Тема 2. Сумматоры

С. Б. Гашков, И. С. Сергеев

Предварительно напомним определение схемы из функциональных элементов (СФЭ). Пусть задано множество функций B, аргументы и значения которых принадлежат множеству M. СФЭ над базисом B — это ориентированный граф без ориентированных циклов с вершинами-входами, которым приписаны символы переменных или константы, и функциональными элементами в других вершинах; некоторые вершины отмечены как выходы. Входы и выходы элементов схемы принимают значения в M, а сами функциональные элементы реализуют функции из базиса B. Более подробное определение и доказательство корректности приводится в соответствующих курсах. *Сложностью* схемы S называется число функциональных элементов в ней и обозначается $L(S)$, а *глубиной* — максимальное число элементов в цепочке, ведущей от входа к выходу схемы, которое обозначается $D(S)$. Сложность (глубина) функции f определяется как минимальная сложность (глубина) схемы, реализующей данную функцию. Обозначения: $L(f)$ и $D(f)$.

Рассмотрим задачу построения n-разрядного сумматора — схемы сложения двоичных n-разрядных чисел

$$A = [a_{n-1}, a_{n-2}, \dots, a_0] \text{ и } B = [b_{n-1}, b_{n-2}, \dots, b_0]$$

(схема строится над базисом двуместных булевых функций). Сумму чисел A и B обозначим через $Z = [z_n, z_{n-1}, \dots, z_0]$.

Лемма 1. *Можно построить n-разрядный сумматор S_n, такой, что*

$$L(S_n) = 5n - 3; \qquad D(S_n) = 2n - 1.$$

Доказательство. Построим схему, реализующую известный метод сложения «столбиком». Введем обозначения $x_i = a_i + b_i$ («+» в булевых выражениях будет означать сумму по модулю 2) и $y_i = a_i b_i$. Метод заключается в том, что на каждом шаге вычисляется очередной разряд числа Z по формуле $z_i = x_i + c_i$, где c_i — перенос из младших разрядов, и следующий перенос $c_{i+1} = y_i + x_i c_i$.

Все x_i и y_i вычисляются со сложностью $2n$ и глубиной 1. По 3 операции необходимо для вычисления каждой пары z_i и c_{i+1}, за исключением самой первой, т.к. $z_0 = x_0$ и $c_1 = y_0$, и старшего разряда $z_n = c_n$. Легко видеть, что c_1 вычисляется на глубине 1, c_2 — на глубине 3 и т.д., и окончательно $c_n = z_n$ вычисляется на глубине $2n-1$. Следовательно,

$$L(S_n) = 2n + 3(n-1) = 5n - 3; \qquad D(S_n) = 2n - 1.$$

Н. П. Редькин в 1981 г. показал, что построенная схема — минимальная по сложности (доказательство относится к числу наиболее сложных в классе нижних оценок сложности конкретных функций).

Естественным образом возникает задача минимизации глубины схемы сумматора. Для ее решения достаточно уметь реализовывать функции переноса c_i с небольшой глубиной. Для всех i справедлива формула

$$c_i = y_{i-1} + x_{i-1}(y_{i-2} + x_{i-2}(\ldots(y_1 + x_1 y_0)\ldots)).$$

Введем обозначение:

$$F_i(y_{i-1}, x_{i-1}, \ldots, x_1, y_0) = y_{i-1} + x_{i-1}(y_{i-2} + x_{i-2}(\ldots(y_1 + x_1 y_0)\ldots)).$$

Переменные x_i и y_i здесь являются независимыми.

Введем также сокращения:

$$F_i(k) = F_i(y_{k+i-1}, x_{k+i-1}, \ldots, x_{k+1}, y_k), \qquad F_i = F_i(0).$$

1 Метод золотого сечения

Лемма 2.

$$F_n = F_k(n-k) + x_{n-1} \cdot \ldots \cdot x_{n-k} F_{n-k}.$$

Для доказательства достаточно раскрыть внешние $k-1$ скобок в определении F_i.

