

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ДВОИЧНЫХ ФУНКЦИЙ, ИМЕЮЩИХ МАЛО «ПОДФУНКЦИЙ»

А. И. ТООМ

(МОСКВА)

Пусть имеется двоичная функция от n переменных: $f(x_1, \dots, x_n)$ (каждое x_i , а также f принимают два значения: 0, 1).

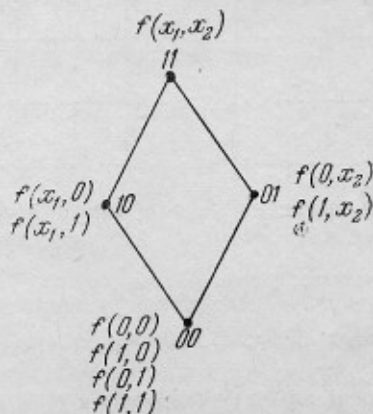
Если мы часть переменных x_{i_1}, \dots, x_{i_k} зафиксируем, то f станет некоторой функцией от остальных переменных

$$f(x_1, \dots, x_n) \Big|_{x_{i_1}=c_{i_1}, \dots, x_{i_k}=c_{i_k}} = f'(x_{j_1}, \dots, x_{j_{n-k}}).$$

Назовем полученную функцию f' *подфункцией* функции f . Очевидно, каждая подфункция f' определяется тем, каким способом поставить в соответствие каждому из x_1, \dots, x_n один из символов 0, 1, \sim в знак того, зафиксировано это x_i нулем, единицей или не зафиксировано. Например, для функции $f(x_1, x_2, x_3, x_4, x_5)$ набор ($\sim 0 \sim 10$) определяет подфункцию

$$f(x_1, 0, x_3, 1, 0).$$

Очевидно, $f(x_1, \dots, x_n)$ имеет 3^n подфункций, некоторые из которых могут быть тождественно равными. Рассмотрим множество M вершин n -мерного куба. Наборы, соответствующие вершинам куба M , а тем самым и вершины, будем обозначать наборами греческих букв: $(\alpha_1 \dots \alpha_n)$, $(\omega_1 \dots \omega_n)$ или сокращенно (α) , (ω) . Подфункции функции $f(x_1, \dots, x_n)$ удобно мыслить расположенными в вершинах куба M следующим образом: в наборе из 0, 1, \sim , определяющем данную подфункцию, заменим 0 и 1 на α , а \sim на ω и каждую подфункцию поместим в ту вершину, которая определяется полученным набором (см. рисунок — там около каждой вершины 2-мерного куба написаны помещенные в нее подфункции).



Объявим эквивалентными две подфункции f' , f'' функции f , если:

- они помещены в одну вершину куба M ;
- f' и f'' тождественно равны.

Тогда все 3^n подфункций функции f разобьются на классы эквивалентности. Каждый такой класс является подмножеством функций, помещенных в одной из вершин куба M . Пусть (α_i) — одна из этих вершин. Число классов эквивалентности функций, помещенных в данную вершину, обозначим через $P_f(\alpha_i)$. Сумма всех $P_f(\alpha_i)$, т. е. число всех классов эквивалентности, очевидно, не меньше 2^n и не больше 3^n . Пусть оно равно $2^n k_f$, где $1 \leq k_f \leq 1,5^n$. Содержание работы состоит в изучении связи числа k_f и сложности реализации функции $f(x_1, \dots, x_n)$ в классе схем из функциональных элементов в базисе $\{\vee, \&, \neg\}^*$.

Теорема 1 (нижняя оценка). Для любых целых $n, a, 1 \leq a \leq n, n \geq n_0, a \geq a_0$, среди таких функций от n переменных, для которых k_f не превышает $1,5^a$, существуют такие, которые не реализуются схемой из функциональных элементов в базисе $\{\vee, \&, \neg\}$ сложности меньшей, чем $\frac{2^a}{a}(1 - \varepsilon)$ (ε произвольное положительное, причем n_0 и a_0 зависят от ε).

