

**Н. А. Карпова**

**О сложности класса  
схем из  
многополюсных  
функциональных  
элементов**

**Рекомендуемая форма библиографической ссылки:**  
Карпова Н. А. О сложности класса схем из многополюсных функциональных элементов // Математические вопросы кибернетики. Вып. 7. — М.: Наука, 1998. — С. 67–84. URL: <http://library.keldysh.ru/mvk.asp?id=1998-67>

## О СЛОЖНОСТИ КЛАССА СХЕМ ИЗ МНОГОПОЛЮСНЫХ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ\*)

Н. А. КАРПОВА

(МОСКВА)

В современной теории вычислений одной из существенных характеристик класса вычислений является сложность, которая может пониматься в самых различных смыслах. В данном случае выбирается один из модельных объектов — такой хорошо известный класс управляющих систем, как схемы из функциональных элементов. Имеется в виду реализация функций алгебры логики схемами в базисе из функциональных  $(m_1, m_2)$ -элементов, содержащих все элементы с  $m_1$  входами и  $m_2$  выходами, реализующие любые системы  $m_2$  функций от  $m_1$  переменных. Предполагается, что все элементы базиса имеют одинаковую сложность (или вес \*\*). Для такого базиса введем обозначение  $B_{m_1, m_2}$ . В качестве меры сложности схемы выбирается сумма весов всех входящих в нее элементов. Сложность схемы  $S$  в таком базисе будем обозначать через  $L_{m_1, m_2}(S)$ . Для этого класса рассматривается задача в шенноновской постановке, т. е. вводится функционал

$$L_{m_1, m_2}(f) = \min_S L_{m_1, m_2}(S)$$

и оценивается величина  $L_{m_1, m_2}(n) = \max_{f(x_1, \dots, x_n)} L_{m_1, m_2}(f)$  (ее принято называть функцией Шеннона). Работа посвящена изучению асимптотического поведения этой характеристики класса в предположении  $m_1(n), m_2(n) \rightarrow \infty$  при  $n \rightarrow \infty$ .

Очевидно, что данная постановка является нетривиальной лишь при  $m_1(n) < n$ . Как будет отмечено далее, наиболее интересный случай, на базе которого могут быть рассмотрены все другие, — это случай  $m_1 = m_2 = m$ .

Основные результаты можно сформулировать следующим образом.

Если \*\*\*)  $m = \log n + \theta$  и  $m$  достаточно отличается от  $n$ , то

$$L_{m, m}(n) \sim \frac{2^{n-m}}{m} \cdot \frac{2^\theta}{1+2^\theta}$$

(более точное соотношение — с оценкой остаточных членов — приведено далее). В частности, при  $\theta \rightarrow -\infty$  (точнее, при  $m \rightarrow \infty$ ,  $m - \log n \rightarrow -\infty$ ) величина  $L_{m, m}(n)$  ведет себя асимптотически как  $2^n / (mn)$ , а при  $\theta \rightarrow \infty$ , т. е. при  $m - \log n \rightarrow \infty$ ,  $m - n + \log n \rightarrow -\infty$ , как  $2^{n-m} / m$ .

\*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 96-01-01206).

\*\*) Ввиду равенства весов всех элементов базиса далее будем считать эти веса равными единице.

\*\*\*) Всюду в этой работе логарифмы берутся по основанию 2.

При  $m$ , близких к  $n$ , а именно, при  $m > n - \log n + 1$ ,  $m \leq n - 1$ , имеем

$$L_{m,m}(n) = 2.$$

Наконец, если  $m = n - \log n - \varphi(n)$ ,  $\varphi(n) \geq 1$ ,  $\varphi(n) < \log \log n$ , то

$$L_{m,m}(n) \asymp 2^{\varphi(n)}.$$

Результаты легко переносятся на общий случай, когда в качестве базиса берется  $B_{m_1, m_2}$  при  $m_1 \neq m_2$ .

В этой связи следует упомянуть работу [4], результаты которой можно интерпретировать как оценку по порядку функции  $L_{2m,m}(n)$ .

Среди перечисленных пяти утверждений технически наиболее сложным (в смысле громоздкости доказательства) является утверждение для  $m = \log n + \theta$ ,  $|\theta| < \log \log n$ . Именно на этом интервале изменения  $m(n)$  при получении асимптотики  $L_{m,m}(n)$  приходится учитывать природу сложности класса. Метод синтеза, позволяющий получить эту оценку, основан на извлечении информации о реализуемой функции частично из «функционального наполнения» элементов, частично из способа их соединения; при этом используется конструкция из [3]. Такой подход, комбинирующий соображения различной природы, применялся ранее в [1], где был предложен критерий «шенноновости» произвольной числовой функции.

Как следует из нижней оценки, асимптотическое поведение функции Шеннона при  $m_1 < m_2$  не зависит от  $m_2$ , и поэтому наибольший интерес представляют случаи  $m_1 = m_2$  и  $m_1 > m_2$ , а также (не рассматриваемые здесь) «неоднородные» базисы, т. е. базисы из элементов с различным числом входов и различным числом выходов.

Для получения верхних оценок величины  $L_{m_1, m_2}(n)$  в случае  $m_1 > m_2$  ( $m_1 - m_2 = c$ ) можно применять те же методы синтеза, что и в базисе  $B_{m,m}$ . При  $m_1 - m_2 \rightarrow \infty$ ,  $m_1/m_2 \rightarrow 1$  метод по существу отличается от метода для  $B_{m,m}$  лишь выбором параметров конструкции. Поэтому далее будет рассмотрен только базис  $B_{m,m}$ , результаты для которого были сформулированы. Для простоты заменим обозначения  $B_{m,m}$  и  $L_{m,m}(n)$  на  $B_m$  и  $L_m(n)$ .

Изложение доказательства верхней оценки построено таким образом, что прежде всего рассматривается более простой случай:  $m = \log n + \log \log n + \varphi(n)$ ,  $\varphi > c$ . На нем будет продемонстрирован метод, дающий асимптотику для  $L_m(n)$  и позволяющий упростить изложение «сложного» случая, т. е. метода, дающего асимптотику  $L_m(n)$  для  $m$  из окрестности  $\log n$  — точнее, при  $m = \log n + \theta$ ,  $-\log \log n \leq \theta \leq \log \log n$ . Наконец, случай, когда значения  $m$  «близки» к  $n$ , также рассмотрен отдельно. Нижняя оценка получается простыми мощностными соображениями, но именно из ее анализа следует необходимость рассмотрения трех отдельных случаев для получения соответствующей верхней оценки.

С целью упрощения изложения реализация некоторых стандартных операторов вынесена в Добавление.

Работа выполнена под руководством О. Б. Лупанова.

## § 1. Нижняя оценка $L_{m_1, m_2}(n)$

Выход  $(m_1, m_2)$ -элемента будем называть *активным в схеме  $S$* , если он является выходом схемы или присоединен к входу одного из элементов схемы. Занумеруем все элементы схемы. Число активных выходов  $i$ -го элемента обозначим  $m_{2,i}$  (выходной элемент схемы, очевидно, имеет только

один активный выход). Обозначим через  $M$  общее число всех активных выходов элементов в схеме  $S$ , т. е.  $\sum_{i=1}^{L(S)} m_{2,i}$ . Очевидно, что для всякой схемы с  $n$  входами должно выполняться соотношение

$$M \leq L m_1 - n. \quad (1)$$

Очевидно, что для любого  $i$  верно неравенство  $m_{2,i} \leq m_2$ . Поэтому

$$M \leq m_2 L. \quad (2)$$

С другой стороны, из (1) следует, что

$$M \leq m_1 L. \quad (3)$$

Обозначим  $\min(m_1, m_2)$  через  $m$ . Тогда из (2) и (3) получаем

$$M \leq mL. \quad (4)$$

**Теорема 1.** Пусть\*)  $n \rightarrow \infty$ ,  $m \rightarrow \infty$ ,  $m_1 \leq n - \log n - c_1$ ,  $c_1 > 0$ . Тогда для всякого положительного  $\epsilon$  и достаточно больших  $n$  справедливо неравенство

$$L_{m_1, m_2}(n) > \frac{2^n}{2^{m_1 m + m_1(n - m_1)}} (1 - \epsilon).$$

(Как видно из утверждения теоремы, при  $m_2 \geq m_1$  нижняя оценка  $L_{m_1, m_2}(n)$  от  $m_2$  не зависит.)

**Доказательство.** Пусть  $N(n, L, M)$  — число  $n$ -местных функций, которые реализуются схемами из  $(m_1, m_2)$ -элементов, имеющими  $M$  активных выходов элементов и сложность не более  $L$ . Поставим в соответствие схеме такого вида граф с  $n + L$  вершинами. Этот граф имеет  $L m_1$  ребер:  $n + L - 1$  ребер в остовном дереве и  $L m_1 - n - L + 1$  ребер не включены в дерево. Число способов их присоединения равно  $m + M$ , число способов приписывания  $i$ -му  $(m_1, m_2)$ -элементу функциональных символов не превосходит  $2^{2^{m_1} m_{2,i}}$ . Тогда

$$\begin{aligned} N(n, L, M) &\leq \prod_{i=1}^L 2^{2^{m_1} m_{2,i}} (n + M)^{L(m_1 - 1) - (n - 1)} c_2^{n + L - 1} = \\ &= 2^{\sum_{i=1}^L 2^{m_1} m_{2,i}} (n + M)^{L(m_1 - 1) - (n - 1)} c_2^{n + L - 1} = 2^{M 2^{m_1}} (n + M)^{L(m_1 - 1) - (n - 1)} c_2^{n + L - 1}, \end{aligned}$$

поэтому\*\*)

$$\begin{aligned} \log N(n, L, M) &\leq M 2^{m_1} + (L(m_1 - 1) - (n - 1)) \log(n + M) + c_3(n + L - 1) = \\ &= M 2^{m_1} + (L(m_1 - 1) \log(n + M) + c_3) - (n - 1)(\log(n + M) + c_3) < \\ &< M 2^{m_1} + (L(m_1 - 1) \log(n + M) + c_3) \stackrel{(4)}{<} L(2^{m_1} m + m_1 \log(n + L m) + c_3). \end{aligned} \quad (5)$$

Пусть  $N(n, L) = \sum_{M=0}^{mL} N(n, L, M)$ . Тогда

$$\log N(n, L) \leq \log(mL) + \log N(n, L, M).$$

Поэтому

$$\begin{aligned} \log N(n, L) &\leq \log(mL) + L(2^{m_1} m + m_1 \log(n + L m) + c_3) < \\ &< L(2^{m_1} m + m_1 \log(n + L m) + c_3'). \end{aligned}$$

\*) Здесь и далее в тексте константы будут обозначаться буквой  $c$  с индексами.

