k$ и $V_n = \bigcup\limits_k V_n^k$. Пусть $V_n^1 = \varnothing$. Пусть множество V_n^k уже построено. Перейдем к построению V_n^{k+1}. Если выполнено условие — для всех $x \in Q_n^{k+1}$ $L^{t(n)}(\overline{x}) \leqslant l(d(Q_n^{k+1})) + z$, то полагаем $V_n^{k+1} = Q_n^{k+1}$, если нет, то полагаем $V_n^{k+1} = V_n^k$. Переходим к этапу $k+2$. Пусть $W_{\alpha(z)} = \bigcup\limits_n V_n$. Нетрудно убедиться, что α перечисляет индексы множеств кодов множеств б. ф. из R_t — для этого следует иметь в виду, что если для некоторого рпм M б. ф. выполнено $\exists C (L_M^t(n) \leqslant l(d(M_n)) + C)$, то найдется индекс z такой, что $\overline{W}_z = M$ и $z > C$. Утверждение доказано.

Посредством $\mathfrak{Q}R$ будем обозначать индексное множество класса $R - \{i \mid \overline{W}_i \in R\}$. Будем пользоваться принятыми обозначениями: „$\leqslant_T$“ и „$\leqslant_1$“ для сводимостей по Тьюрингу и 1—1 сводимостей, Σ_n и Π_n для уровней иерархии Клини-Мостовского [7]. Нам потребуются

следующие „эталонные" множества: $\mathrm{Equal} = \{\langle i, j\rangle \mid \varphi_i = \varphi_j\}$ и $\mathrm{Cofinite} = \{i \mid W_i$ — кофинитно$\}$. Известно, что эти множества являются соответственно Π_2-полным и Σ_3-полным. Через R будем обозначать класс всех рпм б. ф.

Доказательство утверждения 2.4 следует плану доказательства аналогичного факта, формулируемого для классов сложности чрф [12] (в [12] аналог утверждения 2.4 формулируется для сигнализирующей Ф, удовлетворяющей определенным условиям).

2.2 (Робертсон [12]). *Для любой орф t, если класс $R - R_t$ имеет $\Pi_3 \cap \Sigma_3$ представление, то* $\Omega R_t \leqslant_T \mathrm{Equal}$.

Доказательство. Опишем машину Тьюринга с „оракулом" Equal, которая выполняет два процесса параллельно, первый из которых останавливается, если $\overline{W_i} \in R - R_t$, второй определяет принадлежность $\overline{W_i}$ классу R_t. Для выяснения того, выполнено ли $\overline{W_i} \in R - R_t$, перечисляем представление $e_0, e_1, e_2, \ldots$ класса $R - R_t$ и спрашиваем оракул — „принадлежит ли $\langle i, e_0\rangle$ множеству Equal?", затем $\langle i, e_1\rangle$ и так далее. Такое перечисление представления $R - R_t$ возможно, так как по предположению оно принадлежит $\Pi_3 \cap \Sigma_3$, а любое $\Pi_3 \cap \Sigma_3$ множество может быть перечислено машиной Тьюринга с „оракулом" Equal в силу его Π_2-полноты. Аналогичным образом выясняется принадлежность $\overline{W_i}$ классу R_t. Это возможно, так как по 2.1 R_t рекурсивно представим.

2.3. $\exists \tau\, \forall t > \tau\, [\mathrm{Cofinite} \leqslant_1 \Omega R_t]$.

Доказательство. Пусть τ-орф такая, что $L_{\overline{M}} \simeq L_M$, где M — множество всех б. ф. Если Q — некоторое множество н. ч., то через $[Q]_n$ будем обозначать множество $Q \cap \Theta_n$. Пусть далее α есть двухместная орф такая, что $[W_{\alpha(i,j)}]_n = \Theta_n$ если $!\,\varphi_j(n)$ и выполнено — $[W_{\alpha(i,j)}]_n = \{x\}$, где x удовлетворяет условию: $\overline{x}$ есть б. ф. размерности n и $L^{\max(\tau(n),\, \varphi_i(n))}(\overline{x}) = \max\limits_{y \in \Theta_n} L^{\max(\tau(n),\, \varphi_i(n))}(\overline{y})$ если $\neg\, !\,\varphi_j(n)$ (условие $\neg\, !\,\varphi_j(n)$ непроверяемо, однако, так как $x \in \Theta_n$, то $\overline{x} \in W_{\alpha(i,j)}$ независимо от $!\,\varphi_j(n)$ или $\neg\, !\,\varphi_j(n)$). Пусть i — индекс орф t и $t > \tau$. Тогда, как нетрудно убедиться, функция $\lambda_j \alpha(i, j)\ m$ — сводит Cofinite к ΩR_t. Действительно, пусть W_j кофинитно, тогда $\forall_n^{\infty}(!\,\varphi_j(n))$ и $\forall_n^{-}[W_{\alpha(i,j)}]_n = M_n$, а, следовательно, $\alpha(i, j) \in R\Omega_t$. Верна и обратная импликация: если $\alpha(i, j) \in \Omega R_t$, то W_j кофинитно, ибо в противном случае для любой константы C, для бесконечно многих n нарушилось бы неравенство $L_{\overline{[W_{\alpha(i,j)}]_n}} \leqslant L^t_{\overline{[W_{\alpha(i,j)}]_n}} + C$. По функции α может быть построена (учитывая, что φ есть геделевская нумерация с эффективно бесконечными классами) функция α' такая, что если i есть индекс орф t, то $\lambda_j \alpha'(i, j)$ $1-1$ функция, сводящая Cofinite к ΩR_t.