Доказательство. Рассмотрим множество функций $f(x_1, \dots, x_n)$ вида $g(x_1, \dots, x_a)$, т. е. зависящих только от x_1, \dots, x_a . Для каждой из них $k_f \leq 1,5^a$. Из нижней оценки для функции Шеннона (см. [1]) следует доказываемое утверждение **).

Из доказанного видно, что, желая для каждой из $f(x_1, \dots, x_n)$ построить схему тем более простую, чем меньше k_f , нельзя, вообще говоря, ожидать, что сложность этой схемы будет асимптотически меньше, чем

$$\frac{k_f^{\log_1 5^2}}{\log_{1,5} k_f}.$$

Теорема 2 (верхняя оценка). Для любой функции $f(x_1, \dots, x_n)$ существует схема из функциональных элементов в базисе $\{\vee, \&, \neg\}$, реализующая $f(x_1, \dots, x_n)$ и сложности ***) $\prec k_f^2 n^2$.

Доказательство верхней оценки состоит из 10 лемм.

Таблица 1

	1	2
1	a	b
2	c	d
3	a	b

Таблица 2

	1	2
1	c	d
2	a	b
3	b	d

Лемма 1. Пусть имеется N таблиц одинакового формата. Из строки и столбцы пронумерованы. В каждую клетку каждой табли-

*) Аналогичные результаты верны и для других базисов.

**) Можно рассматривать также множество функций вида

$$g(x_1, x_2, \dots, x_{a-1}, x_a \vee x_{a+1} \vee \dots \vee x_n)$$

и аналогичные.

***) Знак \prec здесь и дальше означает следующее: если g, h — функции от одних и тех же переменных, то запись $g \prec h$ значит, что существует такое положительное $c = \text{const}$, что $g \leq ch$.

цы вписана некоторая буква. Во всех таблицах вместе встречается R различных букв. Назовем две строки одной или разных таблиц равными, если на одинаковых по номеру местах в них стоят одинаковые буквы*). Аналогично определим равенство столбцов. Пусть во всех таблицах вместе имеется S различных строк и T различных столбцов. Тогда

$$R \leq S \cdot T.$$

Доказательство леммы 1. Пусть сначала у нас есть только одна таблица. Если в ней есть две одинаковые строки, то вычеркнем одну из них — «лишнюю» (т. е. вычеркнем все ее клетки). Так будем делать до тех пор, пока останутся лишь различные строки. Аналогично вычеркнем все «лишние» столбцы. Легко видеть, что число различных невычеркнутых клеток равно R , а число всех невычеркнутых клеток равно $S \cdot T$.

Для $N = 1$ лемма доказана.

Допустим, что лемма доказана для $N = N_0$, и докажем ее для $N = N_0 + 1$. Пусть у нас есть $N_0 + 1$ таблиц. Выделим из них одну и вычеркнем в ней все те строки и столбцы, которые встречаются и в других таблицах. Пусть в ней осталось s различных невычеркнутых строк и t различных невычеркнутых столбцов. Из доказательства леммы для $N = 1$ следует, что в ней осталось не более st различных невычеркнутых клеток. Очевидно, в остальных таблицах имеется $S - s$ различных строк и $T - t$ различных столбцов. Тогда число различных клеток во всех $N_0 + 1$ таблицах не превосходит

$$(S - s)(T - t) + st = ST - (sT + St) + 2st \leq ST.$$

Лемма 1 доказана.

Лемма 2. Пусть $(\alpha_i), (\beta_i), (\gamma_i) \in M$. Пусть при всех i : $\gamma_i = \alpha_i \& \beta_i$. Тогда $P_f(\gamma_i) \leq P_f(\alpha_i) P_f(\beta_i)$.

Доказательство леммы 2. Эта лемма сразу сводится к лемме 1, если подфункции, вписанные в (γ_i) , считать буквами алфавита (одинаковыми, если они тождественно равны), подфункции, вписанные в (α_i) , — строками, подфункции, вписанные в (β_i) , — столбцами. При этом подфункции, вписанные в (δ_i) , где $\delta_i = \alpha_i \vee \beta_i$, превратятся в таблицы. Каждая строка будет распадаться на буквы так же, как функция, вписанная в (α_i) , «распадается» на 2^r своих подфункций, вписанных в (γ_i) (r — число переменных, зафиксированных в (γ_i) , но не в (α_i)). Тогда определенное в лемме 1 равенство строк и столбцов будет соответствовать тождественному равенству соответствующих им функций.

