

УДК 519.7

О РАНДОМИЗИРОВАННОЙ СЛОЖНОСТИ ФУНКЦИЙ, АППРОКСИМИРУЮЩИХ ФУНКЦИЮ ГОЛОСОВАНИЯ*)

А. В. Чашкин

Рассматривается сложность реализации частичных булевых функций, приближающих булеву функцию от n переменных, являющуюся булевой функцией голосования (по большинству) $M(x_1, \dots, x_n)$. Функции вычисляются на машине с произвольным доступом к памяти, снабженной генератором случайных чисел. Показано, что использование генераторов случайных чисел позволяет вычислять функции, грубо приближающие $M(x_1, \dots, x_n)$, за константное время. При вычислении функций, достаточно близких к $M(x_1, \dots, x_n)$, использование генераторов случайных чисел не позволяет более чем в константное число раз уменьшить сложность вычислений.

Введение

В работе изучается сложность вычисления значений булевых функций на вероятностных машинах с произвольным доступом к памяти (RAM). Подробное описание RAM можно найти, например, в [1]. Используемая ниже модель отличается от описанной в [1] тем, что (1) входная информация хранится не на ленте, а в памяти, что обеспечивает произвольный доступ к входным данным сразу после начала работы; (2) модель снабжена генератором случайных чисел, который порождает с равными вероятностями целые числа из множества $\{0, 1, \dots, 2^s\}$, где $s = \mathcal{O}(\log_2 n)$, а n — число переменных рассматриваемых булевых функций; (3) в каждый момент времени доступно произвольное неотрицательное целое число, не превосходящее $\mathcal{O}(2^s)$. Предполагается, что программы, управляющие работой машин, не содержат ветвлений.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-01175), программы поддержки ведущих научных школ РФФИ (проект 00-15-96103), программы «Университеты России», Федеральной целевой программы «Интеграция» (объединенный проект АО-110).

Пусть $D \subseteq \{0, 1\}^n$. Будем говорить, что РАМ-программа P вычисляет частичную булеву функцию $f : D \rightarrow \{0, 1\}$ с надежностью $1 - \varepsilon$, если для каждого $\mathbf{x} \in D$ вероятность несовпадения вычисленного значения $P(\mathbf{x})$ со значением $f(\mathbf{x})$ не превосходит ε :

$$\Pr(P(\mathbf{x}) \neq f(\mathbf{x})) \leq \varepsilon. \quad (1)$$

Число команд в программе P назовем ее *сложностью* и обозначим через $L(P)$. Сложность самой простой программы, вычисляющей функцию f с надежностью $1 - \varepsilon$, назовем ε -сложностью (*рандомизированной сложностью*) функции f и обозначим через $L(f, \varepsilon)$. Программу, не обращающуюся к генератору случайных чисел, назовем *детерминированной*. Сложность самой простой детерминированной программы, вычисляющей f , назовем сложностью f и обозначим через $L(f)$.

Известно [4], что в случае, когда нет ограничений на длину используемых программ, использование генераторов случайных чисел позволяет уменьшить сложность вычисления булевой функции от n переменных не более чем в n раз. В настоящей работе результаты из [4] обобщаются на случай частичных булевых функций и приводятся примеры частичных функций, аппроксимирующих функцию голосования $M(x_1, \dots, x_n)$, для которых детерминированная сложность с точностью до порядка превосходит рандомизированную сложность в n раз. Ранее было показано [5, 6] (см. также [7]), что в некоторых специальных моделях схем использование вероятности позволяет вычислять аналогичные функции проще, чем функцию $M(x_1, \dots, x_n)$. Примеры функций, рандомизированная сложность которых при вычислении на одноленточных машинах Тьюринга меньше детерминированной, можно найти в [2].

Доказательство того, что рандомизированная сложность конкретной булевой функции значительно меньше ее детерминированной сложности, заключается в установлении нижних оценок детерминированной сложности, превосходящих верхние оценки рандомизированной сложности. Результаты в [2] получены благодаря «слабости» детерминированной модели — для простых функций (например, для определения симметричности двоичного набора) установлены квадратичные нижние оценки. В настоящей работе ситуация иная. Результаты получены благодаря «силе» используемой модели — рандомизированная сложность рассматриваемых функций ограничена сверху константой, а детерминированная сложность оценивается снизу через число существенных переменных.

1. Рандомизированная сложность произвольных булевых функций

Ниже приводятся простейшие соотношения, связывающие рандомизированную и детерминированную сложности булевых функций. Аналогичные результаты в различной форме можно найти, например, в [2–7].

Лемма 1. Пусть $D \subseteq \{0, 1\}^n$, $f : D \rightarrow \{0, 1\}$, $0 < \varepsilon < \frac{1}{|D|}$ и $0 < \delta < \gamma < \frac{1}{2}$. Тогда

$$L(f, \delta) \geq L(f, \gamma), \quad L(f, \varepsilon) = L(f).$$

Доказательство. Первое неравенство из утверждения леммы очевидно, так как любая программа, вычисляющая f с надежностью $1 - \delta$, вычисляет f с надежностью $1 - \gamma$.

Пусть программа P вычисляет частичную булеву функцию $f : D \rightarrow \{0, 1\}$ с надежностью $1 - \varepsilon$ и в процессе вычисления k раз обращается к генератору случайных чисел. Набор порождаемых при этом случайных чисел будем обозначать через $\mathbf{z} = (z_1, z_2, \dots, z_k)$, а множество всех возможных значений \mathbf{z} — через Z . Обозначим через $P(\mathbf{x}, \mathbf{z})$ значение, вычисленное программой P на наборе \mathbf{x} при условии, что генератор случайных чисел порождает набор \mathbf{z} . В этих обозначениях неравенство (1) эквивалентно неравенству

$$\sum_{\mathbf{z} \in Z} (P(\mathbf{x}, \mathbf{z}) \oplus f(\mathbf{x})) \leq \varepsilon |Z|. \quad (2)$$

Если $\varepsilon < \frac{1}{|D|}$, то

$$\sum_{\mathbf{x} \in D} \sum_{\mathbf{z} \in Z} (P(\mathbf{x}, \mathbf{z}) \oplus f(\mathbf{x})) < |Z|.$$

Поэтому найдется такое $\mathbf{z}_0 \in Z$, что $\sum_{\mathbf{x} \in D} (P(\mathbf{x}, \mathbf{z}_0) \oplus f(\mathbf{x})) < 1$. Так как последняя сумма есть целое число, то

$$\sum_{\mathbf{x} \in D} (P(\mathbf{x}, \mathbf{z}_0) \oplus f(\mathbf{x})) = 0.$$

Заменяя в P обращение к генератору случайных чисел соответствующими набору \mathbf{z}_0 целыми числами, получаем детерминированную программу P' , вычисляющую f . Легко видеть, что $L(P') \leq L(P)$. С другой стороны, ясно, что $L(f) \geq L(f, \varepsilon)$ при любом ε . Лемма доказана.

