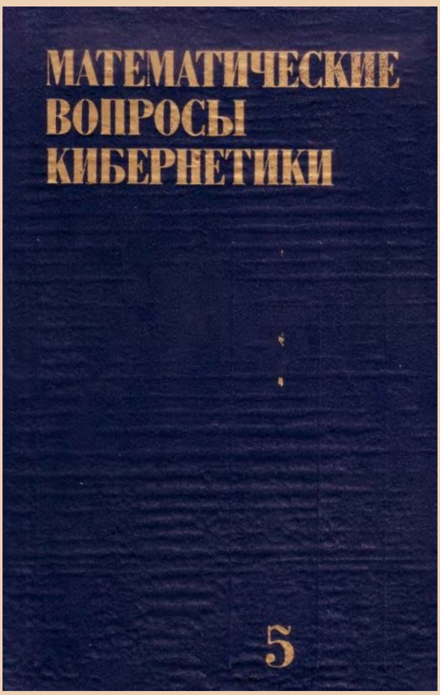

А. А. Семенов

Сложность приближенной реализации булевых функций схемами из функциональных элементов

СЛОЖНОСТЬ ПРИБЛИЖЕННОЙ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ СХЕМАМИ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

А. А. СЕМЕНОВ

(ЯКУТСК)

Введение

Задача приближенной реализации булевых функций в общем виде ставится следующим образом. Пусть для каждой булевой функции $f(x_1, \ldots, x_n)$ из множества P_2^n всех булевых функций от n переменных определена ее τ-окрестность, состоящая из некоторого подмножества множества P_2^n, содержащего саму функцию f. В этом случае будем говорить, что задана система окрестности τ. Схема S из функциональных элементов τ-приближенно реализует функцию f, если она реализует какую-либо функцию из τ-окрестности функции f. Требуется построить оптимальную по сложности схему, τ-приближенно реализующую заданную функцию f. Задача построения оптимальной схемы имеет тривиальное решение, заключающееся в переборе всех схем определенной сложности. Но он малоэффективен, так как требует для своего выполнения очень большого числа шагов.

В данной работе рассматривается асимптотический подход к задаче синтеза оптимальных схем из функциональных элементов для приближенной реализации булевых функций в случае хэмминговых систем окрестностей. Асимптотики функции Шеннона в случаях сильной, средней и слабой определенностей функций, другими словами, в случаях малой, средней и большой мощности окрестностей функций, соответственно, устанавливаются в отдельных параграфах. Среди работ, касающихся оптимальной приближенной реализации булевых функций, отметим [1, 8—10]. Основные результаты данной работы были изложены в [5, 6].

§ 1. Определения и вспомогательные результаты

Пусть B^n — множество двоичных наборов длины n. Через I_m будем обозначать множество $\{1, \ldots, m\}$. *Проекцией набора* $\tilde{a} = (a_1, \ldots, a_m)$ *из* B^m *на подмножество номеров* разрядов $I = \{i_1, \ldots, i_t\}$, $1 \leqslant i_1 < \ldots < i_t \leqslant m$ является набор $\mathrm{Pr}_I \tilde{a} = (a_{i_1}, \ldots, a_{i_t})$ длины t. *Проекцию множества наборов* $M \subseteq B^m$ *на подмножество* $I \subseteq I_m$ определим как $\mathrm{Pr}_I M = \{\mathrm{Pr}_I \tilde{a} \mid \tilde{a} \in M\}$.

Расстояние $\rho(\tilde{a}, \tilde{b})$ между наборами $\tilde{a}$ и $\tilde{b}$ из B^m равно числу разрядов, в которых наборы $\tilde{a}$ и $\tilde{b}$ отличаются. *Расстояние* $\rho_I(\tilde{a}, \tilde{b})$ *на подмножестве* $I \subseteq I_m$ определим как $\rho_I(\tilde{a}, \tilde{b}) = \rho(\mathrm{Pr}_I \tilde{a}, \mathrm{Pr}_I \tilde{b})$.

Пусть $J^1, \ldots, J^s$ — попарно непересекающиеся подмножества множества I_m. Обозначим $I = J^1 \cup \ldots \cup J^s$. Пусть $V_i \subseteq B^{|J^i|}$, $i = 1, \ldots, s$. ***Обобщенным прямым произведением пар*** $(V_1, J^1), \ldots, (V_s, J^s)$ назовем множество

$$(V_1, J^1)\times\ldots\times(V_s, J^s) = \{\mathrm{Pr}_I\tilde{a} \mid \tilde{a}\in B^m, \mathrm{Pr}_{J^i}\tilde{a}\in V_i,\ i=1,\ldots,s\}.$$

Пусть множество I_m разбито на конечное число подмножеств, $I_m = I^1\cup\ldots\cup I^k$, и каждому подмножеству I^i сопоставлено число p_i, $0\leqslant p_i\leqslant 1$, $i=1,\ldots,k$. Для множества пар $\tau=\langle(I^1, p_1), \ldots, (I^k, p_k)\rangle$ *окрестностью набора* $\tilde{a}\in B^m$ объявим множество наборов $V_\tau(\tilde{a}) = \{\tilde{b}\mid\tilde{b}\in B^m, \rho_{I^i}(\tilde{a},\tilde{b})\leqslant p_i|I^i|,\ i=1,\ldots,k\}$.

Такие системы окрестностей будем называть *хэмминговыми*. Мощности окрестностей $V_\tau(\tilde{a})$ будем обозначать $v(\tau)$. Для хэмминговой системы окрестностей τ и для произвольного подмножества $I\subseteq I_m$ введем индуцированную хэммингову систему окрестностей τ_I, определенную на множестве $B^{|I|}$. Пусть $\tau'=\langle(I\cap I^1, p_1), \ldots, (I\cap I^k, p_k), (I_m\backslash I, 0)\rangle$. *Окрестностью* $V_{\tau_I}(\tilde{\beta})$ *набора* $\tilde{\beta}\in B^{|I|}$ объявим множество $V_{\tau_I}(\tilde{\beta}) = \mathrm{Pr}_I V_{\tau'}(\tilde{b})$, где $\tilde{b}$ — произвольный набор из B^m, удовлетворяющий условию $\mathrm{Pr}_I\tilde{b}=\tilde{\beta}$.

Заметим, что хэммингова система окрестностей $\tau=\langle(I^1, p_1), \ldots, (I^k, p_k)\rangle$, заданная на B^m, обладает следующими свойствами.

1°. *Симметричность.* Из условия $\tilde{\alpha}\in V_{\tau_I}(\tilde{\beta})$ следует $\tilde{\beta}\in V_{\tau_I}(\tilde{\alpha})$ для любого $I\subseteq I_m$.

2°. Для каждого τ_I, $I\subseteq I_m$, справедливо $|V_{\tau_I}(\tilde{\alpha})| = |V_{\tau_I}(\tilde{\beta})| = v(\tau_I)$ для всех $\tilde{\alpha}, \tilde{\beta}\in B^{|I|}$.

3°. Число всех различных индуцированных хэмминговых систем окрестностей τ_I, где $I\subseteq I_m$, $|I|=l$, не превосходит k^l.

4°. Во множестве всех индуцированных хэмминговых систем окрестностей τ_I, $I\subseteq I_m$, $|I|=l$, найдется не более чем l^k индуцированных τ_I с попарно различными мощностями окрестностей.

5°. Для любого разбиения $I_m = J^1\cup\ldots\cup J^s$ и набора $\tilde{a}\in B^m$

$$\left(V_{\tau_{J^1}}(\mathrm{Pr}_{J^1}\tilde{a}), J^1\right)\times\ldots\times\left(V_{\tau_{J^s}}(\mathrm{Pr}_{J^s}\tilde{a}), J^s\right)\subseteq V_\tau(\tilde{a}).$$

Пусть $T=\{\tau^1, \tau^2, \ldots\}$ — последовательность некоторых хэмминговых систем окрестностей τ^n, заданных на B^{2^n}, $n=1,2,\ldots$ Для булевой функции $f(x_1,\ldots,x_n)$ из P_2^n через $\vec{f}$ будем обозначать набор $(f(0,\ldots,0,0), f(0,\ldots,0,1), \ldots, f(1,\ldots,1,1))$ значений функции f. Для заданного τ^n под τ^n*-окрестностью* булевой функции $f(x_1,\ldots,x_n)$ будем понимать множество булевых функций $g(x_1,\ldots,x_n)$ таких, что $\vec{g}\in V_{\tau^n}(\vec{f})$.

Возьмем произвольный конечный полный базис $\{E_1,\ldots,E_k\}$ с приведенным весом ρ [4]. Для произвольной функции $g(x_1,\ldots,x_n)$ положим $L(g)=\min L(S)$, где минимум берется по всем схемам S, реализующим g. Для функции $f(x_1,\ldots,x_n)$ и τ^n из последовательности T введем величину

$$L_{\tau^n}(f) = \min_{\vec{g}\in V_{\tau^n}(\vec{f})} L(g).$$

Функцию Шеннона $L_T(n)$ для заданной последовательности $T=\{\tau^1, \tau^2, \ldots\}$ определим следующим образом:

$$L_T(n) = \max_{f\in P_2^n} L_{\tau^n}(f).$$

Далее приведем одну лемму с полным ее доказательством и дадим формулировки известных утверждений, которые используются в данной работе. Здесь и далее под $\log$ и $\ln$ будут подразумеваться логарифмы по основаниям 2 и e соответственно.

Через $E^k_{\tilde{\alpha}}$, где $\tilde{\alpha} \in B^l$, обозначается множество наборов вида $(\tilde{\alpha}^{\sigma_1}, \ldots, \tilde{\alpha}^{\sigma_k}) \in B^{kl}$, где $\sigma_i \in \{0, 1\}$, $\tilde{\alpha}^1 = \tilde{\alpha} = (\alpha_1, \ldots, \alpha_l)$, $\tilde{\alpha}^0 = \bar{\tilde{\alpha}} = (\bar{\alpha}_1, \ldots, \bar{\alpha}_l)$.