Лемма 2 доказана.

Пусть функция $F(a)$ определена при $a \in G$ и множество G содержит N элементов.

Среднее арифметическое функции $F(a)$ на множестве G обозначим так: $CA(F; G)$, т. е.

$$CA(F; G) = \frac{1}{N} \sum_{a \in G} F(a).$$

Так, например, очевидно, что

$$CA(P_f; M) = k_f.$$

Обозначим через Q_h множество тех вершин куба M , в наборах которых имеется ровно h единиц (очевидно, этих вершин C_n^h).

*) Например, строка 1 табл. 1 равна строке 3 табл. 1 и равна строке 2 табл. 2

Лемма 3. Для любого $n \geq 2$ существует такое h , что $\frac{n}{3} \leq h \leq \leq \frac{n}{2}$ и

$$CA(P_f; Q_h) < k_f.$$

Доказательство леммы 3. Как известно, при $n \geq 2$ и некотором $c = \text{const}$

$$\sum_{\frac{n}{3} \leq h \leq \frac{n}{2}} C_n^h \geq \frac{1}{c} 2^n. \quad (1)$$

Очевидно, что

$$\sum_{\frac{n}{3} \leq h \leq \frac{n}{2}} C_n^h CA(P_f; Q_h) \leq 2^n k_f. \quad (2)$$

Допустим, что при всех h , $\frac{n}{3} \leq h \leq \frac{n}{2}$, имеет место следующее:

$$CA(P_f; Q_h) > ck_f.$$

Тогда, учитывая (1) и (2), получим при $n \geq 2$:

$$2^n k_f > ck_f \sum_{\frac{n}{3} \leq h \leq \frac{n}{2}} C_n^h \geq 2^n k_f.$$

Противоречие.

Лемма 3 доказана.

Пусть $(\psi_i) \in M$ и среди чисел ψ_1, \dots, ψ_n не более h единиц. Обозначим через $Q_h^{(\psi_i)}$ множество таких вершин (φ_i) , что

а) $(\varphi_i) \in Q_h$,

б) при всех i из того, что $\psi_i = 1$, следует, что $\varphi_i = 1$.

Лемма 4. Пусть $h \leq \frac{n}{2}$. Тогда

$$P_f(\psi_i) \leq [CA(P_f; Q_h^{(\psi_i)})]^2.$$

Доказательство леммы 4. Рассмотрим все такие пары наборов $(\alpha_i), (\beta_i)$, что

а) $(\alpha_i) \in Q_h^{(\psi_i)}$; $(\beta_i) \in Q_h^{(\psi_i)}$,

б) при всех i $\alpha_i \& \beta_i = \psi_i$.

Множество этих пар обозначим через B (B не пусто, так как $h \leq n/2$). Очевидно,

$$CA\left(\frac{1}{2}[P_f(\alpha_i) + P_f(\beta_i)]; B\right) = CA(P_f; Q_h^{(\psi_i)}).$$

Тогда существует пара $(\alpha_i), (\beta_i)$, для которой

$$\frac{1}{2}[P_f(\alpha_i) + P_f(\beta_i)] \leq CA(P_f; Q_h^{(\psi_i)}).$$

Отсюда следует (поскольку среднее геометрическое не больше среднего арифметического)

$$P_f(\alpha_i) P_f(\beta_i) \leq [CA(P_f; Q_h^{(\psi_i)})]^2.$$

Применив лемму 2, получим отсюда утверждение леммы 4.

Назовем *цепью* такую последовательность наборов из M : $(\varphi_1^0), (\varphi_1^1), \dots, (\varphi_1^q)$, в которой каждый (кроме первого) набор получается из предыдущего набора заменой ровно одной координаты 0 на 1, причем при всех i выполнено $\varphi_1^0 = 0$.

