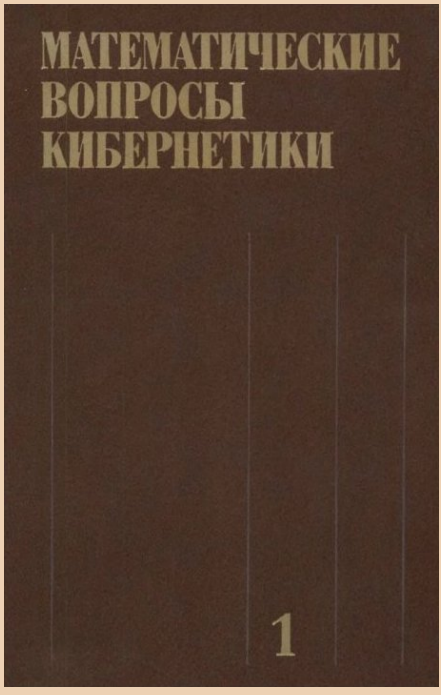
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 1



А. Б. Угольников

О реализации функций из замкнутых классов схемами из функциональных элементов

Рекомендуемая форма библиографической ссылки: Угольников А. Б. О реализации функций из замкнутых классов схемами из функциональных элементов // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 89–113. URL: http://library.keldysh.ru/mvk.asp?id=1988-89

О РЕАЛИЗАЦИИ ФУНКЦИЙ ИЗ ЗАМКНУТЫХ КЛАССОВ СХЕМАМИ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ *)

А. Б. УГОЛЬНИКОВ
(МОСКВА)

Рассматривается задача о реализации булевых функций из замкнутых классов схемами из функциональных элементов в произвольном полном конечном базисе. О. Б. Лупанов [1] получил асимптотически точную формулу для функции Шеннона для класса всех булевых функций. Асимптотически точная формула для функции Шеннона для класса всех монотонных булевых функций получена автором в [4]. В этой работе полностью решается вопрос о поведении функции Шеннона при реализации функций из замкнутых классов над произвольной конечной полной системой функциональных элементов и устанавливаются асимптотически точные формулы для функции Шеннона для всех «нетривиальных» замкнутых классов. Показано, что для любого замкнутого класса функция Шеннона, соответствующая этому классу, или имеет не более чем линейный порядок роста, или асимптотически равна либо $\rho\frac{2^n}{n}$, либо $\rho\frac{2^{n-1}}{n}$, либо $\rho\sqrt{\frac{2}{\pi}}\frac{2^n}{n^{3/2}}$, либо $\rho\frac{1}{\sqrt{2\pi}}\frac{2^n}{n^{3/2}}$, где ρ — константа, зависящая только от базиса.

Введение

Э. Пост [11] описал все замкнутые относительно операции суперпозиции классы булевых функций. Описание этих классов содержится в [7]. Мы будем использовать терминологию последней работы. Функция φ называется α-функцией, если $\varphi(y, \ldots, y) = y$, β-функцией, если $\varphi(y, \ldots, y) = 1$ и γ-функцией, если $\varphi(y, \ldots, y) = 0$. Функция $\varphi(x_1, \ldots, x_n)$ называется самодвойственной, если $\varphi(x_1, \ldots, x_n) = \overline{\varphi}(\overline{x_1}, \ldots, \overline{x_n})$. Функция $\varphi(x_1, \ldots, x_n)$ называется линейной, если $\varphi(x_1, \ldots, x_n) = c_0 \oplus c_1x_1 \oplus \ldots \oplus c_nx_n$**). Говорят, что функция удовлетворяет условию $\langle a^\infty \rangle$ (соответственно $\langle A^\infty \rangle$), если все наборы, на которых функция равна нулю (соответственно единице), имеют общую нулевую (единичную) компоненту. Говорят, что функция удовлетворяет условию $\langle a^\mu \rangle$ (соответственно $\langle A^\mu \rangle$), если любые μ, $\mu \geqslant 2$, наборов, на которых функция равна нулю (соответственно единице), имеют общую нулевую (единичную) компоненту.

Введем отношение порядка для всех двоичных наборов фиксированной длины. Скажем, что набор $\alpha = (\alpha_1, \ldots, \alpha_n)$ покрывает набор $\beta = (\beta_1, \ldots, \beta_n)$, если $\alpha_1 \geqslant \beta_1, \ldots, \alpha_n \geqslant \beta_n$ (обозначение $\alpha \succcurlyeq \beta$). Функция

*) Основные результаты работы изложены в [6].
**) Символ $\oplus$ означает сложение по mod 2.

Таблица

Замкнутый класс	Входящие в него функции
C_1	все булевы функции
C_2	α- и β-функции
C_3	α- и γ-функции
C_4	α- функции
Классы монотонных функций	
A_1	все монотонные функции
A_2	монотонные функции, кроме 0
A_3	монотонные функции, кроме 1
A_4	монотонные функции, кроме 0 и 1
Классы самодвойственных функций	
D_1	самодвойственные α-функции
D_2	самодвойственные монотонные функции
D_3	все самодвойственные функции
Классы линейных функций	
L_1	все линейные функции
L_2	линейные α- и β-функции
L_3	линейные α- и γ-функции
L_4	линейные α-функции
L_5	линейные самодвойственные функции
$\mu \geqslant 2$	
F_1^μ	α-функции, удовлетворяющие условию $\langle a^\mu \rangle$
F_2^μ	монотонные α-функции, удовлетворяющие условию $\langle a^\mu \rangle$
F_3^μ	монотонные функции, удовлетворяющие условию $\langle a^\mu \rangle$
F_4^μ	все функции, удовлетворяющие условию $\langle a^\mu \rangle$
F_5^μ	α-функции, удовлетворяющие условию $\langle A^\mu \rangle$
F_6^μ	монотонные α-функции, удовлетворяющие условию $\langle A^\mu \rangle$
F_7^μ	монотонные функции, удовлетворяющие условию $\langle A^\mu \rangle$
F_8^μ	все функции, удовлетворяющие условию $\langle A^\mu \rangle$
F_1^∞	α-функции, удовлетворяющие условию $\langle a^\infty \rangle$
F_2^∞	монотонные α-функции, удовлетворяющие условию $\langle a^\infty \rangle$
F_3^∞	монотонные функции, удовлетворяющие условию $\langle a^\infty \rangle$
F_4^∞	все функции, удовлетворяющие условию $\langle a^\infty \rangle$
F_5^∞	α-функции, удовлетворяющие условию $\langle A^\infty \rangle$
F_6^∞	монотонные α-функции, удовлетворяющие условию $\langle A^\infty \rangle$
F_7^∞	монотонные функции, удовлетворяющие условию $\langle A^\infty \rangle$
F_8^∞	все функции, удовлетворяющие условию $\langle A^\infty \rangle$

Продолжение табл.

Замкнутый класс	Входящие в него функции
Классы дизъюнкций	все логические суммы (т. е. функции вида $\bigvee_{i=1}^{k} x_i$ $(k=1,2,\ldots)$, и все функции, получающиеся из них путем переименования переменных без отождествления)
S_1	
S_3	логические суммы, 1
S_5	логические суммы, 0
S_6	логические суммы, 0, 1
Классы конъюнкций	определяются двойственным образом
P_1, P_3, P_5, P_6	

φ называется монотонной, если $\varphi(\alpha) \geqslant \varphi(\beta)$ для всяких двух наборов α и β таких, что $\alpha \geqslant \beta$.

В таблице приведено описание всех замкнутых классов, которые содержат функции, существенно зависящие более чем от одной переменной [7]*).

Рассмотрим произвольную полную конечную систему функциональных элементов $\mathfrak{A} = \{B_1, \ldots, B_k\}$. Каждому элементу B_i из $\mathfrak{A}$ приписано некоторое положительное число $L(B_i)$ — *вес* этого элемента. Пусть S — схема над $\mathfrak{A}$. *Сложностью схемы* S называется сумма весов всех входящих в нее элементов. *Сложностью булевой функции* f называется величина

$$L(f) = \min_{S} L(S),$$

где минимум берется по всевозможным схемам S над $\mathfrak{A}$, реализующим функцию f. *Сложностью* конечного *множества* H булевых функций называется величина

$$L(H) = \max_{f \in H} L(f).$$

Пусть H — произвольное множество булевых функций. Будем обозначать через $H(n)$ множество всех функций из H от переменных $x_1, \ldots, x_n$. Аналогичные обозначения используются при реализации систем функций. Системы из m функций от n переменных называются также (n, m)-*операторами*.

С каждой конечной системой $\mathfrak{A} = \{B_1, \ldots, B_k\}$ связано число ρ, определяемое соотношением

$$\rho = \min_{b_i \geqslant 2} \frac{L(B_i)}{(b_i - 1)},$$

где b_i — число входов у элемента B_i [2].

О. Б. Лупанов [2] для класса C_1 всех булевых функций показал, что

$$L(C_1(n)) \sim \rho \frac{2^n}{n}. \tag{1}$$

Оценка функции Шеннона для класса A_1 монотонных функций получена автором в [4]. Она имеет вид

$$L(A_1(n)) \sim \rho \sqrt{\frac{2}{\pi}} \frac{2^n}{n^{3/2}}. \tag{2}$$

*) Классы функций одной переменной обозначаются в [7] через $Q_1, \ldots, Q_9$.

Основным результатом данной работы является
Теорема 1.

$$L(F_3^3(n)) \leqslant \rho \frac{1}{\sqrt{2\pi}} \frac{2^n}{n^{3/2}}.$$

На основе этой оценки и соотношений (1) и (2) доказывается следующая теорема, в которой полностью решается вопрос о поведении функции Шеннона при реализации функций из замкнутых классов схемами над произвольной конечной полной системой функциональных элементов и устанавливаются асимптотические точные формулы для функций Шеннона всех «нетривиальных» замкнутых классов.

Теорема 2. *Для любого замкнутого класса булевых функций функция Шеннона, соответствующая этому классу, или имеет не более чем линейный порядок роста, или асимптотически равна либо* $\rho\frac{2^n}{n}$, *либо* $\rho\frac{2^{n-1}}{n}$, *либо* $\rho\sqrt{\frac{2}{\pi}}\frac{2^n}{n^{3/2}}$, *либо* $\rho\frac{1}{\sqrt{2\pi}}\frac{2^n}{n^{3/2}}$. *Более точно:*

1) *пусть* $\mathcal{H}$ *— один из классов* S_1, S_3, S_5, S_6, P_1, P_3, P_5, P_6, $L_1 - L_5$, $O_1 - O_9$, *тогда*

$$L(\mathcal{H}(n)) = O(n);$$

2) $L(C_i(n)) \sim \rho\frac{2^n}{n}$ $(i = 1, 2, 3, 4)$;

3) *пусть* $\mathcal{H}$ *— один из классов* A_i $(i = 1, 2, 3, 4)$, F_j^2 $(j = 2, 3, 6, 7)$, *тогда*

$$L(\mathcal{H}(n)) \sim \rho\sqrt{\frac{2}{\pi}}\frac{2^n}{n^{3/2}};$$

4) *пусть* $\mathcal{H}$ *— один из классов* D_1, D_3, F_i^∞, F_i^μ $(i = 1, 4, 5, 8;\ \mu = 2, 3, \ldots)$, *тогда*

$$L(\mathcal{H}(n)) \sim \rho\frac{2^{n-1}}{n};$$

5) *пусть* $\mathcal{H}$ *— один из классов* D_2, F_i^∞, F_i^μ $(i = 2, 3, 6, 7;\ \mu = 3, 4, \ldots)$, *тогда*

$$L(\mathcal{H}(n)) \sim \rho\frac{1}{\sqrt{2\pi}}\frac{2^n}{n^{3/2}}.$$

Автор благодарит О. Б. Лупанова за постановку задачи и внимание к работе и О. М. Касим-Заде, прочитавшему работу и сделавшему ряд полезных замечаний, способствовавших ее улучшению.

§ 1. Доказательство теоремы 2

В этом параграфе мы приведем доказательство теоремы 2, используя утверждение теоремы 1. Доказательство теоремы 1 будет приведено в следующих параграфах.

Обозначим через $\tilde{x}$ набор переменных $x_1, \ldots, x_n$.

Лемма 1. *Для любой функции* $f(\tilde{x})$, *удовлетворяющей условию* $\langle a^2 \rangle$, *существуют самодвойственная монотонная функция* $g(\tilde{x})$ *и функция* $h(\tilde{x})$ *такие, что*

$$f(\tilde{x}) = g(\tilde{x}) \vee h(\tilde{x}),$$

причем $h(\alpha) = h(\bar{\alpha})$ *для любого набора* α *значений переменных* $\tilde{x}$.

Доказательство. Построим самодвойственную монотонную функцию g, удовлетворяющую соотношению $g \leqslant f$ (т. е. $g(\tilde{x}) \leqslant f(\tilde{x})$ при

всех $\tilde{x}$). Пусть $\alpha^1, \ldots, \alpha^m$ — все наборы, на которых функция f обращается в нуль. Определим функцию g_0 следующим образом. Положим

$$g_0(\tilde{x}) = Д_{\alpha^1}(\tilde{x}) \,\&\, \ldots \,\&\, Д_{\alpha^m}(\tilde{x}),$$

где $Д_{\alpha^i}(\tilde{x})$ — дизъюнкция всех тех переменных из $\tilde{x}$, для которых соответствующие компоненты набора α^i равны нулю. Легко видеть, что функция g_0 монотонная, удовлетворяет условию $\langle a^2\rangle$ и $g_0 \leqslant f$.