\*\*\*) Запись  $\stackrel{(4)}{<}$  обозначает, что соответствующее неравенство следует из соотношения (4).

Пусть  $L_{m_1, m_2}(n) < \frac{2^n}{2^{m_1}m + m_1(n - m_1)}(1 - \varepsilon)$ ,  $\varepsilon > 0$ . Тогда при  $m_1 < n - \log n - c_1$  получаем

$$\begin{aligned} \log N(n, L) &< \frac{2^n}{2^{m_1}m + m_1(n - m_1)}(1 - \varepsilon)(2^{m_1}m + m_1 \log(n + Lm) + m + c'_3) < \\ &< \frac{2^n}{2^{m_1}m + m_1(n - m_1)}(1 - \varepsilon)(2^{m_1}m + m_1(n - m_1)) = 2^n(1 - \varepsilon) < 2^n(1 - \varepsilon_1) \end{aligned}$$

и, тем самым, приходим к противоречию.

Таким образом, при  $m_2 \geq m_1$  зависимость нижней оценки от  $m_2$  пропадает.

Рассмотрим в качестве примера базис  $B_m$  и попытаемся выделить основные интервалы изменения  $m$  (как функции от  $n$ ), на которых поведение  $L_m(n)$  воспроизводится соответствующими методами синтеза, отвечающими нижней оценке.

Исследуем верхнюю оценку (5) величины  $\log N(n, L)$ , сравнивая ее с  $2^n$ . В главной части оценки (5) второе слагаемое, характеризующее «топологическую» составляющую, т. е. способ соединения элементов в схеме, мажорирует первое, связанное с «функциональным наполнением» элементов, в, грубо говоря, «дологарифмической» области изменения  $m$ ; наоборот, второе преобладает в области «постлогарифмического» роста  $m$ . В окрестности значения  $m = \log n$  оба слагаемые главной части (5) равны по порядку. Именно в силу этого нижняя оценка сложности диктует получение верхней оценки при помощи трех методов синтеза, два из которых отражают природу нижней оценки на концах рассматриваемого интервала изменения  $m$ , а в окрестности значения  $m = \log n$  нужен третий, являющийся комбинацией двух первых.

При  $m$ , близких к  $n$ , приведенная выше нижняя оценка не имеет места, и этот случай изучается отдельно. Для него получено утверждение, сформулированное в виде теоремы 3'.

## § 2. Верхняя оценка $L_m(n)$ при $m > \log n + \log \log n + c$

При  $m \leq \log n - \log \log n$  на базис  $B_m$  можно перенести общий метод синтеза [2]; он позволяет получить для функции  $L_m(n)$  оценку

$$L_m(n) = \frac{2^n}{mn} \left( 1 + O\left(\frac{\log n}{n}\right) \right).$$

Для рассмотрения другого интервала значений  $m$ , а именно, для  $n - \lfloor \log n - \varepsilon \rfloor > m > \log n + \log \log n + c$ ,  $\varepsilon > 0$ , нам понадобятся следующие понятия.

Набор  $\tilde{\gamma}$  длины  $h$  из нулей и единиц будем называть *управляющим*  $(h, l)$ -набором (первого типа), если при разбиении его на  $h$  последовательно расположенных поднаборов длины  $l$  среди них окажется ровно один ненулевой, т. е. для  $\tilde{\gamma} = (\tilde{\gamma}^1, \dots, \tilde{\gamma}^h)$  найдется такое  $i$ , что  $\tilde{\gamma}^i \neq \tilde{0}$  и  $\tilde{\gamma}^j = \tilde{0}$  при  $j \neq i$ . Очевидно, число различных управляющих  $(h, l)$ -наборов первого типа равно  $(2^l - 1)h$ .

Для синтеза удобно из класса всех  $(m, m)$ -элементов выделить подкласс  $X_m^A$  специальных  $(m, m)$ -элементов ( $m = a + l$ ), у которых для построения схемы будут использоваться лишь  $a$  выходов. При этом  $a$  входов (и  $a$  выходов) элемента будем называть *рабочими*,  $l$  (остальных) входов — *управляющими*,  $l$  (не рабочих) выходов — *свободными* или *избыточными*: они не будут присоединяться к входам других элементов, а также объявляться выходами схемы.

Функционирование элементов из  $X_m^A$  происходит следующим образом: если на управляющие входы элемента подается ненулевой набор длины  $l$ , то на рабочих выходах реализуется некоторая зависящая от управляющего набора  $(a, a)$ -функция (от рабочих входов) — множество, состоящее из  $a$  функций от  $a$  переменных; если же на  $l$  управляющих входов специального элемента подается нулевой набор, то элемент реализует тождественную  $(a, a)$ -функцию\*); таким образом, на  $l$  управляющих входов элемента могут подаваться не более  $2^l - 1$  различных ненулевых наборов, поэтому одним элементом можно реализовать не более  $2^l - 1$  различных  $(a, a)$ -функций (зависящих от рабочих входов).

Схемой типа  $X_m^{h,A}$  назовем схему, имеющую  $lh + a$  входов и  $a$  выходов, которая построена из  $h$  специальных  $(m, m)$ -элементов (описанного класса  $X_m^A$ ), соединенных последовательно:  $a$  рабочих выходов предыдущего элемента присоединяются к  $a$  рабочим входам следующего. Все управляющие входы всех элементов такой схемы и рабочие входы первого ее элемента являются входами схемы; выходы схемы — это  $a$  рабочих выходов последнего ее элемента (рис. 1).

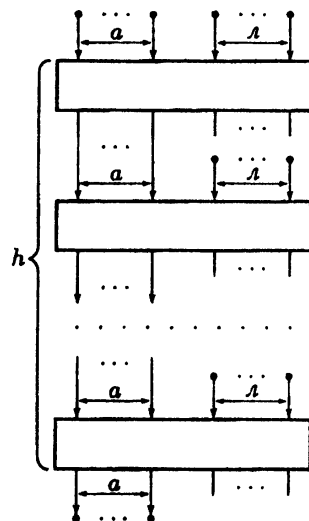


Рис. 1

Всякая схема типа  $X_m^{h,A}$  при фиксированном управляющем  $(h, l)$ -наборе  $\tilde{\gamma}$ , поданном на  $lh$  ее управляющих входов, реализует одну  $(a, a)$ -функцию — именно ту, которую реализует единственный элемент схемы, работающий в режиме 1, т. е. тот элемент, на управляющие входы которого оказался поданным (фиксированный) ненулевой поднабор управляющего  $(h, l)$ -набора (первого типа)  $\tilde{\gamma}$ .

Таким образом, схемой типа  $X_m^{h,A}$  можно реализовать не более  $(2^l - 1)h$  различных  $(a, a)$ -функций, т. е. их число не превосходит числа различных управляющих  $(h, l)$ -наборов первого типа.

Сложность схемы типа  $X_m^{h,A}$  будем обозначать  $L_m(X_m^{h,A})$ . По определению имеем

$$L_m(X_m^{h,A}) = h. \tag{6}$$

Далее нам понадобятся схемы (или блоки), построенные из произвольных (не специальных)  $(m, m)$ -элементов и реализующие следующие операторы.

Оператор  $D^{a,l}$  делит число, представленное двоичным набором длины  $\alpha$ , на число, представленное двоичным набором длины  $l$ , заключенное в отрезке  $[2^{l-1}, 2^l - 1]$ ; частное — это  $(\alpha - l + 1)$ -разрядное число, остаток представляется  $l$ -разрядным числом.

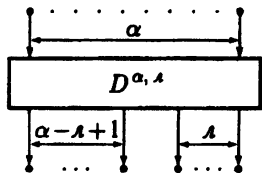


Рис. 2

Схема, реализующая оператор  $D^{a,l}$ , имеет  $\alpha$  входов и две группы выходов:  $\alpha - l + 1$  выходов, на которых реализуется частное, и  $l$  выходов, на которых реализуется остаток (рис. 2). Будем обозначать эти группы выходов через  $\tilde{\lambda}'$  и  $\tilde{\lambda}''$  соответственно.

\* ) Тем самым можно говорить о двух режимах функционирования элементов из  $X_m^A$ : режим 1 осуществляется в случае подачи на управляющие входы элемента ненулевого набора, режим 2 — если на управляющие входы подан нулевой набор.

Лемма Д1\*). Пусть  $m \geq 2$ . Тогда

$$L_m(D^{\alpha, \lambda}) \leq \begin{cases} \left\lceil \frac{\alpha - \lambda}{m - 2\lambda} \right\rceil, & m > 2\lambda, \\ \frac{8\alpha\lambda}{m}, & m \leq 2\lambda. \end{cases} \quad (7)$$

Лемма Д1'. Пусть  $n > 2$ ,  $\lambda = \log A + 1$ ,  $A = a2^a$ . Тогда

$$L_m(D^{\alpha, \lambda}) = L_m(D^{\alpha, \lceil \log A \rceil + 1}) = L_m(D^{\alpha - a, \lceil \log a \rceil + 1}). \quad (8)$$

Если  $\alpha - a \leq m$ , то  $L_m(D^{\alpha, \lambda}) = 1$ .

Оператор  $K^{(t)}$  строит по «первым»  $t$  наборам  $\tilde{\lambda}_i$  (имеется в виду лексикографическое упорядочение) длины  $\lceil \log t \rceil$  набор с одной единицей, расположенной на  $|\tilde{\lambda}_i|$ -м месте\*\*).

Схема для  $K^{(t)}$  имеет  $\lceil \log t \rceil$  входов и  $t$  выходов.

Лемма Д2'. При  $m \geq 2$  имеет место неравенство

$$L_m(K^{(t)}) \leq 8t/m. \quad (9)$$

Оператор  $\Xi^{a, b}$  по наборам  $\tilde{\alpha} = (\alpha_1, \dots, \alpha_a)$  и  $\tilde{\beta} = (\beta_1, \dots, \beta_b)$  строит набор  $\tilde{\gamma}$  (состоящий из  $a$  поднаборов  $\tilde{\gamma}^i$  длины  $b$ ):

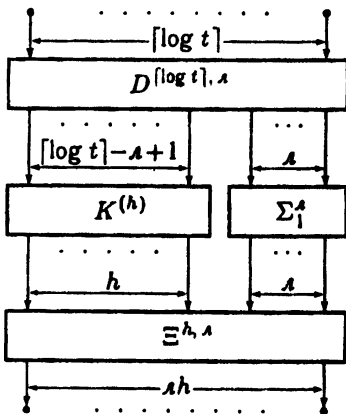
$$\tilde{\gamma} = (\tilde{\gamma}^1, \dots, \tilde{\gamma}^a) = (\gamma_1^1, \dots, \gamma_b^1, \gamma_1^2, \dots, \gamma_b^2, \dots, \gamma_1^a, \dots, \gamma_b^a)$$

следующим образом:  $\gamma_j^i = \alpha_i \& \beta_j$ . Схема для  $\Xi^{a, b}$  имеет  $a + b$  входов и  $ab$  выходов.