Лемма 5. Для всякой цепи $(\varphi_1^0), \dots, (\varphi_1^q)$ существует схема, реализующая все функции, описанные в (φ_1^q) сложности

$$\prec \sum_{i=0}^q P_f(\varphi_i^i).$$

Доказательство леммы 5. При $q = 0$ утверждение очевидно (в вершину $(0, \dots, 0)$ вписаны только константы). Пусть теперь $q \geq 1$ и наборы (φ_1^{q-1}) и (φ_1^q) отличаются в j -м разряде. Тогда любая функция $g(x_1, \dots, x_n)$, вписанная в (φ_1^q) , представляется в виде

$$g(x_1, \dots, x_n) = [x_j \& d(x_1, \dots, x_n)] \vee [x_j \& e(x_1, \dots, x_n)],$$

где $d(x_1, \dots, x_n)$, $e(x_1, \dots, x_n)$ — функции, вписанные в набор (φ_1^{q-1}) . Используя эту формулу, можно последовательно реализовать все функции, вписанные в наборы цепи, тратя на каждую новую функцию четыре элемента.

Лемма 5 доказана.

Лемма 6. Существует такое число h , $\frac{n}{3} \leq h \leq \frac{n}{2}$, и три такие цепи

$$(\varphi_i^0), \dots, (\varphi_i^h); (\psi_i^0), \dots, (\psi_i^h); (\chi_i^0), \dots, (\chi_i^{n-2h}),$$

что

$$а) \frac{1}{n} \sum_{j=0}^h CA(P_f; Q_h^{(\varphi_i^j)}) + \frac{1}{n} \sum_{j=0}^h CA(P_f; Q_h^{(\psi_i^j)}) + \frac{1}{n} \sum_{j=0}^{n-2h} CA(P_f; Q_h^{(\chi_i^j)}) + P_f(\varphi_i^h) + P_f(\psi_i^h) \prec k_f;$$

б) при всех i :

$$\varphi_i^h \vee \psi_i^h \vee \chi_i^{n-2h} = 1,$$

$$\varphi_i^h \& \psi_i^h = \varphi_i^h \& \chi_i^{n-2h} = \psi_i^h \& \chi_i^{n-2h} = 0.$$

Доказательство леммы 6. Выберем по лемме 3 такое

$$h, \frac{n}{3} \leq h \leq \frac{n}{2}, \text{ что } CA(P_f; Q_h) \prec k_f.$$

Рассмотрим среднее арифметическое функции, стоящей в левой части равенства условия а) по всем тройкам цепей

$$(\varphi_i^0), \dots, (\varphi_i^h); (\psi_i^0), \dots, (\psi_i^h); (\chi_i^0), \dots, (\chi_i^{n-2h}),$$

для которых выполняется условие б). Чтобы его вычислить, надо сначала заметить, что значения P_f на всех вершинах, входящих в Q_h , входят в него с равным весом. Этот вес легко вычислить, если положить $P_f \equiv 1$. Как легко проверить, оно равно $(3 + \frac{3}{n}) \cdot CA(P_f; Q_h) \prec k_f$. Значит, можно указать три цепи, удовлетворяющие б) и а).

Лемма 6 доказана.

Лемма 7. *Существуют такие три набора (λ_i) , (μ_i) , (ν_i) , что*

- а) при всех i : $\begin{cases} \lambda_i \vee \mu_i \vee \nu_i = 1, \\ \lambda_i \& \mu_i = \lambda_i \& \nu_i = \mu_i \& \nu_i = 0; \end{cases}$
 б) $P_f(\lambda_i) < k_f$; $P_f(\mu_i) < k_f$;

в) *существует схема сложности $< n^2 k_f^2$, реализующая все функции, описанные в наборы (λ_i) , (μ_i) , (ν_i) .*

Доказательство леммы 7. Рассмотрим цепи из леммы 6 и докажем, что за нужные нам наборы можно принять наборы (φ_i^j) , (ψ_i^j) , (χ_i^j) из леммы 6.