Обозначим через $N(g_0)$ число пар наборов $(\alpha, \bar{\alpha})$ (в каждую пару входят набор и его отрицание) таких, что $g_0(\alpha) = g_0(\bar{\alpha}) = 1$. Пусть $N(g_0) > 0$. Построим монотонную функцию g_1, удовлетворяющую условию $\langle a^2\rangle$, такую, что $g_1 \leqslant g_0$ и $N(g_1) = N(g_0) - 1$. Рассмотрим набор β, который входит в одну из рассматриваемых пар и удовлетворяет условию: для любого набора α такого, что $\alpha \leqslant \beta$, $g_0(\alpha) = 0$. Определим функцию g_1 следующим образом. Положим

$$g_1(\alpha) = \begin{cases} 0, & \text{если } \alpha = \beta, \\ g_0(\alpha) & \text{в противном случае.} \end{cases}$$

Очевидно, что g_1 является монотонной, удовлетворяющей условию $\langle a^2\rangle$ функцией, причем $g_1 \leqslant g_0$ и $N(g_1) = N(g_0) - 1$. Если $N(g_1) > 0$, то применим к функции g_1 вышеописанную процедуру. И так далее, до тех пор, пока не получим некоторую монотонную, удовлетворяющую условию $\langle a^2\rangle$ функцию g такую, что $g \leqslant g_0$ и $N(g) = 0$. Нетрудно убедиться, что функция g является искомой самодвойственной монотонной функцией.

Определим теперь функцию h следующим образом. Положим

$$h(\alpha) = f(\alpha) \,\&\, \bar{g}(\alpha) \vee f(\bar{\alpha}) \,\&\, \bar{g}(\bar{\alpha})$$

для любого набора α. Покажем, что функция h является искомой. В самом деле, для любого набора α такого, что $g(\alpha) = 0$, $\bar{g}(\bar{\alpha}) = 0$ (так как g — самодвойственная функция), и поэтому $h(\alpha) = f(\alpha)$. В противном случае, при $g(\alpha) = 1$ (так как $f \geqslant g$), $f(\alpha) = 1$. Лемма доказана.

Доказательство теоремы 2. Утверждение случая 1) очевидно, утверждение случая 2) следует из (1).

3) В силу двойственности и соотношений $F_2^2 \subset F_3^2 \subset A_2$ и $F_2^2 \subset A_4 \subset A_2 \subset A_1$ достаточно найти нижнюю оценку для функции $L(F_2^2(n))$, асимптотически равную верхней оценке для функции $L(A_1(n))$ (см. (2)).

Рассмотрим множество $\widehat{A}(n)$ функций $f(x_1, \ldots, x_n)$ таких, что:

а) если *) $\|\alpha\| \geqslant \lceil n/2 \rceil$, то $f(\alpha) = 1$;

б) если $\|\alpha\| < \lceil n/2 \rceil - 1$, то $f(\alpha) = 0$.

Легко видеть, что $\widehat{A}(n) \subset F_2^2(n)$ и**) $\log |\widehat{A}(n)| = C_n^{\lceil n/2 \rceil - 1}$. Поэтому ***)

$$L(F_2^2(n)) \geqslant \rho \sqrt{\frac{2}{\pi}} \frac{2^n}{n^{3/2}}.$$

4) Для классов D_1 и D_3 утверждение теоремы следует из (1), очевидного соотношения $\log |D_1(n)| = \log |D_3(n)| - 1 = 2^{n-1} - 1$ и того, что для любой самодвойственной функции $f(\tilde{x})$ имеет место представление

$$f(\tilde{x}) = 1 \oplus x_1 \oplus f(1, x_1 \oplus x_2 \oplus 1, \ldots, x_1 \oplus x_n \oplus 1).$$

Рассмотрим классы F_i^∞, F_i^μ ($i = 1, 4, 5, 8$; $\mu = 2, 3, \ldots$). В силу двойственности достаточно рассмотреть случаи $i = 1$ и $i = 4$. Легко видеть, что $F_1^\infty \subseteq F_1^\mu \subset F_4^\mu \subseteq F_4^2$ и $F_1^\infty \subset F_4^\infty \subset F_4^2$ для всех $\mu = 2, 3, \ldots$

*) Через $\|\alpha\|$ обозначаем число единиц в наборе α.

**) Все логарифмы берутся по основанию 2.

***) Здесь используется мощностной метод получения нижних оценок (см. [2]).

Поэтому достаточно получить нижнюю оценку для функции $L(F_1^\infty(n))$, асимптотически равную верхней оценке для функции $L(F_4^2(n))$.

Пусть $f(x_1, \ldots, x_n)$ — произвольная функция, удовлетворяющая условию $\langle a^2 \rangle$ (см. также [5]). На основании леммы 1 функцию f можно представить в виде $f(\tilde{x}) = g(\tilde{x}) \vee h(\tilde{x})$, где $g \in D_2$, а $h(\alpha) = h(\bar{\alpha})$ для любого набора α значений переменных $\tilde{x}$. Из (2) следует, что $L(g) = o(2^n/n)$. В силу определения функции h имеет место представление

$$h(x_1, \ldots, x_n) = x_1 h(1, x_2, \ldots, x_n) \vee \bar{x}_1 h(1, \bar{x}_2, \ldots, \bar{x}_n) = h(1, x_1 \oplus x_2 \oplus 1, \ldots, x_1 \oplus x_n \oplus 1).$$

Поэтому, в силу (1), $L(h) \leqslant \rho 2^{n-1}/n$. Таким образом,

$$L(F_4^2(n)) \leqslant \rho \frac{2^n}{2n}.$$

Необходимая нижняя оценка для функции $L(F_1^\infty(n))$ получается на основе соотношения

$$\log |F_i^\infty(n)| \geqslant 2^{n-1} - 1.$$

5) для класса D_2 нижняя оценка следует из теоремы Д1 (см. [4, с. 183]), верхняя оценка (см. также [4]) следует из (2) и приведенного выше представления для самодвойственных функций.

Для оставшихся классов в силу двойственности и соотношений $F_2^\infty \subset F_3^\infty \subset F_3^3$ и $F_2^\infty \subseteq F_2^\mu \subset F_3^\mu \subseteq F_3^3$ $(\mu = 3, 4, \ldots)$ достаточно получить нижнюю оценку для функции $L(F_2^\infty(n))$, асимптотически равную верхней оценке для функции $L(F_3^3(n))$.

Нижняя оценка для функции $L(F_2^\infty(n))$ получается на основе соотношения $|F_2^\infty(n)| \geqslant |A_2(n-1)|$. Верхняя оценка для функции $L(F_3^3(n))$ дана в теореме 1.

Теорема 2 доказана.

§ 2. Разбиение множества наборов на цепи

Пусть E — множество всевозможных наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$ длины n из нулей и единиц, а τ — целое число, удовлетворяющее условию $0 < \tau < n/2$. Выделим в множестве E подмножества

$$E_i = \{\alpha: \|\alpha\| = i\}, \quad i = 0, 1, \ldots, n,$$

$$\mathscr{E}_1 = \{\alpha: [n/2] + \tau < \|\alpha\| \leqslant n\}, \quad \mathscr{E}_2 = \{\alpha: [n/2] \leqslant \|\alpha\| \leqslant [n/2] + \tau\},$$

$$\mathscr{E}_3 = \{\alpha: [n/2] - \tau \leqslant \|\alpha\| \leqslant [n/2]\}, \quad \mathscr{E} = \mathscr{E}_2 \cup \mathscr{E}_3, \quad \mathscr{E}_4 = E \setminus (\mathscr{E}_1 \cup \mathscr{E}).$$

Будем называть последовательность наборов $\alpha^1, \ldots, \alpha^m \in E$ *цепью (длины m)*, если выполнены условия:

1) $\alpha^i \leqslant \alpha^j$ для $i \leqslant j$ $(i, j = 1, \ldots, m)$;

2) $\|\alpha^{i-1}\| = \|\alpha^i\| - 1$ для $i = 2, \ldots, m$.

Рассмотрим разбиение Анселя [9] множества E на цепи. Мы будем использовать следующие свойства этого разбиения:

1) цепи не пересекаются;

2) число цепей равно $C_n^{[n/2]}$;

3) число цепей длины $n - 2p + 1$ равно $C_n^p - C_n^{p-1}$, $0 \leqslant p \leqslant [n/2]$ (минимальный элемент каждой такой цепи есть набор с p единицами и $n - p$ нулями, максимальный — с p нулями и $n - p$ единицами).

Разбиение Анселя порождает разбиение множества $\mathscr{E}$ на цепи, которое мы обозначим через R^0. Разбиение R^0 порождает разбиение мно-

жеств $(E_{i-1} \cup E_i)$ $(i = [n/2] - \tau + 1, \ldots, [n/2])$ и множества $\mathscr{E}_2$ на цепи. Обозначим эти разбиения через R_i^0 и $R_{[n/2]+1}^0$ соответственно.

Пусть $\pi_{[n/2]-\tau+1}, \ldots, \pi_{[n/2]+1}$ — произвольный набор подстановок компонент наборов. Подстановки π_i $([n/2] - \tau + 1 \leqslant i \leqslant [n/2])$ применяются к наборам из соответствующих множеств $(E_{i-1} \cup E_i)$, а подстановка $\pi_{[n/2]+1}$ — к наборам из $\mathscr{E}_2$. Подстановки применяются в следующем порядке: сначала подстановка $\pi_{[n/2]-\tau+1}$ к наборам из $(E_{[n/2]-\tau} \cup E_{[n/2]-\tau+1})$, затем подстановка $\pi_{[n/2]-\tau+2}$ к наборам из $(E_{[n/2]-\tau+1} \cup E_{[n/2]-\tau+2})$ и так далее, и в последнюю очередь подстановка $\pi_{[n/2]+1}$ к наборам из $\mathscr{E}_2$. Нетрудно убедиться в том, что в результате применения этих подстановок из разбиения R^0 снова будут получаться некоторые, вообще говоря, другие разбиения множества $\mathscr{E}$ на $C_n^{[n/2]}$ непересекающихся цепей. Рассматривая всевозможные такие наборы подстановок, мы получим $(n!)^{\tau+1}$ разбиений множества $\mathscr{E}$ на $C_n^{[n/2]}$ непересекающихся цепей. Отметим, что среди этих разбиений могут быть и одинаковые.

Пусть B — некоторое подмножество множества $E_{[n/2]-\tau}$. Выделим в множестве $\mathscr{E}$ подмножества

$$B' = \{\alpha\colon \alpha \in \mathscr{E} \text{ и существует набор } \beta \in B \text{ такой, что } \beta \preccurlyeq \alpha\},$$
$$A = \mathscr{E} \setminus B', \quad A_i = A \cap E_i, \quad i = [n/2] - \tau, \ldots, [n/2] + \tau.$$

Рассмотрим класс $M_n^\tau(B)$ функций $f(x_1, \ldots, x_n)$, удовлетворяющих условиям:

1) f монотонна;
2) если $\alpha \in (\mathscr{E}_1 \cup B')$, то $f(\alpha) = 1$;
3) если $\alpha \in \mathscr{E}_4$, то $f(\alpha) = 0$.

Пусть f — произвольная функция из $M_n^\tau(B)$. Зафиксируем некоторое $k > 1$ и разобьем наборы α такие, что $\alpha \in A$ и $f(\alpha) = 1$, на два класса F_k и G_k следующим образом: $\alpha \in F_k$, если среди наборов β таких, что $\beta \preccurlyeq \alpha$ и $\|\beta\| = \|\alpha\| - 1$, не более чем k штук удовлетворяет условию $f(\beta) = 1$, и $\alpha \in G_k$ в противном случае.

Пусть R — разбиение некоторого подмножества множества $\mathscr{E}$ на непересекающиеся цепи. Обозначим через $N(R)$ число цепей в этом разбиении, которое содержит хотя бы один набор из множества A, а через $T(R)$ — число цепей, которые содержат по крайней мере два разных набора из множества F_k.

Определим функцию $\alpha(y)$ следующим образом. Положим

$$\alpha(y) = 1 - y/C_n^{[n/2]-\tau}.$$

Очевидно, что $0 \leqslant \alpha(y) \leqslant 1$ при $0 \leqslant y \leqslant C_n^{[n/2]-\tau}$.