Лемма 1. *Пусть $m = lk$ и $I^1 \cup \ldots \cup I^q \subseteq I_m$, где $I^i \cap I^j = \varnothing$ при $i \neq j$ и $|I^i| \geqslant \delta k$, $\delta > 0$, $i = 1, \ldots, q$. Тогда для любого $\varepsilon > \psi(q, \delta)$, где*

$$\psi(q, \delta) = \frac{\log \delta}{2\sqrt[4]{\delta}} + \frac{1}{\sqrt{\delta}} + q\sqrt{2c_1}\, 2^{-\frac{\log^2\delta}{16\ln 2} - \frac{1}{2}\log\log\delta},$$

и любого $\tilde{a} \in B^m$ найдется набор $\tilde{\alpha} \in B^l$ такой, что для всех наборов $\tilde{\beta} \in E^k_{\tilde{\alpha}}$ и i, $1 \leqslant i \leqslant q$,

$$\rho_{I^i}(\tilde{a}, \tilde{\beta}) < \left(\frac{1}{2} + \varepsilon\right)|I^i|.$$

Доказательство. Множество I_m разобьем на k подмножеств $I_m = J^1 \cup \ldots \cup J^k$, где $J^j = \{l(j-1)+1, l(j-1)+2, \ldots, lj\}$, $j = 1, \ldots, k$. Пусть $I^0 = I_m \setminus \{I^1 \cup \ldots \cup I^q\}$ и $I^{i,j} = I^i \cap J^j$, $i = 0, 1, \ldots, q$, $j = 1, \ldots, k$.

Для мощностей подмножеств $I^{i,j}$, I^i введем обозначения $|I^i| = l_i$, $|I^{i,j}| = l_{i,j}$, $i = 0, 1, \ldots, q$, $j = 1, \ldots, k$. Справедливы соотношения

$$\frac{1}{l_i}\sum_{j=1}^{k} l_{i,j} = 1, \quad i = 0, 1, \ldots, q, \tag{1}$$

$$\sum_{i=0}^{q} l_{i,j} = l, \quad j = 1, \ldots, k. \tag{2}$$

Для произвольного множества чисел J и числа μ через $\{J - \mu\}$ будем обозначать множества $\{j - \mu \mid j \in J\}$.

Пусть $\varphi(\delta) = \dfrac{\log\delta}{2\sqrt[4]{\delta}}$. Для наборов $\tilde{b} \in B^l$ определим k различных окрестностей $\Omega_j(\tilde{b})$, $j = 1, \ldots, k$,

$$\Omega_j(\tilde{b}) = \Big\{\tilde{c} \in B^l \,\Big|\, \text{для } i \text{ таких, что } l_{i,j} \geqslant \sqrt{\delta},\ 1 \leqslant i \leqslant q, \text{ выполнено}$$
$$\left(\frac{1}{2} - \varphi(\delta)\right) l_{i,j} \leqslant \rho_{\{I^{ij} - (j-1)l\}}(\tilde{b}, \tilde{c}) \leqslant \left(\frac{1}{2} + \varphi(\delta)\right) l_{i,j}\Big\}. \tag{3}$$

Из определения (3) следует $\Omega_j(\tilde{b}) = \Omega_j(\bar{\tilde{b}})$ и

$$|\Omega_j(\tilde{b})| = 2^{\,l_{0,j} + \sum\limits_{i: i \neq 0,\, l_{i,j} < \sqrt{\delta}} l_{i,j}} \prod_{i: i \neq 0,\, l_{i,j} \geqslant \sqrt{\delta}} \left(\sum_{\left(\frac{1}{2} - \varphi(\delta)\right) l_{i,j} \leqslant \xi \leqslant \left(\frac{1}{2} + \varphi(\delta)\right) l_{i,j}} C^{\xi}_{l_{i,j}} \right).$$

Воспользуемся соотношением, выводимым из теоремы о больших уклонениях [2],

$$\sum_{\frac{n}{2} - \sqrt{n}\log n \leqslant i \leqslant \frac{n}{2} + \sqrt{n}\log n} C^i_n \geqslant 2^n \left(1 - c_1 2^{-\frac{\log^2 n}{2\ln 2} - \log\log n}\right). \tag{4}$$

Так как $\varphi(\delta) = \log\sqrt{\delta}/\sqrt[4]{\delta}$, то для $l_{i,j} \geqslant \sqrt{\delta}$ выполнено $\varphi(\delta) l_{i,j} \geqslant \sqrt{l_{i,j}}\log l_{i,j}$ и в силу (2), (4)

$$|\Omega_j(\tilde{b})| \geqslant 2^l (1 - \sigma(\delta))^q \geqslant 2^l (1 - q\sigma(\delta)), \text{ где } \sigma(\delta) = c_1 2^{-\frac{\log^2\sqrt{\delta}}{2\ln 2} - \log\log\sqrt{\delta}}.$$

Обозначая $\Phi(q, \delta) = q\sqrt{\sigma(\delta)} = q\sqrt{2c_1}\cdot 2^{-\frac{\log^2\delta}{16\ln 2} - \frac{1}{2}\log\log\delta}$, имеем

$$|\Omega_j(\tilde{b})| \geqslant 2^l \left(1 - \frac{\Phi^2(q, \delta)}{q}\right), \quad j = 1, \ldots, k. \tag{5}$$

Введем параметры $\chi_i(\tilde{a}, \tilde{b})$, $\eta_i(\tilde{a}, \tilde{b})$, $i=1, \ldots, q$, определенные для всех пар наборов $\tilde{a} \in B^m$, $\tilde{b} \in B^l$ следующим образом:

$$\chi_i(\tilde{a}, \tilde{b}) = \frac{1}{l_i} \sum_{j=1}^{k} l_{i,j} \Delta_j(\tilde{b}, \mathrm{Pr}_{J_j} \tilde{a}), \tag{6}$$

$$\eta_i(\tilde{a}, \tilde{b}) = \frac{1}{l_i} \sum_{j=1}^{k} l_{i,j} (1 - \Delta_j(\tilde{b}, \mathrm{Pr}_{J_j} \tilde{a})), \tag{7}$$

где

$$\Delta_j(\tilde{b}, \mathrm{Pr}_{J_j}\tilde{a}) = \begin{cases} 1, & \text{если } \mathrm{Pr}_{J_j}\tilde{a} \in \Omega_j(\tilde{b}), \\ 0 & \text{в противном случае.} \end{cases}$$

Из определения (3) окрестности $\Omega_j(\tilde{b})$ и (6) параметра χ_i следует, что для любого набора $\tilde{a} \in B^m$ и номера i справедливо

$$\sum_{\tilde{b} \in B^l} \chi_i(\tilde{a}, \tilde{b}) = \frac{1}{l_i} \sum_{j=1}^{k} l_{i,j} \left| \Omega_j(\mathrm{Pr}_{J_j}\tilde{a}) \right|. \tag{8}$$

Из (1), (5) и (8) имеем $\frac{1}{2^l} \sum_{\tilde{b} \in B^l} \chi_i(\tilde{a}, \tilde{b}) \geqslant 1 - \frac{\Phi^2(q, \delta)}{q}$.

Так как $\chi_i(\tilde{a}, \tilde{b}) + \eta_i(\tilde{a}, \tilde{b}) = 1$, $i=1, \ldots, q$, то

$$\frac{1}{2^l} \sum_{\tilde{b} \in B^l} \eta_i(\tilde{a}, \tilde{b}) \leqslant \frac{\Phi^2(q, \delta)}{q}. \tag{9}$$

Из соотношения (9) можно заключить, что для каждого i, $1 \leqslant i \leqslant q$, и набора $\tilde{a} \in B^m$ найдется подмножество наборов $B_\delta(i, \tilde{a}) \subseteq B^l$ такое, что $|B_\delta(i, \tilde{a})| \geqslant 2^l \left(1 - \frac{\Phi(q, \delta)}{q}\right)$ и для всех $\tilde{b} \in B_\delta(i, \tilde{a})$ верно $\eta_i(\tilde{a}, \tilde{b}) \leqslant \Phi(q, \delta)$.

Действительно, предположив существование подмножества $B_\delta(i, \tilde{a})$ такого, что $|B_\delta(i, \tilde{a})| < 2^l \left(1 - \frac{\Phi(q, \delta)}{q}\right)$ и для всех наборов $\tilde{b}$ из $B^l \setminus B_\delta(i, \tilde{a})$ верно $\eta_i(\tilde{a}, \tilde{b}) > \Phi(q, \delta)$, получим

$$\frac{1}{2^l} \sum_{\tilde{b} \in B^l} \eta_i(\tilde{a}, \tilde{b}) = \frac{1}{2^l} \left(\sum_{\tilde{b} \in B_\delta} \eta_i + \sum_{\tilde{b} \in B^l \setminus B_\delta} \eta_i \right) >$$

$$> \frac{1}{2^l} \left(0 + 2^l \frac{\Phi(q, \delta)}{q} \Phi(q, \delta) \right) = \frac{\Phi^2(q, \delta)}{q},$$

что противоречит соотношению (9).

Возьмем $B_\delta(\tilde{a}) = B_\delta(1, \tilde{a}) \cap \ldots \cap B_\delta(q, \tilde{a})$. Ясно, что

$$|B_\delta(\tilde{a})| \geqslant 2^l - q \cdot \max_{1 \leqslant i \leqslant q} |B^l \setminus B_\delta(i, \tilde{a})| \geqslant 2^l (1 - \Phi(q, \delta))$$

и для каждого $\tilde{b} \in B_\delta(\tilde{a})$ верно

$$\eta_i(\tilde{a}, \tilde{b}) \leqslant \Phi(q, \delta), \quad i = 1, \ldots, q. \tag{10}$$

Пусть $\tilde{a} \in B^m$, $\tilde{\alpha} \in B_\delta(\tilde{a})$, $\tilde{\beta} \in E^k_{\tilde{\alpha}}$. Из определений окрестностей Ω_j, $j=1, \ldots, k$, параметров χ_i, η_i, $i=1, \ldots, q$, условия леммы $l_i \geqslant k\delta$, соотношения (10), следует

$$\rho_{I^i}(\tilde{a}, \tilde{\beta}) \leqslant \sqrt{\delta} k + l_i \eta_i(\tilde{a}, \tilde{\alpha}) + l_i \left(\frac{1}{2} + \varphi(\delta)\right) \chi_i(\tilde{a}, \tilde{\alpha}) \leqslant$$

$$\leqslant l_i \left(\frac{1}{\sqrt{\delta}} + \Phi(q, \delta) + \frac{1}{2} + \varphi(\delta) \right) \leqslant |I^i| \left(\frac{1}{2} + \psi(\delta) \right),$$

$i = 1, \ldots, q$. Лемма доказана.