Утверждения 2.4 и 2.5 следуют из 2.2 и 2.3.

2.4. *Существует орф* τ *такая, что для всех* $t > \tau$ *неверно, что класс* $R - R_t$ *имеет* $\Pi_3 \cap \Sigma_3$ *представление.*

2.5. *Существует орф* τ *такая, что для всех* $t > \tau$ $\mathfrak{Q}R_t$ Σ_3*-полно.*

Հ. Հ. ՆԱԶԱՐՅԱՆ

ԲՈՒԼՅԱՆ ՖՈՒՆԿՑԻԱՆԵՐԻ ԱԼԳՈՐԻԹՄԻԿ ԼԵԶՈՒՆԵՐՈՒՄ ԻՐԱՑՈՒՄԸ ԱԼԳՈՐԻԹՄԵՐԻ ԺԱՄԱՆԱԿԻ ՍԱՀՄԱՆԱՓԱԿՈՒՄՆԵՐԻ ԱՌԿԱՅՈՒԹՅԱՄԲ

Ա մ փ ո փ ո ւ մ

Դիտարկում են բուլյան ֆունկցիաների բազմությունների բարդությունները բնորոշող Շենոնի ֆունկցիաները այն պայմաններում, երբ ուսումնասիրվող ալգորիթմների աշխատանքի ժամանակը սահմանափակվում է ընդհանուր ռեկուրսիվ ֆունկցիաներով։ Հաստատվում են որոշ անհրաժեշտ և բավարար պայմաններ, որպեսզի նշված Շենոնի ֆունկցիաները ունենան հզորական գնահատականներ։ Ցույց է տրվում, որ գոյություն ունեն այնպիսի բազմություններ, որոնց համար Շենոնի ֆունկցիաների գնահատականները էապես տարբերվում են, երբ դիտարկվում են ալգորիթմները սահմանափակումների առկայության և բացակայության դեպքերում։ Դիտարկվում են բուլյան ֆունկցիաների բազմությունների բարդության դասերը և այդ դասերի դասակարգումները։

ЛИТЕРАТУРА

1. *Барздинь Я. М.* О вычислимости на вероятностных машинах. ДАН СССР, 189, 1969, 699—703.
2. *Заславский И. Д.* О псевдофункциях Шеннона. Зап. научн. семинаров ЛОМИ АН СССР, т. 16, 1969, 65—76.
3. *Звонкин А. К., Левин Л. А.* Сложность конечных объектов и обоснование понятий информации и случайности с помощью теории алгорифмов. УМН, т. 25, вып. 2, 1970, 85—127.
4. *Колмогоров А. Н.* Три подхода к определению понятия «количество информации». Проблемы передачи информации, 1, 1, 1965, 3—11.
5. *Мальцев А. И.* Алгоритмы и рекурсивные функции. «Наука», М., 1965.
6. *Назарян Г. А.* О реализации булевых функций в алгорифмических языках. Сб «Математические вопросы кибернетики и вычислительной техники», Труды ВЦ АН АрмССР и ЕрГУ, VIII, 1974, 36—56.
7. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. М., «Мир», 1972.
8. *Трахтенброт Б. А.* Сложность алгорифмов и вычислений. Новосибирск, 1967.
9. *Blum M.* A machine-independent theory of complexity of recursive functions. JACM, 14, 1967, 322—336.
10. *Borodin A.* Computational complexity and existence of complexity gaps. JACM, 19, 1972, 158—174.
11. *Landweber L. H., Robertson E. L.* Recursive properties of abstract complexity classes. JACM, 19, 1972, 2, 296—309.
12. *Robertson E. L.* Classes of partial recursive functions, JCSS, 1974, 69—87.