Лемма 2. *Для любой функции $f \in M_n^\tau(B)$ и любого целого p, $p > 1$, среди $(n!)^{\tau+1}$ описанных выше разбиений множества $\mathscr{E}$ на $C_n^{[n/2]}$ непересекающихся цепей найдется такое разбиение R_f, что*

$$N(R_f) \leqslant \left(1 + \frac{1}{(p-1)}\right) \alpha(|B|)\, C_n^{[n/2]},$$
$$T(R_f) \leqslant \frac{2k\tau\,(p+1)}{n - 2\tau}\, \alpha(|B|)\, C_n^{[n/2]}.$$

Доказательство. Рассмотрим описанные выше разбиения R_i^0 множеств $(E_{i-1} \cup E_i)$ $(i = [n/2] - \tau + 1, \ldots, [n/2])$ и разбиение $R_{[n/2]+1}^0$ множества $\mathscr{E}_2$ на непересекающиеся цепи. Мы будем строить независимо друг от друга разбиения $R_{[n/2]-\tau+1}, \ldots, R_{[n/2]+1}$ множеств $(E_{[n/2]-\tau} \cup E_{[n/2]-\tau+1}), \ldots, (E_{[n/2]-1} \cup E_{[n/2]})$, $\mathscr{E}_2$ соответственно на непересекающиеся цепи, а затем объединим получившиеся цепи и тем самым получим искомое разбиение R_f. Обозначим через $P(R_i)$ число цепей длины 1 в

разбиении R_i ($[n/2]-\tau+1 \leqslant i \leqslant [n/2]$), содержащихся в A. Из свойств рассматриваемых разбиений следует, что

$$N(R_j) \leqslant N(R_{[n/2]-\tau+1}) + \sum_{i=[n/2]-\tau+2}^{[n/2]} P(R_i) = |A_{[n/2]-\tau}| + \sum_{i=[n/2]-\tau+1}^{[n/2]} P(R_i), \tag{3}$$

$$T(R_j) \leqslant \sum_{i=[n/2]-\tau+1}^{[n/2]+1} T(R_i). \tag{4}$$

Опишем процедуру разбиения множества $(E_{i-1} \cup E_i)$ ($[n/2]-\tau+1 \leqslant i \leqslant [n/2]$) на цепи. Рассмотрим исходное разбиение R_i^0 множества $(E_{i-1} \cup E_i)$ на цепи. В силу свойства 3) (с. 94) $P(R_i^0) \leqslant C_n^i - C_n^{i-1}$. Рассмотрим всевозможные подстановки компонент наборов. Получим $n!$ разбиений $R_i^0, \ldots, R_i^{n!-1}$ множества $(E_{i-1} \cup E_i)$ на цепи. Если $\beta \in A_i$, то β принадлежит цепи длины 1 не более чем в

$$(C_n^i - C_n^{i-1})\, i!\,(n-i)! = \frac{(C_n^i - C_n^{i-1})}{C_n^i}\, n!$$

разбиениях множества $(E_{i-1} \cup E_i)$ на цепи. Поэтому

$$\sum_{l=0}^{n!-1} P(R_i^l) \leqslant \frac{|A_i|}{C_n^i}(C_n^i - C_n^{i-1})\, n!$$

Если $\beta \in (F_k \cap A_i)$, то β принадлежит цепи, содержащей какой-либо набор γ из F_k, $\gamma \neq \beta$, не более чем в (ср. [10])

$$C_n^i (n-i)!\, k\,(i-1)!$$

разбиениях множества $(E_{i-1} \cup E_i)$ на цепи. Поэтому

$$\sum_{l=0}^{n!-1} T(R_i^l) \leqslant |F_k \cap A_i| \frac{kn!}{i}.$$

Рассмотрим два множества индексов:

$$M' = \left\{j:\ T(R_i^j) \geqslant \frac{|F_k \cap A_i|}{i}\, kp\right\},$$

$$M = \left\{j: T(R_i^j) < \frac{|F_k \cap A_i|}{i}\, kp\right\}.$$

Легко видеть, что $|M'| \leqslant n!/p$. Поэтому $|M| \geqslant n!(1-1/p)$. Далее, так как

$$\sum_{l \in M} P(R_i^l) \leqslant \frac{|A_i|}{C_n^i}(C_n^i - C_n^{i-1})\, n!,$$

найдется $j_0 \in M$ такое, что

$$P(R_i^{j_0}) \leqslant \frac{|A_i|(C_n^i - C_n^{i-1})\, n!}{C_n^i |M|} \leqslant \frac{|A_i|}{C_n^i}(C_n^i - C_n^{i-1})\left(1 + \frac{1}{p-1}\right). \tag{5}$$

В то же время

$$T(R_i^{j_0}) < \frac{|F_k \cap A_i|}{i}\, kp. \tag{6}$$

Рассмотрим теперь исходное разбиение $R_{[n/2]+1}^0$ множества $\mathscr{E}_2$ на цепи и всевозможные подстановки компонент наборов. Построим $n!$ разбиений $R_{[n/2]+1}^0, \ldots, R_{[n/2]+1}^{n!-1}$ множества $\mathscr{E}_2$ на цепи. Так же как и ра-

нее, получаем

$$\sum_{l=0}^{n!-1} T\left(R^l_{[n/2]+1}\right) \leqslant \frac{kn!}{n/2} \sum_{i=[n/2]+1}^{[n/2]+\tau} |F_k \cap A_i|.$$

Поэтому найдется такое разбиение $R^{j_1}_{[n/2]+1}$ множества $\mathscr{E}_2$ на цепи, что

$$T\left(R^{j_1}_{[n/2]+1}\right) \leqslant \frac{2k}{n} \sum_{i=[n/2]+1}^{[n/2]+\tau} |F_k \cap A_i|. \tag{7}$$

В силу определения множества A имеем

$$|A_{[n/2]-\tau}| = C_n^{[n/2]-\tau} - |B| = C_n^{[n/2]-\tau}\alpha(|B|),$$

$$|A_i| = C_n^i - |B' \cap E_i| \leqslant C_n^i - |B| \frac{n-[n/2]+\tau}{[n/2]-\tau+1} \cdots \frac{n-i+1}{i} = C_n^i -$$

$$- \frac{|B|}{C_n^{[n/2]-\tau}} C_n^{[n/2]-\tau} \frac{n-[n/2]+\tau}{[n/2]-\tau+1} \cdots \frac{n-i+1}{i} = C_n^i - \frac{|B|}{C_n^{[n/2]-\tau}} C_n^i = C_n^i \alpha(|B|)$$

для всех $i = [n/2]-\tau+1, \ldots, [n/2]+\tau$.

Подставляя (5)—(7) в (3) и (4) и учитывая оценки для $|A_i|$, получаем

$$N(R_f) \leqslant |A_{[n/2]-\tau}| + \sum_{i=[n/2]-\tau+1}^{[n/2]} \frac{|A_i|}{C_n^i}(C_n^i - C_n^{i-1})\left(1 + \frac{1}{p-1}\right) \leqslant$$

$$\leqslant \alpha(|B|)\left(C_n^{[n/2]-\tau} + \left(1+\frac{1}{p-1}\right) \sum_{i=[n/2]-\tau+1}^{[n/2]} (C_n^i - C_n^{i-1})\right) =$$

$$= \alpha(|B|)\left(C_n^{[n/2]-\tau} + \left(1+\frac{1}{p-1}\right)(C_n^{[n/2]} - C_n^{[n/2]-\tau})\right) \leqslant \alpha(|B|)\left(1+\frac{1}{p-1}\right) C_n^{[n/2]},$$

$$T(R_f) \leqslant \sum_{i=[n/2]-\tau+1}^{[n/2]} \frac{|F_k \cap A_i|}{i} kp + \frac{2k}{n} \sum_{i=[n/2]+1}^{[n/2]+\tau} |F_k \cap A_i| \leqslant$$

$$\leqslant \alpha(|B|) C_n^{[n/2]} \left(\frac{kp}{n/2-\tau} + \frac{2\tau k}{n}\right) \leqslant \alpha(|B|) \frac{2k\tau(p+1)}{n-2\tau} C_n^{[n/2]}.$$

Лемма доказана.

Рассмотрим разбиение S множества $E_{[n/2]}$ на подмножества из работы [4, с. 170]. Это разбиение обладает следующими свойствами:

1) подмножества не пересекаются;

2) для любых двух наборов α, β из $E_{[n/2]}$, принадлежащих одному подмножеству, выполняется условие *)

$$\rho(\alpha, \beta) \geqslant 5\tau; \tag{8}$$

3) число подмножеств L удовлетворяет соотношениям

$$L = \sum_{0 \leqslant i \leqslant 5\tau} C_n^i \leqslant n^{5\tau}. \tag{9}$$

Занумеруем подмножества разбиения S числами от 1 до L, а наборы из $E_{[n/2]}$ — числами от 1 до $C_n^{[n/2]}$: сначала в каком-то порядке нумеруются наборы первого подмножества, затем второго и т. д. Обозначим полученную нумерацию наборов из $E_{[n/2]}$ через Q^0. Будем рассматривать всевозможные перестановки подмножеств и соответствующие перенумерации наборов из $E_{[n/2]}$ с сохранением порядка наборов внутри каждого

*) $\rho(\alpha, \beta)$ — число различающихся разрядов у наборов $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$ (расстояние по Хэммингу).

подмножества: нумеруем сначала наборы подмножества, идущего в перестановке первым, затем — идущего вторым, и т. д. Таким образом будут получены $L!$ нумераций $Q^0, \ldots, Q^{L!-1}$ наборов из $E_{[n/2]}$.

Пусть теперь R — произвольное разбиение множества $\mathscr{E}$ на $C_n^{[n/2]}$ непересекающихся цепей. Легко видеть, что каждая цепь разбиения R содержит в точности один набор из $E_{[n/2]}$. Поэтому разбиение S множества $E_{[n/2]}$ на подмножества порождает разбиение множества цепей из R на подмножества (называемые в дальнейшем *блоками*), а нумерации $Q^0, \ldots, Q^{L!-1}$ наборов из $E_{[n/2]}$ порождают упорядочения цепей разбиения R. В самом деле, достаточно отнести к m-му блоку те цепи, которые содержат наборы из m-го подмножества разбиения S, и приписать каждой цепи номер входящего в нее набора из $E_{[n/2]}$. Таким образом, из разбиения R получается $L!$ упорядоченных разбиений $(R, Q^0), \ldots, (R, Q^{L!-1})$ множества $\mathscr{E}$ на цепи, соответствующих нумерациям $Q^0, \ldots, Q^{L!-1}$. Отметим, что порядок цепей внутри каждого блока одинаков для всех $L!$ упорядочений.

Пусть (R, Q) — некоторое упорядоченное разбиение множества $\mathscr{E}$ на непересекающиеся цепи. Обозначим через $T^1((R, Q))$ число цепей, которые содержат по крайней мере один набор α такой, что $\alpha \in G_k$, и на всех предшествующих цепях этого разбиения не существует набора β такого, что $\beta \preccurlyeq \alpha$ и $f(\beta) = 1$.

Лемма 3. *Для любой функции $f \in M_n^\tau(B)$ и любого разбиения R множества $\mathscr{E}$ на $C_n^{[n/2]}$ непересекающихся цепей среди $L!$ упорядоченных разбиений, полученных из разбиения R, найдется такое упорядоченное разбиение (R, Q_f), что*

$$T^1((R, Q_f)) \leqslant C_n^{[n/2]}/k.$$

Доказательство леммы следует из рассуждений, приведенных в [10, с. 47], и свойств разбиения цепей на блоки.

§ 3. Кодирование монотонных функций

Пусть $\varkappa$ — целое число, удовлетворяющее условию $0 \leqslant \varkappa \leqslant C_n^{[n/2]-\tau}$. Рассмотрим класс функций

$$M_{n,\varkappa}^\tau = \bigcup_{B \subseteq E_{[n/2]-\tau}:\ |B|=\varkappa} M_n^\tau(B)$$

и произвольную функцию $f(x_1, \ldots, x_n)$ из $M_{n,\varkappa}^\tau$. Для функции f можно указать некоторое подмножество B множества $E_{[n/2]-\tau}$ такое, что $|B| = \varkappa$ и $f \in M_n^\tau(B)$.

Пусть

$$\tau = [n^{1-3\gamma} - 1], \quad k = [n^\gamma], \quad p =]n^\gamma + 1[, \tag{10}$$

где γ — любое фиксированное число из интервала $(0, 1/6)$, и пусть

$$N_\varkappa = C_n^{[n/2]}\, \alpha(\varkappa)\left(1 + \frac{1}{p-1}\right),$$

$$\hat{t}_1 = C_n^{[n/2]}\left(\frac{2k\tau\,(p+1)}{n-2\tau} + \frac{1}{k}\right).$$

Тогда *)

$$N_\varkappa \leqslant C_n^{[n/2]}\,(\alpha(\varkappa) + 1/n^\gamma), \tag{11}$$

$$\hat{t}_1 \leqslant c_1 C_n^{[n/2]}/n^\gamma. \tag{12}$$

*) Здесь и далее буквы c с индексами обозначают некоторые положительные постоянные.

Пусть (R, Q) — некоторое упорядоченное разбиение множества $\mathscr{E}$ на цепи. Обозначим через $N_{(R,Q),f}$ число цепей в этом разбиении, содержащих наборы из множества A, а через $t_{(R,Q),f}$ — число цепей разбиения (R, Q), которые содержат по крайней мере два набора $\alpha, \beta \in A$ таких, что $f(\alpha)=f(\beta)=1$, и на всех предшествующих цепях не существует набора ε такого, что $\varepsilon \preccurlyeq \alpha$ или $\varepsilon \preccurlyeq \beta$ и $f(\varepsilon)=1$; такие цепи будем называть *плохими*, а остальные цепи из числа $N_{(R,Q),f}$ — *хорошими*. Из лемм 2 и 3 следует, что существует такое упорядоченное разбиение (R_f, Q_f), что $N_{(R_f,Q_f),f} \leqslant N_\varkappa$, $t_{(R_f,Q_f),f} \leqslant \hat{t}_1$.