Теорема 1. Пусть $D \subseteq \{0, 1\}^n$ и δ, ε такие, что $\frac{1}{|D|} \leq \delta < \varepsilon \leq \frac{1}{3}$. Тогда для любой функции $f : D \rightarrow \{0, 1\}$ при $n \rightarrow \infty$ справедливы соотношения *)

$$L(f, \varepsilon) = \Omega\left(L(f, \delta) \frac{\log_2 \varepsilon}{\log_2 \delta}\right), \quad L(f, \varepsilon) = \Omega\left(L(f) \frac{\log_2 1/\varepsilon}{\log_2 |D|}\right).$$

Доказательство. Пусть P' — вероятностная программа сложности $L(f, \varepsilon)$. Используя P' , построим другую программу P , вычисляющую

*) $f(n) = \Omega(g(n))$ означает, что существует такая положительная константа c , что $f(n) \geq c \cdot g(n)$.

f с большей надежностью. Пусть $\mathbf{x} \in D$ и $l = 2l' + 1$, где l' — целое, большее единицы. Независимо l раз вычислим $P'(\mathbf{x})$. К вычисленным значениям применим функцию голосования. Тогда получаем

$$\begin{aligned} \Pr(P(\mathbf{x}) \neq f(\mathbf{x})) &= \sum_{i=l'+1}^l \binom{l}{i} \varepsilon^i (1-\varepsilon)^{l-i} \\ &= (1-\varepsilon)^l \sum_{i=l'+1}^l \binom{l}{i} \varepsilon^i (1-\varepsilon)^{-i} \leq (1-\varepsilon)^l \frac{2^l}{3} \sum_{i=l'+1}^l \varepsilon^i (1-\varepsilon)^{-i} \\ &< (1-\varepsilon)^l \frac{2^l \varepsilon^{l'+1} (1-\varepsilon)^{-l'}}{3} \leq \frac{2^l (\varepsilon(1-\varepsilon))^{l'+1}}{3(1-2\varepsilon)} \leq (4\varepsilon(1-\varepsilon))^{l/2}. \quad (3) \end{aligned}$$

Положив $l' = \left\lceil \frac{\log_2 \delta}{\log_2 (4\varepsilon(1-\varepsilon))} \right\rceil$, видим, что при каждом \mathbf{x} из D справедливо неравенство

$$\Pr(P(\mathbf{x}) \neq f(\mathbf{x})) \leq \delta.$$

Легко видеть, что l с точностью до постоянного множителя совпадает с $\frac{\log_2 \delta}{\log_2 \varepsilon}$ и $L(P) = l \cdot L(P') + \mathcal{O}(l)$. Первое утверждение теоремы доказано.

Теперь положим $l' = \left\lceil \frac{-\log_2 |D|}{\log_2 (4\varepsilon(1-\varepsilon))} \right\rceil$. В этом случае справедливо неравенство $(4\varepsilon(1-\varepsilon))^{l/2} < \frac{1}{|D|}$. Пусть $\gamma = (4\varepsilon(1-\varepsilon))^{l/2}$. Тогда из первого утверждения теоремы следует, что

$$L(f, \varepsilon) = \Omega\left(L(f, \gamma) \frac{\log_2 \varepsilon}{\log_2 \gamma}\right).$$

Так как $\gamma < \frac{1}{|D|}$, то из леммы 1 следует, что $L(f, \gamma) = L(f)$. Поэтому

$$L(f, \varepsilon) = \Omega\left(L(f) \frac{\log_2 \varepsilon}{\log_2 \gamma}\right) = \Omega\left(L(f) \frac{\log_2 \varepsilon}{\log_2 1/|D|}\right).$$

Теорема доказана.

Согласно следующей теореме рандомизированная сложность булевой функции, существенно зависящей от n переменных, с точностью до порядка не меньше n . Ниже будет показано, что этот результат не может быть распространен на частичные функции — существуют частичные функции, которые можно вычислять за константное время рандомизированными программами с высокой надежностью, и любое доопределение таких функций существенно зависит от растущего числа переменных.

Теорема 2. Пусть f — булева функция, существенно зависящая от n переменных. Тогда

$$L\left(f, \frac{1}{3}\right) = \Omega(n).$$

Доказательство. Предположим, что $L(f, \frac{1}{3}) < \frac{1}{3}n - 1$. Пусть P — минимальная вероятностная программа, вычисляющая f с надежностью $\frac{2}{3}$. Тогда согласно (2) для любого \mathbf{x} имеем

$$\sum_{\mathbf{z} \in Z} (P(\mathbf{x}, \mathbf{z}) \oplus f(\mathbf{x})) \leq \frac{1}{3}|Z| \quad (4)$$

и при каждом $\mathbf{z} \in Z$ функция $P(\mathbf{x}, \mathbf{z})$ существенно зависит менее чем от $\frac{n}{3}$ переменных. Следовательно, найдется такая переменная x_j , что менее трети функций $P(\mathbf{x}, \mathbf{z})$ существенно зависят от x_j . Пусть $\mathbf{x}, \mathbf{x}' \in \{0, 1\}^n$ — такие наборы, отличающиеся в j -й компоненте, что $f(\mathbf{x}) \neq f(\mathbf{x}')$. Тогда значения $P(\mathbf{x}, \mathbf{z})$ и $P(\mathbf{x}', \mathbf{z})$ совпадают более чем на $\frac{2}{3}|Z|$ различных наборах \mathbf{z} из Z . Следовательно, либо

$$\sum_{\mathbf{z} \in Z} (P(\mathbf{x}, \mathbf{z}) \oplus f(\mathbf{x})) > \frac{1}{3}|Z|,$$

либо

$$\sum_{\mathbf{z} \in Z} (P(\mathbf{x}', \mathbf{z}) \oplus f(\mathbf{x}')) > \frac{1}{3}|Z|.$$

Противоречие с (4). Теорема доказана.