Замечание. В случае, когда $l = 2^r$, утверждение леммы 1 будет верно для некоторого набора $\tilde{\alpha} \in B^{2^r}$, являющегося набором значений линейной функции от r переменных, и для функции $\psi(q, \delta) = \frac{1}{\sqrt{\delta}} + \frac{1}{\sqrt[6]{\delta}} + \frac{q}{2\sqrt[12]{\delta}}$.

Дадим некоторые пояснения. Пусть $\mathscr{L}_r$ — множество линейных функций от r переменных. Параметры $\chi_i(\tilde{a}, \vec{g})$, $\eta_i(\tilde{a}, \vec{g})$, где $g \in \mathscr{L}_r$ определяются для окрестности $O_j(\tilde{b}) = \{\vec{g} \mid g \in \mathscr{L}_r\} \cap \Omega_j(\tilde{b})$ при $\varphi(\delta) = \frac{1}{\sqrt[6]{\delta}}$. Тогда

$$\frac{1}{2^{r+1}} \sum_{g \in \mathscr{L}_r} \chi_i(\tilde{a}, \vec{g}) \geqslant 1 - \frac{\Phi^2(q, \delta)}{q}, \quad \text{где} \quad \Phi(q, \delta) = \frac{q}{2\sqrt[12]{\delta}},$$

и аналогичные, тем, что и в лемме 1, рассуждения приведут к доказательству данного замечания.

Лемма 2 [2, лемма 9]. *Пусть A — произвольное конечное множество и $D = \{K_1, \ldots, K_l\}$ — такая совокупность его подмножеств, что каждый элемент $\alpha \in A$ принадлежит не менее чем γl подмножествам из D. Тогда существует покрытие множества A подмножествами из D, содержащее не более $\frac{1}{\gamma}(\ln(\gamma|A|) + 1) + 1$ подмножеств.*

Лемма 3 [8, лемма 3]. *Пусть заданы N произвольных наборов $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_N$ из B^n и число r. Тогда найдется такой $(r, n-r)$-оператор $F(x_1, \ldots, x_r) = (f_1(x_1, \ldots, x_r), \ldots, f_{n-r}(x_1, \ldots, x_r))$, что среди наборов $\varphi_F(\tilde{\sigma}_i) = \varphi_F(\sigma_{i,1}, \ldots, \sigma_{i,n}) = (\alpha_{i,1}, \ldots, \alpha_{i,n-r})$, где $\alpha_{i,j} = \sigma_{i,r+j} \oplus f_j(\sigma_{i,1}, \ldots, \sigma_{i,r})$, $j = 1, \ldots, n-r$, $i = 1, \ldots, N$, будет не менее $N - \frac{N^2}{2^{n-r}}$ различных.*

§ 2. Случай сильной определенности реализуемой функции

Пусть последовательность $T = \{\tau^1, \tau^2, \ldots\}$ хэмминговых систем окрестностей $\tau^n = \langle (J^{1,n}, p_{1,n}), \ldots, (J^{k,n}, p_{k,n}) \rangle$, заданных на B^{2^n} и определяющих окрестности функций из P_2^n, удовлетворяют условию

$$\log(2^n - \log v(\tau^n)) \sim n. \tag{11}$$

Будем считать, что условие (11) означает сильную определенность функций и малую мощность хэмминговых окрестностей. Предполагаем k фиксированным числом.

Теорема 1. *Если последовательность $T = \{\tau^1, \tau^2, \ldots\}$, $\tau^n = \langle (J^{1,n}, p_{1,n}), \ldots, (J^{k,n}, p_{k,n}) \rangle$ удовлетворяет условию (11) и $\max_{i,n : p_{i,n} < 1/2} p_{i,n} \leqslant \frac{1}{2} - \varepsilon$, $\varepsilon > 0$, тогда*

$$L_T(n) \sim \rho \frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

Доказательство. Нижняя оценка. Введем множество функций

$$G_{\tau^n} = \left\{ g \in P_2^n \;\middle|\; \exists f \in P_2^n\colon L(g) = \min_{\vec{g}' \in V_{\tau^n}(\vec{f})} L(g'), \vec{g} \in V_{\tau^n}(\vec{f}) \right\}.$$

Из определений функции Шеннона $L_T(n)$ множества G_{τ^n} и свойств 1°, 2° (§ 1) следует, что $L_T(n) = \max_{g \in G_{\tau^n}} L(g)$ и

$$|G_{\tau^n}| \geqslant \frac{2^{2^n}}{v(\tau^n)}. \qquad (12)$$

Условие теоремы 1.1 [4] $\frac{(n+1)\log\log|G_{\tau^n}|}{\log|G_{\tau^n}|} \to 0$ выполняется в силу (11), (12), следовательно,

$$L_T(n) \geqslant \rho \frac{\log|G_{\tau^n}|}{\log\log|G_{\tau^n}|} \geqslant \rho \frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

Верхняя оценка. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция от n переменных, $\tau = \tau^n = \langle (J^1, p_1), \ldots, (J^k, p_k) \rangle$ — хэммингова система окрестностей из T. Параметр $\lambda = \lambda(n)$ удовлетворяет условию

$$\lambda(n) \to \infty \quad \text{при} \quad n \to \infty. \qquad (13)$$

Функцию f представим в виде таблицы D размера $2^\lambda \times 2^{n-\lambda}$, где 2^λ строкам соответствуют наборы $(\sigma_{n-\lambda+1}, \ldots, \sigma_n)$, а столбцам — наборы $(\sigma_1, \ldots, \sigma_{n-\lambda})$. На пересечении строки $(\sigma_{n-\lambda+1}, \ldots, \sigma_n)$ и столбца $(\sigma_1, \ldots, \sigma_{n-1})$ стоит значение $f(\sigma_1, \ldots, \sigma_n)$. Обозначим столбцы этой таблицы в порядке расположения слева направо через $D_1, D_2, \ldots, D_{2^{n-\lambda}}$, $D_i \in B^{2^\lambda}$. Каждому столбцу D_i соответствует множество $I^i = \{2^\lambda(i-1)+1, 2^\lambda(i-1)+2, \ldots, 2^\lambda i\}$ такое, что $D_i = \mathrm{Pr}_{I^i}\vec{f}$, $i = 1, \ldots, 2^{n-\lambda}$.

Для $\tau = \tau^n$ из T введем функционал $\varphi_\tau(I) = |I| - \log v(\tau_I)$, определенный на множестве всех подмножеств $I \subseteq I_{2^n}$.

Введем параметр $M = M(n)$, удовлетворяющий условиям

$$M \sim n, \qquad (14)$$

$$\lambda \sim o(M). \qquad (15)$$

Разделим каждый столбец D_i таблицы на такие куски $D_{i,1}, \ldots, D_{i,m_i}$, что $D_i = (D_{i,1}, \ldots, D_{i,m_i})$, $D_{i,1} = \mathrm{Pr}_{I^{i,1}}\vec{f}, \ldots, D_{i,m_i} = \mathrm{Pr}_{I^{i,m_i}}\vec{f}$ и

$$M - 1 \leqslant \varphi_\tau(I^{i,j}) \leqslant M, \quad j = 1, \ldots, m_i - 1, \qquad (16)$$

$$\varphi_\tau(I^{i,m_i}) < M - 1. \qquad (17)$$

Множество кусков $D_{i,j}$ таблицы, за исключением кусков D_{i,m_i}, $i = 1, \ldots, 2^{n-\lambda}$, разобьем на группы, отнеся в одну группу куски, имеющие одинаковую длину и одинаковую мощность окрестности. Полученные группы обозначим $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$. Аналогичным образом на группы разобьем куски D_{i,m_i}, $i = 1, \ldots, 2^{n-\lambda}$. Группы обозначим $\mathfrak{A}_{r+1}, \ldots, \mathfrak{A}_\mu$. Так как длины кусков не превышают 2^λ, то из выполнения свойства 4° для τ следует, что число различных групп μ не превышает $2^\lambda(2^\lambda)^k$, т. е.

$$\mu \leqslant 2^{\lambda(k+1)}. \qquad (18)$$

Пусть ν_i — длина кусков группы $\mathfrak{A}_i$, v_i — мощность окрестностей кусков из $\mathfrak{A}_i$, l_i — число кусков группы $\mathfrak{A}_i$, $i = 1, \ldots, \mu$.