Заметим, что значения каждой функции f из $M^\tau_{n,\varkappa}$ однозначно определяются следующей информацией:

а) значениями функции f на наборах из $E_{[n/2]-\tau}$ (заданием множества B);

б) разбиением (R_f, Q_f);

в) указанием плохих цепей разбиения (R_f, Q_f);

г) заданием значений функции f на наборах всех плохих цепей;

д) заданием значений функции f на максимальных наборах каждой хорошей цепи, которые не определяются значениями функции f на наборах из всех предшествующих цепей.

Располагая такой информацией, значения искомой функции f на наборах из множества $\mathscr{E}$ можно найти с помощью следующей процедуры.

1. Находим множества B и A (по значениям функции на наборах из $E_{[n/2]-\tau}$) и полагаем значения f на наборах из B равными 1 (см. п. а)).

2. Располагаем все наборы из множества $\mathscr{E}$ в соответствии с упорядоченным разбиением (R_f, Q_f) (см. п. б)).

3. Для каждой цепи (в порядке следования цепей — см. п. 2), содержащей наборы из множества A, поступаем следующим образом.

i) Определяем значения функции f на этой цепи, а именно: если, согласно п. в), цепь плохая, то определяем значения функции на всех наборах этой цепи в соответствии с п. г); если, согласно п. в), цепь хорошая, то для максимального набора α этой цепи, где значение функции f еще не определено по монотонности единичными значениями на предшествующих цепях, определяем значение $f(\alpha)$ в соответствии с п. д); на меньших наборах этой цепи полагаем функцию равной нулю.

ii) Распространяем по монотонности единичные значения с этой цепи на все последующие цепи.

Для произвольного набора α через $l(\alpha)$ будем обозначать длину этого набора, а через $|\alpha|$ — число, двоичная запись которого представляется набором α (старшие разряды расположены справа).

На основе описанного выше задания функций из $M^\tau_{n,\varkappa}$ сопоставим монотонным функциям $f(x_1, \ldots, x_n) \in A_1$ двоичные наборы $v(f)=(v^1(f), v^2(f))$ длины $l_n(f)$ — коды функций, обладающие следующими свойствами:

1) длина l^1_n набора $v^1(f)$ не зависит от функции f и удовлетворяет соотношению

$$l^1_n = O\left(\frac{\log n}{n^\nu} C_n^{[n/2]}\right); \tag{13}$$

2) $$l(v^2(f)) \leqslant C_n^{[n/2]} \min(1, (\alpha(\varkappa) + 1/n^\nu)), \tag{14}$$

где $\varkappa$ — число наборов из $E_{[n/2]-\tau}$, на которых функция f обращается в единицу;

3) наборы $w(f)=(v(f), 0, \ldots, 0)$ одинаковой длины

$$l(w(f)) = l^1_n + C_n^{[n/2]}, \tag{15}$$

отвечающие различным функциям, различны: если $f_1 \neq f_2$, то $w(f_1) \neq w(f_2)$.

Будем называть набор $w(f)$ расширенным кодом функции f.

Набор $v^1(f)$ состоит из шести частей: $a(f)$, $b(f)$, $c(f)$, $d(f)$, $e(f)$ и $g(f)$; первые пять соответствуют п. а)—г) из приведенного выше задания функций из $M_{n,\varkappa}^{\tau}$, а $g(f)$ однозначно определяет функцию f на наборах из множества $(\mathscr{E}_1 \cup \mathscr{E}_4)$. Набор $v^2(f)$ соответствует п. д).

Опишем более подробно каждую часть набора $v(f)$.

1. Набор $a(f)$ есть список значений функции f на наборах из множества $E_{[n/2]-\tau}$. Эти значения выписываются в порядке, соответствующем упорядоченному разбиению (R^0, Q^0) множества $\mathscr{E}$ на цепи. Очевидно, что

$$l(a(f)) = C_n^{[n/2]-\tau}.$$

2. Набор $b(f)$ есть код разбиения R_f множества $\mathscr{E}$ на цепи в соответствии с процедурой, описанной в лемме 2 (мы будем называть его также кодом упорядоченного разбиения (R_f, Q^0)). Он состоит из $\tau+1$ наборов $b^1, \ldots, b^{\tau+1}$, которые являются кодами подстановок $\eta^1, \ldots, \eta^{\tau+1}$ компонент наборов, доставляющих разбиения множеств $(E_{[n/2]-\tau} \cup \cup E_{[n/2]-\tau+1}), \ldots, (E_{[n/2]-1} \cup E_{[n/2]}), \mathscr{E}_2$ соответственно, на цепи. Нетрудно показать, что каждую подстановку η^i $(1 \leqslant i \leqslant \tau+1)$ можно представить в виде произведения n транспозиций *): $\eta^i = (j_n^i, k_n^i) \ldots (j_1^i, k_1^i)$. Набор b^i есть код подстановки η^i. Он состоит из n наборов $b^{i,1}, \ldots, b^{i,n}$; каждый набор $b^{i,m}$ имеет 1 только в j_m^i-м и k_m^i-м разрядах (если $j_m^i = k_m^i = 0$, то $b^{i,m}$ состоит из одних нулей), и его длина равна n. Таким образом,

$$l(b(f)) = (\tau+1)n^2.$$

3. Набор $c(f)$ есть код перестановки блоков. Он состоит из L наборов $c^1, \ldots, c^L$. Каждый из этих наборов имеет длину L и содержит ровно одну единичную компоненту, причем единица, стоящая на i-м месте в j-м наборе, означает, что при перестановке на j-е место переходит блок с номером i. Таким образом,

$$l(c(f)) = L^2.$$

4. Для удобства последующего изложения расширим список плохих цепей в разбиении (R_f, Q_f) для каждой функции $f \in A_1(n)$ за счет некоторого количества хороших цепей до величины $\hat{t} = 2^{\lceil \log \hat{t}_1 \rceil}$.

Набор $d(f)$ есть код расположения $\hat{t}$ плохих цепей разбиения (R_f, Q_f) на $C_n^{[n/2]}$ местах (соответствующих упорядоченному разбиению (R_f, Q^0)). Описание этого кода содержится в ([4], с. 171, п. 2),

$$l(d(f)) = 2\left\lceil \hat{t} \log \frac{2C_n^{[n/2]}}{\hat{t}} \right\rceil.$$

5. Набор $e(f)$ есть код значений функции f на наборах всех плохих цепей. Описание этого кода содержится в [4],

$$l(e(f)) = \hat{t}\lceil \log(2\tau+1) \rceil.$$

6. Набор $g(f)$ есть список значений функции f на наборах из множества $(\mathscr{E}_1 \cup \mathscr{E}_4)$, выписанных в некотором фиксированном порядке. Число этих наборов равно $\sum_{0 \leqslant i < [n/2]-\tau} C_n^i + \sum_{[n/2]+\tau < i \leqslant n} C_n^i$, поэтому

$$l(g(f)) = \sum_{0 \leqslant i < [n/2]-\tau} C_n^i + \sum_{[n/2]+\tau < i \leqslant n} C_n^i.$$

---

*) Подстановка $\eta = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ называется транспозицией, если либо $i_k = k$ для всех $k = 1, \ldots, n$ (обозначение $(0, 0)$), либо существует k, j $(1 \leqslant k, j \leqslant n$ и $k \neq j)$ такие, что $i_m = k$ при $m = j$, $i_m = j$ при $m = k$ и $i_m = m$ в остальных случаях (обозначение (k, j)).

Из (10) (см. [10, с. 51]) следует, что

$$l(g(f)) = O\left(C_n^{[n/2]}\frac{\log n}{n^\nu}\right).$$

7. Набор $v^2(f)$ есть список значений функции f на максимальных наборах каждой хорошей цепи, содержащей наборы из множества A_1, где значения функции не определяются ее значениями на наборах предшествующих цепей в упорядоченном разбиении (R_f, Q_f). Эти значения выписываются в порядке, соответствующем упорядоченному разбиению (R_f, Q^0). Каждой цепи разбиения (R_f, Q_f) (имеется $N_{(R_f,Q_f),f} \leqslant \min\left(C_n^{[n/2]}, N_\varkappa\right)$ таких цепей) соответствует один разряд набора $v^2(f)$; если на цепи нет набора с указанным свойством, то в соответствующем разряде набора стоит нуль.

Таким образом,

$$l(v^2(f)) = \min\left(C_n^{[n/2]}, N_\varkappa\right)$$

($\min\left(C_n^{[n/2]}, N_\varkappa\right) - N_{(R_f,Q_f),f}$ старших разрядов набора $v^2(f)$ равны нулю).

Итак, для каждой функции f из $A_1(n)$ построены набор $v(f) = (v^1(f), v^2(f)) = (a(f), b(f), c(f), d(f), e(f), g(f), v^2(f))$ длины $l_n^1 + l(v^2(f))$ — код функции f — и набор $w(f) = (v(f), 0, \ldots, 0)$ длины $l_n^1 + C_n^{[n/2]}$ — расширенный код функции f, причем разным функциям соответствуют разные расширенные коды. Кроме того, из (9)—(12) и вышеприведенного описания наборов $a(f), \ldots, v^2(f)$ следует, что

$$l_n^1 = O\left(C_n^{[n/2]}\frac{\log n}{n^\nu}\right), \quad l(v^2(f)) \leqslant C_n^{[n/2]} \min\left(1, \alpha(\varkappa) + \frac{1}{n^\nu}\right).$$

Таким образом, выполнены условия (13)—(15).

Пусть $s = C_n^{[n/2]}(2\tau + 1) + \sum\limits_{0 \leqslant i < [n/2]-\tau} C_n^i + \sum\limits_{[n/2]+\tau < i \leqslant n} C_n^i$.

Будем называть *оператором декодирования* $\left(l_n^1 + C_n^{[n/2]}, s, (n+1)\right)$-оператор, который по набору w длины $l_n^1 + C_n^{[n/2]}$, являющемуся расширенным кодом некоторой монотонной функции $f(x_1, \ldots, x_n)$, выдает s наборов $\alpha^1, \ldots, \alpha^s$ длины $l(\alpha^i) = n+1$ $(i = 1, \ldots, s)$ таких, что выполнены условия:

1) для любого $\beta \in E$, $|\beta| \neq 0$, среди наборов α^i имеется ровно один набор $\alpha^{i_0} = \left(\alpha_1^{i_0}, \ldots, \alpha_n^{i_0}, \alpha_{n+1}^{i_0}\right)$ такой, что $\beta = \left(\alpha_1^{i_0}, \ldots, \alpha_n^{i_0}\right)$; при этом $\alpha_{n+1}^{i_0} = f(\beta)$;

2) среди наборов α^i может быть несколько (но не менее одного) наборов, у которых начала длины n состоят из одних нулей; у каждого из них значение $(n+1)$-го разряда равно либо нулю, либо $f(0, \ldots, 0)$, причем значение $f(0, \ldots, 0)$ встречается хотя бы один раз.

Основная лемма. *Существует оператор декодирования* Ψ_n *такой, что*

$$L(\Psi_n) \leqslant 2^n n^{c_0\tau}.$$

В процессе доказательства этой леммы нам понадобятся некоторые вспомогательные операторы, сведения о которых приведены в заключительном § 6.

§ 4. Реализация оператора декодирования

Будем называть матрицу, имеющую m строк и n столбцов, (n, m)-матрицей. Далее, для любой матрицы A обозначим через $(A)_j$ ее j-й столбец, через $(A)^i$ — ее i-ю строку и через $(A)_j^i$ — элемент этой матрицы, стоящий на пересечении i-й строки и j-го столбца. Будем обозначать

строку, состоящую сплошь из единиц, символом $\tilde{1}$, сплошь из нулей — символом $\tilde{0}$; столбец и матрицу, состоящие сплошь из нулей, будем обозначать соответственно через $\tilde{0}$ и (0).

Доказательство основной леммы. Построим схему S, которая реализует некоторый оператор декодирования. Схема S состоит из десяти подсхем $S_1, \ldots, S_{10}$.