Лемма Д3. Пусть  $m \geq 2$ . Тогда

$$L_m(\Xi^{a, b}) \leq 3ab/m + 1. \quad (10)$$

Оператор  $Y^{t, \lambda}$  так преобразует «первые»  $t$  наборов длины  $\lceil \log t \rceil$  в управляющие  $(h, \lambda)$ -наборы (первого типа) для схемы  $X_m^{h, \lambda}$ , где  $h = \lceil t/(2^t - 1) \rceil$ , чтобы различным наборам длины  $\lceil \log t \rceil$  соответствовали различные управляющие наборы. Это осуществляется посредством деления числа, задаваемого набором длины  $\lceil \log t \rceil$ , на  $2^t - 1$  (таким образом, что первый параметр,  $h$ , управляющего  $(h, \lambda)$ -набора равен  $\lceil t/(2^t - 1) \rceil$ ), а также применения стандартных операторов  $K^{(h)}$ ,  $\Xi^{h, \lambda}$  и  $\Sigma_1^{\lambda}$  (см. Добавление). Схема для  $Y^{t, \lambda}$  имеет  $\lceil \log t \rceil$  входов и  $\lambda \lceil t/(2^t - 1) \rceil$  выходов (рис. 3),



$$L_m(Y^{t, \lambda}) \leq L_m(D^{\lceil \log t \rceil, \lambda}) + L_m(K^{(h)}) + L_m(\Xi^{h, \lambda}) + L_m(\Sigma_1^{\lambda}). \quad (11)$$

Теорема 2. Пусть  $m = \log n + \log \log n + \varphi$ ,  $\varphi > c_4$ . Тогда

Рис. 3. Схема для  $Y^{t, \lambda}$ . Параметр  $h$  равен  $\lceil t/(2^t - 1) \rceil$

$$L_m(n) \leq \frac{2^{n-m}}{m} \left( 1 + O\left(\frac{\log m}{m}\right) + O\left(\frac{n-m}{2^{n-m}}\right) \right) + O(1).$$

\*) Доказательство см. в Добавлении.

\*\*) Для набора  $\tilde{\sigma} = (\sigma_1, \dots, \sigma_m)$  обозначаем  $|\tilde{\sigma}| = \sum_{i=1}^m \sigma_i 2^{m-i}$ .

**Доказательство.** Рассмотрим табличное представление произвольной функции  $f(x_1, \dots, x_n)$ . Столбец значений функции (и соответствующих им наборов значений переменных) разобьем на куски длины  $A$  ( $A = 2^a a$ ,  $a < t$ , число  $t$  таких кусков равно  $\lceil 2^n/A \rceil$ , последний кусок имеет длину  $A'$ ,  $A' \leq A$ ). Обозначим множество наборов из  $i$ -го куска через  $\Sigma_i$ . Всякий набор  $\tilde{\sigma}$  из  $\Sigma_i$  позволяет вычислить номер куска, которому он принадлежит, по частному от деления  $|\tilde{\sigma}|$  на  $A$ ; остаток от деления определяет место набора внутри куска.

Пусть  $l = t - a$ .

Рассмотрим схему  $S$ , построенную из блоков, реализующих введенные выше операторы (рис. 4). Если на ее входы (а именно, на входы блока  $D^{n, \lceil \log A \rceil}$ ) подается любой набор из  $\Sigma_i$ , то на первой группе ( $\tilde{\lambda}'$ ) выходов этого блока реализуется один и тот же (для данного  $i$ ) набор  $\tilde{\epsilon}_i$  длины  $\lceil \log t \rceil$ , по которому на выходах блока  $Y^{t, A}$  реализуются управляющие  $(h, l)$ -наборы первого типа одного и того же вида. При этом

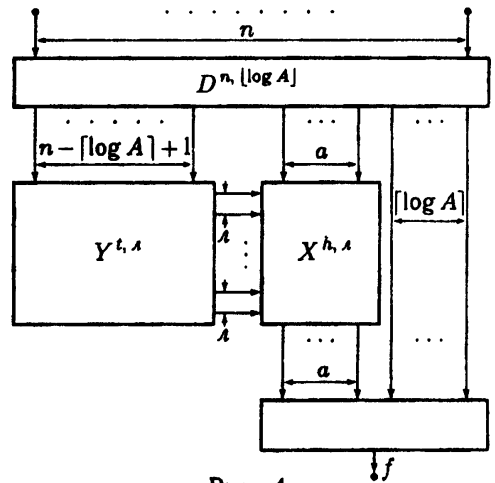


Рис. 4

$$h = \left\lceil \frac{t}{2^a - 1} \right\rceil = \left\lceil \frac{\lceil 2^n/A \rceil}{2^a - 1} \right\rceil = \left\lceil \frac{2^n}{A(2^a - 1)} \right\rceil. \quad (12)$$

Вид набора, т. е. место ненулевого поднабора, определяется частным от деления  $|\tilde{\epsilon}_i|$  на  $2^a - 1$ , а конкретный поднабор длины  $l$  определяется по остатку.

Значения первых  $a$  выходов группы  $\tilde{\lambda}'$  блока  $D^{n, \lceil \log A \rceil}$ , будучи поданными на рабочие входы  $X_m^{h, A}$ , позволяют вычислить значение  $(a, a)$ -функции (одно из  $a$  для одного куска  $\Sigma_i$ ). Значения последних  $\lceil \log a \rceil$  выходов группы  $\tilde{\lambda}'$  позволяют вычислить (одним  $(m, m)$ -элементом, если выполняется условие  $m \geq a + \lceil \log a \rceil$ ) значение  $f$  на рассматриваемом наборе. Таким образом, для всякого набора  $\tilde{\sigma}$  реализуется значение функции  $f(\tilde{\sigma})$ .

По построению имеем

$$L_m(S) = L_m(D^{n, \lceil \log A \rceil}) + L_m(Y^{t, A}) + L_m(X_m^{h, A}) + 1. \quad (13)$$

Итак,  $A = 2^a a$ ,  $m = a + l$ ,  $m > 2$ .

Будем предполагать выполнение условий  $m/a \rightarrow 1$  и  $m \geq a + \lceil \log a \rceil$  (условие на выходной элемент схемы). Для реализации  $D^{n, \lceil \log A \rceil}$  при  $A = 2^a a$  имеем (лемма Д1')  $L_m(D^{n, \lceil \log A \rceil}) = L_m(D^{n-a, \lceil \log a \rceil})$ , и  $m > 2\lceil \log a \rceil$ .

Тогда  $l \geq \lceil \log a \rceil$ , и, полагая  $l = \lceil \log m \rceil$ ,  $a = m - \lceil \log m \rceil$ , из (6)-(13) получаем

$$\begin{aligned} L_m(S) &= L_m(D^{n-a, \lceil \log a \rceil}) + L_m(D^{\lceil \log t \rceil, A}) + L_m(X_m^{h, A}) + L_m(K^{(t)}) + L_m(\Xi^{a, b}) + \\ &+ L_m(\Sigma_1^A) \stackrel{(12)}{\leq} \frac{n-m}{m-2\lceil \log m \rceil} + 8 \frac{2^{n-\lceil \log A \rceil}}{m(2^{\lceil \log m \rceil} - 1)} + 3 \frac{\log m}{m} \frac{2^{n-\lceil \log A \rceil}}{2^{\lceil \log m \rceil}} + \frac{2^n}{A(2^{\lceil \log m \rceil} - 1)} + O(1) \leq \\ &\leq \frac{2^{n-m}}{m} \left( 1 + O\left(\frac{\log m}{m}\right) + O\left(\frac{n-m}{2^{n-m}}\right) \right) + O(1). \end{aligned}$$

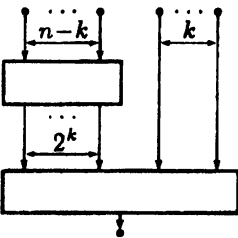
\* На самом деле набор  $\tilde{\epsilon}_i$  имеет длину  $n - \lceil \log A \rceil + 1$ , но при  $n > 3$ ,  $A \geq 6$  эти величины совпадают.



Следствие. Если  $m = n - \lfloor \log n + \varphi(n) \rfloor$ ,  $\varphi(n) \rightarrow \infty$ ,  $\varphi(n) \leq \log \log n$ , то  $L_m(n) \leq 2^{\varphi(n)} \left(1 + O\left(\frac{\log n}{n}\right)\right)$ .

Теорема 3. Пусть  $\varepsilon$  — фиксированное положительное число,  $m > n - \lfloor \log n - \varepsilon \rfloor$ . Тогда при всех достаточно больших  $n$  имеет место неравенство  $L_m(n) \leq 2$ .

Убедимся, что при выполнении условия теоремы величина  $L_m(n)$  не превосходит двух. Рассмотрим, например, схему, изображенную на рис. 5. Чтобы схемой такого вида можно было реализовать произвольную  $n$ -местную функцию, достаточно (при этом используется разложение функции по  $k$  переменным) выполнения условий



$$m \geq n - k, \quad m \geq 2^k + k. \quad (14)$$

Положим  $k = \lfloor \log n - \varepsilon \rfloor$ . Тогда первое из условий (14) совпадает с условием теоремы. Из условия теоремы следует, что

Рис. 5

$$m \geq n - \lfloor \log n - \varepsilon \rfloor \geq n - (\log n - \varepsilon) - 1 \geq n - \log n - 1. \quad (15)$$

Далее,  $2^k = 2^{\lfloor \log n - \varepsilon \rfloor} \leq n/2^\varepsilon$ , т. е.  $2^k \geq Cn$ , где  $C < 1$ , и поэтому для любых положительных констант  $C'$  и  $D'$  и достаточно больших  $n$  имеем

$$2^k \leq n - C' \log n - D'. \quad (16)$$

Положим  $C' = 2$ ,  $D' = 1$ . Тогда окончательно получаем, используя (15) и (16), что для больших  $n$  имеет место неравенство

$$k + 2^k \leq \log n + n - C' \log n - D' \leq n - \log n - 1 \leq m,$$

т. е. второе из условий (14) выполнено. Теорема доказана.