2. Детерминированная сложность функций, аппроксимирующих функцию голосования

Весом произвольного набора $\mathbf{x} = (x_1, \dots, x_n)$ из $\{0, 1\}^n$ назовем величину $w(\mathbf{x}) = \sum_{i=1}^n x_i$.

Далее полагаем, что $n > 2m$, и рассматриваем детерминированную сложность частичной булевой функции $M_{n,m}(\mathbf{x})$, определяемой следующим образом:

$$M_{n,m}(x) = \begin{cases} 1, & \text{если } w(\mathbf{x}) \geq n - m; \\ *, & \text{если } m < w(\mathbf{x}) < n - m; \\ 0, & \text{если } w(\mathbf{x}) \leq m. \end{cases}$$

Функция $M_{n,m}(\mathbf{x})$ аппроксимирует функцию голосования

$$M_n(x_1, \dots, x_n) = \begin{cases} 1, & \text{если } w(x_1, \dots, x_n) \geq \lfloor n/2 \rfloor + 1, \\ 0, & \text{если } w(x_1, \dots, x_n) \leq \lfloor n/2 \rfloor. \end{cases}$$

При $n = 2m + 1$ функция $M_{n,m}(\mathbf{x})$ является полностью определенной булевой функцией. Оценим сложность функции $M_{n,m}(\mathbf{x})$.

Лемма 2. При $n > 2t$ любая полностью определенная булева функция, являющаяся доопределением функции $M_{n,m}(\mathbf{x})$, существенно зависит не менее чем от $2t + 1$ переменных и

$$L(M_{n,m}(\mathbf{x})) = 2t + \mathcal{O}(1). \quad (5)$$

Доказательство. Если $w(\mathbf{x}) \leq t$, то среди первых $2t + 1$ разрядов набора \mathbf{x} найдется не более t единиц, а если $w(\mathbf{x}) \geq n - t$, то среди первых $2t + 1$ разрядов набора \mathbf{x} найдется не более t нулей. Поэтому

$$\begin{aligned} M_{n,m}(x_1, \dots, x_n) &= M_{2t+1,m}(x_1, \dots, x_{2t+1}), \\ L(M_{n,m}(\mathbf{x})) &\leq L(M_{2t+1,m}(\mathbf{x})) \leq 2t + \mathcal{O}(1). \end{aligned}$$

С другой стороны, любая полностью определенная булева функция, являющаяся доопределением частичной функции $M_{n,m}(\mathbf{x})$, существенно зависит не менее чем от $2t + 1$ переменных. Если это не так и некоторое доопределение h существенно зависит от $p \leq 2t$ переменных (без ограничения общности полагаем, что это первые переменные и $p > t$), то

$$1 = M_{n,m}(\underbrace{1 \dots 1}_m \underbrace{0 \dots 0}_{p-m} \underbrace{1 \dots 1}_{n-p}) = h(\underbrace{1 \dots 1}_m \underbrace{0 \dots 0}_{p-m}) = M_{n,m}(\underbrace{1 \dots 1}_m \underbrace{0 \dots 0}_{n-m}) = 0.$$

Противоречие. Следовательно, $L(M_{n,m}(\mathbf{x})) > 2t$. Лемма доказана.

3. Рандомизированная сложность функций, грубо аппроксимирующих функцию голосования

Теорема 3. Пусть $0 \leq \varepsilon \leq \frac{1}{3}$, $\gamma > 0$ — постоянная и $n > (2 + \gamma)t$. Тогда при $n \rightarrow \infty$ *)

$$L(M_{n,m}, \varepsilon) = \Theta\left(\min\left(m, \log_2 \frac{1}{\varepsilon}\right)\right).$$

Утверждение теоремы следует из двух приводимых ниже лемм. Верхняя оценка следует из леммы 3 и условия $n > (2 + \gamma)t$, нижняя оценка — из леммы 4.

Лемма 3. Если $0 \leq \varepsilon \leq \frac{1}{3}$, то при $n \rightarrow \infty$

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \mathcal{O}\left(\left(\frac{n}{n-2m}\right)^2 \log_2 \left(\frac{n}{(n-2m)\varepsilon}\right)\right).$$

*) $f(n) = \Theta(g(n))$ означает, что существуют такие положительные константы c_1 и c_2 , что $c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$.

ДОКАЗАТЕЛЬСТВО. Опишем вероятностную программу $P_{n,l}$, вычисляющую функцию $M_{n,m}(\mathbf{x})$. Зафиксируем целое нечетное $l = 2l' + 1$. Используя генератор случайных чисел, выберем равномерно распределенные на $\{1, 2, \dots, n\}$ целые числа $\{r_1, r_2, \dots, r_l\}$ ^{*)} Далее вычислим функцию голосования от переменных $\{x_{r_1}, x_{r_2}, \dots, x_{r_l}\}$. Очевидно, что сложность программы $P_{n,l}$ пропорциональна l . Пусть $w(\mathbf{x}) \leq m$ (случай $w(\mathbf{x}) \geq n - m$ рассматривается аналогично). Положим $\delta' = \frac{w(\mathbf{x})}{n}$ и $\delta = \frac{m}{n}$. Тогда после преобразований, аналогичных (3), имеем

$$\begin{aligned} \Pr(P_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) &= \Pr(P_{n,l}(\mathbf{x}) = 1) \\ &= \sum_{i=l'+1}^l \binom{l}{i} \delta^i (1 - \delta')^{l-i} \leq \sum_{i=l'+1}^l \binom{l}{i} \delta^i (1 - \delta)^{l-i} < \frac{(4\delta(1 - \delta))^{l/2}}{1 - 2\delta}. \end{aligned}$$

Легко видеть, что при $l' = \left\lceil \frac{\log_2 \varepsilon (1 - 2\delta)}{\log_2 (4\delta(1 - \delta))} \right\rceil$ справедливо неравенство

$$\frac{(4\delta(1 - \delta))^{l/2}}{1 - 2\delta} \leq \varepsilon.$$

Следовательно, при $w(\mathbf{x}) \leq m$ имеем

$$\Pr(P_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) \leq \varepsilon.$$

Так как

$$4\delta(1 - \delta) \leq \frac{4m}{n} \left(1 - \frac{m}{n}\right) = \left(1 - \frac{n - 2m}{n}\right) \left(1 + \frac{n - 2m}{n}\right) = 1 - \left(\frac{n - 2m}{n}\right)^2,$$

то

$$l = \mathcal{O} \left(\frac{\log_2 \left(\varepsilon \frac{n - 2m}{n} \right)}{\log_2 \left(1 - \left(\frac{n - 2m}{n} \right)^2 \right)} \right) = \mathcal{O} \left(\left(\frac{n}{n - 2m} \right)^2 \log_2 \left(\frac{n}{(n - 2m)\varepsilon} \right) \right).$$

Лемма доказана.

