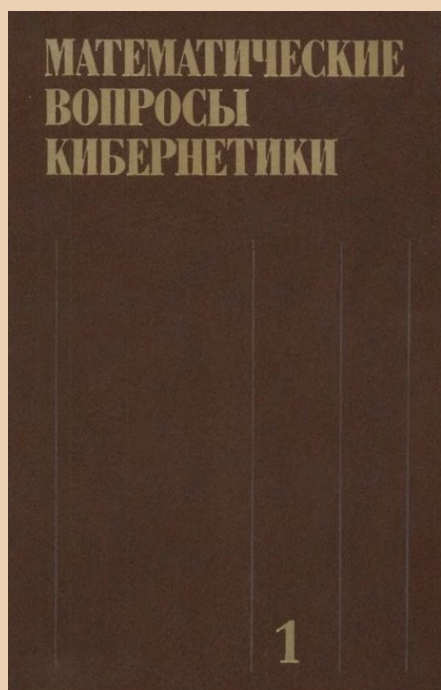




Е. Г. Красулина

**О сложности
реализации
монотонных
симметрических
функций алгебры
логики контактными
схемами**

Рекомендуемая форма библиографической ссылки:
Красулина Е. Г. О сложности реализации монотонных симметрических функций алгебры логики контактными схемами // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 140–167.
URL: <http://library.keldysh.ru/mvk.asp?id=1988-140>

О СЛОЖНОСТИ РЕАЛИЗАЦИИ МОНОТОННЫХ СИММЕТРИЧЕСКИХ ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ КОНТАКТНЫМИ СХЕМАМИ

Е. Г. КРАСУЛИНА

(МОСКВА)

Функция алгебры логики называется симметрической, если она не изменяется ни при какой перестановке своих переменных.

Из этого определения следует, что симметрическая функция $f(x_1, \dots, x_n)$, равная единице на наборе $\tilde{\sigma} = (\sigma_1, \sigma_2, \dots, \sigma_n)$, равна единице и на всяком другом наборе, имеющем столько же единиц, сколько их содержится в $\tilde{\sigma}$.

Число a называется рабочим числом симметрической функции f , если на (всяком) наборе, имеющем a единиц, f равна единице. Очевидно, что всякая симметрическая функция полностью определяется набором своих рабочих чисел.

Каждой симметрической функции $f(x_1, \dots, x_n)$ поставим в соответствие последовательность длины $n+1$ из нулей и единиц $\tilde{\pi}_f = (\pi_0, \pi_1, \dots, \pi_n)$ — характеристическую последовательность, определяемую следующим образом:

$$\pi_a = \begin{cases} 1, & \text{если } a \text{ является рабочим числом функции } f, \\ 0 & \text{в противном случае.} \end{cases}$$

Будем говорить, что симметрическая функция $f(x_1, x_2, \dots, x_n)$ является *монотонной*, если для ее характеристической последовательности $\tilde{\pi}_f = (\pi_0, \pi_1, \dots, \pi_n)$ выполнено условие

$$\pi_i = \begin{cases} 0, & \text{если } i = 0, 1, \dots, p-1, \\ 1, & \text{если } i = p, p+1, \dots, n, \end{cases}$$

где p — некоторое целое число из отрезка $[0, n]$, p называют *порогом* монотонной симметрической функции.

Будем говорить, что симметрическая функция $f(x_1, x_2, \dots, x_n)$ является *периодической* с периодом $\tilde{\tau}^d = (\tau_0, \tau_1, \dots, \tau_{d-1})$ (или имеет период $\tilde{\tau}^d$), если для ее характеристической последовательности $\tilde{\pi}_f = (\pi_0, \pi_1, \dots, \pi_n)$ выполнено условие

$$\pi_{kd+i} = \tau_i \quad (k = 0, 1, \dots, [n/d], \quad i = 0, 1, \dots, d-1),$$

т. е. характеристическая последовательность $\tilde{\pi}_f$ является периодической с периодом $\tilde{\tau}^d$ (без предпериода).

Для периодических симметрических функций известны контактные схемы из работы Шеннона [6].

Поскольку любая симметрическая функция f имеет тривиальный период $\tilde{\tau}^{n+1} = \tilde{\pi}_f$, аппарат контактных схем для периодических сим-

метрических функций может быть использован и для реализации любой симметрической функции (в том числе и для монотонной симметрической функции). Число контактов, используемых для реализации любой монотонной симметрической функции, не превосходит по порядку $n(n+1)$. Это следует из [6].

За счет дробления периода $\tilde{\tau}^d$ на два $\tilde{\tau}^{d_1}$ и $\tilde{\tau}^{d_2}$ таких, что $d_1 d_2 = d \geq n+1$, О. Б. Лупанову [4] удалось получить схему с числом контактов, по порядку не превосходящим $n^{1+1/2}$, для реализации любой монотонной симметрической функции.

На схемном языке — это последовательное соединение двух схем с периодами $\tilde{\tau}^{d_1}$ и $\tilde{\tau}^{d_2}$ некоторым образом между собой.

Естественно возник вопрос: а нельзя ли, дробя дальше период $\tilde{\tau}^d$ ($d \geq n+1$), получить оценку, близкую к линейной. Оказалось, что это сделать можно. Период $\tilde{\tau}^d$ дробится на B периодов $\tilde{\tau}^{d_1}, \tilde{\tau}^{d_2}, \dots, \tilde{\tau}^{d_B}$ таких, что $d_1 d_2 \dots d_B = d \geq n+1$. Число контактов в схеме, реализующей любую монотонную симметрическую функцию, по порядку не превосходит $n(\ln n)^4 / (\ln \ln n)^2$. На схемном языке — это последовательное соединение B схем с периодами $\tilde{\tau}^{d_1}, \tilde{\tau}^{d_2}, \dots, \tilde{\tau}^{d_B}$, где $B = \lceil c \ln n / \ln \ln n \rceil$.

Метод описан по индукции и связан с громоздкими арифметическими вычислениями. Работа содержит две главы.

В первой главе реализована любая монотонная симметрическая функция со сложностью, по порядку не превосходящей $n^{1+n/3}$, на основе дробления периода $\tilde{\tau}^d$ на три $\tilde{\tau}^{d_1}, \tilde{\tau}^{d_2}, \tilde{\tau}^{d_3}$, где $d_1 d_2 d_3 = d \geq n+1$. В этой главе содержатся менее громоздкие арифметические вычисления, и здесь уже просматриваются почти все идеи общего случая.

Во второй главе описан общий случай реализации любой монотонной симметрической функции.

Работа выполнена под руководством О. Б. Лупанова.

ГЛАВА 1

§ 1. Некоторые факты из теории чисел

Очевиден следующий факт.

Лемма 1.1.1. Если *) $(b, c) = 1$, $d_1 \not\equiv d_2 \pmod{c}$, k — произвольное целое неотрицательное число, то $k + d_1 b \not\equiv k + d_2 b \pmod{c}$.

Обозначим через a_1, a_2, a_3 три взаимно простых натуральных числа.

В этой главе, кроме § 4, все суммы, не относящиеся к оценке сложности схем, понимаются по модулю $a_1 a_2 a_3$.

Пусть a, b — некоторые целые числа, где $a \leq b$. Отрезком назовем множество целых подряд идущих чисел. Отрезок, начало которого a , а конец — b , будем обозначать через $[a, b]$.

Лемма 1.1.2. Пусть k — произвольное целое число. Тогда любое целое число из отрезка $[0, a_1 a_2 a_3 - 1]$ может быть представлено в виде

$$k + q_1 a_3 + q_2 a_1 + q_3 a_1 a_2, \quad \text{где } q_s \in [0, a_s - 1]; \quad s = 1, 2, 3. \quad (*)$$

Доказательство. В силу того, что в множестве чисел, представимых в виде (*), содержится $a_1 a_2 a_3$ чисел, достаточно показать, что разность между любыми двумя из них не сравнима с нулем по модулю $a_1 a_2 a_3$. Рассмотрим разность между любыми двумя из них, x_1 и x_2 , и покажем, что если не все числа $\tilde{q}_1, \tilde{q}_2, \tilde{q}_3$ ($\tilde{q}_s \in [-a_s + 1, a_s - 1]$, $s = 1, 2, 3$) равны нулю, то

$$\tilde{q}_1 a_3 + \tilde{q}_2 a_1 + \tilde{q}_3 a_1 a_2 \not\equiv 0 \pmod{a_1 a_2 a_3}.$$

*) Как обычно, символом (b, c) обозначается наибольший общий делитель чисел b и c .

В самом деле, пусть

$$x_1 = k + q'_1 a_3 + q'_2 a_1 + q'_3 a_1 a_2, \quad x_2 = k + q''_1 a_3 + q''_2 a_1 + q''_3 a_1 a_2,$$

тогда

$$x_1 - x_2 = (q'_1 - q''_1) a_3 + (q'_2 - q''_2) a_1 + (q'_3 - q''_3) a_1 a_2.$$

Если $\tilde{q}_1 \neq 0$, тогда

$$\tilde{q}_1 a_3 + \tilde{q}_2 a_1 + \tilde{q}_3 a_1 a_2 \equiv \tilde{q}_1 a_3 \not\equiv 0 \pmod{a_1}.$$

Если $\tilde{q}_1 = 0$, $\tilde{q}_2 \neq 0$, тогда

$$\tilde{q}_1 a_3 + \tilde{q}_2 a_1 + \tilde{q}_3 a_1 a_2 \equiv \tilde{q}_2 a_1 \not\equiv 0 \pmod{a_2}.$$

Если $\tilde{q}_1 = \tilde{q}_2 = 0$, $\tilde{q}_3 \neq 0$, тогда

$$\tilde{q}_1 a_3 + \tilde{q}_2 a_1 + \tilde{q}_3 a_1 a_2 \equiv \tilde{q}_3 a_1 a_2 \not\equiv 0 \pmod{a_3}.$$

Введем обозначения для некоторых множеств чисел. Пусть $i \in [0, a_3 - 1]$. Обозначим через A_i множество всех чисел, представимых в виде $q_1 a_3 + q_2 a_1 + i a_1 a_2$, где $q_1 \in [0, a_1 - 1]$, $q_2 \in [0, a_2 - 1]$.

Пусть, далее, $B_j = \bigcup_{i=0}^j A_i$, $j \in [0, a_3 - 1]$ и $B_\Sigma = \bigcup_{i \in \Sigma} A_i$ (здесь Σ — произвольное подмножество множества $\{0, 1, \dots, a_3 - 1\}$).

Если A — некоторое множество чисел, k — некоторое целое число, то через $k + A$ будем обозначать множество всех чисел $k + a$, где a пробегает A .

Следствие из леммы 1.1.2. Множества $k + A_0$, $k + A_1, \dots, k + A_{a_3-1}$ не пересекаются, и их объединение дает все целые числа отрезка $[0, a_1 a_2 a_3 - 1]$.

§ 2. Построение контактных схем специального вида для периодических симметрических функций с периодом $a_1 a_2 a_3$

Символом $T(n, d, A)$ обозначим симметрическую функцию от n аргументов, у которой рабочие числа устроены следующим образом: каждое a , $a \in A$, определяет $l_a + 1$ рабочих чисел, и эти $l_a + 1$ рабочих чисел образуют арифметическую прогрессию $a, a + d, a + 2d, \dots, a + l_a d$, где $a < d$ и $a + l_a d > n - d$. Такие функции являются периодическими симметрическими функциями с периодом $\tilde{\tau}^d$.

Через $L(n, d, A)$ будем обозначать сложность контактной схемы, которая реализует $T(n, d, A)$.

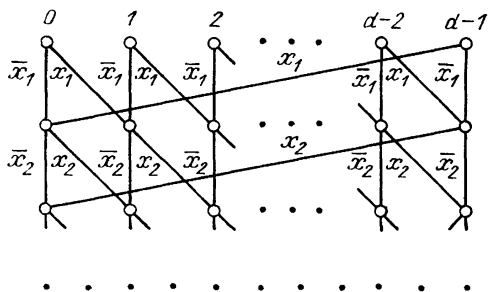


Рис. 1

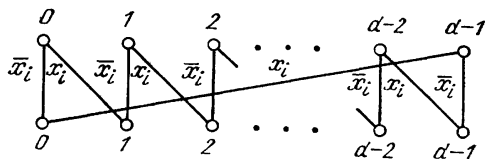


Рис. 2

Обозначим через X_n^d циклическую (периодическую) схему счетчика по модулю d (см. рис. 1). Она состоит из n однотипных блоков (см. рис. 2), соединенных последовательно.

Функция проводимости схемы X_n^d между i -м входом и j -м выходом равна $T(n, d, a)$, где $a = j - i \pmod{d}$.

Очевидно, что число контактов в схеме X_n^d равно $2dn$.

Лемма 1.2.1. Для любых целого k и Σ , $\Sigma \in \{0, 1, \dots, a_3 - 1\}$, существует схема такая, что $L(n, a_1 a_2 a_3, k + B_\Sigma) \leq 2n(a_1 + a_2 + a_3)$.