Из свойства 5° для τ следует

$$\prod_{i=1}^{2^{n-\lambda}} \prod_{j=1}^{m_i} \left(V_{\tau_{I^{i,j}}}(D_{i,j}), I^{i,j}\right) \subseteq V_\tau(\vec{f}). \qquad (19)$$

Т. е. при замене кусков $D_{i,j}$ на наборы из своих окрестностей получается таблица, соответствующая некоторой функции $g \in P_2^n$ такой, что $\vec{g} \in V_\tau(\vec{f})$. В каждой группе $\mathfrak{A}_i$ куски заменим на наборы из их окрестностей так, чтобы число попарно различных наборов было, по возможности, минимальным. Такую замену найдем с помощью алгоритма градиентного покрытия (лемма 2). Считаем, что набор $\tilde{a} \in B^{\nu_i}$ покрывает кусок $D_{\xi,\eta} \in \mathfrak{A}_i$, если $\tilde{a} \in V_{\tau_{I\xi,\eta}}(D_{\xi,\eta})$. Тогда $\gamma = v_i/2^{\nu_i}$. Два куска $D_{\xi,\eta}$ и $D_{s,t}$ назовем идентичными, если $D_{\xi,\eta} = D_{s,t}$ и $\tau_{I\xi,n} = \tau_{Is,t}$. Из свойства 3° (§ 1) следует, что число попарно неидентичных кусков группы $\mathfrak{A}_i$ не превосходит $2^{\nu_i} k^{\nu_i}$. Следовательно, градиентный алгоритм позволяет покрыть группу $\mathfrak{A}_i$ не более чем

$$\frac{2^{\nu_i}}{v_i}\left(\ln\left(\frac{v_i}{2^{\nu_i}}(2k)^{\nu_i}\right)+1\right)+1 \tag{20}$$

наборами из B^{ν_i}, $i = 1, \ldots, \mu$.

Согласно алгоритму все куски $D_{i,j}$ таблицы D заменим на наборы $G_{i,j}$ из их окрестностей. Получим новую таблицу G, соответствующую некоторой функции $g(x_1, \ldots, x_n)$, $\vec{g} \in V_\tau(\vec{f})$.

Учитывая (16), (17) и (18), оценим число попарно различных кусков $G_{i,j}$ таблицы G

$$\sum_{i=1}^{\mu}\left(\frac{2^{\nu_i}}{v_i}\left(\ln\left(\frac{v_i}{2^{\nu_i}}(2k)^{\nu_i}\right)+1\right)+1\right) \leqslant 2^{M+\lambda(k+2)+c_2},$$

где $c_2 = 2 + \log\ln(ek)$.

Произвольным образом занумеруем все различные куски $G_{i,j}$ таблицы G двоичными наборами $\tilde{\varkappa}(G_{i,j})$ длины $\delta =]M + \lambda(k+2) + c_2[$. *Кодом столбца* G_i назовем набор

$$\tilde{\varkappa}(G_i) = (\tilde{\varkappa}(G_{i,1}), \ldots, \tilde{\varkappa}(G_{i,m_i})),$$

а *кодом функции* g длины h —

$$\tilde{\varkappa}(g) = (\tilde{\varkappa}(G_1), \ldots, \tilde{\varkappa}(G_{2^n-\lambda})).$$

Справедливы следующие соотношения:

$$h \leqslant \delta \sum_{i=1}^{\mu} l_i, \tag{21}$$

$$M - 1 \leqslant \nu_i - \log v_i \leqslant M, \quad i = 1, \ldots, r. \tag{22}$$

Из (19) следует

$$\prod_{i=1}^{\mu} v_i^{l_i} \leqslant v(\tau). \tag{23}$$

Для некоторого ε_1, $0 < \varepsilon_1 < 1$, верно

$$\sum_{i=1}^{\mu} l_i \log v_i = (1 - \varepsilon_1)\log v(\tau),$$

а также при соответствующем выборе параметров λ и M

$$\varepsilon_1 = \varepsilon_1(n) = o\left(\frac{2^n - \log v(\tau^n)}{\log v(\tau^n)}\right). \tag{24}$$

В силу (22) и $\log v_i \leqslant \nu_i$, $i = r+1, \ldots, \mu$,

$$(1-\varepsilon_1)\log v(\tau) =$$

$$= \sum_{i=1}^{r} l_i \log v_i + \sum_{i=r+1}^{\mu} l_i \log v_i \leqslant \sum_{i=1}^{r} l_i(\nu_i - M + 1) + \sum_{i=r+1}^{\mu} l_i \nu_i =$$

$$= \sum_{i=1}^{\mu} l_i \nu_i - (M-1)\sum_{i=1}^{r} l_i = 2^n - (M-1)\sum_{i=1}^{r} l_i,$$

откуда, учитывая (24), имеем

$$\sum_{i=1}^{r} l_i \leqslant \frac{2^n - (1-\varepsilon_1)\log v(\tau)}{M-1} \lesssim \frac{2^n - \log v(\tau)}{M}. \tag{25}$$

Следовательно, для длины h, учитывая (15), (21), (25), получаем

$$h \leqslant \left(\sum_{i=1}^{r} l_i + 2^{n-\lambda}\right) \cdot]M + \lambda(k+2) + c_2[\lesssim 2^n - \log v(\tau) + M \cdot 2^{n-\lambda}. \tag{26}$$

Обозначим через Q максимум длин наборов $\tilde{\varkappa}(G_i)$, $i = 1, \ldots, 2^{n-\lambda}$. В каждом столбце G_i содержится не более чем $W = \left] \frac{2^\lambda}{\min(\nu_1, \ldots, \nu_r)} \right[+ 1$ кусков, поэтому $Q \leqslant W\delta$. Из определения групп $\mathfrak{A}_1, \ldots, \mathfrak{A}_r$ следует $M - 1 \leqslant \nu_i - \log v_i \leqslant M$, $i = 1, \ldots, r$, а $M \sim n$. Тогда

$$Q \lesssim \frac{2^\lambda}{n}\delta. \tag{27}$$

Опишем схему для реализации функции $g(x_1, \ldots, x_n)$ (рис. 1). Схема строится в соответствии с принципом неравномерного кодирования [4]. Пусть $\tilde{\sigma}' = (\sigma_1, \ldots, \sigma_{n-\lambda})$, $\tilde{\sigma}'' = (\sigma_{n-\lambda+1}, \ldots, \sigma_n)$.

A_1: $(n-\lambda,\ ]\log h[)$-оператор, по набору $\tilde{\sigma}'$ вычисляющий номер начального разряда куска кода $\tilde{\varkappa}(G_i)$ в коде $\tilde{\varkappa}(g)$ функции g. По теореме Д.4 из [4]

$$L(A_1) \lesssim \frac{2^{n-\lambda}}{n-\lambda}\log h.$$

A_2: $(n-\lambda,\ ]\log Q[)$-оператор по набору $\tilde{\sigma}'$ вычисляющий длину набора $\tilde{\varkappa}(G_i)$

$$L(A_2) \lesssim \frac{2^{n-\lambda}}{n-\lambda}\log Q.$$

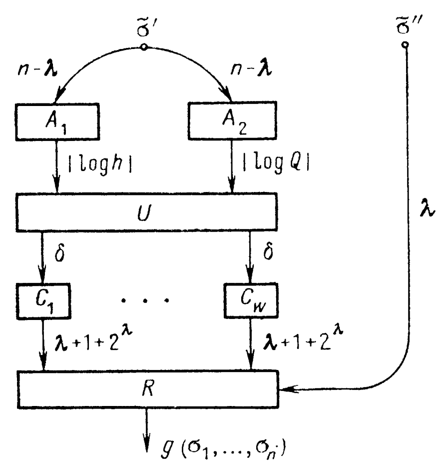

Рис. 1

U: $(]\log h[+]\log Q[,\ W\delta)$-оператор. По номеру начального разряда и длине кода $\tilde{\varkappa}(G_i)$ выдает набор $\left(\tilde{\varkappa}(G_{i,1}), \ldots, \tilde{\varkappa}(G_{i,m_i}), 0, \ldots, 0\right)$.

C_j: $(\delta,\ \lambda + 1 + 2^\lambda)$-оператор. По набору $\tilde{\varkappa}(G_{i,j})$ выдает в крайних слева выходах набор длины $\lambda + 1$, являющийся двоичной записью длины набора $G_{i,j}$, а по следующим выходам выдает набор $(G_{i,j}, 0, \ldots, 0) \in B^{2^\lambda}$,

$$L(C_j) \lesssim (\lambda + 1 + 2^\lambda)\frac{2^\delta}{\delta}, \quad j = 1, \ldots, m_i.$$

Блоки C_j, $j = m_i + 1, \ldots, W$, выдают $(0, \ldots, 0) \in B^{\lambda+1+2^\lambda}$.

R: $((\lambda+1+2^\lambda)W+\lambda,\ 1)$-оператор. По набору $\tilde{\sigma}''$ и выходам блоков $C_1, \ldots, C_W$ выдает $(\|\sigma''\|+1)$-й разряд набора $\left(G_{i,1}, \ldots, G_{i,m_i}\right)=G_i$, т. е. выдает $g(\sigma_1, \ldots, \sigma_n)$. Схема R строится с использованием леммы 2.2 из [4];

$$L(R)\leqslant 2^\lambda W.$$

Выберем параметры $\lambda=\lambda(n)$ и $M=M(n)$ следующим образом. Пусть $\psi(n)=\dfrac{2^n}{2^n-\log v(\tau^n)}$, тогда

$$\lambda=]2\log(\psi(n)n)[,\quad M=n-]\lambda(k+4)+c_2[.$$

По условию теоремы $\log(2^n-\log v(\tau^n))\sim n$, поэтому $\log\psi(n)=\bar{o}(n)$ и параметры λ и M удовлетворяют условиям (14), (15).

Из оценки (12) следует нижняя оценка для длины кода

$$h\geqslant\log\frac{2^{2^n}}{v(\tau^n)}=2^n-\log v(\tau^n). \tag{28}$$

Условия теоремы 2.3 из [4] будут выполнены, если

1) $h\sim 2^n-\log v(\tau^n)$,

2) $\dfrac{Q\log^2 h}{h}\to 0$,

3) $L(A_1)+L(A_2)+L(R)+\sum\limits_{j=1}^{W}L(C_j)=o\left(\dfrac{h}{\log h}\right)$.