Лемма 4. Пусть $0 \leq \varepsilon \leq \frac{1}{3}$, $\gamma > 0$ постоянная и $n > (2 + \gamma)t$. Тогда при $n \rightarrow \infty$

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \Omega \left(\min \left(m, \log_2 \frac{1}{\varepsilon} \right) \right).$$

ДОКАЗАТЕЛЬСТВО. Пусть P — минимальная вероятностная программа, вычисляющая $M_{n,m}(\mathbf{x})$ с надежностью $1 - \varepsilon$, и h — функция, являющаяся доопределением частичной функции $M_{n,m}(\mathbf{x})$, вычисляемая

^{*)} В рассматриваемой модели иногда невозможно получить при некоторых n равновероятное распределение на множестве $\{1, 2, \dots, n\}$. Однако легко показать, что при $s \geq \log_2 n$ можно получить распределение, в котором вероятности появления различных чисел различаются не более чем на n^{-4} . При такой точности проводимые далее рассуждения остаются справедливыми.

программой P . Допустим, что h существенно зависит от k переменных. Из леммы 2 следует, что $k > 2m$ и $L(h) \geq 2m$. Далее рассматриваем функцию $M_{n,m}(\mathbf{x})$ как сужение функции h , т. е. как частичную функцию от k переменных. Тогда в силу теоремы 1 при $\varepsilon \geq \frac{1}{2^{2m+1}}$ имеем

$$L(h, \varepsilon) = \Omega\left(k \frac{\log_2 1/\varepsilon}{\log_2 2^k}\right) = \Omega\left(\log_2 \frac{1}{\varepsilon}\right).$$

Следовательно,

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \Omega\left(\log_2 \frac{1}{\varepsilon}\right).$$

Если $\varepsilon < \frac{1}{2^{2m+1}}$, то $m < \log_2 \frac{1}{\varepsilon}$. Поэтому

$$L(M_{n,m}(\mathbf{x}), \varepsilon) \geq L\left(M_{n,m}, \frac{1}{2^{2m+1}}\right) = \Omega\left(\log_2 \frac{1}{2^{2m+1}}\right) = \Omega\left(\min\left(m, \log_2 \frac{1}{\varepsilon}\right)\right).$$

Лемма доказана.

Следующая теорема 4 является простым следствием теорем 1 и 3. В ней установлен порядок максимально возможного отношения детерминированной и рандомизированной сложности булевых функций.

Положим

$$\mu(n, \varepsilon) = \max \frac{L(f)}{L(f, \varepsilon)},$$

где максимум берется по всем частичным (в том числе и по полностью определенным) булевым функциям от n переменных.

Теорема 4. Если ε удовлетворяет неравенствам $\frac{1}{2^n} \leq \varepsilon \leq \frac{1}{3}$, то

$$\mu(n, \varepsilon) = \Theta\left(\frac{n}{\log_2 1/\varepsilon}\right).$$

Справедливость верхней оценки непосредственно следует из теоремы 1. Нижняя оценка следует из теоремы 2 при $m = \lfloor \frac{n}{3} \rfloor$, так как

$$\log_2 \left(\sum_{i=0}^{\lfloor n/3 \rfloor} \binom{n}{i} \right) = \Theta(n).$$

4. Рандомизированная сложность функций, аппроксимирующих функцию голосования.

Общий случай

Пусть $l = 2l' + 1$ — целое нечетное и $Z(n, l) = \{z_i\}$ — множество всех l -элементных подмножеств множества $\{1, 2, \dots, n\}$. Опишем вероятностный алгоритм $A_{n,l}$, вычисляющий функцию $M_{n,m}(\mathbf{x})$.

1. Используя схему выбора без возвращения, случайно выбираем l -элементное подмножество $\mathbf{z} = \{r_1, r_2, \dots, r_l\}$ из множества $\{1, 2, \dots, n\}$. Очевидно, что любое \mathbf{z} порождается с вероятностью $\binom{n}{l}^{-1}$.

2. Вычисляется функция голосования от переменных $\{x_{r_1}, x_{r_2}, \dots, x_{r_l}\}$.

3. Результатом работы алгоритма $A_{n,l}$ на переменных x_1, x_2, \dots, x_n объявляется значение функции $M_{l,l'}(x_{r_1}, x_{r_2}, \dots, x_{r_l})$.

Как и в случае программ будем говорить, что алгоритм $A_{n,l}$ вычисляет частичную булеву функцию $M_{n,m}(\mathbf{x})$ с надежностью $1 - \varepsilon$, если для каждого \mathbf{x} из области определения функции $M_{n,m}(\mathbf{x})$ вероятность несовпадения вычисленного значения $A_{n,l}(\mathbf{x})$ со значением $M_{n,m}(\mathbf{x})$ не превосходит ε .

Положим $E_0 = \{\mathbf{x} \mid \mathbf{x} \in \{0, 1\}^n, w(\mathbf{x}) = m\}$ и $E_1 = \{\mathbf{x} \mid \mathbf{x} \in \{0, 1\}^n, w(\mathbf{x}) = n - m\}$.