Доказательство. Введем обозначения:

$$\begin{aligned} \beta_0^1 &\equiv k \pmod{a_1}, & 0 \leq \beta_0^1 < a_1, \\ \beta_0^2 &\equiv k \pmod{a_2}, & 0 \leq \beta_0^2 < a_2, \\ \beta_0^3 &\equiv k \pmod{a_3}, & 0 \leq \beta_0^3 < a_3, \\ \beta_{q_1}^1 &\equiv k + q_1 a_3 \pmod{a_1}, & 0 \leq \beta_{q_1}^1 < a_1, \\ \alpha_{q_1}^2 &\equiv \beta_0^2 - k - q_1 a_3 \equiv -q_1 a_3 \pmod{a_2}, & 0 \leq \alpha_{q_1}^2 < a_2, \\ \beta_{q_2}^2 &\equiv k + q_2 a_1 \pmod{a_2}, & 0 \leq \beta_{q_2}^2 < a_2, \\ \alpha_{q_2}^3 &\equiv \beta_0^3 - k - q_2 a_1 \equiv -q_2 a_1 \pmod{a_3}, & 0 \leq \alpha_{q_2}^3 < a_3, \\ \beta_{q_3}^3 &\equiv k + q_3 a_1 a_2 \pmod{a_3}, & 0 \leq \beta_{q_3}^3 < a_3. \end{aligned}$$

Положим $\alpha_0^1 = \alpha_0^2 = \alpha_0^3$.

Требуемая схема получается в результате некоторого соединения трех схем $X_n^{a_1}$, $X_n^{a_2}$, $X_n^{a_3}$.

Входом всей схемы является вход схемы $X_n^{a_1}$ с номером α_0^1 .

Выходы схемы $X_n^{a_1}$ соединяются с входами схемы $X_n^{a_2}$ так, что в результате такого соединения выход с номером $\beta_{q_1}^1$ будет соединен со входом с номером $\alpha_{q_1}^2$, где $q_1 \in [0, a_1 - 1]$.

Выходы схемы $X_n^{a_2}$ соединяются с входами схемы $X_n^{a_3}$ так, что в результате такого соединения выход с номером $\beta_{q_2}^2$ будет соединен с входом с номером $\alpha_{q_2}^3$, где $q_2 \in [0, a_2 - 1]$.

Выход всей схемы получается в результате объединения выходов схемы $X_n^{a_3}$ с номерами $\beta_{q_3}^3$, где $q_3 \in \Sigma$.

Из способа соединения схем следует, что каждая проводящая цепь (цепь с ненулевой проводимостью) всей схемы должна быть устроена следующим образом: она идет от входа α_0^1 схемы $X_n^{a_1}$ к ее некоторому выходу $\beta_{q_1}^1$, где $q_1 \in [0, a_1 - 1]$, затем от входа схемы $X_n^{a_2}$ с номером $\alpha_{q_1}^2$ к ее некоторому выходу с номером $\beta_{q_2}^2$, где $q_2 \in [0, a_2 - 1]$, далее от входа схемы $X_n^{a_3}$ с номером $\alpha_{q_2}^3$ к ее некоторому выходу с номером $\beta_{q_3}^3$, где $q_3 \in \Sigma$.

Такую цепь будем называть *цепью типа* (q_1, q_2, q_3) .

Никаких других проводящих цепей типа (q_1, q_2, q_3) во всей схеме не может быть, так как, во-первых, схемы $X_n^{a_1}$, $X_n^{a_2}$, $X_n^{a_3}$ являются разделительными, во-вторых, каждый выход схемы $X_n^{a_s}$ ($s = 1, 2$) соединен ровно с одним входом схемы $X_n^{a_{s+1}}$ (это вытекает из леммы 1.1.1), в-третьих, все выходы схемы $X_n^{a_3}$ различны (это также следует из леммы 1.1.1).

Покажем, что цепи типа (q'_1, q'_2, q'_3) соответствует рабочее число $a \equiv k + q'_1 a_3 + q'_2 a_1 + q'_3 a_1 a_2 \pmod{a_1 a_2 a_3}$. Предположим, что этой цепи (q'_1, q'_2, q'_3) соответствует некоторое рабочее число b , покажем тогда, что $b = a$.

Из способа соединения трех схем $X_n^{a_1}$, $X_n^{a_2}$, $X_n^{a_3}$ вытекает, что

$$b \equiv \beta_{q_1}^1 \pmod{a_1},$$

$$b \equiv \beta_{q_2}^2 - \alpha_{q_1}^2 \pmod{a_2},$$

$$b \equiv \beta_{q_3}^3 - \alpha_{q_2}^3 \pmod{a_3}.$$

Из определения же $\alpha_{q_1}^2$, $\alpha_{q_2}^3$, $\beta_{q_1}^1$, $\beta_{q_2}^2$, $\beta_{q_3}^3$ следует, что

$$\beta_{q_1}^1 \equiv k + q_1' a_3 \pmod{a_1},$$

$$\beta_{q_2}^2 - \alpha_{q_1}^2 \equiv k + q_2' a_1 + q_1' a_3 \pmod{a_2},$$

$$\beta_{q_3}^3 - \alpha_{q_2}^3 \equiv k + q_3' a_1 a_2 + q_2' a_1 \pmod{a_3}.$$

В силу того, что $a, b \in [0, a_1 a_2 a_3 - 1]$, и a имеет такие же остатки при делении на a_1 , a_2 и a_3 , что и b , получаем $a = b$.

Число контактов в такой схеме не более $2n(a_1 + a_2 + a_3)$.

Следствие из леммы 1.2.1. Для любого целого k

$$L(n, a_1 a_2 a_3, k + B_0) \leq 2n(a_1 + a_2 + a_3),$$

$$L(n, a_1 a_2 a_3, k + B_1) \leq 2n(a_1 + a_2 + a_3),$$

$$\dots \dots \dots$$

$$L(n, a_1 a_2 a_3, k + B_{a_3-1}) \leq 2n(a_1 + a_2 + a_3).$$

§ 3. Факты из теории чисел

Здесь устанавливаются свойства множеств $B_0, B_1, \dots, B_{a_3-2}$ при конкретных соотношениях между числами a_1, a_2, a_3 .

Пусть $a_1 = 2g + 1$, $a_2 = 2g + 2$, $a_3 = 2g + 3$, где g — некоторое натуральное число. Очевидно, что a_1, a_2, a_3 — попарно взаимно простые числа.

Пусть $a' \equiv a \pmod{d}$, $b' \equiv b \pmod{d}$, где $0 \leq a', b' < d$, d — натуральное число. Тогда через $[a, b]_d$ будем обозначать отрезок $[a', b']$, если $a' \leq b'$, и пару отрезков $[0, b']$, $[a', d - 1]$, если $a' > b'$.

Пусть $\mathfrak{A}$ — некоторое множество целых неотрицательных чисел. Будем говорить, что $\mathfrak{A}$ пусто на $[a, b]_d$, если $\mathfrak{A} \cap [a, b]_d = \emptyset$. Множество $\mathfrak{A}$ полно на $[a, b]_d$, если $\mathfrak{A} \cap [a, b]_d = [a, b]_d$.

Лемма 1.3.1. Для любого q_3 ($q_3 \in [2, a_3]$) справедливо неравенство $(a_1 - 1)a_3 + (a_2 - 1)a_1 \leq q_3 a_1 a_2 - 1$.

Замечание 1.3.1. Для любого q_3 ($q_3 \in [0, a_3 - 1]$) все элементы множества A_{q_3} расположены на отрезке $[q_3 a_1 a_2, (a_1 - 1)a_3 + (a_2 - 1)a_1 + q_3 a_1 a_2]_{a_1 a_2 a_3}$. Элемент $q_3 a_1 a_2$ назовем первым элементом множества A_{q_3} , а элемент $(a_1 - 1)a_3 + (a_2 - 1)a_1 + q_3 a_1 a_2$ — последним элементом множества A_{q_3} .

Введем обозначение $t = (a_1 - 1)a_3 + (a_2 - 1)a_1 - a_1 a_2 + 1$.

Лемма 1.3.2. Справедливо неравенство $t < a_1 a_3$.

Лемма 1.3.3. Для любого q_3 ($q_3 \in [0, a_3 - 2]$) множество B_{q_3} пусто на отрезке $[t + (q_3 + 1)a_1 a_2, a_1 a_2 a_3 - 1]_{a_1 a_2 a_3}$ и полно на отрезке $[t, (q_3 + 1)a_1 a_2 - 1]_{a_1 a_2 a_3}$.

Доказательство. Тот факт, что B_{q_3} ($q_3 \in [0, a_3 - 2]$) пусто на отрезке $[t + (q_3 + 1)a_1 a_2, a_1 a_2 a_3 - 1]$, вытекает из замечания 1.3.1, определения величины t и леммы 1.3.1.

Рассмотрим множества $A_0, A_1, \dots, A_{a_3-1}$. Эти множества не пересекаются, их объединение дает все целые числа отрезка $[0, a_1 a_2 a_3 - 1]$, и они получаются друг из друга сдвигом на число, кратное $a_1 a_2$ (это вытекает из следствия леммы 1.1.2 и определения множеств $A_0, A_1, \dots, A_{a_3-1}$).

Каждое из множеств A_{q_3} ($q_3 \in [0, a_3 - 1]$) расположено на отрезке $[q_3 a_1 a_2, (q_3 + 1) a_1 a_2 + t - 1]_{a_1 a_2 a_3}$ (замечание 1.3.1), и, следовательно, расстояние между последним и первым элементами равно $a_1 a_2 + t - 1 = (a_1 - 1) a_3 + (a_2 - 1) a_1$, что меньше или равно $2 a_1 a_2$ (лемма 1.3.1).

В силу того, что для любого q_3 ($q_3 \in [0, a_3 - 1]$) множество A_{q_3} сдвинуто циклически относительно A_{q_3-1} на $a_1 a_2$ (если $q_3 = 0$, то $A_{q_3-1} = A_{a_3-1}$), на отрезке $[q_3 a_1 a_2, t + (q_3 + 1) a_1 a_2 - 1]_{a_1 a_2 a_3}$ могут быть расположены только элементы множеств $A_{q_3-1}, A_{q_3}, A_{q_3+1}$ (если $q_3 = 0$, то $A_{q_3-1} = A_{a_3-1}$ и если $q_3 = a_3 - 1$, то $A_{q_3+1} = A_0$).

Отсюда также следует, что на отрезке $[0, t + (q_3 + 1) a_1 a_2 - 1]$ могут быть расположены элементы множеств $A_{q_3-1}, A_0, A_1, \dots, A_{q_3+1}$, т. е. $A_{q_3-1}, B_{q_3}, A_{q_3+1}$, где $q_3 \in [0, a_3 - 2]$.

Сравним разность между первым элементом множества A_{q_3+1} , $x_{q_3} = (q_3 + 1) a_1 a_2$, где $q_3 \in [0, a_3 - 2]$, и последним элементом множества A_{q_3-1} , $y = t - 1 = (a_1 - 1) a_3 + (a_2 - 1) a_1 - a_1 a_2$.

В силу того, что $x_{q_3} - y = (q_3 + 1) a_1 a_2 - t + 1$, $(q_3 + 1) a_1 a_2 - t$ элементов, расположенных между x_{q_3} и y , принадлежат множествам $A_0, A_1, \dots, A_{q_3}$, т. е. B_{q_3} . Следовательно, на отрезке $[t, (q_3 + 1) a_1 a_2 - 1]_{a_1 a_2 a_3}$ множество B_{q_3} полно ($q_3 \in [0, a_3 - 2]$).

§ 4. Построение контактных схем

для некоторых периодических симметрических функций с периодом $2 a_1 a_3$

Пусть c_1, c_2 — два взаимно простых натуральных числа.

В этом параграфе все суммы, не относящиеся к оценке сложности, понимаются как суммы по модулю $c_1 c_2$ (в отличие от остальных параграфов этой главы).