Рассмотрим упорядоченное разбиение (R^0, Q^0) множества $\mathscr{E}$ на цепи $I_1, \ldots, I_{C_n^{[n/2]}}$. Поставим в соответствие цепи I_j, $1 \leqslant j \leqslant C_n^{[n/2]}$, $(n, 2\tau+1)$-матрицу $\mathbf{A}_j$ и $(1, 2\tau+1)$-матрицу $\mathbf{Y}_j$, определяемые следующим образом. Если в цепи I_j есть набор α из множества $E_{[n/2]+\tau-i+1}$, то $(\mathbf{A}_j)^i = \alpha$ и $(\mathbf{Y}_j)^i = \tilde{1}$; в противном случае $(\mathbf{A}_j)^i = \tilde{0}$ и $(\mathbf{Y}_j)^i = \tilde{0}$ $(i = 1, \ldots, 2\tau+1)$. Всему разбиению (R^0, Q^0) сопоставим $\left(nC_n^{[n/2]}, 2\tau+1\right)$-матрицу

$$\mathscr{A} = \left(\mathbf{A}_1, \ldots, \mathbf{A}_{C_n^{[n/2]}}\right)$$

и $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрицу

$$\mathscr{Y} = \left(\mathbf{Y}_1, \ldots, \mathbf{Y}_{C_n^{[n/2]}}\right).$$

1. Схема S_1 реализует эти фиксированные матрицы $\mathscr{A}$ и $\mathscr{Y}$. Очевидно, что

$$L(S_1) = O(1).$$

2. Схема S_2 по коду значений функции f на наборах из множества $E_{[n/2]-\tau}$ — набору $a(f)$ — реализует $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрицу $\mathscr{F}$. В клетках матрицы $\mathscr{F}$ стоят значения функции f на наборах из множества $\mathscr{E}$, которые определяются «по монотонности» единичными значениями функции f на наборах из $E_{[n/2]-\tau}$, причем матрица $\mathscr{F}$ согласована с матрицей $\mathscr{A}$.

Схема S_2 сначала реализует $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрицу $\mathbf{F}_0 = (0)$. Затем она образует $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрицу $\mathbf{F}_1$ следующим образом: в матрицу $\mathbf{F}_0$ переносятся на соответствующие места разряды набора $a(f)$. Далее определяются значения функции f на наборах α таких, что $\|\alpha\| = [n/2] - \tau + 1$, — строится $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрица $\mathbf{F}_2$. Для каждого такого набора α значение $f(\alpha)$ определяется как

$$f(\alpha) = \varepsilon_1 \vee \ldots \vee \varepsilon_{[n/2]-\tau+1},$$

где $\varepsilon_1, \ldots, \varepsilon_{[n/2]-\tau+1}$ — значения функции f на фиксированных наборах $\alpha^1, \ldots, \alpha^{[n/2]-\tau+1}$, непосредственно предшествующих набору α, т. е. таких, что $\alpha^i \preccurlyeq \alpha$ и $\|\alpha^i\| = \|\alpha\| - 1$ $(i = 1, \ldots, [n/2] - \tau + 1)$. Клетки матрицы $\mathbf{F}_1$, в которых стоят значения $f(\alpha^1), \ldots, f(\alpha^{[n/2]-\tau+1})$, однозначно определяются набором α. После этого аналогичная операция производится для наборов α таких, что $\|\alpha\| = [n/2] - \tau + 2$ (строится $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрица $\mathbf{F}_3$), и т. д. После 2τ шагов получим искомую матрицу $\mathscr{F} = \mathbf{F}_{2\tau+1}$.

Схема S_2 строится в соответствии с этим способом вычисления. Поэтому

$$L(S_2) \lesssim 2^n n.$$

3. Схема S_3 по коду упорядоченного разбиения (R_f, Q^0) множества $\mathscr{E}$ на цепи — набору $b(f)$ — преобразует матрицу $\mathscr{A}$ в $\left(nC_n^{[n/2]}, 2\tau+1\right)$-матрицу $\mathscr{A}_1$, а матрицы $\mathscr{Y}$ и $\mathscr{F}$ — в $\left(C_n^{[n/2]}, 2\tau+1\right)$-матрицы $\mathscr{Y}_1$ и $\mathscr{F}_1$ соответственно. Схема S_3 переставляет подматрицы (соответствующие наборам из $\mathscr{E}$) в матрицах $\mathscr{A}$, $\mathscr{Y}$ и $\mathscr{F}$, оставляя $(\tau+1)$-е строки без изменения; эти строки соответствуют наборам из множества $E_{[n/2]}$. Схе-

ма S_3 состоит из $\tau+1$ подсхем $S_3^1, \ldots, S_3^{\tau+1}$, соединенных последовательно, выходы подсхемы $S_3^{\tau+1}$ являются выходами всей схемы S_3.

Опишем подсхему S_3^i $(1 \leqslant i \leqslant \tau)$. На вход S_3^i поступают $(nC_n^{[n/2]}, 2\tau+1)$-матрица $\mathbf{U}^{i-1}$ $(\mathbf{U}^0 = \mathscr{A})$, $(C_n^{[n/2]}, 2\tau+1)$-матрицы $\mathbf{V}^{i-1}$ и $\mathbf{G}^{i-1}$ $(\mathbf{V}^0 = \mathscr{Y}, \mathbf{G}^0 = \mathscr{F})$ и набор b^i — код подстановки η^i. Выдает схема S_3^i $(nC_n^{[n/2]}, 2\tau+1)$-матрицу $\mathbf{U}^i$ и $(C_n^{[n/2]}, 2\tau+1)$-матрицы $\mathbf{V}^i$ и $\mathbf{G}^i$. Схема S_3^i фактически переставляет в матрицах $\mathbf{U}^{i-1}$, $\mathbf{V}^{i-1}$ и $\mathbf{G}^{i-1}$ подматрицы, соответствующие наборам из $\bigcup_{l=0}^{i-1} E_{[n/2]-\tau+l}$ (все такие подматрицы расположены в нижних i строках матриц $\mathbf{U}^{i-1}$, $\mathbf{V}^{i-1}$ и $\mathbf{G}^{i-1}$), оставляя верхние $2\tau+1-i$ строк в этих матрицах без изменения. Эта схема реализует два оператора $\Phi_{n,i}$ (по набору b^i и нижним $i+1$ строкам матриц $\mathbf{U}^{i-1}$, $\mathbf{V}^{i-1}$ и $\mathbf{G}^{i-1}$, см. с. 112), формируя тем самым $i+1$ нижних строк в матрицах $\mathbf{U}^i$, $\mathbf{V}^i$ и $\mathbf{G}^i$; верхние строки этих матриц определяются следующим образом:

$$(\mathbf{U}^i)^l = (\mathbf{U}^{i-1})^l, \quad (\mathbf{V}^i)^l = (\mathbf{V}^{i-1})^l, \quad (\mathbf{G}^i)^l = (\mathbf{G}^{i-1})^l$$

для всех $l = 1, \ldots, 2\tau - i$. Из леммы 8 следует, что

$$L(S_3^i) \leqslant 2^n n^{c_4}.$$

Схема $S_3^{\tau+1}$ по набору $b^{\tau+1}$ переставляет в матрицах $\mathbf{U}^\tau$, $\mathbf{V}^\tau$ и $\mathbf{G}^\tau$ подматрицы, соответствующие наборам из множества $\bigcup_{l=1}^{\tau} E_{[n/2]+l}$ (все такие подматрицы расположены в τ верхних строках матриц $\mathbf{U}^\tau$, $\mathbf{V}^\tau$ и $\mathbf{G}^\tau$), оставляя нижние $\tau+1$ строк без изменения. Эта схема строится аналогично схеме S_3^τ.

Таким образом,

$$L(S_3) = \sum_{i=1}^{\tau+1} L(S_3^i) \leqslant 2^n n^{c_5}.$$

Отметим, что $(\tau+1)$-я строка в матрице $\mathscr{A}_1$ совпадает с $(\tau+1)$-й строкой матрицы $\mathscr{A}$, т. е. наборы из множества $E_{[n/2]}$ в матрице $\mathscr{A}_1$ стоят на «тех же» местах, что и в матрице $\mathscr{A}$.

4. Схема S_4 по коду расположения плохих цепей — набору $d(f)$ — и коду значений функции f на плохих цепях — набору $e(f)$ — вычисляет $(C_n^{[n/2]}, 2\tau+1)$-матрицу $\mathbf{T}$ и набор t^1 длины $C_n^{[n/2]}$ такие, что:

1) $t_i^1 = 1$ тогда и только тогда, когда i-я цепь упорядоченного разбиения (R_f, Q^0) является плохой в упорядоченном разбиении (R_f, Q_f);

2) столбцы матрицы $\mathbf{T}$, соответствующие плохим цепям (расположенным в естественном порядке), т. е. соответствующие единицам набора t^1, содержат значения функции на этих цепях (эти значения в каждом столбце перечислены подряд сверху вниз, начиная с первой строки), а остальные столбцы состоят из нулей.

Описание этой схемы содержится в [4] (см. схемы $S_3 - S_5$ на с. 177—178). На основе оценок, приведенных для этих схем, и соотношения (12) получаем

$$L(S_4) \leqslant 2^n n^{c_6}.$$

5. Схема S_5 по матрицам $\mathbf{T}$ и $\mathscr{Y}_1$ вычисляет $(C_n^{[n/2]}, 2\tau+1)$-матрицу $\mathbf{T}_1$ следующим образом. Пусть k_j — число нулей, стоящих подряд в верхнем конце j-го столбца в матрице $\mathscr{Y}_1$, $j = 1, \ldots, C_n^{[n/2]}$. Тогда

$$(\mathbf{T}_1)_j^i = \begin{cases} 0, & \text{если } i \leqslant k_j, \\ (\mathbf{T})_j^{i-k_j} & \text{в противном случае;} \end{cases}$$

$j = 1, \ldots, C_n^{[n/2]}$. Схема S_5 сначала вычисляет числа $k_1, \ldots, k_{C_n^{[n/2]}}$, а затем сдвигает каждый столбец матрицы $\mathbf{T}$ на соответствующее число разрядов вниз. Используя (17) и (20), нетрудно показать, что

$$L(S_5) \leqslant 2^n n^{c_7}.$$

Заметим, что матрица $\mathbf{T}_1$ согласована с матрицами $\mathscr{A}_1$ и $\mathscr{Y}_1$.

6. Схема S_6 по матрицам $\mathscr{Y}_1$ и $\mathscr{F}_1$ преобразует набор $\widehat{w} = (v^2(f), 0, \ldots, 0)$*) длины $C_n^{[n/2]}$ в набор w^1 длины $C_n^{[n/2]}$ следующим образом. Пусть $i_1, \ldots, i_{s_1}$, $i_1 < i_2 < \ldots < i_{s_1} (s_1 \leqslant C_n^{[n/2]})$, — номера цепей в упорядоченном разбиении (R_f, Q^0) на цепи множества $\mathscr{E}$, которые содержат такие наборы α, что $f(\alpha)$ не определяется «по монотонности» единичными значениями функции f на наборах из множества $E_{[n/2]\to 1}$. Тогда

$$w_j^1 = \begin{cases} \widehat{w}_k, & \text{если } j = i_k,\ k = 1, \ldots, s_1; \\ 0 & \text{в противном случае.} \end{cases}$$

Схема S_6 состоит из четырех подсхем S_6^1, S_6^2, S_6^3 и S_6^4.

а) Подсхема S_6^1 вычисляет набор δ длины $C_n^{[n/2]}$ такой, что

$$\delta_j = \bigvee_{i=1}^{2\tau+1} (\mathscr{Y}_1)_j^i \,\&\, (\overline{\mathscr{F}}_1)_j^i,$$

$j = 1, \ldots, C_n^{[n/2]}$. Отметим, что $\|\delta\| = s_1$, причем $\delta_j = 1$ тогда и только тогда, когда $j = i_k$ $(1 \leqslant k \leqslant s_1)$. Очевидно, что

$$L(S_6^1) \lesssim 2^n n.$$

Пусть $p = \rceil \log C_n^{[n/2]} [$. Тогда $s_1 \leqslant 2^p \leqslant 2 \cdot C_n^{[n/2]}$.

б) Подсхема S_6^2, во-первых, образует набор γ длины $3C_n^{[n/2]}$ такой, что

$$\gamma_i = \begin{cases} \delta_i, & \text{если } 1 \leqslant i \leqslant C_n^{[n/2]}, \\ 0, & \text{если } C_n^{[n/2]} < i \leqslant 3C_n^{[n/2]} - 2^p + s_1, \\ 1 & \text{в остальных случаях} \end{cases}$$

(отметим, что $\|\gamma\| = 2^p$); во-вторых, образует набор β длины 2^p такой, что $\beta = (\widehat{w}, 0, \ldots, 0)$, и, в-третьих, по набору γ строит $(3C_n^{[n/2]}, \rceil \log (3C_n^{[n/2]}) [)$-матрицу $\mathbf{W}$ следующим образом. Пусть $j_1, \ldots, j_{2^p}$ — номера единичных разрядов в наборе γ, $j_1 < j_2 < \ldots < j_{2^p}$ $(j_k = i_k$ при $1 \leqslant k \leqslant s_1)$. Тогда

$$(\mathbf{W})_i = \widehat{0}, \text{ если } \gamma_i = 0,$$

$$|(\mathbf{W})_{j_k}| = \begin{cases} j_{k+1} - j_k & \text{при } k = 1, \ldots, 2^p - 1, \\ 3C_n^{[n/2]} - j_{2^p} & \text{при } k = 2^p. \end{cases}$$

Легко видеть, что

$$L(S_6^2) \lesssim 2^n n.$$

в) Подсхема S_6^3 реализует оператор $\Pi_{r,q}$, где $r = 3C_n^{[n/2]}$, $q = \rceil \log (3C_n^{[n/2]}) [$. По набору γ и матрице $\mathbf{W}$ она строит $(3C_n^{[n/2]},$

*) Этот набор образуют последние $C^{[n/2]}$ компонент набора $w(f)$ — расширенного кода функции f.