Очевидно, что при  $m < n$  одним  $(m, m)$ -элементом невозможно реализовать функцию, существенно зависящую от  $n$  переменных, поэтому  $L_m(n) \geq 2$ . Отсюда и из теоремы 3 следует

Теорема 3'. Пусть  $\varepsilon$  — фиксированное положительное число. Пусть  $m$  удовлетворяет неравенствам  $n - \lfloor \log n - \varepsilon \rfloor \leq m < n$ . Тогда при всех достаточно больших  $n$  выполняется соотношение  $L_m(n) = 2$ .

### § 3. Верхняя оценка $L_m(n)$ при $m = \log n + \theta$ , $|\theta| \leq \log \log n$

Введем еще некоторые понятия, удобные для описания метода синтеза при  $m = \log n + \theta$ ,  $|\theta| \leq \log \log n$ .

Будем рассматривать множество  $\Gamma$  наборов из нулей и единиц длины  $h\lambda = c\Lambda\lambda$ , имеющих вид  $\tilde{\gamma} = (\tilde{\gamma}^1, \dots, \tilde{\gamma}^c)$ , где каждый поднабор  $\tilde{\gamma}^i$  имеет длину  $\Lambda\lambda$ , и, в свою очередь, разбит на  $\Lambda$  поднаборов длины  $\lambda$ , т. е.  $\tilde{\gamma}^i = (\tilde{\gamma}_1^i, \dots, \tilde{\gamma}_\Lambda^i)$ .

Набор  $\tilde{\gamma}$  из  $\Gamma$  будем называть *управляющим  $c\Lambda\lambda$ -набором второго типа*, если среди его поднаборов  $\tilde{\gamma}^i$ ,  $i = 1, \dots, c$ , найдется единственный ненулевой поднабор  $\tilde{\gamma}^{j_0}$ , обладающий следующими свойствами:

1) один из его поднаборов,  $\tilde{\gamma}_0^{j_0} = (\alpha_1, \dots, \alpha_\lambda)$ , может иметь первые  $\lambda - 2$  компонент равными нулю, т. е.  $\alpha_1 = \dots = \alpha_{\lambda-2} = 0$ , лишь при  $\alpha_{\lambda-1} = \alpha_\lambda = 1$  (т. е.  $\tilde{\gamma}_0^{j_0}$  имеет вид либо  $(\tilde{0}, 1, 1)$ , либо  $(\tilde{\alpha}, \alpha_{\lambda-1}, \alpha_\lambda)$ , где  $\tilde{\alpha} \neq \tilde{0}$ );

2) все поднаборы  $\tilde{\gamma}_j^{j_0}$  при  $j \neq j_0$  имеют вид  $(\tilde{0}, 0, 1)$ .

Очевидно, число различных управляющих  $s\Lambda$ -наборов второго типа равно  $s\Lambda(2^a - 3)$ .

Набор  $\tilde{\gamma}$  из  $\Gamma$  назовем *управляющим  $s\Lambda$ -набором третьего типа*, если все его поднаборы  $\tilde{\gamma}_j^i$  имеют вид  $(0, \dots, 0, 1, 0)$ .

Прочие наборы из  $\Gamma$  (кроме управляющих наборов второго и третьего типов) рассматриваться не будут.

Для дальнейшего нам понадобится еще один подкласс класса  $(m, m)$ -элементов — класс  $\mathfrak{X}_m^a$ . Элементы из  $\mathfrak{X}_m^a$  имеют  $m - l$  рабочих выходов, которые (как и в уже рассмотренном случае) будут использоваться при построении схемы (остальные  $l$  выходов будут *свободными* или *избыточными*),  $m - l$  рабочих входов — они соединены либо с входами схемы, либо с выходами других элементов; наконец,  $l$  входов (не рабочих) всякого элемента этого класса выступают в роли *управляющих* работой этого элемента. При подаче на управляющие входы элемента этого класса набора  $\tilde{\gamma}_j^i$  длины  $l$  (поднабора управляющего набора второго или третьего типа) элемент может функционировать в одном из следующих четырех режимов в зависимости от вида поданного набора  $\tilde{\gamma}_j^i$ ,  $\tilde{\gamma}_j^i = (\tilde{\alpha}, \alpha_{\lambda-1}, \alpha_\lambda)$ .

**Режим 1.** Набор  $\tilde{\gamma}_j^i$  таков, что либо  $\tilde{\alpha} \neq \tilde{0}$ , либо  $\tilde{\gamma}_j^i = (\tilde{0}, 1, 1)$ . На рабочих выходах элемента реализуется некоторая  $(m - l, m - l)$ -функция, зависящая от набора  $\tilde{\gamma}_j^i$ .

**Режим 2.** Набор  $\tilde{\gamma}_j^i$  есть  $(\tilde{0}, 0, 0)$ . На рабочих выходах реализуется тождественная  $(m - l, m - l)$ -функция  $\{x_1, \dots, x_{m-l}\}$ .

**Режим 3.** Набор  $\tilde{\gamma}_j^i$  есть  $(\tilde{0}, 0, 1)$ . На всех рабочих выходах реализуется константа 0.

**Режим 4.** Набор  $\tilde{\gamma}_j^i$  есть  $(\tilde{0}, 1, 0)$ . На всех рабочих выходах реализуются дизъюнкции всех  $m - l$  рабочих входов элемента.

Таким образом, различие классов  $\mathfrak{X}_m^a$  и  $\mathfrak{X}_m^a$  состоит в количестве режимов функционирования элементов.

Пусть  $m = \log n + \theta$ ,  $|\theta| \leq \log \log n$ . Если значение  $m$  заключено в указанном интервале, произвольную функцию  $n$  переменных реализуем схемой, сложность которой асимптотически равна сложности одной из ее подсхем — определяемой далее подсхемы типа  $X_{aBc}$ , в которой часть информации о реализуемой функции содержится в  $(m, m)$ -элементах (как в уже рассмотренном случае), другая часть — в соединении этих элементов между собой. Такая схема функционирует в двух режимах; при работе в одном из них содержащаяся в реализуемой функции информация извлекается из реализуемых  $(m, m)$ -элементами функций, в другом — она заключена в соединениях элементов между собой.

Другие подсхемы лишь управляют этими режимами в зависимости от входного набора значений переменных реализуемой функции.

Выбор способа функционирования подсхемы  $X_{aBc}$  (извлекать ли информацию из элементов или из способа их соединения) осуществляется при помощи управляющих наборов второго или третьего типов, определяемых входным набором.

Далее рассматриваем объекты, построенные на основе  $aBc$ -схем\*) (см. [3]; сохранены обозначения этой работы). Поставим в соответствие каждому блоку  $aBc$ -схемы некоторый  $(m, m)$ -элемент из класса  $\mathfrak{X}_m^a$  с  $a$  рабочими входами и  $a$  рабочими выходами, соответствующими входам и выходам блоков,  $m = a + l$ . Соединения рабочих входов и выходов элементов соответствуют соединениям соответствующих блоков  $aBc$ -схемы. В результате получим схему, имеющую  $aBa^c$  рабочих входов,  $aBa^c$  рабочих выходов и  $lBa^c$  управляющих входов. Назовем такие схемы *схемами типа  $S_{aBc}$* .

\*) Напомним, что  $B = 2^b$ .

Схемой типа  $X_{aBc}$  (или просто схемой  $X_{aBc}$ ) будем называть такое объединение  $\nabla$  схем типа  $S_{aBc}$ , в котором все входы  $S_{aBc}$  являются входами  $X_{aBc}$ , а все выходы — выходы  $S_{aBc}$ . Можно считать, что  $(m, m)$ -элементы схемы  $X_{aBc}$  расположены в узлах прямоугольной решетки. Занумеруем их по «строкам» (или ярусам), число которых равно  $c$ , а число элементов в каждой строке есть  $\nabla B a^c = \Lambda$ . На управляющие входы  $\Lambda$  последовательно расположенных в этой нумерации (а не соединенных!) элементов (одного,  $i$ -го, яруса схемы  $S_{aBc}$ ) подаются поднаборы  $\tilde{\gamma}_j^i$ ,  $j = 1, \dots, \Lambda$ , управляющего набора.

Схема  $X_{aBc}$  функционирует в одном из двух режимов.

**Режим I.** Управляющий набор, подаваемый на управляющие входы элементов  $X_{aBc}$ , — набор второго типа. При этом во всей схеме  $X_{aBc}$  только один  $(m, m)$ -элемент работает в режиме 1, все элементы, расположенные в одном с ним ярусе, работают в режиме 3, т. е. реализуют тождественные нули, прочие элементы функционируют в режиме 2, т. е. значения на их рабочих выходах совпадают с значениями на одноименных (рабочих) входах элементов. (Считаем, что входы (выходы) элементов занумерованы, и под одноименными понимаются входы (выходы) различных элементов, имеющие одинаковые номера.)

Таким образом, на некоторых  $m - l$  выходах одной из подсхем  $S_{aBc}$ ,  $m - l = a$ , будет реализована некоторая  $(a, a)$ -функция. Значения всех прочих (одноименных с теми, где реализуется  $(a, a)$ -функция) выходов элементов этой подсхемы, являющихся выходами самой схемы, будут нулевыми, как и значения всех выходов всех прочих подсхем  $S_{aBc}$  схемы  $X_{aBc}$ . Поэтому если считать результатом работы схемы  $X_{aBc}$  в режиме I некоторую  $(a, a)$ -функцию, достаточно далее реализовать дизъюнкции всех одноименных выходов выходных элементов схемы  $X_{aBc}$ .

**Режим II.** Управляющий набор является набором третьего типа, и, следовательно, все  $(m, m)$ -элементы схемы  $X_{aBc}$  реализуют дизъюнкции входов, т. е. эта схема по существу превращается в множество схем  $S_{aBc}$ , см. [3].

**Теорема 4.** Пусть  $m = \log n + \theta$ ,  $|\theta| \leq \log \log n$ . Тогда

$$L_m(n) < \frac{2^{n-m}}{m} \cdot \frac{2^\theta}{1+2^\theta} \left( 1 + O\left(\frac{\log \log n}{\log n}\right) \right).$$

**Доказательство.** Рассмотрим представление произвольной функции, позволяющее реализовать ее схемой нужной сложности.

Произвольную  $n$ -местную функцию  $f(\tilde{r}, \tilde{p}, \tilde{x}, \tilde{y})$ , где  $\tilde{r} = (r_1, \dots, r_d)$ ,  $\tilde{p} = (p_1, \dots, p_l)$ ,  $\tilde{x} = (x_1, \dots, x_k)$ ,  $\tilde{y} = (y_1, \dots, y_b)$ ,  $d + l + k + b = n$ , разложим по  $d$  переменным:  $f(\tilde{r}, \tilde{p}, \tilde{x}, \tilde{y}) = \bigvee_{\tilde{\mu}} K_{\tilde{\mu}}(\tilde{r}) f(\tilde{\mu}, \tilde{p}, \tilde{x}, \tilde{y})$ .