Выполнение условий а) и б) очевидно (см. условия а) и б) леммы 6). Далее, из результата леммы 6 следует, что

$$\sum_{j=0}^h \text{CA}(P_f; Q_h^{(\varphi_i^j)}) + \sum_{j=0}^h \text{CA}(P_f; Q_h^{(\psi_i^j)}) + \sum_{j=0}^{n-2h} \text{CA}(P_f; Q_h^{(\chi_i^j)}) < nk_f.$$

Возведя обе части в квадрат и опустив слева все произведения (оставив квадраты), получим:

$$\sum_{j=0}^h [\text{CA}(P_f; Q_h^{(\varphi_i^j)})]^2 + \sum_{j=0}^h [\text{CA}(P_f; Q_h^{(\psi_i^j)})]^2 + \sum_{j=0}^{n-2h} [\text{CA}(P_f; Q_h^{(\chi_i^j)})]^2 < n^2 k_f^2.$$

Отсюда по лемме 4 следует:

$$\sum_{j=0}^n P_f(\varphi_i^j) + \sum_{j=0}^n P_f(\psi_i^j) + \sum_{j=0}^{n-2h} P_f(\chi_i^j) < n^2 k_f^2.$$

Отсюда по лемме 7 следует выполнение условия в).

Лемма 7 доказана.

Лемма 8. Рассмотрим переменную z , которая пробегает k значений: $1, 2, \dots, k$. Пусть имеется некоторое множество G функций $F_i(z)$, принимающих значения $0, 1$. Тогда над этими функциями можно определить обычные действия $\vee, \&, \neg$ и рассматривать схемы из функциональных элементов с этими функциями в качестве входов, реализующие тоже функции от z .

Назовем два значения a, b переменной z эквивалентными, если для всех $F_i(z) \in G$

$$F_i(a) = F_i(b).$$

Тогда все значения z разобьются на l классов эквивалентности W_1, \dots, W_l . Очевидно, схема с функциями $F_i(z) \in G$ в качестве входов может реализовать только функцию, постоянную на каждом W_j . Назовем *характеристической* для некоторого множества H значений z такую функцию от z , которая равна 1 при $z \in H$ и равна 0 при $z \notin H$.

Теперь сформулируем утверждение леммы: *существует схема из функциональных элементов сложности $< l \leq l$ из функций $F_i \in G$ в качестве входов, реализующая характеристические функции для всех W_1, \dots, W_l .*

Доказательство леммы 8. Возьмем какую-нибудь из $F_i \in G$ вместе с ее отрицанием. Реализация этих двух функций обойдется в один элемент. Они являются характеристическими для таких двух непустых множеств H_1, H_2 , что

- а) $H_1 \cup H_2$ — это множество всех значений z ,
 б) $H_1 \cap H_2 = \emptyset$.

Далее, реализовав функцию F' , характеристическую для множества H' , не совпадающего еще ни с каким W_j , мы можем «раздробить» это множество на две части, реализовав характеристические для них функции

$$F' \& F'', \quad F' \& (\neg F''),$$

где $F'' \in G$ и F'' не постоянна на множестве H' . Так, тратя на каждое дробление три новых элемента, мы, в конце концов, получим нужную схему.

Лемма 8 доказана.

Л е м м а 9. Пусть наборы (ε_i) , (ζ_i) , (η_i) , таковы, что при всех i :

$$\begin{cases} \varepsilon_i = \zeta_i \vee \eta_i, \\ \zeta_i \& \eta_i = 0. \end{cases}$$

Пусть $g(x_1, \dots, x_n)$ — одна из подфункций, помещенных в вершине (ε_i) .

Тогда существует схема, реализующая $g(x_1, \dots, x_n)$ сложности $< P_f(\zeta_i)$, входы которой — все подфункции, помещенные в вершине (ζ_i) , и не более чем $P_f(\zeta_i)$ из тех, что помещены в вершину (η_i) .