Лемма 1.4.1. Для любых целого k и p из $[0, c_1 c_2 - 1]$

$$L(n, c_1 c_2, [k, k + p]_{c_1 c_2}) \leq 2n(c_1 + 2c_2).$$

Доказательство. Пусть $p = l c_1 + m$. Введем обозначения:

$$\begin{aligned} \delta_0^1 &\equiv k \pmod{c_1}, & 0 &\leq \delta_0^1 < c_1, \\ \delta_0^{21} &\equiv k \pmod{c_2}, & 0 &\leq \delta_0^{21} < c_2, \\ \delta_0^{22} &\equiv k + m + 1 \pmod{c_2}, & 0 &\leq \delta_0^{22} < c_2, \\ \delta_{q_1}^1 &\equiv k + q_1 \pmod{c_1}, & 0 &\leq \delta_{q_1}^1 < c_1, \quad q_1 \in [0, c_1 - 1], \\ \gamma_{q_1}^{21} &\equiv \delta_0^{21} - k - q_1 \equiv -q_1 \pmod{c_2}, & 0 &\leq \gamma_{q_1}^{21} < c_2, \quad q_1 \in [0, m], \\ \delta_{q_2}^{21} &\equiv k + q_2 c_1 \pmod{c_2}, & 0 &\leq \delta_{q_2}^{21} < c_2, \quad q_2 \in [0, l], \\ \gamma_{q_1}^{22} &\equiv \delta_0^{22} - k - q_1 \equiv m + 1 - q_1 \pmod{c_2}, & 0 &\leq \gamma_{q_1}^{22} < c_2, \quad q_1 \in [m + 1, \\ & & & c_1 - 1], \\ \delta_{q_2}^{22} &\equiv k + m + 1 + q_2 c_1 \pmod{c_2}, & 0 &\leq \delta_{q_2}^{22} < c_2, \quad q_2 \in [0, l - 1]. \end{aligned}$$

Положим $\gamma_0^1 = \gamma_0^{21} = \gamma_0^{22} = 0$.

Требуемая схема получается в результате некоторого соединения трех схем $X_n^{c_1}$, $X_n^{c_2}$, $X_n^{c_2}$. Входом всей схемы является вход схемы $X_n^{c_1}$ с номером γ_0^1 .

Выходы схемы $X_n^{c_1}$ соединяются со входами двух схем $X_n^{c_2}$ так, что при $q_1 \in [0, m]$ выход с номером $\delta_{q_1}^1$ соединяется со входом первой схемы $X_n^{c_2}$ с номером $\gamma_{q_1}^{21}$, а при $q_1 \in [m+1, c_1-1]$ выход с номером $\delta_{q_1}^1$ соединяется со входом второй схемы $X_n^{c_2}$ с номером $\gamma_{q_1}^{22}$.

Выход всей схемы получается в результате объединения выходов первой схемы $X_n^{c_2}$ с номерами $\delta_{q_2}^{21}$ ($q_2 \in [0, l]$) и выходов второй схемы $X_n^{c_2}$ с номерами $\delta_{q_2}^{22}$, где $q_2 \in [0, l-1]$.

Из способа соединения схем следует, что каждая проводящая цепь (цепь с ненулевой проводимостью) всей схемы должна быть устроена следующим образом: она идет от входа γ_0^1 схемы $X_n^{c_1}$ к некоторому выходу $\delta_{q_1}^1$, где $q_1 \in [0, c_1-1]$.

Если $q_1 \in [0, m]$, то цепь идет дальше к входу первой схемы $X_n^{c_2}$ с номером $\gamma_{q_1}^{21}$ и затем к выходу схемы $X_n^{c_2}$ с номером $\delta_{q_2}^{21}$, где $q_2 \in [0, l]$.

Если же $q_1 \in [m+1, c_1-1]$, то цепь дальше идет к входу второй схемы $X_n^{c_2}$ с номером $\gamma_{q_1}^{22}$ и затем к выходу схемы $X_n^{c_2}$ с номером $\delta_{q_2}^{22}$, где $q_2 \in [0, l-1]$.

Такие цепи будем называть *цепями типа* (q_1, q_2) .

Никаких других проводящих цепей во всей схеме не может быть, так как, во-первых, схемы $X_n^{c_1}$, $X_n^{c_2}$ являются разделительными, во-вторых, каждый выход схемы $X_n^{c_1}$ соединен ровно с одним входом либо первой схемы $X_n^{c_2}$, либо с одним входом второй схемы $X_n^{c_2}$ (это вытекает из леммы 1.1.1).

Покажем, что цепи типа (q'_1, q'_2) соответствует рабочее число

$$c \equiv k + q'_1 + q'_2 c_1 \pmod{c_1 c_2},$$

причем если $q'_1 \in [0, m]$, то $q'_2 \in [0, l]$, а если $q'_1 \in [m+1, c_1-1]$, то $q'_2 \in [0, l-1]$.

Предположим, что этой цепи (q'_1, q'_2) соответствует рабочее число b , покажем тогда, что $b = c$.

Рассмотрим сначала случай, когда

$$c \equiv k + q'_1 + q'_2 c_1 \pmod{c_1 c_2} \quad \text{и} \quad q'_1 \in [0, m], \quad q'_2 \in [0, l].$$

Из способа соединения схем $X_n^{c_1}$, $X_n^{c_2}$ вытекает, что

$$b \equiv \delta_{q'_1}^1 \pmod{c_1}, \quad q'_1 \in [0, m],$$

$$b \equiv \delta_{q'_1}^{21} - \gamma_{q'_2}^{21} \pmod{c_2}, \quad q'_1 \in [0, m], \quad q'_2 \in [0, l].$$

Из определения $\gamma_{q'_2}^{21}$, $\delta_{q'_1}^1$, $\delta_{q'_1}^{21}$ следует, что

$$\delta_{q'_1}^1 \equiv k + q'_1 \pmod{c_1}, \quad q'_1 \in [0, m],$$

$$\delta_{q'_1}^{21} - \gamma_{q'_2}^{21} \equiv k + q'_2 c_1 + q'_1 \pmod{c_2}, \quad q'_1 \in [0, m], \quad q'_2 \in [0, l].$$

Аналогично рассмотрим случай, когда

$$c \equiv k + q'_1 + q'_2 c_1 \pmod{c_1 c_2} \quad \text{и} \quad q'_1 \in [m + 1, c_1 - 1], \quad q'_2 \in [0, l - 1].$$

Из способа соединения схем $X_n^{c_1}, X_n^{c_2}$ вытекает, что

$$b \equiv \delta_{q'_1}^1 \pmod{c_1}, \quad q'_1 \in [m + 1, c_1 - 1],$$

$$b \equiv \delta_{q'_1}^{22} - \gamma_{q'_2}^{22} \pmod{c_2}, \quad q'_1 \in [m + 1, c_1 - 1], \quad q'_2 \in [0, l - 1].$$

Из определения $\delta_{q'_1}^1, \delta_{q'_1}^{22}, \gamma_{q'_2}^{22}$ следует, что

$$\delta_{q'_1}^1 \equiv k + q'_1 \pmod{c_1}, \quad q'_1 \in [m + 1, c_1 - 1],$$

$$\delta_{q'_1}^{22} - \gamma_{q'_2}^{22} \equiv k + q'_2 c_1 + m + 1 - m - 1 - q'_1 \equiv k + q'_2 c_1 + q'_1 \pmod{c_2},$$

$$q'_1 \in [m + 1, c_1 - 1], \quad q'_2 \in [0, l - 1].$$

В силу того, что $b, c \in [0, c_1 c_2 - 1]$, и c имеет такие же остатки при делении на $c_1 c_2$, что и b , $b = c$.

Заметим, что все множество рабочих чисел c совпадает с $[k, k + p]_{c_1 c_2}$.

Число контактов в такой схеме не более $2n(c_1 + 2c_2)$.

Следствие из леммы 1.4.1. Для любых целого k и p из $[0, 2a_1 a_3 - 1]$

$$L(n, 2a_1 a_3, [k, k + p]_{2a_1 a_3}) \leq 4n(a_1 + a_3).$$

Доказательство. Достаточно в лемме 1.4.1 выбрать $c_1 = 2a_1$, $c_2 = a_3$.

§ 5. Специальное соединение контактных схем

Пусть r_1, r_2, r_3 — некоторые неотрицательные целые числа, а d — натуральное число, тогда через $D(r_1, r_2, r_3, d)$ будем обозначать класс множеств целых неотрицательных чисел, которые полны на $[r_1, r_1 + r_2 - 1]_d$ и пусты на $[r_1 + r_2 + r_3, d - 1]_d$.

Замечание 1.5.1. Для любого q_3 ($q_3 \in [0, a_3 - 2]$) множество B_{q_3} принадлежит классу $D(t, (q_3 + 1)a_1 a_2 - t, t, a_1 a_2 a_3)$, где $t = (a_1 - 1)a_3 + (a_2 - 1)a_1 - a_1 a_2 + 1$.

Это вытекает из леммы 1.3.3 и определения множеств $D(r_1, r_2, r_3, d)$.

Лемма 1.5.1. Для любых целого k и l из $[1, a_1 a_2 a_3 - 2t]$, некоторого множества D , $D \in D(t, l, t, a_1 a_2 a_3)$,

$$L(n, a_1 a_2 a_3, k + D) \leq 4n(a_1 + a_2 + a_3).$$

Доказательство разбивается на два случая: $l \in [1, a_2 - 1]$, $l \in [a_2, a_1 a_2 a_3 - 2t]$.

При $l \in [1, a_2 - 1]$ положим $k_1 = k$ и $k_2 = k + l + t - a_1 a_2$. Из замечания 1.5.1 следует, что множества $k_1 + B_0$ и $k_2 + B_0$ принадлежат соответственно классам $k_1 + D(t, a_1 a_2 - t, t, a_1 a_2 a_3)$ и $k_2 + D(t, a_1 a_2 - t, t, a_1 a_2 a_3)$.

Легко проверить, что множество $(k_1 + B_0) \cap (k_2 + B_0) - k$ (которое мы обозначим через D) принадлежит $D(t, l, t, a_1 a_2 a_3)$ (см. рис. 3, а) — здесь и далее черными прямоугольниками будем обозначать подмножества множества, которые полны на соответствующих отрезках, белыми прямоугольниками — подмножества множества, которые пусты на соответствующих отрезках, а заштрихованными прямоугольниками — подмножества множества, которые мы в данный момент не рассматриваем).

По следствию из леммы 1.2.1

$$L(n, a_1 a_2 a_3, k_1 + B_0) \leq 2n(a_1 + a_2 + a_3),$$

$$L(n, a_1 a_2 a_3, k_2 + B_0) \leq 2n(a_1 + a_2 + a_3).$$

В результате последовательного соединения этих двух схем получится схема со сложностью

$$L(n, a_1 a_2 a_3, k + D) \leq 4n(a_1 + a_2 + a_3).$$

При $l \in [a_2, a_1 a_2 a_3 - 2t]$ положим $k_1 = k$ и $k_2 = k + l - t - (q_3 + 1)a_1 a_2$, где q_3 — наибольшее целое из отрезка $[0, a_3 - 2]$ такое, что $(q_3 + 1)a_1 a_2 \leq t + l$.

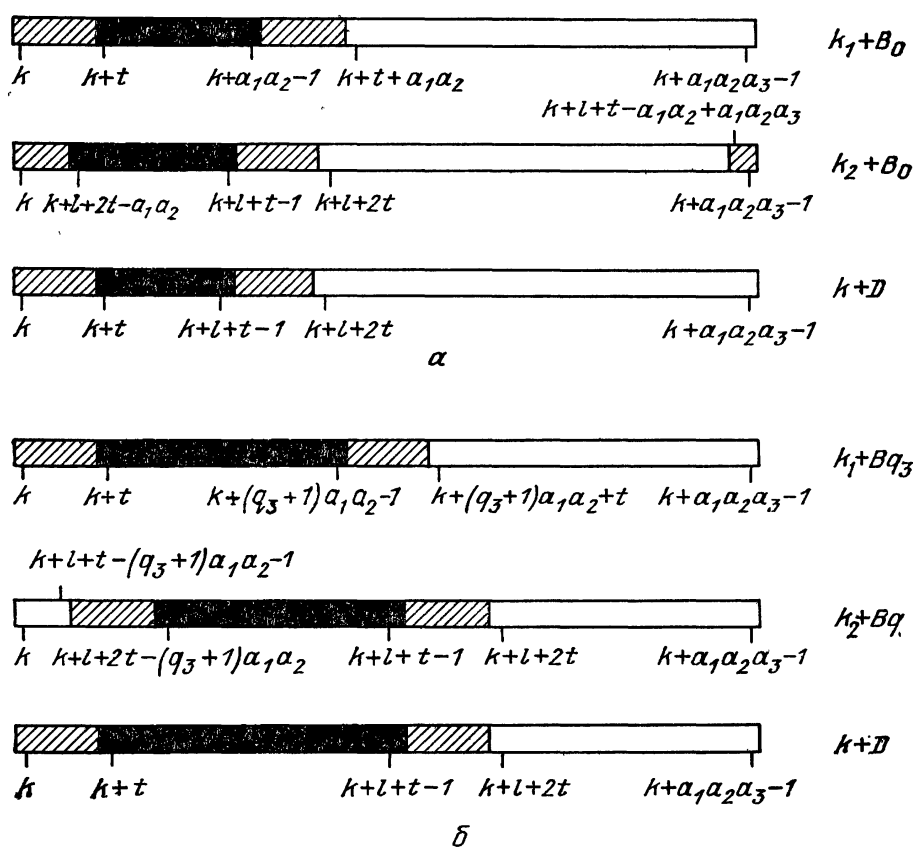


Рис. 3

Из замечания 1.5.1 следует, что множества $k_1 + B_{q_3}$ и $k_2 + B_{q_3}$ принадлежат соответственно классам $k_1 + D(t, (q_3 + 1)a_1 a_2 - t, t, a_1 a_2 a_3)$ и $k_2 + D(t, (q_3 + 1)a_1 a_2 - t, a_1 a_2 a_3)$.