Из (26), (27), (28) и выше определенных параметров λ и M следует, что условия 1), 2) и 3) выполнены и по теореме 2.3 [4]

$$L(g)\leqslant\rho\frac{2^n-\log v(\tau^n)}{\log(2^n-\log v(\tau^n))}.$$

Так как $\vec{g}\in V_{\tau^n}(\vec{f})$, то $L_{\tau^n}(f)\leqslant L(g)$ и в силу произвольности функции f

$$L_T(n)\leqslant\rho\frac{2^n-\log v(\tau^n)}{\log(2^n-\log v(\tau^n))}.$$

Теорема доказана

§ 3. Случай средней определенности реализуемой функции

Под случаем средней определенности функций из P_2^n или случаем средней мощности хэмминговых окрестностей будем понимать тот случай, когда для τ^n выполняется

$$2^{n-\log^2 n}\geqslant 2^n-\log v(\tau^n)\geqslant\frac{1}{n}2^{n/2}. \tag{29}$$

Теорема 2. *Пусть для последовательности* $T=\{\tau^1, \tau^2, \ldots\}$ *хэмминговых систем окрестностей* $\tau^n=\langle(I^{1,n}, p_{1,n}), \ldots, (I^{k,n}, p_{k,n})\rangle$, *заданных на* B^{2^n}, *выполняется* (29) *и* $\left|p_{i,n}-\frac{1}{2}\right|>\varepsilon$, $\varepsilon>0$, $i=1, \ldots, k$, $n=1, 2, \ldots$ *Тогда*

$$L_T(n)\sim\rho\frac{2^n-\log v(\tau^n)}{\log(2^n-\log v(\tau^n))}.$$

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция и $\tau=\tau^n$. Без ограничения общности будем считать, что $p_{i,n}<1/2$, $i=1, \ldots, q$, $p_{j,n}>1/2$, $j=q+1, \ldots, k$, $q=q(n)$.

Сначала получим некоторые вспомогательные соотношения.

Известно следующее соотношение [2, приложение]:

$$2^{nH(p)-\log n} \leqslant \sum_{i=0}^{pn} C_n^i \leqslant 2^{nH(p)}, \tag{30}$$

где $0 \leqslant p < 1/2$, $H(p) = -p \log p - (1-p)\log(1-p)$.

Мощность $v(\tau)$ окрестности любого набора из B^{2^n} при заданной системе окрестностей τ равна

$$v(\tau) = \prod_{i=1}^{k} \sum_{j=1}^{p_i|I^{i,n}|} C^j_{|I^{i,n}|}.$$

Учитывая, что $\sum\limits_{i=1}^{k} |I^{i,n}| = 2^n$, и (30), оценим выражение $2^n - \log v(\tau)$:

$$\sum_{i=1}^{q} \left[|I^{i,n}|(1 - H(p_i)) + \log |I^{i,n}| \right] + (k-q) \geqslant$$

$$\geqslant 2^n - \log v(\tau) \geqslant \sum_{i=1}^{q} |I^{i,n}|(1 - H(p_i)). \tag{31}$$

Откуда следует

$$2^n - \log v(\tau^n) \sim \sum_{i=1}^{q} |I^{i,n}|(1 - H(p_i)).$$

Пусть для произвольных подмножеств $I_0^{i,n} \subseteq I^{i,n}$, $i = 1, \ldots, q$, может быть пустых, выполнено

$$|I_0^{1,n} \cup \ldots \cup I_0^{q,n}| \sim |I^{1,n} \cup \ldots \cup I^{q,n}|. \tag{32}$$

Обозначим $I^0 = I_0^{1,n} \cup \ldots \cup I_0^{q,n}$, $I = I^{1,n} \cup \ldots \cup I^{q,n}$. Из (30), (32) и аналогичных (31) неравенств следует

$$2^n - \log v(\tau) \sim |I| - \log v(\tau_I) \sim |I^0| - \log v(\tau_{I^0}). \tag{33}$$

Подмножества $I, I^{q+1,n}, \ldots, I^{k,n}$ множества $I_{2^n} = \{1, 2, \ldots, 2^n\}$ будем разбивать на два класса следующим образом.

Введем обозначения $2^n - \log v(\tau) = M(n)$, $|I| = l_0(n)$, $|I^{q+1,n}| = l_1(n), \ldots, |I^{k,n}| = l_{k-q}(n)$.

Без ограничения общности положим $l_1(n) \leqslant \ldots \leqslant l_{k-q}(n)$.

Обозначим $a_i(n) = \dfrac{\log l_i(n) - \log M(n)}{\log n}$, $i = 1, \ldots, k-q$, тогда $l_i(n) = n^{a_i(n)} M(n)$ и $a_1(n) \leqslant \ldots \leqslant a_{k-q}(n)$.

Если $a_1(n) \geqslant 4$, то образуем два класса $G_1 = \{I\}$ и $G_2 = \{I^{q+1,n} \cup \ldots \cup I^{k,n}\}$. Если же $a_1(n) < 4$, то найдем номер p такой, что $a_{p+1} \geqslant 2a_p + 4$. В силу конечности числа k такой номер найдется. Образуем классы $G_1 = \{I \cup I^{q+1,n} \cup \ldots \cup I^{q+p,n}\}$ и $G_2 = \{I^{q+p+1,n} \cup \ldots \cup I^{k,n}\}$. Обозначим $|G_1| = N$. Тогда $|G_2| = 2^n - N$.

Из (31) следует оценка для $|I|$

$$|I| \leqslant c_3 M(n), \text{ где } 1/c_3 = \min_{1 \leqslant i \leqslant q} (1 - H(p_i)).$$

Для $|I^{q+i,n}| = l_i(n)$ имеем оценки $|I^{q+i,n}| \leqslant n^{a_p(n)} M(n)$, $i = 1, \ldots, p$. Тогда

$$N \leqslant (c_3 + kn^t) M(n), \quad |I^{i,n}| \geqslant n^{2t+4} M(n), \quad i = q+p+1, \ldots, k, \tag{34}$$

где, если $a_1(n) \geqslant 4$, то $p = 0$, $t = 0$, а если $a_1(n) < 4$, то $t = a_p(n)$.

Пусть $r = n - \log M(n) - (2t+3)\log n$, тогда

$$n - r \sim \log M(n), \tag{35}$$

$$2^{n-r} = 2^{2t+3} M(n), \tag{36}$$

$$|I^{i,n}| \geqslant n \cdot 2^{n-r}, \quad i = q+p+1, \ldots, k. \tag{37}$$

В таблице T значений функции $f(x_1, \ldots, x_n)$ наборы $(0, \ldots, 0), \ldots \ldots, (1, \ldots, 1)$ пронумеруем номерами $1, \ldots, 2^n$ соответственно. Выделим в таблице T наборы $D = \{\tilde\sigma_1, \ldots, \tilde\sigma_N\} \subseteq B^n$ с номерами из G_1. К наборам из D при выбранном r применим лемму 3. Отображение $\varphi_F\colon B^n \to B^{n-r}$ является сюръективным, и каждый набор из B^{n-r} имеет ровно 2^r прообразов.

В таблице T строка состоит из набора и значения функции f на этом наборе, т. е. имеет вид $(\tilde\sigma, f(\tilde\sigma))$. Таблицу T разрежем на полосы по 2^{n-r} строк и заметим, что отображение φ_F отображает множество наборов каждой полосы биективно в множество B^{n-r}.

Таблицу T преобразуем в таблицу T' такого же размера, состоящую из 2^{n-r} полос по 2^r строк по следующему правилу. Сначала в 1-й, 2-й, …, 2^r-й полосах таблицы T найдем те строки $(\tilde\sigma, f(\tilde\sigma))$, для которых выполнено $\varphi_F(\tilde\sigma) = (0, \ldots, 0)$. Эти 2^r строк образуют первую полосу новой таблицы T', причем порядок следования строк такой же, как и в таблице T. Аналогично поступим со строками $(\tilde\sigma, f(\tilde\sigma))$ такими, что $\varphi_F(\sigma) = (0, \ldots, 0, 1)$. Они составят вторую полосу таблицы T'. Аналогичным образом составим 3-ю, …, 2^{n-r}-ю полосы таблицы T'.

В результате проделанной процедуры 1-я, 2-я, …, 2^n-я строки таблицы T становятся i_1-й, i_2-й, …, i_{2^n}-й строками таблицы T'. Данную перестановку обозначим $\Pi = \begin{pmatrix} 1 & 2 & \ldots & 2^n \\ i_1 & i_2 & \ldots & i_{2^n} \end{pmatrix}$. Операцию перестановки Π будем применять как к подмножествам $I \subseteq I_{2^n}$, так и к подмножествам наборов $A \subseteq B^{2^n}$ следующим образом:

$$\Pi(1) = i_1, \ldots, \Pi(2^n) = i_{2^n},$$

$$\Pi(I) = \{\Pi(i) \mid i \in I\},$$

$$\Pi(\tilde a) = \Pi(a_1, \ldots, a_{2^n}) = (a_{\Pi(1)}, \ldots, a_{\Pi(2^n)}),$$

$$\Pi(A) = \{\Pi(\tilde a) \mid \tilde a \in A\}, \quad A \subseteq B^{2^n},$$

$$\Pi(\tilde a) = \tilde b \Leftrightarrow \tilde a = \Pi^{-1}(\tilde b), \text{ где } \Pi^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots & i_{2^n} \\ 1 & 2 & \ldots & 2^n \end{pmatrix}.$$

Обозначим $\Pi(I^{i,n}) = J^{i,n}$, $i = 1, \ldots, k$, $\Pi(G_1) = G_1' = \{J^{1,n} \cup \ldots \cup J^{q+p,n}\}$, $\Pi(G_2) = G_2' = \{J^{q+p+1,n} \cup \ldots \cup J^{k,n}\}$, $\Pi(\vec f) = \vec f'$. Введем новую хэммингову систему окрестностей $\tau' = \langle (J^{1,n}, p_1), \ldots, (J^{k,n}, p_k) \rangle$. Тогда

$$V_{\tau'}(\tilde b) = \Pi(V_\tau(\Pi^{-1}(\tilde b))) \text{ для любого } \tilde b \in B^{2^n}.$$

Согласно лемме 3 перестановка Π обладает тем свойством, что не менее чем $N - \dfrac{N^2}{2^{n-r}}$ полос таблицы T' содержат строки с наборами из $D = \{\tilde\sigma_1, \ldots, \tilde\sigma_N\}$.