Доказательство леммы 9. Можно считать, что номера 1, 2, ..., a таковы, что $\zeta_1 = \zeta_2 = \dots = \zeta_a = 1$, номера $a+1, a+2, \dots, a+b$ таковы, что $\eta_{a+1} = \eta_{a+2} = \dots = \eta_{a+b} = 1$, а остальные $a+b+1, \dots, n$ таковы, что $\varepsilon_{a+b+1} = \dots = \varepsilon_n = 0$. Очевидно, что $g(x_1, \dots, x_n)$ является функцией только от x_1, \dots, x_{a+b} :

$$g(x_1, \dots, x_n) \equiv g(x_1, \dots, x_{a+b}).$$

Среди подфункций, вписанных в вершину (ζ_i) , имеется лишь $P_f(\zeta_i)$ различных; обозначим их через

$$l_1(x_1, \dots, x_a), \dots, l_{P_f(\zeta_i)}(x_1, \dots, x_a).$$

Легко видеть, что $g(x_1, \dots, x_{a+b})$ представляется в виде

$$g(x_1, \dots, x_{a+b}) = \bigvee_{k=1}^{P_f(\zeta_i)} [l_k(x_1, \dots, x_a) \& h_k(x_{a+1}, \dots, x_{a+b})],$$

где $h_k(x_{a+1}, \dots, x_{a+b}) = 1$ при таких и только таких значениях $\sigma_{a+1}, \dots, \sigma_{a+b}$ переменных x_{a+1}, \dots, x_{a+b} , что

$$g(x_1, \dots, x_a, \sigma_{a+1}, \dots, \sigma_{a+b}) \equiv l_k(x_1, \dots, x_a).$$

Остается реализовать функции $h_k(x_{a+1}, \dots, x_{a+b})$, потратив на это $< P_f(\zeta_i)$ элементов. Схема, реализующая их, построена в лемме 8, где за переменную z надо принять совокупность переменных x_{a+1}, \dots, x_{a+b} , а за функции $F_j \in G$ принять подфункции, вписанные в (η_i) . Тогда эквивалентными будут такие два набора $\sigma_{a+1}, \dots, \sigma_{a+b}$ и $\tau_{a+1}, \dots, \tau_{a+b}$ значений x_{a+1}, \dots, x_{a+b} , что

$$g(x_1, \dots, x_a, \sigma_{a+1}, \dots, \sigma_{a+b}) \equiv g(x_1, \dots, x_a, \tau_{a+1}, \dots, \tau_{a+b}),$$

и характеристическими для классов эквивалентности будут нужные нам $h_i(x_{a+1}, \dots, x_{a+b})$.

Лемма 9 доказана.

Л е м м а 10. Пусть наборы (λ_i) , (μ_i) , (ν_i) таковы, что при всех i :

$$\begin{cases} \lambda_i \vee \mu_i \vee \nu_i = 1, \\ \lambda_i \& \mu_i = \lambda_i \& \nu_i = \mu_i \& \nu_i = 0. \end{cases}$$

Пусть $f(x_1, \dots, x_n)$ — некоторая функция. Тогда существует схема сложности $\prec P_f(\lambda_i) P_f(\mu_i)$, входы которой — функции, вписанные в наборы (λ_i) , (μ_i) , (ν_i) , реализующая $f(x_1, \dots, x_n)$.

Доказательство леммы 10. Положим для всех i : $\omega_i = \mu_i \vee \nu_i$. По лемме 9 существует схема, реализующая $f(x_1, \dots, x_n)$ сложности $\prec P_f(\lambda_i)$, входы которой — функции, вписанные в набор (λ_i) , и некоторые

$$g_1, \dots, g_{P_f(\lambda_i)}$$

из функций, вписанных в набор (ω_i) . Каждая из функций $g_1, \dots, g_{P_f(\lambda_i)}$ по лемме 9 реализуется схемой сложности $\prec P_f(\mu_i)$, входы которой — функции, соответствующие наборам (μ_i) и (ν_i) . Итак, чтобы реализовать все $g_1, \dots, g_{P_f(\lambda_i)}$, надо $\prec P_f(\lambda_i) P_f(\mu_i)$ элементов.

Чтобы реализовать $f(x_1, \dots, x_n)$, надо

$$\prec P_f(\lambda_i) + P_f(\lambda_i) P_f(\mu_i) \prec P_f(\lambda_i) P_f(\mu_i)$$

элементов.

Лемма 10 доказана.

Из лемм 7 и 10 следует верхняя оценка.

ЛИТЕРАТУРА

1. Лупанов О. Б., Об одном методе синтеза схем, Известия вузов, Радиофизика 1, 1, 1958.

Поступило в редакцию 15 XII 1964.