Легко проверить, что множество $(k_1 + B_{q_3}) \cup (k_2 + B_{q_3}) - k$ (которое мы обозначим через D) принадлежит $D(t, l, t, a_1 a_2 a_3)$ (рис. 3, б)).

По следствию из леммы 1.2.1

$$L(n, a_1 a_2 a_3, k_1 + B_{q_3}) \leq 2n(a_1 + a_2 + a_3),$$

$$L(n, a_1 a_2 a_3, k_2 + B_{q_3}) \leq 2n(a_1 + a_2 + a_3).$$

В результате параллельного соединения этих двух схем получится схема со сложностью

$$L(n, a_1 a_2 a_3, k + D) \leq 4n(a_1 + a_2 + a_3).$$

Пусть h — некоторое натуральное число. Через $F(h, [a, b]_d)$ будем обозначать множество неотрицательных целых чисел на отрезке $[0, h-1]$ вида $\bigcup_{i=0}^{\infty} ([a, b]_d + id) \cap [0, h-1]$.

Лемма 1.5.2. Для любого целого k

$$L(n, a_1 a_2 a_3, [k, k+t-1]_{a_1 a_2 a_3}) \leq 4n(2a_1 + a_2 + 2a_3).$$

Доказательство. Выберем $k_1 = k-t$. Множество $k_1 + D$, где $D \in D(t, t, t, a_1 a_2 a_3)$, является полным на $[k, k+t-1]_{a_1 a_2 a_3}$ и пустым на $[k+2t, k+a_1 a_2 a_3-t-1]_{a_1 a_2 a_3}$.

Множество $[k, k+t-1]_{a_1 a_2 a_3}$ получается в результате пересечения множества $k_1 + D$ с множеством $F(a_1 a_2 a_3, [k, k+t-1]_{2a_1 a_3})$ (см. рис. 4). Надо проверить только, что множество $F(a_1 a_2 a_3, [k, k+t-1]_{2a_1 a_3})$ пусто на отрезках $[k-t, k-1]_{a_1 a_3 a_3}$ и $[k+t, k+2t-1]_{a_1 a_2 a_3}$. Это следует из того, что $F(a_1 a_2 a_3, [k, k+t-1]_{2a_1 a_3})$ пусто на отрезках $[k-2a_1 a_3 + t, k-1]_{a_1 a_2 a_3}$, $[k+t, k+2a_1 a_3-1]_{a_1 a_2 a_3}$, и длина каждого из этих отрезков, равная $2a_1 a_3 - t - 1$ (расстояние между последним и первым элементами), больше, чем длина каждого из отрезков $[k-t, k-1]_{a_1 a_2 a_3}$, $[k+t, k+2t-1]_{a_1 a_2 a_3}$, равная $t-1$. Последнее следует из леммы 1.3.2.

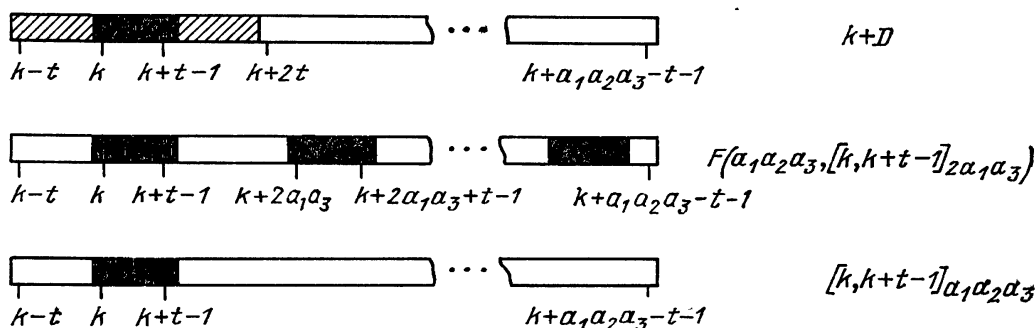


Рис. 4

По лемме 1.5.1 для некоторого D из $D(t, t, t, a_1 a_2 a_3)$

$$L(n, a_1 a_2 a_3, k_1 + D) \leq 4n(a_1 + a_2 + a_3).$$

По следствию из леммы 1.4.1

$$L(n, 2a_1 a_3, [k, k+t-1]_{2a_1 a_3}) \leq 4n(a_1 + a_3).$$

При последовательном соединении этих двух схем получится схема со сложностью

$$L(n, a_1 a_2 a_3, [k, k+t-1]_{a_1 a_2 a_3}) \leq 4n(2a_1 + a_2 + 2a_3).$$

Лемма 1.5.3. Для любых целого k и p из $[0, a_1 a_2 a_3 - 1]$

$$L(n, a_1 a_2 a_3, [k, k+p]_{a_1 a_2 a_3}) \leq 4n(5a_1 + 3a_2 + 5a_3).$$

Доказательство. Положим $k_1 = k$, $k_2 = k+p-t+1$. Доказательство разобьем на три случая:

$$p \in [0, t-1]; \quad p \in [t, 2t-1]; \quad p \in [2t, a_1 a_2 a_3 - 1].$$

В первом случае рассмотрим множества $R_1 = [k_1, k_1+t-1]_{a_1 a_2 a_3}$ и $R_2 = [k_2, k_2+t-1]_{a_1 a_2 a_3}$.

Легко видеть, что $R_1 \cap R_2 = [k, k+p]_{a_1 a_2 a_3}$ (рис. 5, а).

По лемме 1.5.2

$$L(n, a_1 a_2 a_3, R_1) \leq 4n(2a_1 + a_2 + 2a_3),$$

$$L(n, a_1 a_2 a_3, R_2) \leq 4n(2a_1 + a_2 + 2a_3).$$

При последовательном соединении этих двух схем получим схему со сложностью

$$L(n, a_1 a_2 a_3, [k, k+p]_{a_1 a_2 a_3}) \leq 8n(2a_1 + a_2 + 2a_3).$$

Во втором случае рассмотрим множества $R_1 = [k_1, k_1 + t - 1]_{a_1 a_2 a_3}$ и $R_2 = [k_2, k_2 + t - 1]_{a_1 a_2 a_3}$.

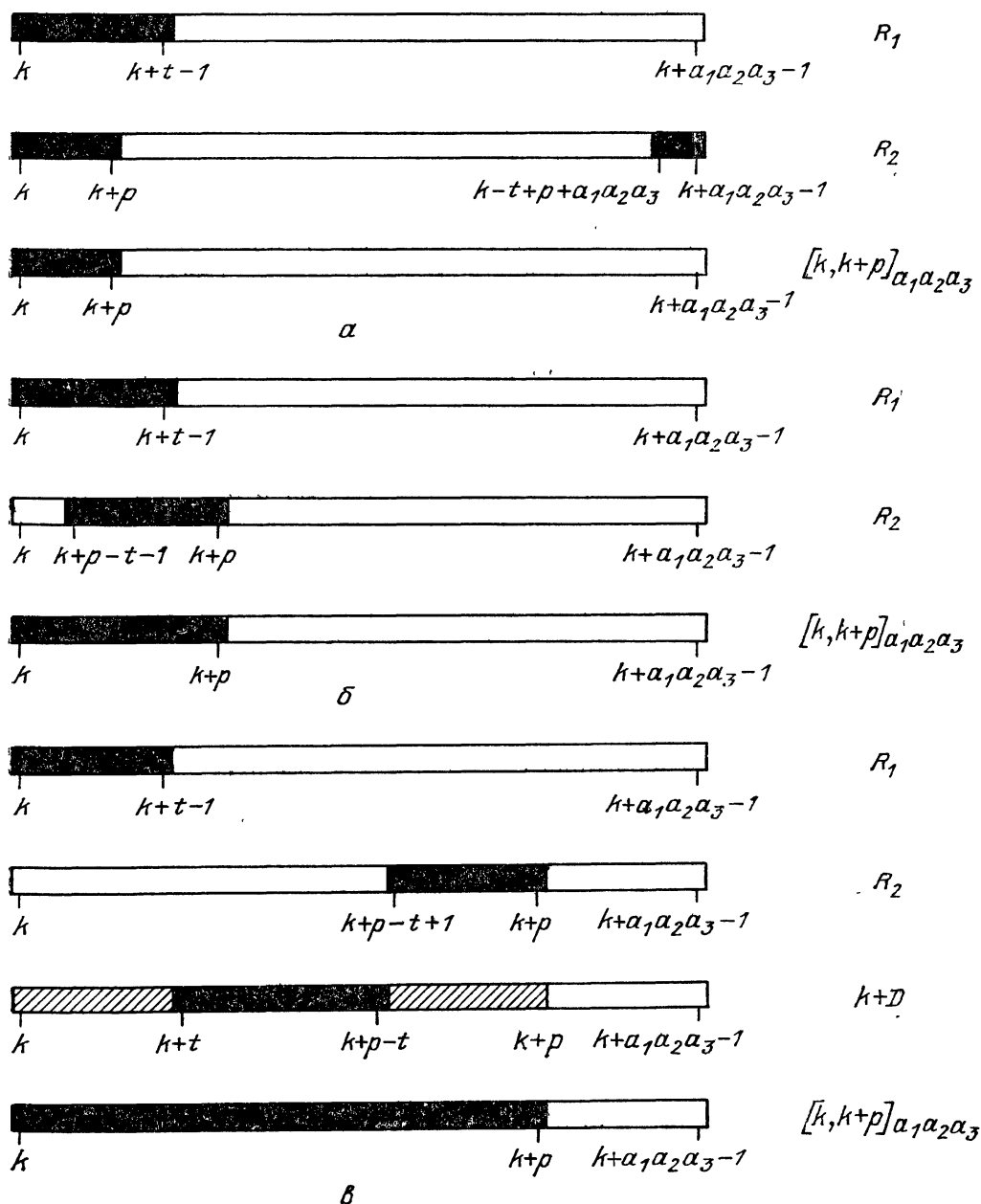


Рис. 5

Легко видеть, что $R_1 \cup R_2 = [k, k+p]_{a_1 a_2 a_3}$ (рис. 5, 6).

По лемме 1.5.2

$$L(n, a_1 a_2 a_3, R_1) \leq 4n(2a_1 + a_2 + 2a_3),$$

$$L(n, a_1 a_2 a_3, R_2) \leq 4n(2a_1 + a_2 + 2a_3).$$

При параллельном соединении этих двух схем получим схему со сложностью

$$L(n, a_1 a_2 a_3, [k, k+p]_{a_1 a_2 a_3}) \leq 8n(2a_1 + a_2 + 2a_3).$$

В третьем случае рассмотрим множества $R_1 = [k_1, k_1 + t - 1]_{a_1 a_2 a_3}$ и $R_2 = [k_2, k_2 + t - 1]_{a_1 a_2 a_3, k + D}$, где D — произвольное множество из $D(t, p - 2t + 1, t, a_1 a_2 a_3)$.

Легко видеть, что $R_1 \cup R_2 \cup (k + D) = [k, k + p]_{a_1 a_2 a_3}$ (рис. 5, в).

По лемме 1.5.2

$$L(n, a_1 a_2 a_3, R_1) \leq 4n(2a_1 + a_2 + 2a_3),$$

$$L(n, a_1 a_2 a_3, R_2) \leq 4n(2a_1 + a_2 + 2a_3).$$

По лемме 1.5.1 для некоторого D , $D \in D(t, p - 2t + 1, t, a_1 a_2 a_3)$, существует схема со сложностью

$$L(n, a_1 a_2 a_3, k + D) \leq 4n(a_1 + a_2 + a_3).$$

При параллельном соединении этих трех схем получим схему со сложностью

$$L(n, a_1 a_2 a_3, [k, k+p]_{a_1 a_2 a_3}) \leq 4n(5a_1 + 3a_2 + 5a_3).$$

§ 6. Реализация монотонных симметрических функций контактными схемами

Через M_n^r обозначим монотонную симметрическую функцию от n аргументов с порогом r .

Теорема 1.6.1. Для любого $\bar{p}$ из $[0, n]$ существует схема, реализующая $M_n^{\bar{p}}$, со сложностью по порядку не более $n^{1+1/3}$.

Доказательство. Это следует из леммы 1.5.3, если положить

$$a_1 = 2 \lceil \sqrt[3]{n}/2 \rceil + 1, \quad a_2 = 2 \lceil \sqrt[3]{n}/2 \rceil + 2, \quad a_3 = 2 \lceil \sqrt[3]{n}/2 \rceil + 3,$$

$$k = \bar{p}, \quad p = n - \bar{p}.$$

При этом сложность схемы для $M_n^{\bar{p}}$ не превосходит $104(\sqrt[3]{n}/2 + 1)n$.