В тех полосах таблицы T', которые содержат набор из D, отметим один из наборов D. Пусть $J' \subseteq G_1'$ — множество номеров отмеченных наборов. Из леммы 3 следует

$$|J'| \geqslant N - \frac{N^2}{2^{n-r}}. \tag{38}$$

Из леммы 1, примененной к множествам $J^{q+p+1,n}, \ldots, J^{k,n}$, где $|J^{i,n}| \geqslant n2^{n-r}$, $i = q+p+1, \ldots, k$ (37), при $m = 2^n$, $l = 2^r$ следует, что для любого $\varepsilon_1 \geqslant \psi(k-q-p, n)$ найдется набор $\tilde{\alpha} \in B^{2^r}$ такой, что для произвольного $\tilde{c} \in E_{\tilde{\alpha}}^{2^{n-r}}$ верно

$$\rho_{J^{i,n}}(\vec{f'}, \tilde{c}) \leqslant \left(\frac{1}{2} + \varepsilon_1\right)|J^{i,n}|, \quad i = q+p+1, \ldots, k. \tag{39}$$

Так как $\psi \to 0$ при $n \to \infty$, то для ε (из условия теоремы) найдется n_0: $\psi(q+p+1, n) \leqslant \varepsilon$ для всех $n \geqslant n_0$, и соотношение (39) верно для $\varepsilon_1 = \varepsilon$.

Полосы таблицы T' пронумеруем от 1 до 2^{n-r}. Пусть I^1 — номера полос, содержащих наборы с номерами из $J' \cap (J^{1,n} \cup \ldots \cup J^{q,n})$, $I^1 \subseteq I_{2^{n-r}} = \{1, 2, \ldots, 2^{n-r}\}$, I^2 — номера полос, содержащих наборы с номерами из $J' \setminus (J^{1,n} \cup \ldots \cup J^{q,n})$, $I^3 = I_{2^{n-r}} \setminus (I^1 \cup I^2)$.

Полосам таблицы T' сопоставим 0 или 1 по следующему правилу. Полосам с номерами из I^3 сопоставим произвольным образом 0 или 1. Все остальные полосы содержат наборы с номерами из J', т. е. отмеченные наборы. Если в полосе заменим кусок столбца f' на набор $\tilde{\alpha}$ (из леммы 1) и если при этом строка с отмеченным набором остается неизменной, то этой полосе сопоставим 0. В противном случае сопоставим 1. Сопоставленные числа запишем в порядке следования полос. Полученный набор длины 2^{n-r} обозначим g. Набору $\vec{g}$ соответствует некоторая булева функция $g(x_1, \ldots, x_{n-r})$.

На множестве $B^{2^{n-r}}$ введем хэммингову систему окрестностей τ'' следующим образом. Обозначим

$$J_0^{i,n} = J' \cap J^{i,n}, \quad i = 1, \ldots, q+p. \tag{40}$$

Через I_i^1 обозначим номера полос таблицы T', содержащих наборы с номерами из $J_0^{i,n}$, $i = 1, \ldots, q$, а I_j^2 — номера полос, содержащих наборы с номерами $J_0^{j,n}$, $j = q+1, \ldots, q+p$.

Теперь определим

$$\tau'' = \langle (I_1^1, p_1), \ldots, (I_q^1, p_q), (I_{q+1}^2, p_{q+1}), \ldots, (I_{q+p}^2, p_{q+p}), (I^3, 1) \rangle.$$

Из определений τ' и τ'' следует, что для $J_0 = J_0^{1,n} \cup \ldots \cup J_0^{q,n}$ и I^1 индуцированные τ'_{J_0} и τ''_{I^1} равны.

Сравним мощности J_0 и $J = J^{1,n} \cup \ldots \cup J^{q,n}$. Так как $J_0 = J' \cap J$ (40), $J \subseteq G_1'$, $J' \subseteq G_1'$, $|G_1'| = N$, то учитывая (34), (36), (38) имеем

$$|J| \geqslant |J_0| \geqslant |J| - \frac{N^2}{2^{n-r}} \geqslant |J| - M(n)\left(\frac{c_3^2}{n^{2t+3}} + \frac{2kc_3}{n^{t+3}} + \frac{k^2}{n^3}\right).$$

Так как из (31) следует $M(n) \leqslant |J| + q\log|J| + (k-q)$, то

$$|J_0| \sim |J|,$$

т. е. выполнено условие (32), поэтому в силу (33)

$$|J_0| - \log v(\tau'_{J_0}) \sim 2^n - \log v(\tau^n).$$

А имея в виду, что $|J_0| = |I^1|$ и $v\left(\tau'_{J_0}\right) = v\left(\tau''_{I^1}\right)$, получаем

$$|I^1| - \log v\left(\tau''_{I^1}\right) \sim 2^n - \log v\left(\tau^n\right).$$

Для τ'' справедливо $v(\tau'') = v\left(\tau''_{I^1}\right) v\left(\tau''_{I^2}\right) v\left(\tau''_{I^3}\right)$, значит,

$$2^{n-r} - \log v(\tau'') \sim 2^{n-r} - |I^2| - |I^3| - \log v\left(\tau''_{I^1}\right) = |I^1| - \\ - \log v\left(\tau''_{I^1}\right) \sim 2^n - \log v\left(\tau^n\right) = M(n). \quad (41)$$

Возьмем набор $\tilde{\alpha} \in B^{2^r}$, для которого верно (39), и набор $\vec{g'}$ из окрестности $V_{\tau''}(\vec{g})$ набора $\vec{g}$. Одновременной подстановкой в наборе $\vec{g'}$: вместо 0 — набор $\tilde{\alpha}$, а вместо 1 — набор $\tilde{\tilde{\alpha}}$ — получим набор $\tilde{c} \in E^{2^{n-r}}_{2\tilde{\alpha}}$. Если $n \geqslant n_0$, то из (39) следует

$$\rho_{I^{i,n}}\left(\vec{f}, \Pi^{-1}(\tilde{c})\right) = \rho_{J^{i,n}}\left(\vec{f'}, \tilde{c}\right) \leqslant p_i \left|J^{i,n}\right|, \quad i = q + p + 1, \ldots, k.$$

Обозначим $H = G'_1 \setminus J'$ и $\overline{H} = I_{2^n} \setminus H$. Из описанной выше конструкции следует $\mathrm{Pr}_{\overline{H}} \tilde{c} \in V_{\tau'_{\overline{H}}}\left(\mathrm{Pr}_{\overline{H}} \vec{f'}\right)$.

Возьмем набор $\vec{h}$ длины 2^n с не более чем $|H|$ единицами такой, что $\mathrm{Pr}_{\overline{H}} \vec{h} = (0, \ldots, 0) \in B^{|\overline{H}|}$ и $\mathrm{Pr}_H \vec{h} = \mathrm{Pr}_H (\tilde{\tau} \oplus \vec{f'})$, где $\oplus$ — операция поразрядного сложения наборов по модулю 2. Для такого набора $\vec{h}$ имеем

$$\tau \oplus \vec{h} \in V_{\tau'}(\vec{f'}) \quad \text{и} \quad \Pi^{-1}(\tau \oplus \vec{h}) \in V_\tau(\vec{f}).$$

Для числа единиц $\rho(\vec{h}, \tilde{0})$ набора $\vec{h}$ в силу (38) справедливо

$$\rho\ (\vec{h}, \tilde{0}) \leqslant |H| = |G'_1 \setminus J'| \leqslant N^2/2^{n-r}.$$

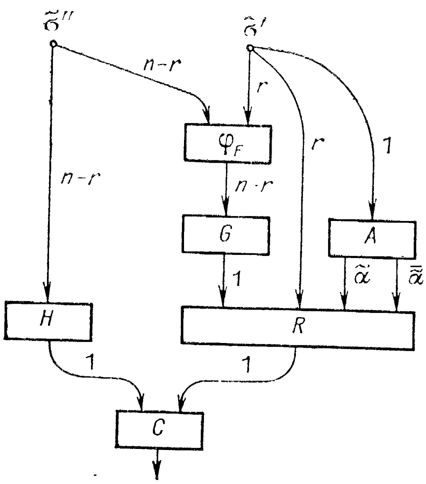

Рис. 2

Опишем схему, τ^n-приближенно реализующую $f(x_1, \ldots, x_n)$ (рис. 2). Пусть $\tilde{\sigma}' = (\sigma_1, \ldots, \sigma_r)$, $\tilde{\sigma}'' = (\sigma_{r+1} \ldots, \sigma_n)$.

φ_F: $(n, n-r)$-оператор. По наборам $\tilde{\sigma}'$, $\tilde{\sigma}''$ вычисляет $\varphi_F(\sigma_1, \ldots, \sigma_n) = \tilde{\sigma}'' \oplus F(\tilde{\sigma}')$, где F — $(r, n-r)$-оператор из леммы 3. Из теоремы Д.4 [4]

$$L(\varphi_F) \lesssim (n-r)\frac{2^r}{r} + (n-r).$$

G: τ''-приближенно реализует функцию $g(x_1, \ldots, x_{n-r})$.