Множество  $\{\tilde{\mu}\}$  наборов значений переменных  $\tilde{r}$  разобьем на два подмножества:  $M_{\Delta_1}$  и  $M_{\Delta_2}$ . Подмножество  $M_{\Delta_1}$  содержит  $\Delta_1 = \lceil 2^{d+\theta} / (1+2^\theta) \rceil$  наборов, подмножество  $M_{\Delta_2}$  состоит из  $\Delta_2 = 2^d - \lceil 2^{d+\theta} / (1+2^\theta) \rceil$  наборов.

В соответствии с этим разложением таблица значений функции разобьется на две части. При реализации части  $T_{\Delta_1}$  (соответствующей множеству  $M_{\Delta_1}$  и содержащей  $2^{n-d} \Delta_1$  строк) подсхема  $X_{aBc}$  будет работать в режиме I. При реализации другой части —  $T_{\Delta_2}$  — в режиме II, как в [3].

Множество наборов значений переменных  $(\tilde{p}, \tilde{x}, \tilde{y})$ , соответствующее одному набору  $\tilde{\mu}$  из  $M_{\Delta_1}$ , т. е. соответствующее множеству  $2^{n-d}$  строк таблицы, разбивается следующим образом. В наборе длины  $n - d$  выбираем  $n - d - \delta - a$  старших разрядов (набор  $\tilde{\omega}$ ), оставшиеся разряды разбиваем на поднаборы длины  $\delta$  и  $a$ . Часть таблицы  $T_{\Delta_1}$ , соответствующая набору

$(\tilde{\mu}, \tilde{\omega})$ , т. е. часть, задаваемая  $2^{d+a}$  наборами, имеющими фиксированное начало  $(\tilde{\mu}, \tilde{\omega})$ , разбивается на полосы ширины  $a$ )  $A$ ,  $A = a2^a$ . Поэтому число таких полос для одного фиксированного набора  $(\tilde{\mu}, \tilde{\omega})$  равно  $\lceil 2^d/a \rceil$ . Каждая полоса представляет одну  $(a, a)$ -функцию, и в таблице  $T_{\Delta_1}$  в этом смысле содержится не более  $\Delta_1 2^{n-d-d-a} \lceil 2^d/a \rceil$  различных  $(a, a)$ -функций.

Для реализации одной  $(a, a)$ -функции достаточно одного  $(m, m)$ -элемента схемы  $X_{aBc}$  при одном управляющем наборе длины  $l$ , число таких наборов не превышает  $2^l - 3$ ; следовательно, один такой элемент всего реализует не более  $2^l - 3$  различных  $(a, a)$ -функций, и при выбранном базисе такое их число реализовать возможно. Таким образом, если схема  $X_{aBc}$  содержит  $L_{aBc}$  элементов, реализующих  $(a, a)$ -функции, то ею можно реализовать  $(2^l - 3)L_{aBc}$  различных  $(a, a)$ -функций. Поэтому для реализации  $T_{\Delta_1}$  требуем выполнения соотношения

$$(2^l - 3)L_{aBc} \geq \Delta_1 2^{n-d-d-a} \lceil 2^d/a \rceil. \quad (17)$$

Подтаблица  $T_{\Delta_1}$  будет реализована той же  $X_{aBc}$ -схемой в режиме II. Представим эту подтаблицу для схемной реализации следующим разбиением. Соответствующее каждому набору  $\tilde{\mu}$  из  $T_{\Delta_1}$  (упорядоченное) множество  $\{\tilde{\lambda}\}$  наборов длины  $l$  (их  $2^l$  штук) значений переменных  $\tilde{p}$  разобьем на подмножества  $Q_x$  мощности  $a^c$  (последнее из них может быть меньшей мощности), где  $c = \lceil 2^k/(s(a-1)) \rceil$ ,  $s$  — некоторый параметр, значение которого будет определено далее);  $x = 1, \dots, \lceil 2^l/a^c \rceil$ . При таком соответствии множество строк таблицы будет разбито на куски величины  $a^c 2^k 2^b$  (кроме некоторых — последних в соответствующих частях разбиения). Каждая пара  $(\tilde{\mu}, x)$  задает некоторую подфункцию, и она будет реализовываться далее  $S_{aBc}$ -схемой, соответствующей  $aBc$ -схеме  $S_{\mu x}$ , см. [3, с. 17]; число таких подсхем, очевидно, есть  $\nabla = \Delta_2 \lceil 2^l/a^c \rceil$ , сложность каждой равна  $c 2^b a^c$ . Двоичный набор  $\tilde{\lambda}$  длины  $l$  при этом внутри куска можно закодировать  $a$ -ичным набором  $\tilde{\alpha}$  длины  $s$ . Множество наборов  $\tilde{\sigma}$  длины  $k$ , соответствующее одному набору  $\tilde{\lambda}$ , разобьем на подмножества  $\Sigma_\gamma$  мощности  $(a-1)s$ ,  $\gamma = 1, \dots, \lceil 2^k/((a-1)s) \rceil$ . Каждое  $\Sigma_\gamma$  разобьем на подмножества  $\Sigma_{\gamma\delta}$  мощности  $s$ ,  $\delta = 1, \dots, a-1$ . Таким образом, вся таблица  $T_{\Delta_1}$  окажется разбитой на полосы ширины  $2^b s$ . В каждой полосе  $\Sigma_{\gamma\delta}$  набору  $(\tau_1, \dots, \tau_b)$  соответствуют  $s$  различных наборов  $(\sigma_{k-\lfloor \log_2 s \rfloor - 1}, \dots, \sigma_k)$ . Каждую полосу  $\Sigma_{\gamma\delta}$  можно интерпретировать как функцию  $F(x, y)$  из  $\mathfrak{F}_{\Sigma_{\gamma\delta}}$ , см. [3]. Всякую специальную функцию из  $\mathfrak{F}_{\Sigma_{\gamma\delta}}$  можно представить через другую функцию этого множества как подстановку над  $\tilde{\tau}$ .

Сложность схемы  $X_{aBc}$  мы можем оценить, исходя из представления  $T_{\Delta_1}$ , следующим образом:

$$L_m(X_{aBc}) = \nabla L_m(S_{\mu x}) = \nabla c 2^b a^c = \Delta_2 c 2^b a^c \lceil 2^l/a^c \rceil$$

или

$$L_{aBc} = \Delta_2 c 2^b a^c \lceil 2^l/a^c \rceil. \quad (18)$$

Отсюда и из (17) получаем

$$\Delta_2 c 2^b a^c \lceil 2^l/a^c \rceil \geq \Delta_1 2^{n-d-d-a} \lceil 2^d/a \rceil / (2^l - 3). \quad (19)$$

\* ) Здесь и далее при разбиениях последнее множество может оказаться меньшим.

Для построения схемы  $S$  (рис. 6), реализующей произвольную  $n$ -местную функцию  $f$ , рассмотрим следующие подсхемы, которые построены из блоков, реализующих приведенные в Добавлении операторы.

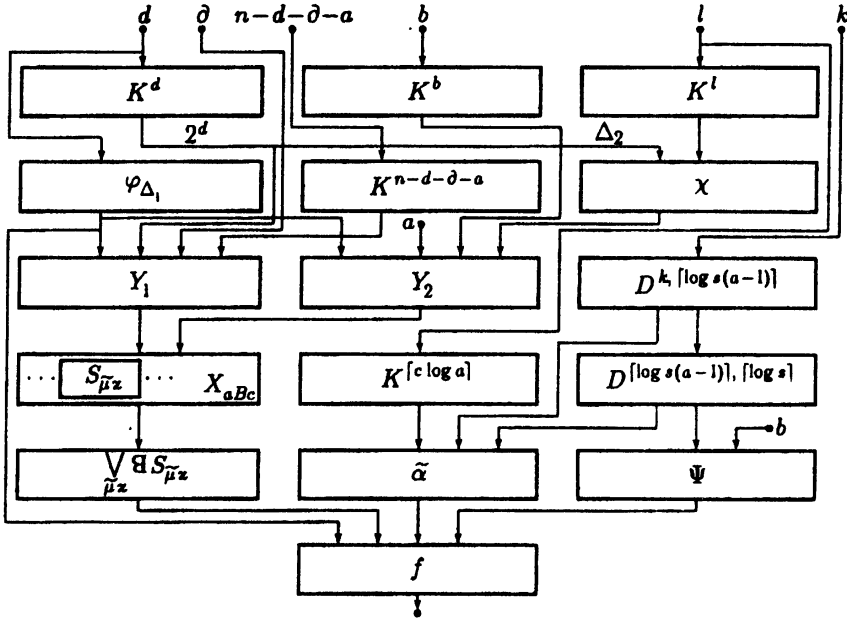


Рис. 6

Подсхема  $K^d$  своими входами имеет  $d$  первых (старших) входов схемы и строит систему конъюнкций, соответствующую входному набору  $\tilde{\mu}$ . По лемме 2 имеем

$$L_m(K^d) \leq 2^{d+2}/m. \tag{20}$$

Подсхема  $K^{n-d-d-a}$  реализует по следующим  $n-d-d-a$  входным разрядам схемы соответствующую входному набору  $\tilde{\omega}$  систему конъюнкций. По лемме 2 имеем

$$L_m(K^{n-d-d-a}) \leq 2^{n-d-d-a+2}/m. \tag{21}$$

Подсхема  $\varphi_{\Delta_1}$  строит характеристическую функцию множества  $M_{\Delta_1}$  по  $d$  входам схемы. Она имеет один выход и такова, что

$$L_m(\varphi_{\Delta_1}) \leq c_5 d / (m - 1). \tag{22}$$

Подсхема  $Y_1$  реализует управляющие наборы для управляющих входов схемы  $X_{aBc}$ ; это управляющие наборы второго или третьего типа в зависимости от принадлежности набора  $\tilde{\mu}$  к  $M_{\Delta_1}$  или к  $M_{\Delta_2}$ . Ее входы: один вход — выход подсхемы  $\varphi_{\Delta_1}$ ,  $2^d$  входов — конъюнкции, соответствующие набору  $\tilde{\mu}$  (выходы подсхемы  $K^d$ ),  $2^{n-d-d-a}$  выходов — конъюнкции, соответствующие набору  $\tilde{\omega}$  (выходы подсхемы  $K^{n-d-d-a}$ ),  $d$  входных переменных. Подсхема  $Y_1$  имеет  $L_m(X_{aBc})l$  выходов. Каждый  $(m, m)$ -элемент может реализовать не более  $\lfloor m/l \rfloor$  поднаборов длины  $l$ . Потребуем выполнения условия

$$\partial + \lfloor m/l \rfloor + 3 \leq m. \tag{23}$$

Подсхема  $Y_1$  построена из трех ярусов  $(m, m)$ -элементов. Первый реализует (по наборам  $\tilde{\mu}$  и  $\tilde{\omega}$  — точнее, по соответствующим этим наборам конъюнкциям — и по  $d$  входным переменным) набор длины  $sLl$