ГЛАВА 2

§ 1. Свойства некоторых множеств натуральных чисел

Пусть B — натуральное число, не меньшее $c_1 \ln n / \ln \ln n$, где c_1 — некоторая константа. Через $p_1, p_2, \dots, p_{2B}$ обозначим $2B$ простых чисел, идущих подряд, где $p_1 \geq 3B$. Через a_i обозначим числа вида $a_i = p_{B-i+1} p_{2B-i+1}$, где $i \in [1, B]$. Пусть c — натуральное число из отрезка $[2, B]$. Через $b_1^c, b_2^c, \dots, b_c^c$ обозначим c взаимно простых натуральных чисел таких, что

$$b_i^c = a_i, \quad i \in [1, c-1]; \quad (1)$$

$$b_c^c = p_{B-c+1}. \quad (2)$$

Будем обозначать через a^c и b^c числа следующего вида:

$$a^c = \prod_{i=1}^c a_i, \quad b^c = \prod_{i=1}^c b_i^c.$$

В этой главе все суммы, не относящиеся к оценке сложности, рассматриваются как суммы по модулю a^c либо b^c (какой модуль брать, ясно из контекста).

Лемма 2.1.1. Пусть k — произвольное целое число, $c \in [3, B]$, тогда любое целое число из отрезка $[0, a^c - 1]$ может быть представлено в виде

$$k + \sum_{s=1}^{c-1} \left(q_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + q_c \prod_{i=1}^{c-1} a_i, \quad (**)$$

где

$$q_s \in [0, a_s - 1], \quad s \in [1, c].$$

Доказательство. В силу того, что в множестве чисел, представимых в виде (**), содержится a^c чисел, достаточно показать, что разность между любыми двумя из них не сравнима с нулем по модулю a^c .

Для этого достаточно показать, что если не все числа $\tilde{q}_1, \tilde{q}_2, \dots, \tilde{q}_c$ ($\tilde{q}_s \in [-a_s + 1, a_s - 1], s \in [1, c]$) равны нулю, то

$$\sum_{s=1}^{c-1} \left(\tilde{q}_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + \tilde{q}_c \prod_{i=1}^{c-1} a_i \not\equiv 0 \pmod{a^c}. \quad (***)$$

Пусть r — наименьшее натуральное число из отрезка $[1, c]$ такое, что в выражении (***) $\tilde{q}_r = 0$. Возможны два случая: $r < c$ и $r = c$.

Если $r < c$, то

$$\sum_{s=1}^{c-1} \left(\tilde{q}_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + \tilde{q}_c \prod_{i=1}^{c-1} a_i \equiv \tilde{q}_r \prod_{\substack{i=1 \\ i \neq r, r+1}}^c a_i \not\equiv 0 \pmod{a_r}.$$

Если $r = c$, то

$$\sum_{s=1}^{c-1} \left(\tilde{q}_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + \tilde{q}_c \prod_{i=1}^{c-1} a_i \equiv \tilde{q}_c \prod_{i=1}^{c-1} a_i \not\equiv 0 \pmod{a_c}.$$

В обоих случаях

$$\sum_{s=1}^{c-1} \left(\tilde{q}_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + \tilde{q}_c \prod_{i=1}^{c-1} a_i \not\equiv 0 \pmod{a^c}.$$

Лемма 2.1.2. Пусть k — произвольное целое число, $c \in [3, B]$, тогда любое целое число из отрезка $[0, b^c - 1]$ может быть представлено в виде

$$k + \sum_{s=1}^{c-1} \left(\phi_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c \right) + \phi_c \prod_{i=1}^{c-1} b_i^c,$$

где

$$\phi_s \in [0, b_s^c - 1], \quad s \in [1, c].$$

Доказательство аналогично доказательству леммы 2.1.1.

Введем обозначения для некоторых множеств чисел. Пусть $q_c \in [0, a_c - 1]$, $\phi_c \in [0, b_c^c - 1]$. Обозначим через $D_{q_c}^c$ множество всех чисел, представимых в виде

$$\sum_{s=1}^{c-1} \left(q_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + q_c \prod_{i=1}^{c-1} a_i, \quad \text{где } q_s \in [0, a_s - 1], \quad s \in [1, c-1],$$

а через $E_{\phi_c}^c$ — множество всех чисел, представимых в виде

$$\sum_{s=1}^{c-1} \left(\phi_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c \right) + \phi_c \prod_{i=1}^{c-1} b_i^c, \quad \text{где } \phi_s \in [0, b_s^c - 1], \quad s \in [1, c-1].$$

Пусть, далее,

$$F_j^c = \bigcup_{q_c=0}^j D_{q_c}^c, \quad j \in [0, a_c - 1], \quad F_{\Sigma'}^c = \bigcup_{q_c \in \Sigma'} D_{q_c}^c$$

(здесь Σ' — произвольное подмножество множества $\{0, 1, \dots, a_c - 1\}$) и пусть

$$H_j^c = \bigcup_{\varphi_c=0}^j E_{\varphi_c}^c, \quad j \in [0, b_c^c - 1], \quad H_{\Sigma}^c = \bigcup_{\varphi_c \in \Sigma''} E_{\varphi_c}^c$$

(здесь Σ'' — произвольное подмножество множества $\{0, 1, \dots, b_c^c - 1\}$).

Следствие из леммы 2.1.1. Множества $k + D_0^c, k + D_1^c, \dots, k + D_{a_c-1}^c$ не пересекаются, и их объединение дает все целые числа отрезка $[0, a^c - 1]$.

Следствие из леммы 2.1.2. Множества $k + E_0^c, k + E_1^c, \dots, k + E_{b_c^c-1}^c$ не пересекаются, и их объединение дает все целые числа из отрезка $[0, b^c - 1]$.

§ 2. Построение специальных контактных схем для периодических симметрических функций с периодами a^c и b^c

Лемма 2.2.1. Для любых целого k и $\Sigma, \Sigma \subseteq \{0, 1, \dots, a_c - 1\}$,

$$L(n, a^c, k + F_{\Sigma}^c) \leq 2n \sum_{i=1}^c a_i.$$

Доказательство. Введем обозначения:

$$\beta_0^s \equiv k \pmod{a_s}, \quad 0 \leq \beta_0^s < a_s, \quad s \in [1, c],$$

$$\beta_{q_s}^s \equiv k + q_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \pmod{a_s}, \quad 0 \leq \beta_{q_s}^s < a_s, \quad s \in [1, c-1],$$

$$\beta_{q_c}^c \equiv k + q_c \prod_{i=1}^{c-1} a_i \pmod{a_c}, \quad 0 \leq \beta_{q_c}^c < a_c,$$

$$\alpha_{q_{s-1}}^s \equiv \beta_0^s - k - q_{s-1} \prod_{\substack{i=1 \\ i \neq s-1, s}}^c a_i \equiv -q_{s-1} \prod_{\substack{i=1 \\ i \neq s-1, s}}^c a_i \pmod{a_s},$$

$$0 \leq \alpha_{q_{s-1}}^s < a_s, \quad s \in [2, c].$$

Положим $\alpha_0^s = 0$ ($s \in [1, c]$). Требуемая схема получается в результате некоторого соединения с схем $X_n^{a_1}, X_n^{a_2}, \dots, X_n^{a_c}$.

Входом всей схемы является вход схемы $X_n^{a_1}$ с номером α_0^1 .

Выходы схемы $X_n^{a_s}$ соединяются со входами схемы $X_n^{a_{s+1}}$ так, что в результате такого соединения выход с номером $\beta_{q_s}^s$ будет соединен со входом с номером $\alpha_{q_s}^{s+1}$, где $q_s \in [0, a_s - 1]$ ($s \in [1, c-1]$).

Выход всей схемы получается в результате объединения выходов схемы $X_n^{a_c}$ с номерами $\beta_{q_c}^c$, где $q_c \in \Sigma$.

Из способа соединения схем следует, что каждая проводящая цепь (цепь с нулевой проводимостью) всей схемы должна быть устроена следующим образом: она идет от входа схемы $X_n^{a_1}$ с номером α_0^1 к ее некоторому выходу $\beta_{q_1}^1$, где $q_1 \in [0, a_1 - 1]$, затем от входа схемы $X_n^{a_2}$

с номером $\alpha_{q_{s-1}}^s$ к ее некоторому выходу $\beta_{q_s}^s$, где $q_s \in [0, a_s - 1]$ ($s \in [2, c - 1]$), далее от входа схемы $X_n^{a_c}$ с номером $\alpha_{q_{c-1}}^s$ к ее некоторому выходу $\beta_{q_c}^c$, где $q_c \in \Sigma$.

Такую цепь будем называть *цепью типа* $(q_1, q_2, \dots, q_c)$.

Никаких других проводящих цепей во всей схеме не может быть, так как, во-первых, схемы $X_n^{a_s}$ ($s \in [1, c - 1]$) являются разделительными, во-вторых, каждый выход схемы $X_n^{a_s}$ ($s \in [1, c - 1]$) соединен ровно с одним входом схемы $X_n^{a_{s+1}}$ (это вытекает из леммы 1.1.1), в-третьих, все выходы схемы $X_n^{a_s}$ различны (это следует из леммы 1.1.1).

Покажем, что цепи типа $(q'_1, q'_2, \dots, q'_c)$ соответствует рабочее число

$$a \equiv k + \sum_{s=1}^{c-1} \left(q'_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i \right) + q'_c \prod_{i=1}^{c-1} a_i \pmod{a^c}.$$

Предположим, что этой цепи $(q'_1, q'_2, \dots, q'_c)$ соответствует некоторое рабочее число b ; покажем тогда, что $b = a$.

Из способа соединения схем $X_n^{a_1}, X_n^{a_2}, \dots, X_n^{a_c}$ вытекает, что

$$b \equiv \beta_{q'_1}^1 \pmod{a_1},$$

$$b \equiv \beta_{q'_s}^s - \alpha_{q'_{s-1}}^s \pmod{a_s}, \quad s \in [2, c],$$

а из определения $\alpha_{q_{s-1}}^s$ ($s \in [2, c]$) и $\beta_{q'_s}^s$ ($s \in [1, c]$) следует, что

$$\beta_{q'_1}^1 \equiv k + q'_1 \prod_{i=2}^c a_i \pmod{a_1},$$

$$\beta_{q'_s}^s - \alpha_{q'_{s-1}}^s \equiv k + q'_s \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i + q'_{s-1} \prod_{\substack{i=1 \\ i \neq s-1, s}}^c a_i \pmod{a_s}, \quad s \in [2, c-1],$$

$$\beta_{q'_c}^c - \alpha_{q'_{c-1}}^c \equiv k + q'_c \prod_{i=1}^{c-1} a_i + q'_{c-1} \prod_{i=1}^{c-2} a_i \pmod{a_c}.$$

В силу того, что $a, b \in [0, a^c - 1]$, и a имеет такие же остатки при делении на a_s ($s \in [1, c]$), что и b , $a = b$.

Число контактов в такой схеме не более чем $2n \sum_{i=1}^c a_i$.

Лемма 2.2.2. Для любых целого k и Σ' , $\Sigma' \subseteq \{0, 1, \dots, b_c^c - 1\}$,

$$L(n, b^c, k + H_{\Sigma'}^c) \leq 2n \sum_{i=1}^c b_i^c.$$

Доказательство аналогично доказательству леммы 2.2.1.

Следствие из леммы 2.2.1. Для любого целого k

$$L(n, a^c, k + F_0^c) \leq 2n \sum_{i=1}^c a_i,$$

$$L(n, a^c, k + F_1^c) \leq 2n \sum_{i=1}^c a_i,$$

$$\dots \dots \dots$$

$$L(n, a^c, k + F_{a_{c-1}}^c) \leq 2n \sum_{i=1}^c a_i.$$

Лемма 2.3.3. *Справедливо неравенство*

$$\sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c < (c-1) \prod_{i=1}^{c-1} b_i^c.$$

Доказательство. Покажем, что для любого $s \in [1, c-1]$ справедливо неравенство

$$(b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c < \prod_{i=1}^{c-1} b_i^c. \quad (5)$$

Для $s = c-1$ неравенство (5) верно, так как

$$(b_{c-1}^c - 1) \prod_{i=1}^{c-2} b_i^c < \prod_{i=1}^{c-1} b_i^c \quad \text{или} \quad b_{c-1}^c - 1 < b_{c-1}^c.$$

Если же $s \in [1, c-2]$, то (5) эквивалентно более простому неравенству

$$(b_s^c - 1) b_c^c < b_s^c b_{s+1}^c,$$

следующему из неравенства $b_c^c < b_{s+1}^c$, которое справедливо по лемме 2.3.1, так как $c > s+1$.