A: по одному из входов $\tilde{\sigma}'$ вычисляет константы 0 и 1. Константы выдаются на выход таким образом, чтобы получились наборы $\tilde{\alpha}$ и $\tilde{\tilde{\alpha}}$,

$$L(A) = \mathrm{const}.$$

R: $(1 + r + 2^{r+1}, 1)$-оператор. Если выход блока G равен 0, то в наборе $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{2^r})$ выделяется $(\|\tilde{\sigma}'\| + 1)$-й разряд и выдается на выход. Если же выход блока G равен 1, то на выход выдается $(\|\tilde{\sigma}'\| + 1)$-й разряд набора $\tilde{\tilde{\alpha}}$. Схема строится по лемме 2.2 [4],

$$L(R) \lesssim 2^r + r.$$

H: реализует функцию $h(x_1, \ldots, x_n)$. Функция h равна 1 не более чем на $N^2/2^{n-r}$ наборах, поэтому, представив функцию h в виде совершенной д. н. ф., имеем

$$L(H) \leqslant nN^2/2^{n-r}.$$

C: суммирует по модулю 2 выходы блоков H и R

$$L(C) = \mathrm{const}.$$

Так как $r = n - \log M(n) - (2t+3)\log n$, $N \leqslant (c_3 + kn^t)M(n)$ и для $M(n) = 2^n - \log v(\tau^n)$ выполняется (29), то

$$\log M(n) \sim n - r, \tag{42}$$

$$(n-r)\frac{2^r}{r} + 2^r + r + n\frac{N^2}{2^{n-r}} = \bar{o}\left(\frac{M(n)}{\log M(n)}\right). \tag{43}$$

Из (41), (42) имеем

$$\log(2^{n-r} - \log v(\tau''))\sim \log M(n) \sim n - r.$$

Следовательно, условие теоремы 1 (§ 2) выполняется для последовательности систем окрестности τ''. Тогда получаем

$$L(G) = L_{\tau''}(g) \leqslant \rho\,\frac{2^{n-r} - \log v(\tau'')}{\log(2^{n-r} - \log v(\tau''))} \sim \rho\,\frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))},$$

$$L_{\tau^n}(f) \leqslant L(\varphi_F) + L(H) + L(A) + L(R) + L(C) + L(G) \leqslant \rho\,\frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

В силу произвольности функции f такая же верхняя оценка верна для $L_T(n)$.

Нижняя оценка доказывается так же, как в теореме 1. Теорема доказана.

§ 4. Случай слабой определенности реализуемой функции

Если для хэмминговой системы окрестностей τ^n, заданной на B^{2^n} и определяющей окрестности функций из P_2^n, выполняются

$$2^{\frac{n}{2} - \frac{1}{2}\log n} \geqslant 2^n - \log v(\tau^n) \geqslant n\log^{1+\delta} n, \tag{44}$$

где $\delta > 0$, то будем говорить, что имеем случай слабой определенности функций из P_2^n и случай большой мощности хэмминговых окрестностей.

Теорема 3. *Пусть для последовательности* $T = \{\tau^1, \tau^2, \ldots\}$, $\tau^n = \langle (I^{1,n}, p_{1,n}), \ldots, (I^{q,n}, p_{q,n}), \quad (I^{q+1,n}, p_{q+1,n}), \ldots, (I^{k,n}, p_{k,n})\rangle$, *заданных на* B^{2^n}, *выполняются* (44) *и*

$$\begin{gathered} p_{i,n} < 1/2,\ i = 1, \ldots, q,\ p_{j,n} > 1/2,\ j = q+1, \ldots, k, \\ |p_{i,n} - 1/2| > \varepsilon,\ i = 1, \ldots, k,\ n = 1, 2, \ldots, \\ |I^{j,n}| \geqslant \varphi(n)\,|I^{1,n} \cup \ldots \cup I^{q,n}|^2,\ j = q+1, \ldots, k, \end{gathered} \tag{45}$$

где $\varphi(n)$ — *произвольная функция, стремящаяся к* ∞ *при* $n \to \infty$, $\varepsilon > 0$. *Тогда*

$$L_T(n) \sim \rho\,\frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

Доказательство. Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция, n достаточно большое, τ^n — хэммингова система окрестностей из T. Образуем два класса $G_1=\{I^{1,n}\cup\ldots\cup I^{q,n}\}$ и $G_2=\{I^{q+1,n}\cup\ldots\cup I^{k,n}\}$. Введем обозначения

$$2^n-\log v(\tau^n)=M(n),\quad |G_1|=N.$$

Используя неравенства (30) для $M(n)$, получим аналогичное (31) соотношение

$$\sum_{i=1}^{q}\left[|I^{i,n}|(1-H(p_i))+\log|I^{i,n}|\right]+(k-q)\geqslant M(n)\geqslant\sum_{i=1}^{q}|I^{i,n}|(1-H(p_i)),$$

откуда следует, что найдутся константы c_4, c_5 такие, что

$$c_4M(n)\leqslant N\leqslant c_5M(n). \tag{46}$$

Положим $d=]2\log N[$. Наборы $\tilde\sigma\in B^n$ будем разбивать на куски длины d, за исключением, может быть, крайнего левого куска. Будем обозначать $\tilde\sigma=(\tilde\sigma_1,\ldots,\tilde\sigma_r)$, где $r=]n/d[$, $\tilde\sigma_i\in B^d$, $i=2,\ldots,r$, $\tilde\sigma_1\in B^{d'}$, $d'\leqslant d$. Наборы $\tilde\sigma_i$ являются двоичными записями чисел $\|\tilde\sigma_i\|$. Возьмем простое число p из интервала $(2^d,2^{d+1})$. Наборы $\tilde\sigma\in B^n$ будем рассматривать как элементы r-мерного векторного пространства $V_r(p)$ над полем Галуа $GF(p)=\{0,1,\ldots,p-1\}$, т. е. набору $\tilde\sigma=(\tilde\sigma_1,\ldots,\tilde\sigma_r)\in B^n$ соответствует вектор $\bar\sigma=(\|\tilde\sigma_1\|,\ldots,\|\tilde\sigma_r\|)\in V_r(p)$.

Для N справедливы соотношения

$$\frac{1}{2\sqrt2}2^{(d+1)/2}\leqslant N\leqslant 2^{d/2}, \tag{47}$$

$$N^2\geqslant\frac14 p. \tag{48}$$

В таблице F значений функции $f(x_1,\ldots,x_n)$ пронумеруем строки $(0,\ldots,0,f(\tilde 0)),\ldots,(1,\ldots,1,f(\tilde 1))$ сверху вниз номерами $1,\ldots,2^n$ соответственно. Пусть $\tilde b^1,\ldots,\tilde b^N$ — наборы из B^n, соответствующие строкам таблицы F с номерами из G_1. Наборам $\tilde b^1,\ldots,\tilde b^N$ соответствуют векторы $\bar b^1,\ldots,\bar b^N$ из $V_r(p)$.

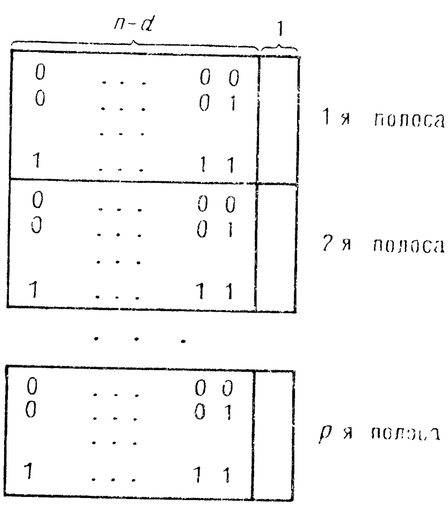

Рис. 3

Из работы [3] следует существование отображения f пространства $V_r(p)$ в поле $GF(p)$ такого, что все $f_i(\bar b^1),\ldots,f_i(\bar b^N)$ будут попарно различными. Отображение $f_i(\bar u)$, $\bar u=(u_1\ldots\ldots,u_r)\in V_r(p)$, представляет собой линейную функцию с коэффициентами $a_1,\ldots,a_r$ из $GF(p)$, т. е. $f_i(\bar u)=a_1u_1+\ldots\ldots+a_ru_r$, где умножение и сложение берутся по модулю p. Отображению $f_i(\bar u)\colon V_r(p)\to GF(p)$ сопоставим функционал $\Phi\colon B^n\to GF(p)$ такой, что для всех $\tilde b\in B^n$, $\Phi(\tilde b)=f_i(\bar b)=a_1\|\tilde b_1\|+\ldots\ldots+a_r\|\tilde b_r\|$. Ясно, что значения функционала Φ на наборах $\tilde b^1,\ldots,\tilde b^N$ попарно различны.

Построим таблицу T размера $p2^{n-d}\times(n-d+1)$. Сначала таблицу заполним, за исключением правого крайнего столбца, так, как показано на рис. 3. Все p полос одинаковы и заполнены наборами из B^{n-d}, которые следуют в лексикографическом порядке. Таблицу F задания функции f разрежем на полосы по 2^d наборов. Для заполнения правого столбца таблицы T будем последовательно просматривать все строки таблицы F.

Пусть $(\tilde{\beta}, f(\tilde{\beta}))$ — очередная просматриваемая строка, $\tilde{\beta}=(\tilde{\beta}_1, \ldots, \tilde{\beta}_r)$. Вычислим значение функционала $\Phi(\tilde{\beta})$. В таблице T в $(\Phi(\tilde{\beta})+1)$-й полосе найдем строку с набором $(\tilde{\beta}_1, \ldots, \tilde{\beta}_{r-1})$ и в правую незаполненную клетку впишем значение $f(\tilde{\beta})$. При этом номеру строки таблицы F с набором $\tilde{\beta}$ сопоставим номер строки таблицы T, куда вписали значение $f(\tilde{\beta})$. Строки таблицы T пронумерованы от 1 до $p2^{n-d}$ сверху вниз. В результате просмотра всех 2^n строк таблицы F в таблице T окажутся заполненными полностью 2^n строк. Остальные пустые клетки заполним 0 или 1 произвольным образом. Множество пар сопоставлений номеров строк таблицы F и T является инъективным отображением $\chi\colon I_{2^n} \to I_{2^{-d}}$.

Обозначим $\{\chi(j)\,|\,j\in I^{i,n}\} = J^{i,n}$, $i=1, \ldots, k$. Строки с номерами из $G_1' = \{J^{1,n} \cup \ldots \cup J^{q,n}\}$ расположены в различных полосах.