Лемма 5. Пусть $l < m$. Тогда:

(i) Если $\mathbf{x} \in E_0 \cup E_1$, то

$$\Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) = \sum_{j=l'+1}^l \binom{l}{j} \binom{n-l}{m-j} / \binom{n}{m}.$$

(ii) Если при некотором $\mathbf{z} \in Z$ имеет место неравенство

$$\sum_{\mathbf{x} \in E_0 \cup E_1} (A_{n,l}(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) \leq \varepsilon \left(\binom{n}{m} + \binom{n}{n-m} \right), \quad (6)$$

то алгоритм $A_{n,l}$ вычисляет функцию $M_{n,m}(\mathbf{x})$ с надежностью $1 - \varepsilon$.

ПОКАЗАТЕЛЬСТВО. Легко видеть, что при любом $\mathbf{x} \in E_0$

$$\begin{aligned} \Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) &= \binom{n}{l}^{-1} \sum_{\mathbf{z} \in Z} (A_{n,l}(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) \\ &= \binom{n}{l}^{-1} \sum_{i_1, \dots, i_l} M_l(x_{i_1}, \dots, x_{i_l}) = \binom{n}{l}^{-1} \sum_{j=l'+1}^l \binom{m}{j} \binom{n-m}{l-j}. \end{aligned}$$

Аналогичные соотношения справедливы и для $\mathbf{x} \in E_1$. Поэтому при любом $\mathbf{x} \in E_0 \cup E_1$ имеем

$$\Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) = \binom{n}{l}^{-1} \sum_{j=l'+1}^l \binom{m}{j} \binom{n-m}{l-j}. \quad (7)$$

Так как

$$\binom{m}{j} \binom{n-m}{l-j} \binom{n}{m} = \binom{l}{j} \binom{n-l}{m-j} \binom{n}{l}, \quad (8)$$

то при любом $\mathbf{x} \in E_0 \cup E_1$

$$\begin{aligned} \Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) \\ = \binom{n}{l}^{-1} \sum_{j=l'+1}^l \binom{m}{j} \binom{n-m}{l-j} = \binom{n}{m}^{-1} \sum_{j=l'+1}^l \binom{l}{j} \binom{n-l}{m-j}. \end{aligned}$$

Первое равенство леммы доказано.

Легко видеть, что при любом фиксированном $\mathbf{z} = (i_1, \dots, i_l)$

$$\begin{aligned} \sum_{\mathbf{x} \in E_0} (A_{n,l}(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) \\ = \sum_{\mathbf{x} \in E_1} (A_{n,l}(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) = \sum_{j=l'+1}^l \binom{l}{j} \binom{n-l}{m-j}, \quad (9) \end{aligned}$$

т. е. значение суммы не зависит от \mathbf{z} . Отсюда и из (6) следует, что

$$\sum_{\mathbf{z} \in Z} \sum_{\mathbf{x} \in E_0 \cup E_1} (A_{n,l}(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) \leq \varepsilon \binom{n}{l} \left(\binom{n}{m} + \binom{n}{n-m} \right). \quad (10)$$

Из (7), (8) и (9) имеем

$$\begin{aligned} \sum_{\mathbf{z} \in Z} \sum_{\mathbf{x} \in E_0 \cup E_1} (A_{n,l}(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) &= 2 \binom{n}{l} \sum_{j=l'+1}^l \binom{l}{j} \binom{n-l}{m-j} \\ &= 2 \binom{n}{m} \sum_{j=l'+1}^l \binom{m}{j} \binom{n-m}{l-j} = \left(\binom{n}{m} + \binom{n}{n-m} \right) \sum_{j=l'+1}^l \binom{m}{j} \binom{n-m}{l-j}. \end{aligned}$$

Подставляя (10) в последнее неравенство, имеем

$$\sum_{j=l'+1}^l \binom{m}{j} \binom{n-m}{l-j} \leq \varepsilon \binom{n}{l}.$$

Следовательно, для каждого $\mathbf{x} \in E_0 \cup E_1$ алгоритм $A_{n,l}$ вычисляет функцию $M_{n,m}$ с требуемой надежностью. Легко видеть, что на других наборах из области определения надежность вычисления не меньше. Лемма доказана.

Лемма 6. Пусть $0 \leq \varepsilon \leq \frac{1}{3}$, $L(M_{n,m}(\mathbf{x}), \varepsilon) < m$ и l — минимально возможное целое, при котором алгоритм $A_{n,l}$ вычисляет функцию $M_{n,m}(\mathbf{x})$ с надежностью $1 - \varepsilon$. Тогда

$$L(M_{n,m}(\mathbf{x}), \varepsilon) \geq l.$$

ДОКАЗАТЕЛЬСТВО. Пусть P' — минимальная программа, вычисляющая функцию $M_{n,m}(\mathbf{x})$ с надежностью $1 - \varepsilon$. Заменяем обращение к датчикам случайных чисел в P' соответствующими компонентами набора \mathbf{z} . В результате получим новую детерминированную программу P_z такую, что $P_z(\mathbf{x}) = P'(\mathbf{x}, \mathbf{z})$. Допустим, что функция, вычисляемая программой P_z , существенно зависит только от p переменных. Очевидно, что $p \leq L(P')$. Далее полагаем также, что $p < m$.

Легко видеть, что для $N(P_z)$ — числа наборов \mathbf{x} из $E_0 \cup E_1$, на которых $P_z(\mathbf{x}) \neq M_{n,m}(\mathbf{x})$, справедливо равенство

$$N(P_z) = \sum_{0 \leq i \leq p} \sum_{\substack{\mathbf{x} \in \{0,1\}^p \\ w(\mathbf{x})=i}} \left(P_z(\mathbf{x}) \binom{n-p}{m-i} + \overline{P_z(\mathbf{x})} \binom{n-p}{n-m-i} \right).$$

Далее оценим снизу $N(P_z)$. Так как

$$\begin{aligned} & \binom{n-p}{m-i} / \binom{n-p}{n-m-i} \\ &= \frac{(n-p)!(n-m-i)!(n-p-n+m+i)!}{(m-i)!(n-p-m+i)!(n-2p)!} \\ &= \frac{(n-m-i)!(m-p+i)!}{(m-i)!(n-p-m+i)!} \\ &= \frac{(n-m-i) \dots (m-i+1)}{((n-m-i)-(p-2i)) \dots ((m-i+1)-(p-2i))}, \end{aligned}$$