Введем обозначения:

$$t^c = \sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i - \prod_{i=1}^{c-1} a_i + 1,$$

$$r^c = \sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c - \prod_{i=1}^{c-1} b_i^c + 1.$$

Лемма 2.3.4. *Справедливо неравенство*

$$t^c > r^c. \quad (6)$$

Доказательство. В самом деле,

$$\begin{aligned} t^c - r^c &= \sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i - \prod_{i=1}^{c-1} a_i + 1 - \\ &\quad - \left(\sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c - \prod_{i=1}^{c-1} b_i^c + 1 \right) = (\text{см. (1)}) = \\ &= \sum_{s=1}^{c-1} (a_s - 1) (a_c - b_c^c) \prod_{\substack{i=1 \\ i \neq s, s+1}}^{c-1} a_i. \end{aligned}$$

По определению, $a_c > b_c^c$, следовательно, $t^c - r^c > 0$.

Лемма 2.3.5. *Справедливо неравенство*

$$r^c > t^{c-1}.$$

Доказательство. В самом деле,

$$\begin{aligned} r^c - t^{c-1} &= \sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c - \prod_{i=1}^{c-1} b_i^c - 1 - \\ &\quad - \left(\sum_{s=1}^{c-2} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^{c-1} a_i - \prod_{i=1}^{c-2} a_i + 1 \right) = (\text{см. (1)}) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{s=1}^{c-2} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^{c-2} a_i (b_c^c - 1) + (a_{c-1} - 2) \prod_{i=1}^{c-2} a_i - \prod_{i=1}^{c-1} a_i = \\
&= \sum_{s=1}^{c-2} (a_s - 1) \prod_{i=1}^{c-2} a_i (b_c^c - 1) - 2 \prod_{i=1}^{c-2} a_i = \\
&= \sum_{s=1}^{c-3} (a_s - 1) \prod_{i=1}^{c-3} a_i (b_c^c - 1) + \prod_{i=1}^{c-3} a_i ((a_{c-2} - 1)(b_c^c - 1) - 2a_{c-2}).
\end{aligned}$$

В полученном выражении первое слагаемое положительное. Рассмотрим второе слагаемое. Легко видеть, что

$$(a_{c-2} - 1) \prod_{i=1}^{c-3} a_i (b_c^c - 1) - 2 \prod_{i=1}^{c-2} a_i = \prod_{i=1}^{c-3} a_i ((a_{c-2} - 1)(b_c^c - 1) - 2a_{c-2}) > 0,$$

так как

$$(a_{c-2} - 1)(b_c^c - 1) - 2a_{c-2} > 0$$

(по определению, $a_{c-2} > 3$ и из (2) следует, что $b_c^c > 3$).

Следовательно, $r^c > t^{c-1}$.

Лемма 2.3.6. *Справедливо неравенство*

$$2t^c + r^c < \prod_{i=1}^{c-1} a_i p_{B-c+1}. \quad (7)$$

Доказательство. Ввиду (6) неравенство (7) следует из более сильного неравенства

$$3t^c < \prod_{i=1}^{c-1} a_i p_{B-c+1}. \quad (8)$$

По лемме 2.3.2 и определению t^c ,

$$t^c \leq (c-2) \prod_{i=1}^{c-1} a_i.$$

Отсюда и из (8) имеем

$$3(c-2) \prod_{i=1}^{c-1} a_i < \prod_{i=1}^{c-1} a_i p_{B-c+1}. \quad (9)$$

Неравенство (9) эквивалентно более простому неравенству

$$3(c-2) < p_{B-c+1}. \quad (10)$$

Докажем (10). В самом деле,

а) из определения c и (3) имеем $p_{B-c+1} > p_1$,

б) по определению, $p_1 \geq 3B$,

в) $3B > 3(B-2) \geq 3(c-2)$.

Из а)–в) следует справедливость (10), а следовательно, и (7).

Лемма 2.3.7. *Справедливо неравенство*

$$\sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c < (c-2) \prod_{i=1}^{c-2} b_i^c b_c^c + \prod_{i=1}^{c-1} b_i^c. \quad (11)$$

Доказательство. Неравенство (11) будет доказано, если будет показано, что:

1) для любого $s \in [1, c-2]$

$$(b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c < b_c^c \prod_{i=1}^{c-1} b_i^c; \quad (12)$$

2) для $s = c - 1$

$$(b_{c-1}^c - 1) \prod_{i=1}^{c-2} b_i^c < \prod_{i=1}^{c-1} b_i^c. \quad (13)$$

Докажем (12). Оно эквивалентно неравенству

$$(b_s^c - 1) b_{c-1}^c < b_s^c b_{s+1}^c,$$

справедливость которого вытекает из (3).

Докажем (13). Справедливость его вытекает из эквивалентности неравенству

$$b_{c-1}^c - 1 < b_{c-1}^c.$$

Лемма 2.3.8. *Справедливо неравенство*

$$2r^c + t^{c-1} < \prod_{i=1}^{c-1} b_i^c. \quad (14)$$

Доказательство. Из леммы 2.3.5 и (14) следует, что

$$3r^c < \prod_{i=1}^{c-1} b_i^c. \quad (15)$$

Из (11) и определения r^c имеем

$$r^c < (c - 2) \prod_{i=1}^{c-2} b_i^c b_c^c,$$

поэтому из (15) следует, что

$$3(c - 2) \prod_{i=1}^{c-2} b_i^c b_c^c < \prod_{i=1}^{c-1} b_i^c. \quad (16)$$

Неравенство (16) эквивалентно более простому неравенству

$$3(c - 2) b_c^c < b_{c-1}^c. \quad (17)$$

В силу того, что $b_c^c = p_{B-c+1}$, а $b_{c-1}^c = p_{B-c+2} p_{2B-c+2}$, (17) эквивалентно неравенству

$$3(c - 2) p_{B-c+1} < p_{B-c+2} p_{2B-c+2}. \quad (18)$$

Докажем (18). По определению чисел B , c и p_i , где $i \in [1, 2B]$,

а) $p_{B-c+1} < p_{2B-c+2}$, так как $B - c + 1 < 2B - c + 2$;

б) $p_{2B-c+2} > p_1$, так как $1 < 2B - c + 2$;

в) $p_1 \geq 3B$;

г) $3B > 3(B - 2) \geq 3(c - 2)$.

Из а) — г) следует справедливость (18), а следовательно, и (14).

Лемма 2.3.9. *Для любого q_c из $[c, a_c - 1]$ справедливо неравенство*

$$\sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i < q_c \prod_{i=1}^{c-1} a_i.$$

Доказательство следует из леммы 2.3.2.

Лемма 2.3.10. *Для любого ϕ_c из $[c, b_c^c - 1]$ справедливо неравенство*

$$\sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c < \phi_c \prod_{i=1}^{c-1} b_i^c.$$

Доказательство следует из леммы 2.3.2.

Замечание 2.3.1. Для любого целого q_c из $[0, a_c - 1]$ все элементы $D_{q_c}^c$ расположены на отрезке

$$\left[q_c \prod_{i=1}^{c-1} a_i, \sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i + (a_c - 1) \prod_{i=1}^{c-1} a_i \right]_{a^c}.$$

Элемент $q_c \prod_{i=1}^{c-1} a_i$ назовем *первым* элементом множества $D_{q_c}^c$, а элемент $\sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i + q_c \prod_{i=1}^{c-1} a_i$ — *последним* элементом $D_{q_c}^c$.

Замечание 2.3.2. Для любого целого ϕ_c из $[0, b_c^c - 1]$ все элементы $E_{\phi_c}^c$ расположены на отрезке

$$\left[\phi_c \prod_{i=1}^{c-1} b_i^c, \sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c + (b_c^c - 1) \prod_{i=1}^{c-1} b_i^c \right]_{b^c}.$$

Элемент $\phi_c \prod_{i=1}^{c-1} b_i^c$ назовем *первым* элементом множества $E_{\phi_c}^c$, а элемент $\sum_{s=1}^{c-1} (b_s^c - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c b_i^c + \phi_c \prod_{i=1}^{c-1} b_i^c$ — *последним* элементом $E_{\phi_c}^c$.

Лемма 2.3.11. Для любого q_c из $[0, a_c - c]$ множество $F_{q_c}^c$ пусто на отрезке $\left[t_c^c + (q_c + 1) \prod_{i=1}^{c-1} a_i, \prod_{i=1}^c a_i - 1 \right]_{a^c}$ и для любого q_c из $[c - 2, a_c - 2]$ множество $F_{q_c}^c$ полно на отрезке $\left[t_c^c, (q_c + 1) \prod_{i=1}^{c-1} a_i - 1 \right]_{a^c}$.

Доказательство. Тот факт, что $F_{q_c}^c$, где $q_c \in [0, a_c - c]$, пусто на отрезке $\left[t_c^c + (q_c + 1) \prod_{i=1}^{c-1} a_i, a_c - 1 \right]_{a^c}$, вытекает из замечания 2.3.1, определения величины t_c^c и леммы 2.3.9.

Рассмотрим множества $D_0^c, D_1^c, \dots, D_{a_c-1}^c$. Эти множества не пересекаются, их объединение дает все числа отрезка $[0, a_c - 1]$, и они получаются друг из друга сдвигом на число, кратное $\prod_{i=1}^{c-1} a_i$ (это вытекает из следствия леммы 2.1.1 и определения множеств $D_0^c, D_1^c, \dots, D_{a_c-1}^c$). Каждое из множеств $D_{q_c}^c$ ($q_c \in [0, a_c - 1]$) расположено на отрезке

$$\left[q_c \prod_{i=1}^{c-1} a_i, \sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i + q_c \prod_{i=1}^{c-1} a_i \right]_{a^c},$$

и, следовательно, расстояние между последним и первым элементами равно $\sum_{s=1}^{c-1} (a_s - 1) \prod_{\substack{i=1 \\ i \neq s, s+1}}^c a_i$, что меньше или равно $c \prod_{i=1}^{c-1} a_i$ (это вытекает из леммы 2.3.9).

В силу того, что каждое из множеств $D_{q_c}^c$ ($q_c \in [0, a_c - 1]$) сдвинуто циклически относительно $D_{q_c-1}^c$ на $\prod_{i=1}^{c-1} a_i$ (если $q_c = 0$, то $D_{q_c-1}^c = D_{a_c-1}^c$),

на отрезке $\left[q_c \prod_{i=1}^{c-1} a_i, t^c + (q_c + 1) \prod_{i=1}^{c-1} a_i - 1 \right]_{a^c}$ могут быть расположены только элементы множеств $D_{q_c-(c-1)}^c, D_{q_c-(c-2)}^c, \dots, D_{q_c-1}^c, D_{q_c}^c, D_{q_c+1}^c, \dots, D_{q_c+(c-2)}^c, D_{q_c+(c-1)}^c$ (если $q_c - i = 0$, где $i \in [0, c-2]$, то надо положить $D_{q_c-i-j}^c = D_{a_c-j}^c$ для всех $j \in [1, c-i-1]$, если же $q_c + i = a_c - 1$, где $i \in [0, c-2]$, то надо положить $D_{q_c+i+j}^c = D_{j-1}^c$ для всех $j \in [1, c-i-1]$).

Отсюда также вытекает, что на отрезке $\left[0, t^c + (q_c + 1) \prod_{i=1}^{c-1} a_i - 1 \right]_{a^c}$ могут быть расположены элементы множеств

$$D_{a_c-(c-1)}^c, D_{a_c-(c-2)}^c, \dots, D_{a_c-1}^c, D_0^c, D_1^c, \dots, D_{a_c+(c-1)}^c,$$

т. е.

$$D_{a_c-(c-1)}^c, D_{a_c-(c-2)}^c, \dots, D_{a_c-1}^c, F_{q_c}^c, D_{a_c+1}^c, \dots, D_{a_c+(c-1)}^c,$$

где $q_c \in [0, a_c - c]$.

Сравним разность между первым элементом множества $D_{q_c+1}^c$, $x_{q_c} = (q_c + 1) \prod_{i=1}^{c-1} a_i$, и последним элементом множества $D_{a_c-1}^c$, $y = t^c - 1$, где $q_c \in [0, a_c - c]$.

В силу того, что $x_{q_c} - y = (q_c + 1) \prod_{i=1}^{c-1} a_i - t^c + 1$, $(q_c + 1) \prod_{i=1}^{c-1} a_i - t^c$ элементов, расположенных между y и x_{q_c} , принадлежат множествам $D_0^c, D_1^c, \dots, D_{q_c}^c$, т. е. $F_{q_c}^c$. Следовательно, на отрезке $\left[t^c, (q_c + 1) \prod_{i=1}^{c-1} a_i - 1 \right]_{a^c}$ множество $F_{q_c}^c$ полно ($q_c \in [0, a_c - c]$).

Лемма 2.3.12. Для любого ϕ_c из $[0, b_c^c - c]$ множество $H_{\phi_c}^c$ пусто на отрезке $\left[r^c + (\phi_c + 1) \prod_{i=1}^{c-1} b_i^{c-1}, \prod_{i=1}^c b_i^c - 1 \right]_{b^c}$, и для любого ϕ_c из $[c-2, b_c^c - 2]$ множество $H_{\phi_c}^c$ полно на отрезке $\left[r^c, (\phi_c + 1) \prod_{i=1}^{c-1} b_i^c - 1 \right]_{b^c}$.