с единственным ненулевым поднабором длины  $l$ , место которого определяется наборами  $\tilde{\mu}$  и  $\tilde{\omega}$ , т. е. управляющий  $(c\Lambda, l)$ -набор первого типа. На входы каждого из  $(m, m)$ -элементов этого яруса подаются  $d$  входных переменных, а также

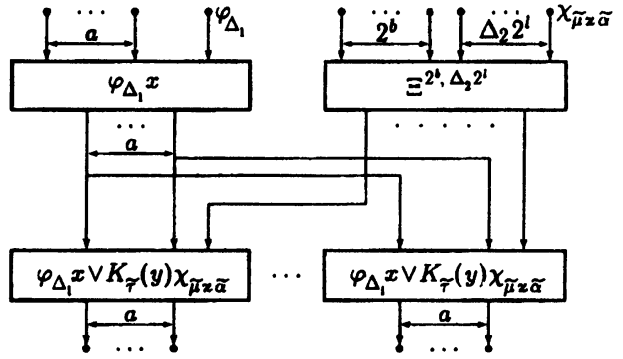


Рис. 7

часть выходов подсхемы  $K_d$  и часть выходов подсхемы  $K^{n-d-d-a}$  таким образом, чтобы на выходах этого элемента реализовалась часть  $(c\Lambda, l)$ -набора — а именно,  $\lfloor m/l \rfloor$  поднаборов длины  $l$ . При выполнении (23) это возможно. Первый ярус имеет  $L_m(X_{aBc})l = c\Lambda l$  выходов, а число элементов не превышает  $c_6 \lfloor L_m(X_{aBc})l/m \rfloor$ . Вы-

ходы первого яруса разбиты на  $s$  подмножеств, каждое из которых содержит  $\Lambda l$  выходов. Второй ярус строит дизъюнкции всех выходов для каждого из этих подмножеств, и  $s$  выходов второго яруса, только один из которых — единица, позволяют элементам третьего яруса реализовать по  $\varphi_{\Delta_1}$  (если  $\varphi_{\Delta_1} = 1$ ) и выходам первого яруса управляющий  $(c\Lambda, l)$ -набор второго типа. При  $\varphi_{\Delta_1} = 0$  этот признак, поданный на входы всех элементов третьего яруса, заставляет независимо от результатов работы первых двух ярусов строить управляющий  $(c\Lambda, l)$ -набор третьего типа. Таким образом,

$$L_m(Y_1) \leq c_7 L_m(X_{aBc})l/m = L_m(X_{aBc})O(l/m). \tag{24}$$

Подсхема  $K^l$  имеет своими входными переменными  $\tilde{p}$ ; по лемме Д2 для нее имеем

$$L_m(K^l) \leq 2^{l+2}/m. \tag{25}$$

Подсхема  $K^{\lceil \log a \rceil}$  имеет своими входными переменными  $p_1 - \lceil \log a \rceil, \dots, p_l$ ; по лемме Д2 для нее имеем

$$L_m(K^{\lceil \log a \rceil}) \leq 2^{\lceil \log a \rceil}/m. \tag{26}$$

Подсхема  $\chi$  строит характеристические функции  $\chi_{\tilde{\mu}\tilde{\omega}}$  интервалов схем  $S_{\tilde{\mu}\tilde{\omega}}$ . Входы:  $\Delta_2$  (первые, старшие  $\Delta_2$  выходов схемы  $K^d$ ),  $2^l$  выходов подсхемы  $K^l$ . Выходы:  $\Delta_2^{2^l}$  штук. Эта схема реализует оператор  $\Xi^{\Delta_2, 2^l}$ . По лемме Д3 имеем

$$L_m(\chi) \leq 3\Delta_2^{2^l}/m + 1. \tag{27}$$

Подсхема  $K^b$  реализует конъюнкции  $b$  переменных  $\tilde{y}$ ; по лемме Д2 для нее имеем

$$L_m(K^b) \leq 2^{b+2}/m. \tag{28}$$

Подсхема  $Y_2$  готовит информацию для рабочих входов схемы  $X_{aBc}$  (рис. 7). Ее входы:  $a$  переменных (входы схемы  $S$  — для рабочих входов схемы  $X_{aBc}$  в случае  $\varphi_{\Delta_1} = 1$ ),  $2^b$  входов — выходы схемы  $K^b$ , один вход — выход схемы  $\varphi_{\Delta_1}$ , характеристические функции  $\chi_{\tilde{\mu}\tilde{\omega}}$  интервалов схем  $S_{\tilde{\mu}\tilde{\omega}}$ ; выходы:  $\Lambda a = c_3 L_m(X_{aBc})a/m$  штук. Для сложности этой подсхемы имеем

$$L_m(Y_2) \leq \frac{a+1}{m} + 3 \frac{\Delta_2^{2^b+1}}{m} + \frac{(m-a)\Delta_2^{2^b+1}}{m} \leq c_9 \frac{L_m(X_{aBc})}{c}. \tag{29}$$

Подсхема  $D^{k \lceil \log s(a-1) \rceil}$  имеет  $k$  входов (входы схемы — значения переменных  $\tilde{x}$ ) и две группы выходов: одна представляет набор  $\tilde{\gamma}$ , на выходах второй — информация для построения набора  $\tilde{\delta}$  и числа  $s$ ; по лемме Д1 имеем

$$L_m(D^{k \lceil \log s(a-1) \rceil}) \leq \begin{cases} \left\lceil \frac{k - \lceil \log s(a-1) \rceil}{m - 2 \lceil \log s(a-1) \rceil} \right\rceil, & m > 2 \lceil \log s(a-1) \rceil, \\ 8 \frac{k \lceil \log s(a-1) \rceil}{m-2}, & m \leq 2 \lceil \log s(a-1) \rceil. \end{cases} \tag{30}$$

Подсхема  $D^{[\log s(a-1)], [\log s]}$ . Ее входы —  $[\log s(a-1)]$  выходов подсхемы  $D^k, [\log s(a-1)]$ , а на выходах реализуются набор  $\tilde{\delta}$  и число  $s$ . По лемме Д1 имеем

$$L_m(D^{[\log s(a-1)], [\log s]}) \leq \begin{cases} \left\lceil \frac{[\log s(a-1)] - [\log s]}{m - 2[\log s]} \right\rceil, & m > 2[\log s], \\ 8 \frac{[\log s(a-1)][\log s]}{m - 2}, & m \leq 2[\log s]. \end{cases} \quad (31)$$

Подсхема  $\bigvee_{\tilde{\mu}z} \mathfrak{B}S_{\tilde{\mu}z}$  имеет  $\nabla 2^b a^c (m - l) = \Delta_2 2^b a^c [2^l / a^c] (m - l)$  входов,  $2^b a^c$  выходов и реализует дизъюнкцию одноименных выходов\*) схем  $S_{\tilde{\mu}z}$ . Для ее сложности имеем

$$L_m\left(\bigvee_{\tilde{\mu}z} \mathfrak{B}S_{\tilde{\mu}z}\right) \leq [\Delta_2 2^b a^c [2^l / a^c] (m - l) / m] \leq L_m(X_{aBc}) O(1/c). \quad (32)$$

Подсхема  $\tilde{\alpha}$  реализует оператор  $\tilde{\alpha}_{\tilde{\gamma}, s}(a)$  (лемма Д4), причем

$$L_m(\tilde{\alpha}) \leq (c_{10} c \log a) / m. \quad (33)$$

Подсхема  $\Psi$  реализует функцию  $\psi(y)$ , см. [3], причем

$$L_m(\Psi) \leq O(cb^2 a^{c+s} / m). \quad (34)$$

Подсхема  $f$  по выходам схем  $\bigvee_{\tilde{\mu}z} \mathfrak{B}S_{\tilde{\mu}z}$ ,  $\tilde{\alpha}$ ,  $\varphi_{\Delta_1}$  и  $\Psi$  строит функцию  $f$  с оценкой сложности

$$L_m(f) \leq (c_{11} c \log a) / m. \quad (35)$$

Из (17)–(35) получаем

$$\begin{aligned} L_m(S) \leq & L_{aBc} \left(1 + O\left(\frac{1}{c}\right) + O\left(\frac{l}{m}\right) + \frac{2^{d+2}}{m} + \frac{2^{n-d-\partial-a+2}}{m} + \right. \\ & + O\left(\frac{d}{m}\right) + \frac{2^{l+2}}{m} + 2\left(3\frac{\Delta_2 2^l}{m} + 1\right) + \frac{2^{b+2}}{m} + O\left(\frac{c \log a}{m}\right) + O\left(\frac{cb^2 a^{c+s}}{m}\right) + \\ & \left. + 8\frac{k[\log s(a-1)]}{m-2} + 8\frac{[\log s(a-1)][\log s]}{m-2}\right). \end{aligned} \quad (36)$$

По условию,  $m = \lfloor \log n + \theta \rfloor$ ,  $c = \lceil 2^k / (sa) \rceil$ ,  $\Delta_1 = \lceil 2^{d+\theta} / (1 + 2^\theta) \rceil$ ,  $\Delta_2 = 2^d - \Delta_1$ ,  $\partial \leq m(1 - 1/l) - 3$ ,  $a = m - \lfloor \log m \rfloor$ ,  $l = \lfloor \log m \rfloor$ . Тогда из (18) имеем

$$L_{aBc} \leq \frac{2^\theta}{1 + 2^\theta} \cdot \frac{2^{n-m}}{m} \left(1 + O\left(\frac{\log m}{m}\right)\right). \quad (37)$$

Выбираем  $k = \lfloor \frac{3}{2} \log n \rfloor$ ,  $s = \lfloor n - 3 \frac{\log \log n}{\log n} \sqrt{n} \rfloor$ ,  $b = \lfloor n - 2 \frac{\log \log n}{\log n} \sqrt{n} \rfloor$ ,  $d = \lfloor \log n \rfloor$ . Тогда  $l = 2 \frac{\log \log n}{\log n} \sqrt{n} - O(\log n)$ . При выбранных значениях параметров соотношение (17) выполняется. Из (36), (37) получаем

$$\begin{aligned} L_m(S) \leq & \frac{2^\theta}{1 + 2^\theta} \cdot \frac{2^{n-m}}{m} \left(1 + O\left(\frac{\log m}{m}\right)\right) \left(1 + o\left(\frac{1}{n}\right) + O\left(\frac{\log n}{\sqrt{n}}\right) + O\left(\frac{\log m}{m}\right)\right) = \\ & = \frac{2^\theta}{1 + 2^\theta} \cdot \frac{2^{n-m}}{m} \left(1 + O\left(\frac{\log m}{m}\right)\right). \end{aligned}$$

Таким образом,  $L_m(n) \leq \frac{2^\theta}{1 + 2^\theta} \cdot \frac{2^{n-m}}{m} \left(1 + O\left(\frac{\log \log n}{\log n}\right)\right)$ , и теорема доказана.