то легко видеть, что $p-2i \geq 0$ при $i \leq \frac{p}{2}$. Поэтому

$$\binom{n-p}{m-i} \geq \binom{n-p}{n-m-i}.$$

Если $i > p$, то $2p-2i < 0$. Следовательно,

$$\binom{n-p}{n-m-i} > \binom{n-p}{m-i}.$$

Таким образом

$$N(P_z) \geq \sum_{i=0}^{\lfloor p/2 \rfloor} \binom{p}{i} \binom{n-p}{n-m-i} + \sum_{i=\lfloor p/2 \rfloor + 1}^p \binom{p}{i} \binom{n-p}{m-i}.$$

Легко видеть, что для функции

$$M_p(x_1, \dots, x_n) = \begin{cases} 1, & \text{если } w(x_{i_1}, \dots, x_{i_p}) \geq \lfloor p/2 \rfloor + 1, \\ 0, & \text{если } w(x_{i_1}, \dots, x_{i_p}) \leq \lfloor p/2 \rfloor, \end{cases}$$

существенно зависящей только от переменных x_{i_1}, \dots, x_{i_p} , справедливо равенство

$$N(M_p) = \sum_{i=0}^{\lfloor p/2 \rfloor} \binom{p}{i} \binom{n-p}{n-m-i} + \sum_{i=\lfloor p/2 \rfloor + 1}^p \binom{p}{i} \binom{n-p}{m-i}.$$

Следовательно, для каждого $\mathbf{z} \in Z$

$$N(P_z) \geq N(M_p).$$

Множество Z разобьем на непересекающиеся подмножества Z_j такие, что

$$\mathbf{z} \in Z_j \iff P_z \text{ существенно зависит от } j \text{ переменных.}$$

Пусть j — минимальное, при котором в Z_j найдется такое \mathbf{z} , что

$$\sum_{\mathbf{x} \in E_0 \cup E_1} (P(\mathbf{x}, \mathbf{z}) \oplus M_{n,m}(\mathbf{x})) \leq \varepsilon \left(\binom{n}{m} + \binom{n}{n-m} \right).$$

В этом случае из второго утверждения леммы 5 следует, что алгоритм $A_{n,j}$ вычисляет функцию $M_{n,m}(\mathbf{x})$ с надежностью $1 - \varepsilon$. Так как $L(P') \geq j$ и $j \geq l$, то лемма доказана.

Теорема 5. Пусть $0 \leq \varepsilon \leq \frac{1}{3}$. Тогда при $n \rightarrow \infty$

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \mathcal{O} \left(\min \left(m, \left(\frac{n}{n-2m} \right)^2 \log_2 \left(\frac{n}{(n-2m)\varepsilon} \right) \right) \right),$$

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \Omega \left(\min \left(m, \left(\frac{n}{n-2m} \right)^2 \log_2 \left(\frac{1}{\varepsilon} \right) \right) \right).$$

Верхняя оценка теоремы следует из леммы 3. Нижняя оценка при условии $n - 2m = \Omega(n)$ следует из леммы 4. Для других значений разности $n - 2m$ нижняя оценка доказывается в приводимых ниже леммах 7 и 8. При доказательстве леммы 7 используются следующие известные неравенства: при любом $n \geq 1$

$$\sqrt{2\pi n} \left(\frac{n}{e} \right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n} \left(\frac{n}{e} \right)^n e^{\frac{1}{12n}};$$

при любом $x \geq 2$

$$\frac{1}{4} \leq \left(1 - \frac{1}{x} \right)^x \leq \frac{1}{2}.$$

Лемма 7. Пусть $0 \leq \varepsilon \leq \frac{1}{3}$, $2m < n < 3m$ и $l = 2l' + 1$ такое нечетное целое, что $l < \frac{1}{16} \min \left(n, \left(\frac{n}{n-2m} \right)^2 \log_2 \frac{1}{\varepsilon} \right)$. Тогда

$$\Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) \geq \frac{\varepsilon}{100}.$$

ДОКАЗАТЕЛЬСТВО. Будем полагать, что $\mathbf{x} \in E_0 \cup E_1$. Доказательство леммы для других \mathbf{x} аналогично. В силу утверждения (i) леммы 5 для любого $\mathbf{x} \in E_0 \cup E_1$ справедливо равенство

$$\Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) = \sum_{j=l'+1}^l \binom{l}{j} \binom{n-l}{m-j} / \binom{n}{m}.$$

Тогда при любом $\mathbf{x} \in E_0 \cup E_1$ имеем

$$\Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) \geq \sum_{j=l'+1}^{l'+\sqrt{l'}/8} \binom{l}{j} \binom{n-l}{m-j} / \binom{n}{m}. \quad (11)$$

Поэтому для доказательства леммы оценим величину, стоящую в правой части последнего неравенства. Сначала оценим $\binom{l}{j}$. Положим $j = l' + j'$ и $0 < j' \leq \frac{\sqrt{l'}}{8}$. Тогда

$$\begin{aligned} \binom{l}{l'+j'} / \binom{l}{l'+1} &= \frac{l' \dots (l' - j' + 2)}{(l' + j') \dots (l' + 2)} \geq \left(\frac{l' - j'}{l'} \right)^{j'} \\ &> \left(1 - \frac{j'}{l'} \right)^{\frac{j'^2}{l'}} > \left(\frac{1}{4} \right)^{1/64} > \frac{3}{4}. \end{aligned}$$

Так как $\binom{l}{l'+1} \geq \frac{2^l}{\sqrt{2l}}$ при $l \geq 7$, то при $l' < j \leq l' + \frac{\sqrt{l'}}{8}$

$$\binom{l}{j} > \frac{3}{4} \binom{l}{l'+1} \geq \frac{3}{4} \frac{2^l}{\sqrt{2l'+1}} \geq \frac{2^l}{3\sqrt{l'}}. \quad (12)$$