Доказательство аналогично доказательству леммы 2.3.11.

§ 4. Специальное соединение контактных схем

Замечание 2.4.1. Для любого q_c из $[c-2, a_c - c]$ множество $F_{q_c}^c$ принадлежит классу $D \left(t^c, (q_c + 1) \prod_{i=1}^{c-1} a_i - t^c, t^c, a^c \right)$.

Это вытекает из леммы 2.3.11 и определения множеств $D(r_1, r_2, r_3, d)$.

Замечание 2.4.2. Для любого ϕ_c из $[c-2, b_c^c - 2]$ множество $H_{\phi_c}^c$ принадлежит классу $D \left(r^c, (\phi_c + 1) \prod_{i=1}^{c-1} b_i^c - r^c, r^c, b^c \right)$.

Это вытекает из леммы 2.3.12 и определения множеств $D(r_1, r_2, r_3, d)$.

Лемма 2.4.1. Для любых целого $k, l \in \left[1, \prod_{i=1}^c a_i - 2t^c \right]$ и некоторого множества $D_1 (D_1 \in D(t^c, l, t^c, a^c))$

$$L(n_1 a^c, k + D_1) \leq 4n \sum_{i=1}^c a_i.$$

Доказательство разбивается на два случая:

- 1) $l \in \left[1, (c-1) \prod_{i=1}^{c-1} a_i - t^c \right]$;
- 2) $l \in \left[(c-1) \prod_{i=1}^{c-1} a_i - t^c + 1, a^c - 2t^c \right]$.

В первом случае положим $k_1 = k$ и $k_2 = k + l + t^c - (c-1) \prod_{i=1}^{c-1} a_i$.

Из замечания 2.4.1 следует, что множества $k_1 + F_{c-2}^c$ и $k_2 + F_{c-2}^c$ принадлежат соответственно классам

$$k_1 + D \left(t^c, (c-1) \prod_{i=1}^{c-1} a_i - t^c, t^c, a^c \right)$$

и

$$k_2 + D \left(t^c, (c-1) \prod_{i=1}^{c-1} a_i - t^c, t^c, a^c \right).$$

Легко проверить, что множество $(k_1 + F_{c-1}^c) \cap (k_2 + F_{c-2}^c) - k$ (которое мы обозначим через D) принадлежит классу $D(t^c, l, t^c, a^c)$ (рис. 6, а).

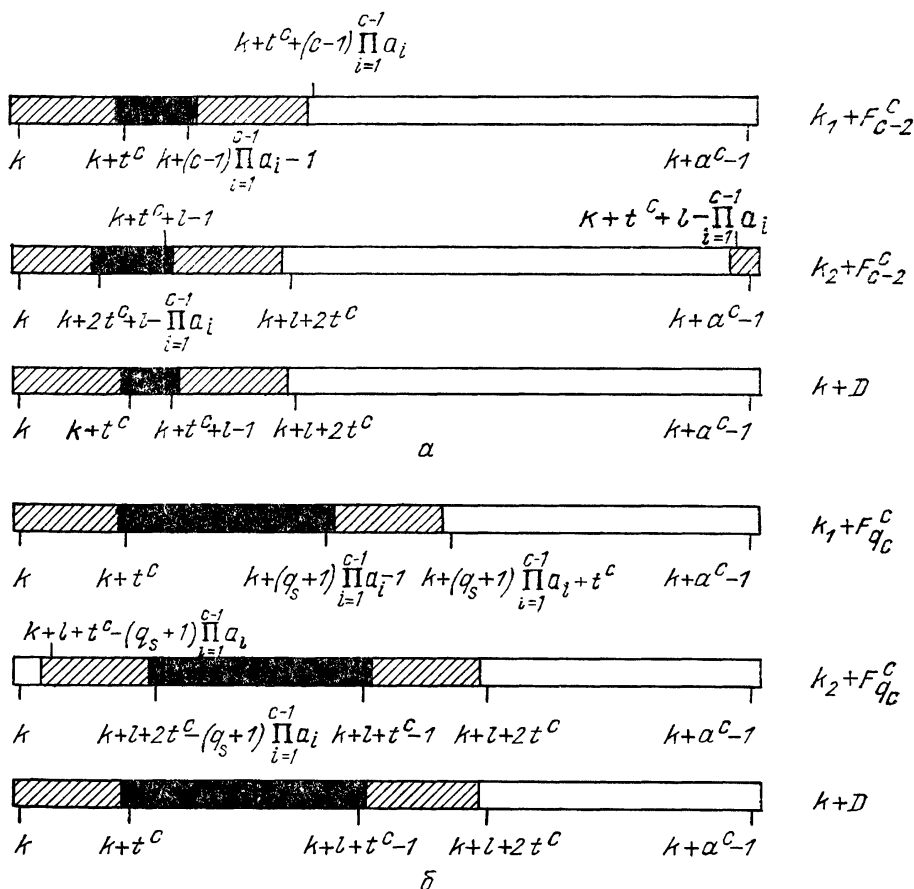


Рис. 6

По следствию из леммы 2.2.1

$$L(n, a^c, k_1 + F_{c-2}^c) \leq 2n \sum_{i=1}^c a_i, \quad L(n, a^c, k_2 + F_{c-2}^c) \leq 2n \sum_{i=1}^c a_i,$$

При последовательном соединении этих двух схем получится схема со сложностью

$$L(n, a^c, k + D) \leq 4n \sum_{i=1}^c a_i.$$

Во втором случае положим $k_1 = k$ и $k_2 = k + l + t^c - (q_c + 1) \prod_{i=1}^{c-1} a_i$, где q_c — наибольшее целое из отрезка $[c - 2, a_c - c]$, такое что

$$(q_c + 1) \prod_{i=1}^{c-1} a_i \leq t^c + l.$$

Из замечания 2.4.1 следует, что множества $k_1 + F_{q_c}^c$ и $k_2 + F_{q_c}^c$ принадлежат соответственно классам

$$k_1 + D \left(t^c, (q_c + 1) \prod_{i=1}^{c-1} a_i - t^c, t^c, a^c \right)$$

и

$$k_2 + D \left(t^c, (q_c + 1) \prod_{i=1}^{c-1} a_i - t^c, t^c, a^c \right).$$

Легко проверить, что множество $(k_1 + F_{q_c}^c) \cup (k_2 + F_{q_c}^c) - k$ (которое мы обозначим через D) принадлежит классу $D(t^c, l, t^c, b^c)$ (рис. 6, б). По следствию из леммы 2.2.1

$$L(n, a^c, k_1 + F_{q_c}^c) \leq 2n \sum_{i=1}^c a_i, \quad L(n, a^c, k_2 + F_{q_c}^c) \leq 2n \sum_{i=1}^c a_i.$$

При параллельном соединении этих двух схем получится схема, у которой

$$L(n, a^c, k + D) \leq 4n \sum_{i=1}^c a_i.$$

Лемма 2.4.2. Для любых целого k, l из $\left[1, \prod_{i=1}^c b_i^c - 2r^c\right]$ и некоторого множества D_2 ($D_2 \in D(r^c, l, r^c, b^c)$)

$$L(n, b^c, k + D_2) \leq 4n \sum_{i=1}^c b_i^c.$$

Доказательство аналогично доказательству леммы 2.4.1.

Теорема 2.4.1. Для любых целого k, l из $[0, a^c - 1]$ и c из $[2, B]$ существует схема со сложностью

$$L(n, a^c, [k, k + l]_{a^c}) \leq c^2 a_1 n.$$

Доказательство. Вначале будут получены схемы со сложностью

$$L(n, a^c, k + D_*^c) \leq c^2 a_1 n, \quad L(n, a^c, k + D_{**}^c) \leq c^2 a_1 n,$$

где $D_*^c \in D(0, l, t^c, a^c)$, $D_{**}^c \in D(t^c, l, 0, a^c)$, $l \in [1, a^c - t^c - 1]$.

Схемы будут построены по индукции, по числу c .

Построим схему со сложностью $L(n, a^c, k + D_1^c) \leq c^2 a_1 n$.

Для $c=2$ по лемме 1.4.1 для любых целого k и l из $[0, a^2 - 1]$ можно построить схему со сложностью

$$L(n, a^2, [k, k + l]_{a^2}) \leq 2n(a_1 + 2a_2).$$

Проверим, что $2n(a_1 + 2a_2) \leq 2^2 a_1 n$. Это верно, так как

$$2n(a_1 + 2a_2) \leq 6na_1 \leq 4a_1 n.$$

Заметим, что множество $[k, k + l]_{a^2}$, где $l \in [0, a^2 - 1]$, принадлежит классу $k + D_*^2$, $D_*^2 \in D(0, l, t^2, a^2)$.

Предположим, что для любых целого k, l из $[0, a^{c-1} - t^{c-1} - 1]$ и некоторого D_*^{c-1} , $D_*^{c-1} \in D(0, l, t^{c-1}, a^{c-1})$, существует схема со сложностью

$$L(n, a^{c-1}, k + D_*^{c-1}) \leq (c-1)^2 a_1 n.$$

Покажем, как, исходя из этой схемы, получить схему со сложностью $L(n, a^c, k + D_*^c) \leq c^2 a_1 n$, где $D_*^c \in D(0, l, t^c, a^c)$, k — любое целое, $l \in [0, a^c - t^c - 1]$.

Докажем две вспомогательные леммы.

Лемма 2.4.3. Для любых целого k, l из $[0, a^c - t^c - 1]$ и некоторого $D_*^c (D_*^c \in D(0, l, t^c, a^c))$

$$L(n, a^c, k + D_*^c) \leq c^2 a_1 n.$$

Доказательство разбивается на два этапа.

На первом этапе будет получена схема со сложностью

$$L(n, b^c, k + D_1^c) \leq c^2 a_1 n,$$

где $D_1^c \in D(0, l, r^c, b^c)$, k — любое целое, $l \in [0, b^c - r^c - 1]$.

На втором этапе будет получена схема со сложностью

$$L(n, a^c, k + D_*^c) \leq c^2 a_1 n,$$

где $D_*^c \in D(0, l, t^c, a^c)$, k — любое целое, $l \in [0, a^c - t^c - 1]$.

Первый этап. Выберем $k_1 = k - r^c$. Множество $k_1 + D_2^c$, где $D_2^c \in D(r^c, r^c, r^c, b^c)$, является полным на $[k, k + r^c - 1]_{b^c}$ и пустым на $[k + 2r^c, k + b^c - r^c - 1]_{b^c}$.

Множество $k + D_3^c$, где $D_3^c \in D(0, r^c, r^c, b^c)$, получается в результате пересечения $k_1 + D_2^c$ с множеством $k + D_1^{c-1}$, где $D_1^{c-1} \in D(0, r^c, t^{c-1}, a^{c-1})$.

Множество $k_1 + D_1^{c-1}$ пусто на отрезке $[k - a^{c-1} + r^c + t^{c-1}, k - 1]_{a^c}$.

Из леммы 2.3.8 следует, что $2r^c + t^{c-1} < a^{c-1}$, поэтому длина отрезка $[k - a^{c-1} + r^c + t^{c-1}, k - 1]_{a^{c-1}}$ (равная $a^{c-1} - t^{c-1} - r^c - 1$) больше длины отрезка $[k - r^c, k - 1]_{b^c}$ (равной $r^c - 1$).

По лемме 2.4.2 для некоторого D_2^c , где $D_2^c \in D(r^c, r^c, r^c, b^c)$, существует схема со сложностью

$$L(n, b^c, k_1 + D_2^c) \leq 4n \sum_{i=1}^c b_i^c.$$

По индуктивному предположению существует схема со сложностью

$$L(n, a^{c-1}, k + D_1^{c-1}) \leq (c-1)^2 a_1 n$$

для любого целого k и $D_1^{c-1} \in D(0, r^c, t^{c-1}, b^{c-1})$.

При последовательном соединении этих двух схем получится схема со сложностью

$$L(n, b^c, k + D_3^c) \leq 4n \sum_{i=1}^c b_i^c + (c-1)^2 a_1 n \leq 4nca_1 + (c-1)^2 a_1 n \leq c^2 a_1 n,$$

где k — любое целое, $D_3^c \in D(0, r^c, r^c, b^c)$.

Чтобы получить множество $k + D_1^c$, где $D_1^c \in D(0, l, r^c, b^c)$, k — любое целое, $l \in [0, b^c - r^c - 1]$, надо объединить два множества $k + D_3^c$ и $k + D_4^c$, где $D_3^c \in D(0, r^c, r^c, b^c)$, $D_4^c \in D(r^c, l - r^c, r^c, b^c)$.