$]\log(3C_n^{[n/2]})[)$-матрицу $\mathbf{W}_1$ такую, что

$$(\mathbf{W}_1)_i = \begin{cases} (\mathbf{W})_{j_i} & \text{при } 1 \leqslant i \leqslant 2^p, \\ \widehat{0} & \text{в противном случае.} \end{cases}$$

Из леммы 6 следует, что

$$L(S_6^3) \leqslant 2^n n^{c_8}.$$

Обозначим через $\mathbf{W}_2(2^p,]\log(3C_n^{[n/2]})[)$-матрицу, образованную первыми 2^p столбцами матрицы $\mathbf{W}_1$.

г) Подсхема S_6^4 реализует оператор $\mathbf{T}_{2^p, 3C_n^{[n/2]}, 1}$. Она по матрице $\mathbf{W}_2$ и набору β выдает набор ε длины $3C_n^{[n/2]}$, первые $C_n^{[n/2]}$ разрядов которого образуют искомый набор w^1. Из леммы 7 следует, что

$$L(S_6^4) \leqslant 2^n n^{c_9}.$$

Таким образом,

$$L(S_6) \leqslant 2^n n^{c_{10}}.$$

7. Пусть в рассматриваемом разбиении цепей из R^0 на блоки (см. с. 97) i-й блок $(1 \leqslant i \leqslant L)$ содержит L_i цепей.

Схема S_7 преобразует матрицы $\mathscr{F}_1$, $\mathscr{Y}_1$ и $\mathbf{T}_1$ в $(C_n^{[n/2]}L, 2\tau+1)$-матрицы $\mathscr{F}_2$, $\mathscr{Y}_2$ и $\mathbf{T}_2$ соответственно, набор t^1 — в набор t^2 длины $C_n^{[n/2]}L$, а набор w^1 — в набор w^2 длины $C_n^{[n/2]}L$. Столбцы матриц $\mathscr{F}_2$, $\mathscr{Y}_2$, $\mathbf{T}_2$ и разряды наборов t^2, w^2 разбиты на L групп по $C_n^{[n/2]}$ (расположенных подряд) столбцов и соответственно наборов в каждой. Они соответствуют блокам в рассматриваемом разбиении цепей на блоки. Столбцы матриц $\mathscr{F}_1$, $\mathscr{Y}_1$ и $\mathbf{T}_1$, соответствующие наборам i-го блока (L_i столбцов), помещаются на первые L_i мест i-й группы столбцов матриц $\mathscr{F}_2$, $\mathscr{Y}_2$ и $\mathbf{T}_2$ соответственно; остальные столбцы матриц $\mathscr{F}_2$, $\mathscr{Y}_2$ и $\mathbf{T}_2$ состоят из нулей. Аналогичным образом преобразуются наборы w^1 и t^1 (см. также [4, с. 179]). Очевидно, что

$$L(S_7) = O(1).$$

8. Схема S_8 — это основная схема декодирования (ср. со схемой S_7 из [4, с. 179—180]). Эта схема в соответствии с описанным выше процессом декодирования (см. с. 99) определяет значения функции f на всех наборах из множества $\mathscr{E}$. Схема S_8 состоит из L подсхем $P_1, \ldots, P_L$, соединенных последовательно, выходы подсхемы P_L являются выходами всей схемы S_8.

Пусть $\begin{pmatrix} \eta_1 & \eta_2 & \ldots & \eta_L \\ 1 & 2 & \ldots & L \end{pmatrix}$ — перестановка блоков, определяемая кодом функции — набором $c(f) = (c^1, \ldots, c^L)$ длины L^2. Подсхема P_i преобразует $(C_n^{[n/2]}L, 2\tau+1)$-матрицу $\mathscr{D}_{i-1}$ $(\mathscr{D}_0 = \mathscr{F}_2)$ в $(C_n^{[n/2]}L, 2\tau+1)$-матрицу $\mathscr{D}_i$, в которой содержатся вычисленные после i-го этапа работы алгоритма декодирования значения функции f. Это, во-первых, значения функции на всех наборах из цепей η_1-го, ..., η_i-го блоков и, во-вторых, все значения функции, определенные «по монотонности» значениями на цепях из η_1-го, ..., η_i-го блоков и значениями функции f на наборах из множества $E_{[n/2]-\tau}$.

Заметим, что в силу (8) наборы из разных цепей внутри одного блока несравнимы. Поэтому определение значений функции на всех наборах каждого блока можно производить одновременно.

Опишем подсхему P_i $(1 \leqslant i \leqslant L)$. Она состоит из четырех подсхем $P_i^1, P_i^2, P_i^3, P_i^4$.

а) Подсхема P_i^1 по набору $c^i=(c_1^i, \ldots, c_L^i)$ длины L выбирает в матрицах $\mathscr{Y}_2$, $\mathbf{T}_2$, $\mathscr{D}_{i-1}$ и наборах t^2 и w^2 части, соответствующие η_i-му блоку. Она выдает $(C_n^{[n/2]}, 2\tau+1)$-матрицы $\mathscr{Y}_2^i$, $\mathbf{T}_2^i$ и $\mathbf{D}^{i-1}$ и наборы u^i и z^i длины $C_n^{[n/2]}$. Определим, например, матрицу $\mathscr{Y}_2^i$:

$$(\mathscr{Y}_2^i)_j = \bigvee_{k=0}^{L-1} \left(c_{k+1}^i \,\&\, (\mathscr{Y}_2)_{j+kC_n^{[n/2]}}\right),$$

$j=1, \ldots, C_n^{[n/2]}$. Матрицы $\mathbf{T}_2^i$, $\mathbf{D}^{i-1}$ и наборы u^i и z^i определяются аналогичным образом (u^i возникает из t^2, а z^i — из w^2). Подсхема P_i^1 построена в соответствии с этим определением. Поэтому, учитывая (9),

$$L(P_i^1) \leqslant 2^n n^{c_{11}\tau}.$$

б) Подсхема P_i^2 вычисляет значения функции f на всех наборах из η_i-го блока в соответствии с алгоритмом декодирования. Она по матрицам $\mathscr{Y}_2^i$ и $\mathbf{T}_2^i$ и наборам u^i и z^i преобразует матрицу $\mathbf{D}^{i-1}$ в $(C_n^{[n/2]}, 2\tau+1)$-матрицу $\mathbf{D}^i$, определяемую следующим образом:

$$(\mathbf{D}^i)_k^j = (\mathscr{Y}_2^i)_k^j \,\&\, ((\mathbf{D}^{i-1})_k^j \vee u_k^i \,\&\, (\mathbf{T}_2^i)_k^j) \vee (\mathscr{Y}_2^i)_k^j \,\&\, \bar{u}_k^i \,\&\, z_k^i \,\&$$

$$\& \begin{cases} 1, & \text{если } j=1, \\ (\mathbf{D}^{i-1})_k^{j-1}, & \text{если } 2 \leqslant j \leqslant 2\tau+1; \end{cases}$$

$k=1, \ldots, C_n^{[n/2]}$.

Подсхема P_i^2 построена в соответствии с этим определением. Поэтому

$$L(P_i^2) \leqslant 2^n n.$$

в) Подсхема P_i^3 в матрице $\mathscr{D}_{i-1}$ заменяет подматрицу $\mathbf{D}^{i-1}$ на матрицу $\mathbf{D}^i$; в результате получается матрица $\widehat{\mathscr{D}}_{i-1}$:

$$(\widehat{\mathscr{D}}_{i-1})_{j+kC_n^{[n/2]}} = (\mathscr{D}_{i-1})_{j+kC_n^{[n/2]}} \vee c_{k+1}^i \,\&\, (\mathbf{D}^i)_j$$

$(j=1, \ldots, C_n^{[n/2]};\ k=0, \ldots, L-1)$.

Подсхема P_i^3 строится в соответствии с этим определением. Поэтому

$$L(P_i^3) \leqslant 2^n n^{C_{12}\tau}.$$

г) Подсхема P_i^4 «распространяет по монотонности» значения функции f, вычисленные к этому моменту. Сначала это делается для наборов α таких, что $\|\alpha\| = [n/2] - \tau + 1$. Для каждого такого набора α «новое значение» δ' функции f определяется как

$$\delta' = \delta \vee \bigvee_{\substack{\beta: \\ \|\beta\|=[n/2]-\tau, \\ \rho(\gamma(\alpha),\gamma(\beta)) \leqslant 2\tau}} \Omega_n(\beta, \alpha) \,\&\, \varepsilon(\beta),$$

где δ — «старое значение» функции f на наборе α, $\gamma(\alpha)$ и $\gamma(\beta)$ — наборы из $E_{[n/2]}$, принадлежащие тем же цепям, что и наборы α и β соответственно, а $\varepsilon(\beta)$ — «новое значение» функции f на наборе β. Клетки матрицы $\mathscr{A}_1$, в которых стоят наборы β, однозначно определяются набором α, ибо все наборы из множества $E_{[n/2]}$ стоят на фиксированных местах в матрице $\mathscr{A}_1$. Значения δ и $\varepsilon(\beta)$ берутся из соответствующих мест матрицы $\widehat{\mathscr{D}}_{i-1}$. Заметим, что все наборы μ длины n такие, что $\mu \leqslant \alpha$ и $\|\mu\| = [n/2] - \tau$ входят в число наборов β, по которым берется дизъюнкция. Затем аналогичная операция производится для наборов α таких, что $\|\alpha\| = [n/2] - \tau + 2$ и т. д.

Подсхема P_i^4 преобразует матрицу $\widehat{\mathscr{D}}_{i-1}$ в $(C_n^{[n/2]}L, 2\tau+1)$-матрицу $\mathscr{D}_i$. Она строится в соответствии с этим способом вычисления. Поэтому, учитывая (22),

$$L(P_i^4) \leqslant 2^n n^{c_{13}\tau}.$$

Таким образом,

$$L(S_8) = \sum_{i=1}^{L} L(P_i) \leqslant 2^n n^{c_{14}\tau}.$$

Заметим, что матрица $\mathscr{F}_3 = \mathscr{D}_L$ содержит все значения функции f на наборах из множества $\mathscr{E}$.

9. Схема S_9 осуществляет переработку информации, противоположную той, которая производилась схемой S_7. Схема S_9 «сжимает» матрицу $\mathscr{F}_3$ в $(C_n^{[n/2]}, 2\tau+1)$-матрицу $\mathscr{F}_4$ следующим образом: первые L_j столбцов в j-й группе столбцов помещаются в столбцы матрицы $\mathscr{F}_4$, номера которых равны $\sum_{i=1}^{j-1} L_i + 1, \ldots, \sum_{i=1}^{j-1} L_i + L_j$ соответственно. Очевидно, что

$$L(S_9) = 0.$$

Заметим, что матрица $\mathscr{F}_4$ содержит значения функции f на всех наборах из множества $\mathscr{E}$, причем эти значения согласованы с матрицей $\mathscr{A}_1$.

10. Схема S_{10} по матрицам $\mathscr{A}_1$ и $\mathscr{F}_4$ и коду значений функции f на наборах из множества $(\mathscr{E}_1 \cup \mathscr{E}_4)$ — набору $g(f)$ — строит $(n+1, s)$-матрицу $\mathscr{A}_2$ (напомним, что $s = C_n^{[n/2]}(2\tau+1) + \sum_{0<i<[n/2]-\tau} C_n^i + \sum_{[n/2]+\tau<i\leqslant n} C_n^i$), в которой перечислены все наборы из множества E и значения функции f на них (подробнее см. [4, с. 181]).

Очевидно, что

$$L(S_{10}) = O(1).$$

Таким образом, построенная схема S реализует некоторый оператор декодирования Ψ_n. Из приведенных выше оценок сложности подсхем $S_1 - S_{10}$ следует, что

$$L(S) \leqslant 2^n n^{c_0\tau},$$

и поэтому

$$L(\Psi_n) \leqslant 2^n n^{c_0\tau}.$$

Тем самым основная лемма полностью доказана.

§ 5. Доказательство теоремы 1

Пусть $X = \{x_1, \ldots, x_n\}$. Рассмотрим произвольное семейство k-подмножеств множества X

$$\mathscr{R} = \{Y\colon\ Y \subset X,\ |Y| = k\},$$

где k — натуральное число, не превышающее n.

Следующая лемма представляет собой модификацию леммы Франкла [8].

Лемма 4. *Пусть $\mathscr{R}_1$ и $\mathscr{R}_2$ — подсемейства семейства $\mathscr{R}$ такие, что для любых Y_1, $Y_2 \in \mathscr{R}_1$ и любых Z_1, $Z_2 \in \mathscr{R}_2$ выполняются условия $Y_1 \cup Y_2 \cup Z_1 \neq X$ и $Z_1 \cup Z_2 \cup Y_1 \neq X$. Тогда если $n/3 \leqslant k \leqslant n/2$, то*

$$|\mathscr{R}_1| + |\mathscr{R}_2| \leqslant 2C_{n-1}^k.$$

Доказательство. Рассмотрим некоторое циклическое упорядочение $\mathscr{U}$ элементов множества X, например 1, 2, ..., n, 1. Пусть A

и B — совокупности таких множеств из семейства $\mathcal{R}_1$ и $\mathcal{R}_2$ соответственно, которые состоят из последовательных элементов относительно упорядочения $Ц$, и пусть $|A| = r_1$, $|B| = r_2$. Покажем, что $r_1 + r_2 \leqslant 2(n-k)$.