Далее оценим отношение $\binom{n-l}{m-j} / \binom{n}{m}$, учитывая, что $n > 2m$ и $3m > n > 16l$:

$$\begin{aligned} \binom{n-l}{m-j} / \binom{n}{m} &= \frac{(n-l)!m!(n-m)!}{n!(m-j)!(n-l-m+j)!} \\ &\geq \frac{1}{2} \sqrt{\frac{(n-l)m(n-m)}{(m-j)(n-m-l+j)n}} \frac{(n-l)^{n-l}m^m(n-m)^{n-m}}{(m-j)^{m-j}(n-m-l+j)^{n-m-l+j}n^n} \\ &\geq \frac{1}{4} \frac{(n-l)^{n-l}m^m(n-m)^{n-m}}{(m-j)^{m-j}(n-m-l+j)^{n-m-l+j}n^n} \\ &= \frac{1}{4} \left(\frac{m}{n} \right)^j \left(\frac{n-m}{n} \right)^{l-j} \left(\frac{m(n-m-l+j)}{(m-j)(n-m)} \right)^{m-j} \left(\frac{(n-m)(n-l)}{(n-m-l+j)n} \right)^{n-l}. \end{aligned} \quad (13)$$

Преобразуем второй и третий сомножители в (13). Положим $s = \sqrt{l'}$, $t = n - 2m$. Так как $l' < \frac{1}{32}(\frac{n}{t})^2 \log_2 \frac{1}{\varepsilon}$, то $(\frac{t}{n})^2 < \frac{\log_2 1/\varepsilon}{32l'}$. Поэтому при $l' \leq j \leq l' + \frac{s}{8}$ имеем

$$\begin{aligned}
 \left(\frac{m}{n}\right)^j \left(\frac{n-m}{n}\right)^{l-j} &= \left(\frac{n-t}{2n}\right)^j \left(\frac{n+t}{2n}\right)^{l-j} = \left(\frac{1}{2}\right)^l \left(1 - \frac{t}{n}\right)^j \left(1 + \frac{t}{n}\right)^{l-j} \\
 &\geq \left(\frac{1}{2}\right)^l \left(1 - \frac{t}{n}\right)^{l'+s/8} \left(1 + \frac{t}{n}\right)^{l'-s/8} \geq \left(\frac{1}{2}\right)^l \left(1 - \left(\frac{t}{n}\right)^2\right)^{l'} \left(1 - \frac{t}{n}\right)^{s/4} \\
 &\geq \left(\frac{1}{2}\right)^l \left(1 - \frac{\log_2 1/\varepsilon}{32l'}\right)^{l'} \left(1 - \sqrt{\frac{\log_2 1/\varepsilon}{32l'}}\right)^{s/4} \\
 &\geq \left(\frac{1}{2}\right)^l \left(\frac{1}{4}\right)^{\frac{1}{32} \log_2 1/\varepsilon + \frac{1}{16} \log_2 1/\varepsilon} \geq \left(\frac{1}{2}\right)^l \varepsilon^{\frac{1}{8}}.
 \end{aligned} \tag{14}$$

Далее оцениваем два последних сомножителя в (13):

$$\begin{aligned}
 &\left(\frac{m(n-m-l+j)}{(m-j)(n-m)}\right)^{m-j} \left(\frac{(n-m)(n-l)}{(n-m-l+j)n}\right)^{n-l} \\
 &= \left(\frac{mn-m^2-ml+mj}{mn-m^2+mj-jn}\right)^{m-j} \left(\frac{n^2-mn-nl+ml}{n^2-mn-nl+nj}\right)^{n-l} \\
 &= \left(1 + \frac{jn-ml}{mn-m^2+mj-jn}\right)^{m-j} \left(1 - \frac{jn-ml}{n^2-mn-nl+nj}\right)^{n-l} \\
 &\geq \left(1 + \frac{jn-ml}{m(n-m-l')}\right)^{m-j} \left(1 - \frac{jn-ml}{n(n-m-l')}\right)^{n-l}.
 \end{aligned} \tag{15}$$

Введем функцию $\varphi = \frac{jn-ml}{n-m-l'}$ и оценим ее при условии $l' + 1 \leq j \leq l' + \frac{\sqrt{l'}}{8}$. Преобразуя числитель, получаем

$$\begin{aligned}
 jn - ml &= jn - \frac{n-t}{2}l = n\left(j - \frac{l}{2}\right) + \frac{lt}{2} \leq \frac{n\sqrt{l'}}{4} + \frac{\sqrt{l}\sqrt{lt}}{2} \\
 &\leq \frac{n\sqrt{l'}}{4} + t\sqrt{l'} \frac{n\sqrt{\log_2 1/\varepsilon}}{4t} \leq \frac{n\sqrt{l'} \log_2 1/\varepsilon}{2}.
 \end{aligned}$$

Так как $t = n - 2m < \frac{n}{3}$, $\sqrt{l'} \leq l' < \frac{l}{2} < \frac{n}{32}$, то для числителя φ справедливо неравенство

$$jn - ml = \frac{n\sqrt{l'}}{4} + \frac{lt}{2} \leq \frac{n^2}{48}.$$

Следовательно,

$$\varphi \leq \frac{n\sqrt{l' \log_2 1/\varepsilon}}{2(n-m-l')} \leq \frac{16}{15} \sqrt{l' \log_2 1/\varepsilon}, \tag{16}$$

$$\varphi \leq \frac{n}{20}. \tag{17}$$

В силу (17) имеем $\left(\frac{3\varphi}{n}\right)^2 < \frac{2\varphi}{n} < \frac{1}{2}$. Далее, продолжим цепочку неравенств (15) при условии $l' + 1 \leq j \leq l' + \frac{\sqrt{l'}}{8}$:

$$\begin{aligned}
 & \left(1 + \frac{\varphi}{m}\right)^{m-j} \left(1 - \frac{\varphi}{n}\right)^{n-l} \geq \left(1 + \frac{2\varphi}{n}\right)^{m-j} \left(1 - \frac{\varphi}{n}\right)^{n-l} \\
 & \geq \left(\left(1 + \frac{2\varphi}{n}\right) \left(1 - \frac{\varphi}{n}\right)^2\right)^{(n-l)/2} \left(1 + \frac{2\varphi}{n}\right)^{(2m-2j-n+l)/2} \\
 & \geq \left(1 - \left(\frac{3\varphi}{n}\right)^2\right)^{(n-l)/2} \left(1 + \frac{2\varphi}{n}\right)^{-\sqrt{l'}/8-t/2} \\
 & \geq \left(1 - \left(\frac{3\varphi}{n}\right)^2\right)^{\left(\frac{3\varphi}{n}\right)^2 \left(\frac{n}{3\varphi}\right)^2 \frac{n-l}{2}} \left(1 + \frac{2\varphi}{n}\right)^{\frac{2\varphi}{n} \frac{n}{2\varphi} (-\sqrt{l'}/8-t/2)} \\
 & \geq \left(\frac{1}{4}\right)^{\frac{9\varphi^2}{2n}} \left(\frac{1}{4}\right)^{\frac{\varphi}{4n}(t+\sqrt{l'}/4)} = \left(\frac{1}{4}\right)^{\frac{9\varphi^2}{2n} + \frac{\varphi t}{4n} + \frac{\varphi\sqrt{l'}}{16n}}. \tag{18}
 \end{aligned}$$