По лемме 2.4.2 для некоторого D_4^c , где $D_4^c \in D(r^c, l - r^c, r^c, b^c)$, $l \in [r^c, b^c - 2r^c - 1]_{b^c}$,

$$L(n, b^c, k + D_4^c) \leq 4n \sum_{i=1}^c b_i^c.$$

При параллельном соединении двух схем со сложностями

$$L(n, b^c, k + D_3^c) \leq c^2 a_1 n, \quad L(n, b^c, k + D_4^c) \leq 4n \sum_{i=1}^c b_i^c$$

получится схема со сложностью

$$L(n, b^c, k + D_1^c) \leq c^2 a_1 n + 4n \sum_{i=1}^c b_i^c \leq c^2 a_1 n + 4nca_1 \leq c^2 a_1 n,$$

где $D_1^c \in (0, l, r^c, b^c)$, k — любое целое, $l \in [0, b^c - r^c - 1]$.

Второй этап. Выберем $k_2 = k - t^c$. Множество $k_2 + D_5^c$, где $D_5^c \in D(t^c, t^c, t^c, a^c)$, является полным на $[k, k + t^c - 1]$ и пустым на $[k + 2t^c, k + a^c - t^c - 1]_{a^c}$.

Множество $k + D_6^c$, где $D_6^c \in (0, t^c, t^c, a^c)$, получается в результате пересечения множества $k_2 + D_5^c$ с множеством $k + D_1^c$, где $D_1^c \in D(0, t^c, r^c, b^c)$.

Множество $k + D_1^c$ пусто на отрезке $[k - b^c + t^c + r^c, k - 1]_{b^c}$.

Из (1), (2), определения b^c и леммы 2.3.6 следует, что $2t^c + r^c < b^c$, поэтому длина отрезка $[k - b^c + r^c + t^c, k - 1]$ (равная $b^c - r^c - t^c - 1$) больше, чем длина отрезка $[k - t^c, k - 1]_{a^c}$ (равная $t^c - 1$), и поэтому множество $k + D_1^c$ пусто на отрезке $[k - t^c, k - 1]_{b^c}$.

По лемме 2.4.1 для некоторого D_5^c , где $D_5^c \in D(t^c, t^c, t^c, a^c)$, существует схема со сложностью

$$L(n, a^c, k_2 + D_5^c) \leq 4n \sum_{i=1}^c a_i.$$

На первом этапе была построена схема со сложностью

$$L(n, b^c, k + D_1^c) \leq c^2 a_1 n,$$

где $D_1^c \in D(0, t^c, r^c, b^c)$, k — любое целое.

При последовательном соединении этих двух схем получится схема со сложностью

$$L(n, a^c, k + D_6^c) \leq 4n \sum_{i=1}^c a_i + c^2 a_1 n \leq 4nca_1 + c^2 a_1 n \leq ca_1 n,$$

где k — любое целое, $D_6^c \in D(0, t^c, t^c, a^c)$.

Чтобы получить множество $k + D_*^c$, где $D_*^c \in D(0, l, t^c, a^c)$, k — любое целое, $l \in [0, a^c - t^c - 1]$, надо объединить два множества $k + D_6^c$ и $k + D_7^c$, где $D_6^c \in D(0, t^c, t^c, a^c)$, $D_7^c \in D(t^c, l - t^c, t^c, a^c)$, $l \in [t^c, a^c - 2t^c - 1]$.

По лемме 2.4.1 для некоторого D_7^c , где $D_7^c \in D(t^c, l - t^c, t^c, a^c)$ и $l \in [t^c, a^c - 2t^c - 1]$, существует схема со сложностью

$$L(n, a^c, k + D_7^c) \leq 4n \sum_{i=1}^c a_i.$$

При параллельном соединении двух схем со сложностями

$$L(n, a^c, k + D_6^c) \leq c^2 a_1 n, \quad L(n, a^c, k + D_7^c) \leq 4n \sum_{i=1}^c a_i$$

получится схема со сложностью

$$L(n, a^c, k + D_*^c) \leq c^2 a_1 n + 4n \sum_{i=1}^c a_i \leq c^2 a_1 n + 4n c a_1 \leq c^2 a_1 n.$$

Лемма доказана.

Построим схему со сложностью $L(n, a^c, k + D_{**}^c) \leq c^2 a_1 n$.

Для $c = 2$ по лемме 1.4.1 для любых целого k и $l \in [0, a^2 - 1]$ можно построить схему со сложностью

$$L(n, a^2, [k, k + l]_{a^2}) \leq 2n(a_1 + 2a_2).$$

Проверим, что $2n(a_1 + 2a_2) \leq 2^2 a_1 n$. Это верно, так как

$$2n(a_1 + 2a_2) \leq 6na_1 \leq 4a_1 n.$$

Заметим, что множество $[k, k + l]_{a^2}$, где $l \in [0, a^2 - 1]$, принадлежит классу $k + D_{**}^2$, $D_{**}^2 \in D(t^2, l, 0, a^2)$.

Предположим, что для любых целого k и l , $l \in [0, a^{c-1} - 1]$, и некоторого $D_{**}^{c-1} \in D(t^{c-1}, l, 0, a^{c-1})$ существует схема со сложностью

$$L(n, a^{c-1}, k + D_{**}^{c-1}) \leq (c-1)^2 a_1 n.$$

Покажем, как, исходя из этой схемы, получить схему со сложностью

$$L(n, a^c, k + D_{**}^c) \leq c^2 a_1 n,$$

где $D_{**}^c \in D(t^c, l, 0, a^c)$, k — любое целое, $l \in [0, a^c - t^c - 1]$.

Лемма 2.4.4. Для любых целого k , l из $[0, a^c - t^c - 1]$ и некоторого D_{**}^c , $D_{**}^c \in D(t^c, l, 0, a^c)$,

$$L(n, a^c, k + D_{**}^c) \leq c^2 a_1 n.$$

Доказательство аналогично доказательству леммы 2.4.3.

Продолжим доказательство теоремы. Оставшаяся часть доказательства разбивается на три случая:

- 1) $l \in [0, t^c - 1]$;
- 2) $l \in [t^c, 2t^c - 1]$;
- 3) $l \in [2t^c, a^c - 1]$.

В первом случае $l \in [0, t^c - 1]$. Положим $k_1 = k$, $k_2 = k + l - 2t^c + 1$.

Рассмотрим множества $k_1 + D_1$, где $D_1 \in D(0, t^c, t^c, a^c)$, и $k_2 + D_2$, где $D_2 \in D(t^c, t^c, 0, a^c)$. При пересечении они образуют $[k, k + l]_{a^c}$.

По лемме 2.4.3

$$L(n, a^c, k_1 + D_1) \leq c^2 a_1 n.$$

По лемме 2.4.4

$$L(n, a^c, k_2 + D_2) \leq c^2 a_1 n.$$

Эти две схемы надо соединить последовательно.

Во втором случае $l \in [t^c, 2t^c - 1]$. Положим $k_1 = k$, $k_2 = k + l - 3t^c + 1$. Рассмотрим множества $k_1 + D_1$ и $k_2 + D_2$, где $D_1 \in D(0, 2t^c, t^c, a^c)$, $D_2 \in D(t^c, 2t^c, 0, a^c)$. При пересечении они образуют $[k, k + l]_{a^c}$.

По лемме 2.4.3

$$L(n, a^c, k_1 + D_1) \leq c^2 a_1 n.$$

По лемме 2.4.4

$$L(n, a^c, k_2 + D_2) \leq c^2 a_1 n.$$

Эти две схемы надо соединить последовательно.

В третьем случае $l \in [2t^c, a^c - 1]$. Положим $k_1 = k_3 = k$, $k_2 = k + l - 2t^c + 1$.

Рассмотрим множества $k_1 + D_1$, $k_2 + D_2$, $k_3 + D_3$, где $D_1 \in D(0, t^c, t^c, a^c)$, $D_2 \in D(t^c, t^c, 0, a^c)$, $D_3 \in D(t^c, 1 + l - 2t^c, t^c, a^c)$. Объединение этих множеств дает множество $[k, k + l]_{a^c}$.

По лемме 2.4.3

$$L(n, a^c, k_1 + D_1) \leq c^2 a_1 n.$$

По лемме 2.4.4

$$L(n, a^c, k_2 + D_2) \leq c^2 a_1 n.$$

По лемме 2.4.1

$$L(n, a^c, k_3 + D_3) \leq 4n \sum_{i=1}^c a_i \leq (\text{см. (3)}) \leq 4nca_1.$$

Эти три схемы надо соединить параллельно.

Очевидно, что в каждом из трех случаев

$$L(n, a^c, [k, k + l]_{a^c}) \leq c^2 a_1 n + c^2 a_1 n + 4nca_1 \leq c^2 a_1 n.$$

Теорема доказана.

§ 5. Реализация монотонных симметрических функций контактными схемами

Теорема 2.5.1. Для любого $\bar{p}$, $\bar{p} \in [0, n]$, существует схема для $M_n^{\bar{p}}$ такая, что ее сложность не превосходит по порядку

$$n(\ln n)^4 / (\ln \ln n)^2.$$

Доказательство. В теореме 2.4.1 положим

$$k = \bar{p},$$

$$l = n - \bar{p},$$

$$c = B = \lfloor c_1 \ln n / \ln \ln n \rfloor,$$

где c_1 — некоторая константа. Тогда

$$p_{2B} \leq \ln n,$$

$$a_1 = p_B p_{2B} \leq \ln^2 n,$$

$$a_1 a_2 \dots a_B = p_B p_{2B} p_{B-1} p_{2B-1} \dots p_1 p_{B+1} \geq n + 1.$$

Поэтому

$$B^2 a_1 n \leq n(\ln n)^4 / (\ln \ln n)^2.$$

Добавление

Пусть f — монотонная функция (не обязательно симметрическая!), $L(f)$ — наименьшее число контактов, достаточное для реализации функции f контактной схемой, и $L^+(f)$ — схемой, содержащей лишь замыкающие контакты.

Пусть $\lambda(f) = L^+(f)/L(f)$ и $\lambda(n) = \max \lambda(f)$ (максимум берется по всем монотонным функциям от n аргументов).

Н. А. Карпова показала [1], что

$$\lambda(n) \geq 3/2.$$

О. Б. Лупанов показал [3], что

$$\lambda(n) \rightarrow \infty \quad (n \rightarrow \infty),$$

точнее,

$$\lambda(n) \gtrsim \log n / \log \log n.$$

Из результатов Р. Е. Кричевского [2] следует, что

$$\lambda(n) \gtrsim \log n.$$

О. Б. Лупанов показал [4], что

$$\lambda(n) \gtrsim \sqrt{n}.$$

Докажем более сильное утверждение.

Теорема Д.1.1. $\lambda(n) \gtrsim n (\ln \ln n)^2 / (\ln n)^4$.

Доказательство. Рассмотрим монотонную симметрическую функцию $M_n^{[n/2]+1}$.

А. А. Марковым [5] показано, что в классе контактно-вентильных схем, содержащих лишь замыкающие контакты, функция $M_n^{[n/2]+1}$ требует для своей реализации $[(n+1)/2](n+1 - [(n+1)/2]) \sim n^2/4$ контактов.

Отсюда следует, что

$$L^+(M_n^{[n/2]+1}) \gtrsim n^2. \quad (19)$$

С другой стороны, в силу теоремы 2.5.1

$$L(M_n^{[n/2]+1}) \leq n (\ln n)^4 / (\ln \ln n)^2. \quad (20)$$

По (19) и (20)

$$\lambda(M_n^{[n/2]+1}) \gtrsim n (\ln \ln n)^2 / (\ln n)^4,$$

и, следовательно,

$$\lambda(n) \gtrsim n (\ln \ln n)^2 / (\ln n)^4.$$

СПИСОК ЛИТЕРАТУРЫ

1. Карпова Н. А. О контактных схемах для монотонных функций // ДАН СССР.— 1958.— 123, № 1.— С. 25—27.
2. Кричевский Р. Е. О сложности параллельно-последовательных контактных схем, реализующих одну последовательность булевых функций // Проблемы кибернетики. Вып. 12.— М.: Наука, 1964.— С. 45—56.
3. Лупанов О. Б. О сравнении сложности реализации монотонных функций контактными схемами, содержащими лишь замыкающие контакты, и произвольными контактными схемами // ДАН СССР.— 1962.— 144, № 6.— С. 1245—1248.
4. Лупанов О. Б. К вопросу о реализации симметрических функций алгебры логики контактными схемами // Проблемы кибернетики. Вып. 15.— М.: Наука, 1965.— С. 85—99.
5. Марков А. А. О минимальных контактно-вентильных двуполюсниках для монотонных симметрических функций // Проблемы кибернетики.— Вып. 8.— М.: Физматгиз, 1962.— С. 117—122.
6. Shannon C. E. The synthesis of two-terminal switching circuits // Bell Syst. Techn. J.— 1949.— 28, № 1.— Р. 59—98. (Рус. пер.: Шеннон К. Работы по теории информации и кибернетике.— М.: ИЛ, 1963.— С. 59—101.)