\*) По построению только одна схема  $S_{\tilde{\mu}z}$  может иметь ненулевые выходы.

### Добавление

Оператор  $D^{\alpha, l}$  делит число, представленное двоичным набором длины  $\alpha$ , на число, представленное двоичным набором длины  $l$ , заключенное в отрезке  $[2^{l-1}, 2^l - 1]$ . При этом частное — это  $(\alpha - l + 1)$ -разрядное число, а остаток представляется  $l$ -разрядным числом.

Лемма Д1. Пусть  $m > 2$ . Тогда

$$L_m(D^{\alpha, l}) \leq \begin{cases} \left\lceil \frac{\alpha - l}{m - 2l} \right\rceil, & m > 2l, \\ 8 \frac{\alpha l}{m - 2}, & m \leq 2l. \end{cases}$$

Доказательство. Схема для  $D^{\alpha, l}$  строится из  $(m', m')$ -блоков (где  $m' \geq m$ , а значение  $m'$  будет определено далее)  $\Lambda_1, \dots, \Lambda_\beta$ , осуществляющих деление  $(m' - l)$ -разрядного числа на число, не превосходящее  $2^l - 1$  и не меньшее  $2^{l-1}$ , т. е. на число, представленное  $l$  разрядами, причем старший разряд равен единице\*), см. рис. Д1.

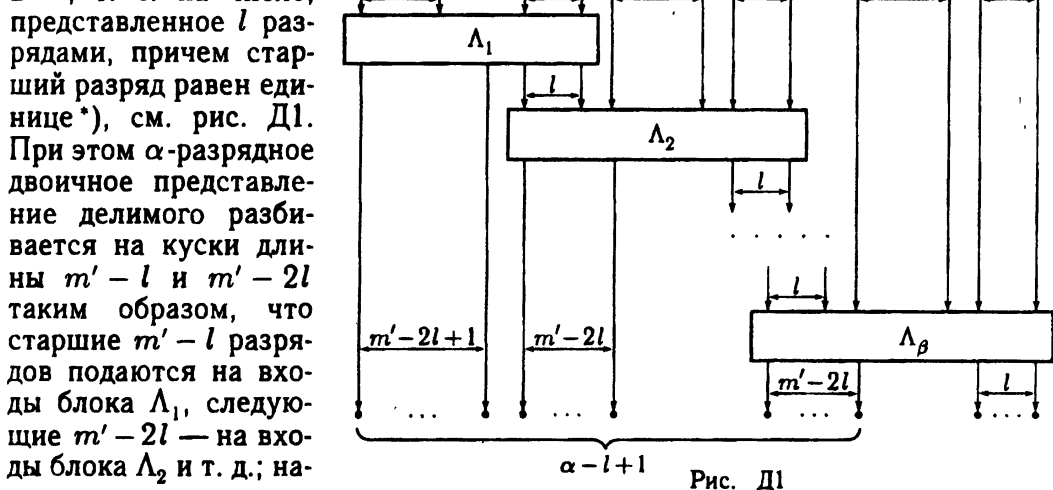


Рис. Д1

При этом  $\alpha$ -разрядное двоичное представление делимого разбивается на куски длины  $m' - l$  и  $m' - 2l$  таким образом, что старшие  $m' - l$  разрядов подаются на входы блока  $\Lambda_1$ , следующие  $m' - 2l$  — на входы блока  $\Lambda_2$  и т. д.; наконец, последние  $\alpha - (\beta - 2)(m' - 2l) - m' + l$  разрядов подаются на входы блока  $\Lambda_\beta$ . На старшие  $l$  входов блоков  $\Lambda_i, i = 2, \dots, \beta$ , при этом подаются  $l$  разрядов остатка от деления, полученных на выходах блока  $\Lambda_{i-1}$ . Таким образом, каждый блок  $\Lambda_i, i = 1, \dots, \beta$ , оперирует с  $(m' - l)$ -разрядным делимым. Кроме того, на входы каждого блока  $\Lambda_i$  подаются  $l$  разрядов делителя. Выходы каждого блока разбиваются на две группы:  $\tilde{\lambda}'_i$  для реализации частного и  $\tilde{\lambda}''_i$  для реализации остатка. Группа  $\tilde{\lambda}'_i$  состоит из  $m' - 2l$  выходов (для блока  $\Lambda_1$  это  $m' - 2l + 1$  выходов), группа  $\tilde{\lambda}''_i$  — из  $l$  выходов. Блоки соединены последовательно:  $l$  выходов предыдущего блока ( $\tilde{\lambda}''_{i-1}$ ) соединены с  $l$  входами (фактически старшими) следующего. Таким образом, вся схема на  $\alpha - l + 1$  выходах реализует частное, а на  $l$  — остаток. Очевидно, что

$$L_m(D^{\alpha, l}) \leq \beta L_m(\Lambda_i), \quad \beta = \lceil (\alpha - l) / (m' - 2l) \rceil. \quad (38)$$

При  $m > 2l$  выбираем  $m' = m$ . В этом случае  $\Lambda_i$  есть  $(m, m)$ -элемент,  $L_m(\Lambda_i) = 1$ , и  $L_m(D^{\alpha, l}) \leq \lceil (\alpha - l) / (m' - 2l) \rceil$ .

При  $m \leq 2l$  выбираем  $m' = 2l + 1$ . Каждый блок  $\Lambda_i, i = 1, \dots, \beta$ , осуществляет тогда вычисление только одного разряда частного. Строим такой блок из  $2\gamma$  штук  $(m, m)$ -элементов. При этом  $\gamma = \lceil \frac{m' - l}{\lfloor (m - 1) / 2 \rfloor} \rceil$

\*) Строго говоря, блок  $\Lambda_\beta$  может отличаться от предыдущих тем, что на его входы может подаваться менее  $m' - 2l$  разрядов делимого, но на оценку сложности схемы это не влияет.



и  $L_m(\Lambda_i) \leq 2\gamma$ . Отсюда и из (38) получаем

$$L_m(D^{\alpha, l}) \leq \beta L_m(\Lambda_i) = \left\lceil \frac{\alpha - l}{m' - 2l} \right\rceil L_m(\Lambda_i) \leq 2 \left\lceil \frac{\alpha - l}{m' - 2l} \right\rceil \left\lceil \frac{m' - l}{(m - 1)/2} \right\rceil = \\ = 2(\alpha - l) \left\lceil \frac{l + 1}{[(m - 1)/2]} \right\rceil \leq 2(\alpha - l) \frac{4l}{m - 2} \leq 8 \frac{\alpha l}{m - 2}.$$

В частном случае, когда  $l$ -разрядное число  $Q$  имеет вид  $q2^q$ , оператор  $D^{\alpha, l}$  можно реализовать, воспользовавшись редукцией его к оператору  $D^{\alpha - q, l - q}$ . Дело в том, что двоичное представление числа  $q2^q$  имеет младшие  $q$  разрядов нулевыми, поэтому деление на  $Q = q2^q$  можно рассматривать как деление  $(\alpha - l)$ -разрядного числа на  $(l - q)$ -разрядное. При этом младшие  $q$  разрядов остатка для  $D^{\alpha, l}$  просто совпадут с младшими  $q$  разрядами делимого, в качестве старших разрядов остатка  $D^{\alpha, l}$  будут выступать разряды остатка оператора  $D^{\alpha - q, l - q}$ , частное же для  $D^{\alpha, l}$

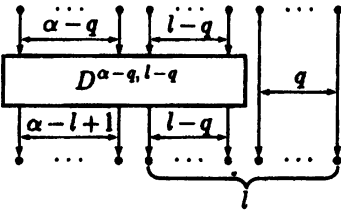


Рис. Д2. Реализация блока  $D^{\alpha, l}$  на базе  $D^{\alpha - q, l - q}$

будет представлено частным  $D^{\alpha - q, l - q}$  (рис. Д2), и, очевидно, в этом случае  $L_m(D^{\alpha, l}) = L_m(D^{\alpha - q, l - q})$ . Если  $\alpha + l < m$ , то  $L_m(D^{\alpha, l}) = 1$ .

**Лемма Д1'.** Пусть  $m > 2$ ,  $l = \lfloor \log Q \rfloor + 1$ ,  $Q = q2^q$ . Тогда

$$L_m(D^{\alpha, \lfloor \log Q \rfloor + 1}) = L_m(D^{\alpha - q, \lfloor \log q \rfloor + 1}).$$

Если  $\alpha + l < m$ , то  $L_m(D^{\alpha, \lfloor \log Q \rfloor + 1}) = 1$ .

**Оператор  $K^\delta$ .** По набору  $\tilde{\lambda}$  длины  $\delta$  этот оператор строит набор длины  $2^\delta$ , имеющий только одну единицу, расположенную на  $|\tilde{\lambda}|$ -м месте, т. е.  $K^\delta$  реализует систему всех конъюнкций от  $\delta$  переменных.

**Лемма Д2.** При  $m \geq 2$  имеет место оценка  $L_m(K^\delta) \leq 2^{\delta + 2}/m$ .

**Доказательство.** Схема для  $K^\delta$  строится из  $(m, m)$ -элементов, реализующих конъюнкции, и имеет  $\delta$  входов и  $2^\delta$  выходов.

Пусть  $\mu = \lfloor \log m \rfloor$ ,  $m \geq 2$ . При этом  $\log m - 1 < \mu \leq \log m$ ,  $m/2 < 2^\mu \leq m$ . Тогда при всех  $\delta$ ,  $\delta \leq \mu$ , схема для  $K^\delta$  состоит из одного  $(m, m)$ -элемента, т. е.  $L_m(K^\delta) = 1$ , и лемма для этого случая справедлива.

Пусть  $\delta > \mu$ . Предположим, что схема для  $K^{\delta - \mu}$  построена; она имеет  $\delta - \mu$  входов и  $2^{\delta - \mu}$  выходов, на которых реализуется система всех конъюнкций  $\{x_1^{\sigma_1} \dots x_{\delta - \mu}^{\sigma_{\delta - \mu}}\}$  длины  $\delta - \mu$ .