Используя (16), оценим показатель экспоненты, стоящей в (18):

$$\begin{aligned}
 & \frac{9\varphi^2}{2n} + \frac{\varphi t}{4n} + \frac{\varphi\sqrt{l'}}{16n} \\
 & \leq \frac{9}{2} \left(\frac{16}{15}\right)^2 \frac{l' \log_2 1/\varepsilon}{n} + \frac{16}{15} \frac{t \sqrt{l' \log_2 1/\varepsilon}}{4n} + \frac{16}{15} \frac{l' \sqrt{\log_2 1/\varepsilon}}{16n} \\
 & \leq \frac{16}{15} \log_2 \frac{1}{\varepsilon} \left(\frac{24}{5 \cdot 32} + \frac{1}{16\sqrt{n}} + \frac{1}{16 \cdot 16}\right) < \frac{1}{4} \log_2 \frac{1}{\varepsilon}. \tag{19}
 \end{aligned}$$

Объединяя (18) и (19), при $l' + 1 \leq j \leq l' + \frac{1}{8}\sqrt{l'}$ имеем

$$\left(\frac{m(n-m-l+j)}{(m-j)(n-m)}\right)^{m-j} \left(\frac{(n-m)(n-l)}{(n-m-l+j)n}\right)^{n-l} \geq \sqrt{\varepsilon}. \tag{20}$$

Объединяя (12)–(14) и (20), при $l' + 1 \leq j \leq l' + \frac{1}{8}\sqrt{l'}$ имеем

$$\binom{l}{j} \binom{n-l}{m-j} / \binom{n}{m} \geq \frac{\varepsilon}{12\sqrt{l'}}. \tag{21}$$

Подставляя (21) в (11), получаем

$$\sum_{j=l'+1}^{l'+\lfloor \sqrt{l'}/8 \rfloor} \binom{l}{j} \binom{n-l}{m-j} / \binom{n}{n-m} \geq \frac{\varepsilon}{100}.$$

Лемма доказана.

Лемма 8. Если ε и m такие, что $0 \leq \varepsilon \leq \frac{1}{3}$, $2m < n < 3m$, то при $n \rightarrow \infty$

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \Omega \left(\min \left(m, \left(\frac{n}{n-2m} \right)^2 \log_2 \frac{1}{\varepsilon} \right) \right).$$

Доказательство. Положим $\delta = \frac{\varepsilon}{100}$. Рассмотрим случай $\delta \geq \frac{1}{2^m}$. Легко видеть, что размер области определения функции $M_{n,m}(\mathbf{x})$ больше 2^m . Следовательно, можно воспользоваться теоремой 1. Из этой теоремы следует, что

$$L(M_{n,m}(\mathbf{x}), \varepsilon) = \Omega \left(L(M_{n,m}(\mathbf{x}), \delta) \frac{\log_2 \varepsilon}{\log_2 \delta} \right) = \Omega(L(M_{n,m}(\mathbf{x}), \delta)). \quad (22)$$

Далее оцениваем снизу величину $L(M_{n,m}(\mathbf{x}), \delta)$. Если $L(M_{n,m}(\mathbf{x}), \delta) \geq m$, то утверждение леммы следует из (22). Далее полагаем, что $L(M_{n,m}(\mathbf{x}), \delta) < m$. Пусть l — такое нечетное целое, что

$$\Pr(A_{n,l}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) \leq \delta, \quad (23)$$

$$\Pr(A_{n,l-2}(\mathbf{x}) \neq M_{n,m}(\mathbf{x})) > \delta. \quad (24)$$

Из (23) и леммы 7 следует, что $l \geq \frac{1}{16} \min(n, (\frac{n}{n-2m})^2 \log_2 \frac{1}{\varepsilon})$. В то же время из (23), (24) и леммы 6 следует, что $L(M_{n,m}(\mathbf{x}), \delta) > l$. Поэтому

$$L(M_{n,m}(\mathbf{x}), \delta) > \frac{1}{16} \min \left(n, \left(\frac{n}{n-2m} \right)^2 \log_2 \frac{1}{\varepsilon} \right). \quad (25)$$

Объединяя (22) и (25), при $\delta \geq \frac{1}{2^m}$ получаем требуемое неравенство.

Утверждение леммы при $\delta < \frac{1}{2^m}$ легко следует из справедливости леммы при $\delta_0 = \frac{1}{2^m}$, равенства $\log_2 \frac{1}{\delta_0} = m$ и леммы 1. Лемма доказана.

ЛИТЕРАТУРА

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.
2. Фрейвалд Р. В. Ускорение распознавания некоторых множеств применением датчика случайных чисел // Проблемы кибернетики. М.: Наука, 1979. Вып. 36. С. 209–224.
3. Чашкин А. В. О вычислении булевых функций вероятностными программами // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 3. С. 49–68.

4. **Adleman L.** Two theorems on random polynomial time // 19th Symposium on foundations of computer science. Long Beach, Calif.: IEEE, 1978. P. 75–83.
5. **Ajtai M., Ben-Or M.** A theorem on probabilistic constant depth computations // Proc. of 16th annual ACM symposium on theory of computing. New York: ACM, 1984. P. 471–474.
6. **Stockmeyer L.** The complexity of approximate counting // Proc. of 15th annual ACM symposium on theory of computing. New York: ACM, 1983. P. 118–129.
7. **Wegener I.** The complexity of Boolean functions. Stuttgart: B. G. Teubner, 1987.

Адрес автора:

МГУ, мех.-мат. факультет,
Воробьевы горы,
119899 Москва, Россия.
E-mail: chash@online.ru

Статья поступила
22 июня 2000 г.