Если $A \cap B = \varnothing$, тогда $r_1 + r_2 \leqslant n \leqslant 2(n-k)$ (так как по условию $k \leqslant n/2$). В противном случае найдется множество $Y_0 \in \mathcal{R}_1 \cap \mathcal{R}_2$, состоящее из последовательных элементов относительно $Ц$. Без ограничения общности можно считать, что последний элемент множества Y есть n, т. е. $Y_0 = \{x_{n-k+1}, \ldots, x_n\}$. С каждым множеством Y из $(A \cup B)$, $Y \neq Y_0$, связываем число — индекс его последнего элемента, а с множеством Y_0 связываем $3k - n + 1$ чисел n, $n+1$, ..., $3k$. Таким образом, с множествами из A и из B мы связали $r_1 + 3k - n$ и $r_2 + 3k - n$ чисел соответственно, причем все эти числа принадлежат множеству $M = \{1, \ldots, 3k\}$. Разобьем M на k подмножеств $M_0, \ldots, M_{k-1}$ следующим образом: $M_i = \{i, k+i, 2k+i\}$ $(i = 0, \ldots, k-1)$.

Предположим, что в A найдутся такие множества Y_1, Y_2, Y_3, что индексы, связанные с ними, покрывают какое-либо из множеств M_i. Тогда в B нет ни одного множества Z такого, что связанный с этим множеством индекс принадлежит M_i. В противном случае множество Z вместе с какими-либо двумя из множеств Y_1, Y_2, Y_3 образуют покрытие множества X, что противоречит условиям леммы. Аналогичное рассуждение справедливо для множеств из B. Таким образом, в каждом из множеств $M_0, \ldots, M_{k-1}$ либо найдутся два различных индекса, с которыми мы не связали ни одного множества из A (или из B), либо найдется индекс, с которым мы не связали ни одного множества из A и индекс, с которым мы не связали ни одного множества из B. Поэтому $r_1 + r_2 + 2(3k - n) \leqslant 3k + 3k - 2k$, а значит, и $r_1 + r_2 \leqslant 2(n-k)$.

Подсчитаем теперь общее число пар $(Ц', Y)$ и $(Ц', Z)$, где $Ц'$ — некоторое циклическое упорядочение, а Y и Z — множества из $\mathcal{R}_1$ и $\mathcal{R}_2$ соответственно, состоящие из последовательных элементов относительно $Ц'$.

С одной стороны, каждое множество $Y \in \mathcal{R}_1$ и каждое множество $Z \in \mathcal{R}_2$ могут составить пару с $k!\,(n-k)!$ циклическими упорядочениями; а значит, семейства $\mathcal{R}_1$ и $\mathcal{R}_2$ могут составить всего $(|\mathcal{R}_1| + |\mathcal{R}_2|)\,k!\,(n-k)!$ пар. С другой стороны, каждое циклическое упорядочение по доказанному выше может составить пары не более чем с $2(n-k)$ множествами $Y \in \mathcal{R}_1$, $Z \in \mathcal{R}_2$, а всего циклических упорядочений $(n-1)!$ Поэтому

$$(|\mathcal{R}_1| + |\mathcal{R}_2|)\,k!\,(n-k)! \leqslant (n-1)!\,2(n-k),$$

$$|\mathcal{R}_1| + |\mathcal{R}_2| \leqslant 2C_{n-1}^{k}.$$

Лемма доказана.

Пусть $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ — монотонные функции. Будем называть функции f и g *связанными*, если для любых четырех наборов α, β, γ, δ таких, что $f(\alpha) = f(\beta) = g(\gamma) = g(\delta) = 0$, выполняются условия $\alpha \vee \beta \vee \gamma \neq \tilde{1}$ и $\alpha \vee \gamma \vee \delta \neq \tilde{1}$. Обозначим через $\varkappa(f)$ число наборов из $E_{[n/2]-\tau}$, на которых функция $f(x_1, \ldots, x_n)$ принимает значение 1.

Лемма 5. *Пусть $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ — связанные монотонные функции, $v(f)$ и $v(g)$ — коды функций f и g соответственно и выполняется условие $[n/2] - \tau \geqslant n/3$. Тогда имеет место соотношение*

$$l(v(f)) + l(v(g)) \leqslant \left(1 + \frac{c_2 \log n}{n^{\gamma}}\right) C_n^{[n/2]}.$$

Доказательство. На основании кодирования монотонных функций, приведенного в § 3, имеем

$$l(v(f)) \leqslant C_n^{[n/2]}\left(\min\left(1, \alpha(\varkappa(f)) + \frac{1}{n^\gamma}\right) + O\left(\frac{\log n}{n^\gamma}\right)\right),$$

$$l(v(g)) \leqslant C_n^{[n/2]}\left(\min\left(1, \alpha(\varkappa(g)) + \frac{1}{n^\gamma}\right) + O\left(\frac{\log n}{n^\gamma}\right)\right).$$

Так как по условию $[n/2] - \tau \geqslant n/3$, то из леммы 4 следует, что

$$C_n^{[n/2]-\tau} - \varkappa(f) + C_n^{[n/2]-\tau} - \varkappa(g) \leqslant 2C_{n-1}^{[n/2]-\tau}.$$

Отсюда, учитывая (10), получаем

$$\alpha(\varkappa(f)) + \alpha(\varkappa(g)) = 1 - \frac{\varkappa(f)}{C_n^{[n/2]-\tau}} + 1 - \frac{\varkappa(g)}{C_n^{[n/2]-\tau}} \leqslant$$

$$\leqslant \frac{2C_{n-1}^{[n/2]-\tau}}{C_n^{[n/2]-\tau}} = 2\frac{n - [n/2] + \tau}{n} \leqslant 1 + \frac{2(\tau+1)}{n} \leqslant 1 + \frac{2}{n^{3\gamma}}.$$

Поэтому найдется константа c_2 такая, что

$$l(v(f)) + l(v(g)) \leqslant \left(1 + \frac{c_2 \log n}{n^\gamma}\right) C_n^{[n/2]}.$$

Лемма доказана.

Пусть

$$l_n = \left]C_n^{[n/2]}\left(1 + \frac{c_3 \log n}{n^\gamma}\right)\right[+ \left]\log\left(C_n^{[n/2]}\left(1 + \frac{c_3 \log n}{n^\gamma}\right)\right)\right[, \qquad (16)$$

причем постоянная c_3 выбрана так, что $l_n \geqslant l_n^1 + C_n^{[n/2]}$.

Следствие. *Если выполняется соотношение* $[n/2] - \tau \geqslant n/3$, *то пары связанных монотонных функций* f *и* g *можно кодировать наборами* $\eta(f, g) = (\eta_1(f), v(f), v(g), 0, \ldots, 0)$ *длины* l_n, *где набор* $\eta_1(f)$ *имеет длину* $\left]\log\left(C_n^{[n/2]}\left(1 + \frac{c_3 \log n}{n^\gamma}\right)\right)\right[$ *и таков, что* $|\eta_1(f)| = l(v(f))$.

Доказательство теоремы 1. Пусть $f(x_1, \ldots, x_n)$ — произвольная монотонная функция, удовлетворяющая условию $\langle a^3 \rangle$, и

$$k =]c_0 n^{1-3\tau} \log n + 2 \log n[.$$

Определим функции $g(x_1, \ldots, x_{n-1})$ и $h(x_1, \ldots, x_{n-1})$ следующим образом:

$$g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 1),$$

$$h(x_1, \ldots, x_{n-1}) = f(\bar{x}_1, \ldots, \bar{x}_k, x_{k+1}, \ldots, x_{n-1}, 0).$$

Легко видеть, что для любого двоичного набора $\sigma = (\sigma_1, \ldots, \sigma_k)$ функции $g_\sigma(x_{k+1}, \ldots, x_{n-1}) = g(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_{n-1})$ и $h_\sigma(x_{k+1}, \ldots, x_{n-1}) = h(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_{n-1})$ являются связанными монотонными функциями. Пусть n достаточно велико*). Тогда в силу следствия из леммы 5 пару функций g_σ и h_σ можно закодировать набором $\eta(g_\sigma, h_\sigma)$ длины l_{n-k-1}.

Построим схему U, реализующую функции g и h. Она состоит из трех подсхем U_1, U_2 и U_3.

---

*) Настолько, что выполняется неравенство

$$[(n-k-1)/2] - [(n-k-1)^{1-3\tau} - 1] \geqslant (n-k-1)/3.$$

1. Подсхема U_1 по набору $\sigma=(\sigma_1, \ldots, \sigma_k)$ выдает код пары связанных монотонных функций g_σ и h_σ — набор $\eta(g_\sigma, h_\sigma)$ длины l_{n-k-1}. В силу (16) и выбора параметра k

$$\frac{\log(l_{n-k-1})}{2^k} \to 0,$$

тогда из результатов О. Б. Лупанова (см. [2, с. 105, теорема Д8]) следует, что подсхема может быть выбрана так, что

$$L(U_1) \leqslant \rho \frac{2^k l_{n-k-1}}{\log l_{n-k-1} + k}.$$

2. Подсхема U_2, во-первых, выделяет из набора $\eta(g_\sigma, h_\sigma)$ длины l_{n-k-1} два набора η_2 и η_3 длины l_{n-k-1} (реализует оператор $\Gamma_{l_{n-k-1}}$), первые $l^1_{n-k-1} + C^{[(n-k-1)/2]}_{n-k-1}$ компонент которых составляют расширенные коды функций g_σ и h_σ соответственно, и, во-вторых, реализуют два оператора декодирования Ψ_{n-k-1} для каждого из этих наборов в соответствии с основной леммой. Поэтому, учитывая (21),

$$L(U_2) \lesssim l_{n-k-1} \log(l_{n-k-1}) + 2^{n-k}(n-k)^{c_0(n-k)^{1-3\gamma}}.$$

3. Подсхема U_3 по результату работы схемы U_2 — матрицам $\mathscr{A}_2(g_\sigma)$ и $\mathscr{A}_2(h_\sigma)$ — и набору $(\sigma_{k+1}, \ldots, \sigma_{n-1})$ выдает $g(\sigma_1, \ldots, \sigma_{n-1})$ и $h(\sigma_1, \ldots, \sigma_{n-1})$ в соответствии со следующими формулами:

$$g(\sigma_1, \ldots, \sigma_{n-1}) = \bigvee \overline{(\alpha_{k+1} \oplus \sigma_{k+1} \vee \ldots \vee \alpha_{n-1} \oplus \sigma_{n-1})} \,\&\, g(\sigma_1, \ldots, \sigma_k, \alpha_{k+1}, \ldots, \alpha_{n-1}),$$

$$h(\sigma_1, \ldots, \sigma_{n-1}) = \bigvee \overline{(\beta_{k+1} \oplus \sigma_{k+1} \vee \ldots \vee \beta_{n-1} \oplus \sigma_{n-1})} \,\&\, h(\sigma_1, \ldots, \sigma_k, \beta_{k+1}, \ldots, \beta_{n-1})$$

(дизъюнкции берутся по всем наборам $\alpha=(\alpha_{k+1}, \ldots, \alpha_{n-1})$ и $\beta=(\beta_{k+1}, \ldots, \beta_{n-1})$ из соответствующих мест матриц $\mathscr{A}_2(g_\sigma)$ и $\mathscr{A}_2(h_\sigma)$, вырабатываемых операторами декодирования. Очевидно, что

$$L(U_3) \leqslant 2^{n-k} n^{c_{15}}.$$

Таким образом,

$$L(U) \leqslant \rho \frac{1}{\sqrt{2\pi}} \frac{2^n}{n^{3/2}}.$$

В силу определения функций g и h имеет место соотношение

$$f(x_1, \ldots, x_n) = x_n g(x_1 \oplus x_n \oplus 1, \ldots, x_k \oplus x_n \oplus 1, x_{k+1}, \ldots, x_{n-1}) \vee \bar{x}_n h(x_1 \oplus x_n \oplus 1, \ldots, x_k \oplus x_n \oplus 1, x_{k+1}, \ldots, x_{n-1}).$$

Поэтому

$$L(f) \leqslant L(U) + O(n) \leqslant \rho \frac{1}{\sqrt{2\pi}} \frac{2^n}{n^{3/2}}.$$

Теорема 1 доказана.