Схему для  $K^\delta$  будем строить, присоединяя к каждому выходу схемы для  $K^{\delta - \mu}$  один  $(m, m)$ -элемент, на  $\mu$  входов которого подаются переменные  $\{x_{\delta - \mu + 1}, \dots, x_\delta\}$  (очевидно, что  $\mu + 1 \leq m$ ). На  $2^\mu$  выходах каждого из этих элементов реализуются  $2^\mu$  конъюнкций длины  $\delta$ . Число таких элементов, очевидно, равно  $2^{\delta - \mu}$ , и на их выходах реализуется система всех конъюнкций длины  $\delta$ . Тогда

$$L_m(K^\delta) = L_m(K^{\delta - \mu}) + 2^{\delta - \mu} = \frac{2^\delta}{2^\mu} + \frac{2^\delta}{2^{2\mu}} + L_m(K^{\delta - 2\mu}) = \dots \\ \dots = \frac{2^\delta}{2^\mu} \left( 1 + \frac{1}{2^\mu} + \frac{1}{2^{2\mu}} + \dots \right) \leq \frac{2^{\delta + 2}}{m}.$$

Полезно также рассмотреть оператор  $K^{(t)}$ , который по первым  $t$  (имеется в виду лексикографическое упорядочение) наборам  $\tilde{\lambda}_i$  длины  $\lfloor \log t \rfloor$  строит наборы с одной единицей, расположенной на  $|\tilde{\lambda}_i|$ -м месте, т. е.  $K^{(t)}$  определен на множестве первых  $t$  наборов длины  $\lfloor \log t \rfloor$ . Тогда  $K^\delta = K^{(2^\delta)}$ . Очевидно, что

$$L_m(K^{(t)}) \leq L_m(K^{(2^{\lfloor \log t \rfloor})}) = L_m(K^{\lfloor \log t \rfloor}) \leq 2^{\lfloor \log t \rfloor + 2}/m \leq 8t/m.$$

**Лемма Д2'.** При  $m \geq 2$  имеет место оценка  $L_m(K^{(t)}) \leq 8t/m$ .

Оператор  $\Xi^{a,b}$  по наборам  $\tilde{\alpha} = (\alpha_1, \dots, \alpha_a)$  и  $\tilde{\beta} = (\beta_1, \dots, \beta_b)$  строит набор  $\tilde{\gamma}$  (состоящий из  $a$  поднаборов  $\tilde{\gamma}^i$  длины  $b$ ):  $\tilde{\gamma} = (\tilde{\gamma}^1, \dots, \tilde{\gamma}^a) = (\gamma_1^1, \dots, \gamma_b^1, \gamma_1^2, \dots, \gamma_b^2, \dots, \gamma_1^a, \dots, \gamma_b^a)$ , следующим образом:

$$\gamma_j^i = \alpha_i \& \beta_j.$$

**Лемма Д3.** Пусть  $m \geq 2$ ,  $b > 1$ . Тогда  $L_m(\Xi^{a,b}) \leq 3ab/m + 1$ .

**Доказательство.** При  $b < m$  и  $ab \leq m$  для реализации  $\Xi^{a,b}$  достаточно одного  $(m, m)$ -элемента, и лемма верна.

При  $b < m$  и  $ab > m$  одним элементом можно реализовать  $\lceil m/b \rceil$  поднаборов  $\tilde{\gamma}^i$ , поэтому не менее  $m/b$  поднаборов реализуются двумя элементами. Тогда для реализации всего набора  $\tilde{\gamma}$  достаточно  $2\lceil a/(m/b) \rceil$  элементов. Следовательно,

$$L_m(\Xi^{a,b}) \leq 2\left\lceil \frac{a}{m/b} \right\rceil \leq 2\left(\frac{a}{m/b} + 1\right) \leq \left(3\frac{ab}{m} + 1\right).$$

При  $b \geq m$  для реализации одного поднабора  $\tilde{\gamma}^i$  достаточно  $\lceil b/(m-1) \rceil$  элементов. Для всего набора  $\tilde{\gamma}$  тогда достаточно  $a\lceil b/(m-1) \rceil$  элементов. Поэтому

$$L_m(\Xi^{a,b}) \leq a(b/(m-1) + 1).$$

Далее, в силу того, что  $m-1 \geq m/2$  и  $b/m \geq 1$ , имеем

$$a\left(\frac{b}{m-1} + 1\right) \leq a\left(\frac{2b}{m} + 1\right) < \frac{3ab}{m},$$

и, следовательно, в этом случае также  $L_m(\Xi^{a,b}) \leq 3ab/m + 1$ .

Оператор  $Y^{t,t}$  определен на первых  $t$  наборах длины  $\lceil \log t \rceil$ . Всякий набор  $\tilde{\alpha}$  из этого множества он преобразует в набор  $\tilde{\beta}$  длины  $lb$ , где  $b = \lceil t/(2^l - 1) \rceil$ , состоящий из поднаборов длины  $l$ , среди которых в точности один ненулевой, причем различные наборы  $\tilde{\alpha}$  длины  $\lceil \log t \rceil$  преобразуются в различные наборы. Для этого число, заданное набором  $\tilde{\alpha}$ , делится на  $2^l - 1$  (оператором  $D^{\lceil \log t \rceil, l}$ ), и двоичная запись остатка от деления (к которому прибавляется единица оператором  $\Sigma_1^l$ ) задает ненулевой поднабор, частное же преобразуется оператором  $K^{(b)}$  в набор длины  $b$  с единицей на том месте, номер которого определяется величиной частного. По этим двум наборам с помощью оператора  $\Xi^{b,l}$  формируется результирующий набор.

Очевидно, что

$$L_m(Y^{t,t}) \leq L_m(D^{\lceil \log t \rceil, l}) + L_m(\Sigma_1^l) + L_m(K^{(b)}) + L_m(\Xi^{b,l}) + 1.$$

Оператор  $\tilde{\alpha}_{\tilde{\gamma}, \delta}(a)$  по набору  $\tilde{\alpha} = (\alpha_1, \dots, \alpha_c)$ , каждая компонента которого — двоичный набор длины  $\lceil \log a \rceil$ , по двоичному набору  $\tilde{\gamma}$ ,  $|\tilde{\gamma}| \leq c$ , и числу  $\delta$ ,  $\delta < a - 1$ , заданному в виде двоичной записи набором из нулей и единиц, вычисляет набор\*)

$$\tilde{\alpha}_{\tilde{\gamma}, \delta} = (\alpha_1, \dots, \alpha_{\gamma-1}, \alpha_{\gamma} +_a \delta, \alpha_{\gamma+1}, \dots, \alpha_c).$$

**Лемма Д4.** Имеет место неравенство

$$L_m(\tilde{\alpha}_{\tilde{\gamma}, \delta}(a)) \leq (c_{12}c \log a)/m.$$

\*) Символ  $+_a$  обозначает здесь сложение по модулю  $a$ ,  $\gamma$  — число, двоичной записью которого является набор  $\tilde{\gamma}$ , т. е.  $\gamma = |\tilde{\gamma}|$ .

Доказательство. Оператор  $\tilde{\alpha}_{\tilde{\gamma}, \delta}(a)$  можно реализовать схемой из  $(m, m)$ -элементов, состоящей из следующих блоков (рис. Д3).

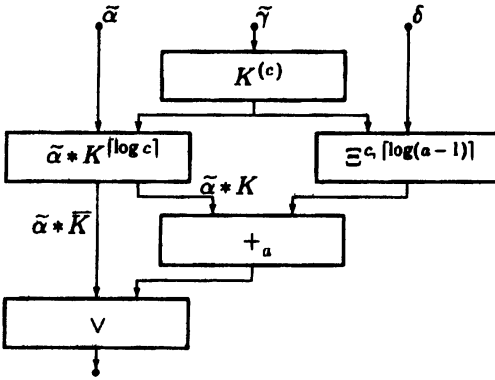


Рис. Д3. Реализация оператора  $\tilde{\alpha}_{\tilde{\gamma}, \delta}(a)$

Блок  $K^{(c)}$  по набору  $\tilde{\gamma}$  строит набор длины  $\lceil \log c \rceil$  с одной единицей на  $|\tilde{\gamma}|$ -м месте. По лемме Д2' имеем  $L_m(K^{(c)}) \leq 8c/m$ .

Блок  $\Xi^{c, \lceil \log(a-1) \rceil}$  строит набор  $(\tilde{0}, \dots, \tilde{0}, \tilde{\delta}, \tilde{0}, \dots, \tilde{0})$ . По лемме Д3 имеем

$$L_m(\Xi^{c, \lceil \log(a-1) \rceil}) \leq \frac{3c \lceil \log(a-1) \rceil}{m} + 1 \leq \frac{c_{13} c \log a}{m}.$$

Блок  $\tilde{\alpha} * K^{\lceil \log c \rceil}$  строит два набора:  $\tilde{\alpha} \bar{K} = (\alpha_1, \dots, \alpha_{\gamma-1}, 0, \alpha_{\gamma+1}, \dots, \alpha_c)$  и  $\tilde{\alpha} K = (0, \dots, 0, \alpha_\gamma,$

$0, \dots, 0)$ . Для этого блока  $L_m(\tilde{\alpha} * K^{\lceil \log c \rceil}) \leq (c_{14} c \log a)/m$ .

Блок  $+_a$  строит набор  $(0, \dots, 0, \alpha_\gamma +_a \delta, 0, \dots, 0)$ . Для этого блока

$$L_m(+_a) \leq (c_{15} c \log a)/m.$$

Блок  $V$  строит набор  $\tilde{\alpha}_{\tilde{\gamma}, \delta}(a)$ . Для этого блока  $L_m(V) \leq (2c \log a)/m$ .

Таким образом,  $L_m(\tilde{\alpha}_{\tilde{\gamma}, \delta}(a)) \leq (c_{12} c \log a)/m$ .

#### СПИСОК ЛИТЕРАТУРЫ

1. Карпова Н. А. О некоторых свойствах функций Шеннона // Математич. заметки. — 1970. — Т. 8, № 5. — С. 663–674.
2. Лупанов О. Б. Об одном методе синтеза схем // Известия вузов. Сер. Радиофизика. — 1958. — Т. 1, № 1. — С. 120–140.
3. Лупанов О. Б. Об одном классе схем из функциональных элементов // Проблемы кибернетики. Вып. 7. — М.: Физматгиз, 1962. — С. 61–114.
4. Maroка А. Complexity based on partitioning of Boolean circuits and their relation to multivalued circuits // IEEE Trans. on computers. — 1986. — V. C-35, № 2. — P. 115–123.

Поступило в редакцию 24 VI 1998