Правый крайний столбец таблицы T обозначим $\vec{T}$. К набору $\vec{T}$ и множествам $J^{q+1,n}, \ldots, J^{k,n}$ применим лемму 1. Условия леммы 1 выполнены. Действительно, из (45) и (48) имеем

$$|J^{i,n}| \geqslant \varphi(n) N^2 \geqslant \frac{\varphi(n)}{4} p, \quad i=q+1, \ldots, k.$$

Согласно замечанию леммы 1, найдется набор $\vec{\alpha}\in B^{2^{n-d}}$, являющийся набором значений некоторой линейной функции $\alpha(x_1, \ldots, x_{n-d})$ такой, что для произвольного набора $\tilde{c}\in E^p_{\vec{\alpha}}$ и $\varepsilon_1 > \psi\left(k-q, \frac{\varphi(n)}{4}\right)$, $\psi(\xi, \delta) = \frac{1}{\sqrt{\delta}} + \frac{1}{\sqrt[6]{\delta}} + \frac{\xi}{2\sqrt[12]{\delta}}$ выполнены неравенства

$$\rho_{J^{i,n}}(\vec{T}, \tilde{c}) \leqslant \left(\frac{1}{2} + \varepsilon_1\right)|J^{i,n}|, \qquad i=q+1, \ldots, k. \tag{49}$$

Найдется номер n_0 такой, что для всех $n \geqslant n_0$ будет выполнено $\psi\left(k-q, \frac{\varphi(n)}{4}\right) < \varepsilon$, где $\varepsilon > 0$, $\left|p_{i,n} - \frac{1}{2}\right| > \varepsilon$ и соотношение (49) будет верно для $\varepsilon_1 = \varepsilon$.

Множество номеров полос таблицы T, в которых расположены строки с номерами из G_1', обозначим K. Для K выполняются $K \subseteq I_p$, $|K| = |G_1'| = |G_1|$. Множество номеров полос, содержащих строки с номерами из $J^{i,n}$, обозначим через $K^{i,n}$, $i=1, \ldots, q$.

Теперь определим функцию $g(y_1, \ldots, y_{d+1})$. Пусть на наборах $\tilde{\gamma}\in B^{d+1}$ таких, что $\|\tilde{\gamma}\|+1 \in I_{2^{d+1}} \setminus K$, функция g принимает значение 0 или 1 произвольным образом. Значение функции g на наборах $\tilde{\gamma}$ таких, что $\|\tilde{\gamma}\|+1\in K$, определим так. Если при замене в $(\|\tilde{\gamma}\|+1)$-й полосе таблицы T крайнего правого столбца на $\vec{\alpha}$, строка с номером из G_1' остается неизменной, то в наборе $\tilde{\gamma}$ функция принимает значение 0, в противном случае — 1.

Введем хэммингову систему окрестностей τ', определенную на множестве $B^{2^{d+1}}$:

$$\tau' = \left\langle (K^{1,n}, p_{1,n}), \ldots, (K^{q,n}, p_{q,n}), (I_{2^{d+1}} \setminus K, 1) \right\rangle. \tag{50}$$

Так как $|K^{i,n}| = |J^{i,n}| = |I^{i,n}|$, $i=1, \ldots, q$, то индуцированные хэмминговы системы окрестностей τ_{G_1} и τ_K' равны.

Для $v(\tau')$ и $v(\tau^n)$ справедливы

$$v(\tau') = v(\tau_K')\, 2^{2^{d+1}-|K|}, \quad v(\tau^n) = v(\tau_{G_1}) \prod_{i=q+1}^{k} \left(\sum_{j=0}^{p_i |I^{i,n}|} C^j_{|I^{i,n}|} \right),$$

где $p_i > 1/2$, $i=q+1, \ldots, k$.

Поэтому

$$\log v(\tau_{G_1}) + 2^n - |G_1| - (k-q) \leqslant \log v(\tau^n) \leqslant \log v(\tau_{G_1}) + 2^n - |G_1|,$$

и, учитывая, что $v(\tau_{G_1}) = v(\tau'_K)$, $|K| = |G_1|$, получаем

$$|K| - \log v(\tau'_K) \leqslant 2^n - \log v(\tau^n) \leqslant |K| - \log v(\tau'_K) + (k-q). \quad (52)$$

Из (46), (47), (51) и (52) следует

$$2^{d+1} - \log v(\tau') = |K| - \log v(\tau'_K) \geqslant 2^n - \log v(\tau^n) - (k-q) =$$
$$= M(n) - (k-q) \geqslant \frac{1}{c_5 2\sqrt{2}} 2^{(d+1)/2} - (k-q);$$

т. е. для последовательности хэмминговых систем окрестностей, определенных по (50), выполняются условия теоремы 2 (§ 3), и поэтому

$$L_{\tau'}(g) \leqslant \rho \frac{2^{d+1} - \log v(\tau')}{\log(2^{d+1} - \log v(\tau'))} \sim \rho \frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

Опишем схему, τ^n-приближенно реализующую функцию $f(x_1, \ldots, x_n)$ (рис. 4). Пусть $\tilde{\sigma} = (\tilde{\sigma}_1, \ldots, \tilde{\sigma}_r)$, где $r =]n/d[$.

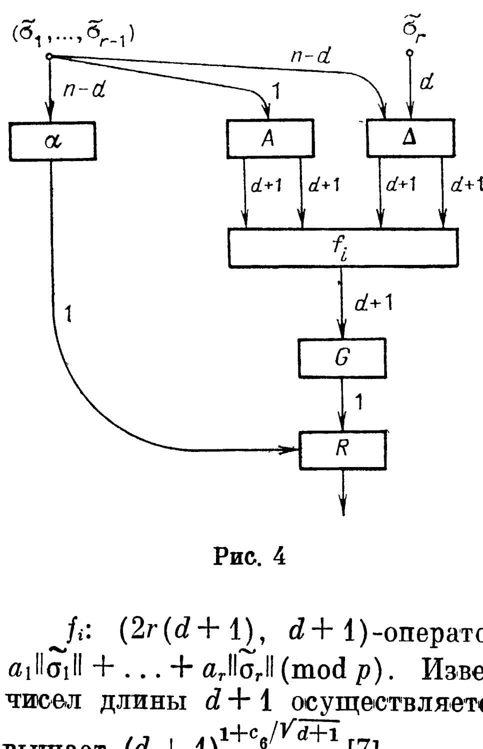

Рис. 4

α: $(n-d, 1)$-оператор. Вычисляет значение линейной функции $\alpha(x_1, \ldots, x_{n-d})$ в наборе $(\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{r-1})$,

$$L(\alpha) \leqslant n - d.$$

A: $(1, r(d+1))$-оператор. По одному из входов вычисляет константы 0 и 1, и выдает их в таком порядке, чтобы на выходе получились двоичные записи длины $d+1$ коэффициентов $a_1, \ldots, a_r \in \{0, 1, \ldots \ldots, p-1\}$ линейного отображения f_i

$$L(A) = \text{const}.$$

Δ: $(n, r(d+1))$-оператор. Выдает r наборов длины $d+1$: $(0, \ldots, 0, \tilde{\sigma}_1), (0, \tilde{\sigma}_2), \ldots, (0, \tilde{\sigma}_r)$,

$$L(\Delta) = \text{const}.$$

f_i: $(2r(d+1), d+1)$-оператор. Вычисляет значение выражения $a_1\|\tilde{\sigma}_1\| + \ldots + a_r\|\tilde{\sigma}_r\| \pmod p$. Известно, что умножение двух двоичных чисел длины $d+1$ осуществляется схемой, сложность которого не превышает $(d+1)^{1+c_6/\sqrt{d+1}}$ [7],

$$L(f_i) \leqslant n.$$

G: $(d+1, 1)$-оператор; τ'-приближенно реализует $g(y_1, \ldots, y_{n-d})$.

R: $(2, 1)$-оператор. Если выход блока G равен 0, то на выход подается $\alpha(\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{r-1})$, в противном случае — $\bar{\alpha}(\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{r-1})$,

$$L(R) = \text{const}.$$

Итак, при $2^n - \log v(\tau^n) \geqslant n \log^{1+\delta} n$, $\delta > 0$ имеем

$$L_{\tau^n}(f) \leqslant L(\alpha) + L(A) + L(\Delta) + L(f_i) + L(R) + L(G) \leqslant \rho \frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

Ввиду произвольности функции f заключаем, что

$$L_T(n) \leqslant \rho \frac{2^n - \log v(\tau^n)}{\log(2^n - \log v(\tau^n))}.$$

Нижняя оценка получается так же, как и в теореме 1. Теорема доказана.

В заключение автор выражает глубокую благодарность С. А. Ложкину, под руководством которого выполнена настоящая работа.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А. Е. Универсальный принцип самокорректирования // Математический сборник. Новая серия.— 1985.— Т. 127, вып. 2.— С. 147—172.
2. Дискретная математика и математические вопросы кибернетики/Под общей редакцией С. В. Яблонского и О. Б. Лупанова. Т. 1.— М.: Наука, 1974.
3. Ложкин С. А., Семенов А. А. Об одном методе сжатия информации и о сложности реализации монотонных симметрических функций // Изв. вузов. Математика.— 1988.— № 7.— С. 44—52.
4. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики.— Вып. 14.— М.: Наука, 1965.— С. 31—110.
5. Семенов А. А. О сложности приближенной реализации булевых функций // Некоторые вопросы вычислительной математики, математической физики и программного обеспечения.— М.: Изд-во МГУ, 1988.— С. 84—86.
6. Семенов А. А. Приближенная реализация булевых функций для хэмминговых систем окрестностей // Тез. докл. VIII Всесоюзной конф. «Проблемы теоретической кибернетики». Ч.2. Горький, июль 1988 г.— Горький, 1988.— С. 105.
7. Тоом А. Л. О сложности схемы из функциональных элементов, реализующей умножение целых чисел // Докл. АН СССР.— 1963.— Т. 3.— С. 496—498.
8. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики.— Вып. 21.— М.: Наука, 1969.— С. 215—226.
9. Pippenger N. J. Information theory and the complexity of switching network // 16th Ann. IEEE Symp. on Fourd. Comput. Sci.— Berkeley, 1975.— P. 113—118.
10. Pippenger N. J. Information theory and the complexity of boolean functions // Mathemotical Systems Theory.— 1977.— № 10.— P. 129—167.

Поступило в редакцию 20.I.1991