§ 6. Вспомогательные операторы

1. Оператор сложения Σ_n (по модулю 2^n) — это $(2n, n)$-оператор. Он по наборам α и β длины n выдает набор γ длины n такой, что $|\gamma| = |\alpha| + |\beta| \pmod{2^n}$. Очевидно, что

$$L(\Sigma_n) = O(n). \tag{17}$$

2. Оператор Δ_n — это $(2n, 1)$-оператор:

$$\Delta_n(\alpha, \beta) = \begin{cases} 1, & \text{если } \alpha = \beta, \\ 0 & \text{в противном случае.} \end{cases}$$

Очевидно, что

$$L(\Delta_n) = O(n). \tag{18}$$

3. Оператор транспозиции Θ_n — это $(2n, n)$-оператор. Он по наборам α и β длины n выдает набор $\gamma = \Theta_n(\alpha, \beta)$ длины n, удовлетворяющий следующим условиям: если $\|\beta\| = 2$, то оператор Θ_n устраивает перестановку разрядов набора α, соответствующих единицам набора β; если $\|\beta\| = 0$, то $\gamma = \alpha$. Легко видеть, что

$$L(\Theta_n) = O(n). \tag{19}$$

4. Оператор сдвига Λ_n — это $]\log n[+n, n)$-оператор. Он по набору α длины n и набору β длины $]\log n[$ сдвигает набор α на $|\beta|$ единиц влево, т. е. выдает набор γ длины n такой, что

$$\gamma_i = \begin{cases} \alpha_{i+|\beta|}, & \text{если } i \leqslant n - |\beta|, \\ 0 & \text{в противном случае.} \end{cases}$$

Нетрудно показать, что

$$L(\Lambda_n) = O(n \log n). \tag{20}$$

5. Оператор Γ_n — это $(]\log n[+n, 2n)$-оператор. Он по набору β длины $]\log n[$ и набору α длины n выдает наборы γ и δ длины n такие, что

$$\gamma_i = \begin{cases} \alpha_i, & \text{если } i \leqslant |\beta|, \\ 0 & \text{в противном случае,} \end{cases}$$

$$\delta_i = \begin{cases} \alpha_{i+|\beta|}, & \text{если } i \leqslant n - |\beta|, \\ 0 & \text{в противном случае.} \end{cases}$$

Нетрудно показать, что

$$L(\Gamma_n) = O(n \log n). \tag{21}$$

6. Оператор Ω_n — это $(2n, 1)$-оператор;

$$\Omega_n(\alpha, \beta) = \begin{cases} 1, & \text{если } \alpha \preccurlyeq \beta \text{ и } \|\alpha\| = \|\beta\| - 1, \\ 0 & \text{в противном случае.} \end{cases}$$

Очевидно, что

$$L(\Omega_n) = O(n). \tag{22}$$

7. Оператор $\Pi_{n,M}$ — это $(n + nM, nM)$-оператор. Он по набору α длины n преобразует (n, M)-матрицу $\mathbf{C}$ в (n, M)-матрицу $\mathbf{D}$ следующим образом. Пусть $i_1, \ldots, i_{s_2}$ — все номера единичных разрядов набора α, $i_1 < i_2 < \ldots < i_{s_2}$, тогда

$$(\mathbf{D})_j = \begin{cases} (\mathbf{C})_{i_j} & \text{при } 1 \leqslant j \leqslant s_2, \\ \widehat{0} & \text{в противном случае.} \end{cases}$$

Лемма 6.

$$L(\Pi_{n,M}) \preccurlyeq Mn \log^2 n.$$

Доказательство леммы почти дословно повторяет доказательство леммы δ2 из [3, с. 130].

8. Оператор $\mathrm{T}_{2^p,N,M}$ (здесь $2^p < N$) — это $(2^p]\log N[+2^pM, N + NM)$-оператор. Он преобразует $(2^p,]\log N[)$-матрицу $\mathbf{A}$ и $(2^p, M)$-

матрицу $\mathbf{D}$ в (N, M)-матрицу $\mathbf{B}$ и образует набор α длины N следующим образом.

Пусть $H = 2^p$ и $m_{H-j} = N - \sum_{i=0}^{j} |(\mathbf{A})_{H-i}|$ $(j = 0, \ldots, H-1)$.

Если $m_H > m_{H-1} > \ldots > m_1$, то

$$\begin{cases} (\mathbf{B})_k = \widetilde{0} & \text{и } \alpha_k = 0, \text{ если } k \neq m_i \text{ для всех } i = 1, \ldots, H;\ k = 1, \ldots, N, \\ (\mathbf{B})_{m_k} = (\mathbf{D})_k & \text{и } \alpha_{m_k} = 1, \text{ если } 1 \leqslant k \leqslant H. \end{cases}$$

Лемма 7.

$$L(\mathrm{T}_{2^p,N,M}) \leqslant pN \log N (p \log N + M).$$

Доказательство этой леммы см. в [4, с. 175].

9. Пусть k — целое число, удовлетворяющее условию $1 \leqslant k \leqslant \tau$. Рассмотрим упорядоченное разбиение (R^0, Q^0) множества $\mathscr{E}$ на $C_n^{[n/2]}$ непересекающихся цепей $I_1, \ldots, I_{C_n^{[n/2]}}$. Поставим в соответствие разбиению (R^0, Q^0) и числу k последовательность U_k^0 наборов длины n, $U_k^0 = \left(\alpha^1, \ldots, \alpha^{C_n^{[n/2]}}\right)$, следующим образом. Если в цепи I_j есть набор α из $E_{[n/2]-\tau+k}$, то $\alpha^j = \alpha$; в противном случае $\alpha^j = \widetilde{0}$, $j = 1, \ldots, C_n^{[n/2]}$.

Оператор $\Phi_{n,k}$ — это $\left((n+1)(k+1)C_n^{[n/2]} + n^2,\ (n+1)(k+1)C_n^{[n/2]}\right)$-оператор. Он по набору δ длины n^2, $(n, k+1)$-матрицам $\mathbf{A}_1, \ldots, \mathbf{A}_{C_n^{[n/2]}}$ и $(1, k+1)$-матрицам $\mathbf{Y}_1, \ldots, \mathbf{Y}_{C_n^{[n/2]}}$ выдает $(n, k+1)$-матрицы $B_1, \ldots, B_{C_n^{[n/2]}}$ и $(1, k+1)$-матрицы $Z_1, \ldots, Z_{C_n^{[n/2]}}$.

Обозначим наборы длины n, образованные первой и второй строками матрицы $\mathbf{A}_j$, через α^j и β^j соответственно, $j = 1, \ldots, C_n^{[n/2]}$. Пусть выполняются условия:

а) набор $\delta = (\delta^1, \ldots, \delta^n)$ является кодом некоторой подстановки компонент наборов η (и устроен в соответствии с описанием, данным на с. 100, т. е. набор δ^i длины n является кодом некоторой транспозиции η^i, и либо имеет две единичные компоненты, либо состоит из одних нулей, причем $\eta = \eta^n \ldots \eta^1$);

б) последовательность наборов $\left(\alpha^1, \ldots, \alpha^{C_n^{[n/2]}}\right)$ образует последовательность U_k^0;

в) среди наборов $\beta^1, \ldots, \beta^{C_n^{[n/2]}}$ каждый набор из $E_{[n/2]-\tau+k-1}$ встречается ровно один раз, причем если $\beta^j \neq \widetilde{0}$, то $\alpha^j \neq \widetilde{0}$ и $\|\beta^j\| = [n/2] - \tau + k - 1$ $(j = 1, \ldots, C_n^{[n/2]})$;

г) если $(A_j)^i = \widetilde{0}$, то $(A_j)^{i+1} = \ldots = (A_j)^{k+1} = \widetilde{0}$ и $(Y_j)^i = \ldots = (Y_j)^{k+1} = \widetilde{0}$ для всех $i = 1, \ldots, k+1$; $j = 1, \ldots, C_n^{[n/2]}$. Тогда матрицы B_j и Z_j для всех $j = 1, \ldots, C_n^{[n/2]}$ определяются следующим образом:

1) $(B_j)^1 = \alpha^j$ и $(Z_j)^1 = (Y_j)^1$;

2) если $\alpha^j = \widetilde{0}$, то $(B_j)^i = \widetilde{0}$ и $(Z_j)^i = \widetilde{0}$ для всех $i = 1, \ldots, k+1$;

3) если $\alpha^j \neq \widetilde{0}$, а $\beta^{q_j} = \widetilde{0}$, где индекс q_j $\left(1 \leqslant q_j \leqslant C_n^{[n/2]}\right)$ однозначно определяется из соотношения $\eta(\alpha^{q_j}) = \alpha^j$, то $(B_j)^i = \widetilde{0}$ и $(Z_j)^i = \widetilde{0}$ для всех $i = 2, \ldots, k+1$;

4) если $\alpha^j \neq \widetilde{0}$ и $\beta^{q_j} \neq \widetilde{0}$, то $(B_j)^i = (A_{r_j})^i$ и $(Z_j)^i = (Y_{r_j})^i$ для всех $i = 2, \ldots, k+1$, где индекс r_j $\left(1 \leqslant r_j \leqslant C_n^{[n/2]}\right)$ однозначно определяется из соотношения $\eta(\beta^{q_j}) = \beta^{r_j}$.

Лемма 8.

$$L(\Phi_{n,k}) \leqslant 2^n n^6 k.$$

Доказательство. Рассмотрим сначала случай, когда подстановка η является транспозицией, кодом которой является набор δ^1 длины n. Легко видеть, что в этом случае имеют место представления

$$(B_j)^i = \bigvee_{\substack{s,p:\\ \rho(\alpha^s,\alpha^j)\leqslant 2\\ \rho(\alpha^p,\alpha^j)\leqslant 2}} (\Delta_n(\alpha^j, \Theta_n(\alpha^s, \delta^1)) \,\&\, \Delta_n(\beta^p, \Theta_n(\beta^s, \delta^1))) \,\&\, (A_p)^i,$$

$$(Z_j)^i = \bigvee_{\substack{s,p:\\ \rho(\alpha^s,\alpha^j)\leqslant 2\\ \rho(\alpha^p,\alpha^j)\leqslant 2}} (\Delta_n(\alpha^j, \Theta_n(\alpha^s, \delta^1)) \,\&\, \Delta_n(\beta^p, \Theta_n(\beta^s, \delta^1))) \,\&\, (Y_p)^i$$

для всех $i = 2, \ldots, k+1$; $j = 1, \ldots, C_n^{[n/2]}$. Поскольку расположение наборов α^j в матрицах A_j известно, в каждую дизъюнкцию входит не более чем n^4 членов. Схема S' для частного случая оператора $\Phi_{n,k}$ строится в соответствии с этими представлениями. Поэтому, а также в силу (18) и (19) имеем $L(S') \leqslant 2^n n^5 k$.

Рассмотрим теперь общий случай. Схема S для оператора $\Phi_{n,k}$ состоит из n подсхем $S_1, \ldots, S_n$, соединенных последовательно, выходы подсхемы S_n являются выходами всей схемы S. Каждая подсхема S_i $(1 \leqslant i \leqslant n)$ реализует рассмотренный выше частный случай оператора $\Phi_{n,k}$. Она по набору δ^i — коду транспозиции η^i — преобразует $(n, k+1)$-матрицы $G_1^{i-1}, \ldots, G_{C_n^{[n/2]}}^{i-1}$ и $(1, k+1)$-матрицы $V_1^{i-1}, \ldots, V_{C_n^{[n/2]}}^{i-1}$ в $(n, k+1)$-матрицы $G_1^i, \ldots, G_{C_n^{[n/2]}}^i$ и $(1, k+1)$-матрицы $V_1^i, \ldots, V_{C_n^{[n/2]}}^i$ соответственно; при этом $G_j^0 = A_j$, $V_j^0 = Y_j$, $G_j^n = B_j$ и $V_j^n = Z_j$ для всех $j = 1, \ldots, C_n^{[n/2]}$. Таким образом, $L(S) \leqslant nL(S') \leqslant 2^n n^6 k$. Лемма доказана.

СПИСОК ЛИТЕРАТУРЫ

1. Лупанов О. Б. Об одном методе синтеза схем // Изв. вузов. Радиофизика.— 1958.— 1.— С. 120—140.
2. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14.— М.: Наука, 1965.— С. 31—110.
3. Лупанов О. Б. О синтезе схем из пороговых элементов // Проблемы кибернетики. Вып. 26.— М.: Наука, 1973.— С. 109—140.
4. Угольников А. Б. О реализации монотонных функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 31.— М.: Наука, 1976.— С. 167—185.
5. Угольников А. Б. Синтез схем и формул в неполных базисах // ДАН СССР.— 1979.— 249, № 1.— С. 60—63.
6. Угольников А. Б. О реализации функций из замкнутых классов схемами из функциональных элементов в полном базисе // ДАН СССР.— 1983.— 271, № 1.— С. 49—51.
7. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста.— М.: Наука, 1966.
8. Frankl P. On Sperner families satisfying an additional condition // J. Comb. Theory (A).— 1976.— 20.— P. 1—11. [Рус. пер.: Франкл П. О семействах Шпернера, удовлетворяющих дополнительному условию // Кибернетический сборник. Новая серия. Вып. 21.— 1984.— С. 105—116.]
9. Hansel G. Sur le nombre des fonctions booleennes montones de variables // C. R. Acad. Sci. Paris.— 262.— 1966.— P. 1088—1090. [Рус. пер.: Ансель Ж. О числе монотонных булевых функций переменных // Кибернетический сборник. Новая серия. Вып. 5.— 1968.— С. 53—57.]
10. Kleitman D. On Dedekind's problem: the number of monotone Boolean functions // Proc. of the Amer. Math. Soc.— 1969.— 21, № 3.— P. 677—682. [Рус. пер.: Клейтмен Д. О проблеме Дедекинда: число булевых монотонных функций // Кибернетический сборник. Новая серия. Вып. 7.— 1970.— С. 43—52.]
11. Post E. Two-valued iterative systems of mathematical logic.— Princeton, 1941.