Пусть $\{\Phi_i\} = 1, 1, 2, 3, 5, 8, \ldots$ — последовательность Фибоначчи, в которой $\Phi_i = \lfloor \varphi^i/\sqrt{5} \rceil$ и $\varphi = (\sqrt{5}+1)/2$ — пропорция золотого сечения ($\lfloor x \rceil$ обозначает ближайшее целое к числу x). Справедлива лемма

Лемма 3. $D(F_{\Phi_m}) \leq m - 1$.

Доказательство. Воспользуемся индукцией. Непосредственно проверяется, что $D(F_{\Phi_2}) = 0$ и $D(F_{\Phi_3}) = 2$.

Пусть выполнено $D(F_{\Phi_m}) \le m-1$ и $D(F_{\Phi_{m-1}}) \le m-2$. Заметим дальше, что конъюнкция n переменных реализуется с глубиной $\lceil \log_2 n \rceil$. В частности, конъюнкция Φ_m переменных реализуется с глубиной не более $m-2$, т.к. $\Phi_i \le 2^{i-2}$ для всех $i \ge 2$.

Окончательно, соотношение $D(F_{\Phi_{m+1}}) \le m$ следует из предыдущей леммы при выборе параметров $n = \Phi_{m+1}$ и $k = \Phi_m$, т.к. $\Phi_{m+1} = \Phi_m + \Phi_{m-1}$.

Следствие 1.

$$D(F_n) \le \lceil \log_\varphi(\sqrt{5}n) \rceil - 1 < \log_\varphi n + 1,68.$$

Оценка следует из того, что n не превосходит числа Фибоначчи с индексом $\lceil \log_\varphi(\sqrt{5}n) \rceil$.

Оценим сложность метода. Обозначим $L(n,d)$ сложность реализации всех функций $F_i(y_{i-1},\ldots,y_0)$ для $i \le n$ одной схемой с глубиной d.

Лемма 4.

$$L(\Phi_m, m-1) \le (m+1)\Phi_{m+1}.$$

Будем строить схему, вычисляющую не только все F_i, но и все конъюнкции $x_{i-1} \cdot \ldots \cdot x_0$, $i = 1,\ldots,n$ (ее сложность обозначим через L_n). Докажем, что $L_{\Phi_m} \le (m+1)\Phi_{m+1}$. Очевидно, это верно при $m = 1, 2$.

Рассмотрим индуктивный переход. При $n = \Phi_{m+1}$ воспользуемся схемами, реализующими

$$F_i, \quad i = 1,\ldots,\Phi_{m-1},$$

$$x_{i-1} \cdot \ldots \cdot x_0, \quad i = 1,\ldots,\Phi_{m-1},$$

$$F_i(\Phi_{m-1}), \quad i = 1,\ldots,\Phi_m,$$

$$x_{i+\Phi_{m-1}-1} \cdot \ldots \cdot x_{\Phi_{m-1}}, \quad i = 1,\ldots,\Phi_m,$$

Недостающие функции $F_{\Phi_{m-1}+1},\ldots,F_{\Phi_{m+1}}$ вычисляются при помощи леммы 2, для чего требуется дополнительно $2\Phi_m$ функциональных элементов. Еще Φ_m функциональных элементов требуется для вычисления оставшихся конъюнкций. Имеем,

$$\begin{aligned} L_{\Phi_{m+1}} \le L_{\Phi_m} + L_{\Phi_{m-1}} + 3\Phi_m \le (m+1)\Phi_{m+1} + m\Phi_m + 3\Phi_m \le \\ \le (m+2)\Phi_{m+2} - \Phi_{m+1} + \Phi_m < (m+2)\Phi_{m+2}. \end{aligned}$$

Лемма доказана.

Как следствие, получаем, что сложность реализации набора функций F_i, $i \leq n$ в методе золотого сечения составляет $O(n \log n)$. Значит, справедливо

Следствие 2. *Можно реализовать n-разрядный сумматор схемой сложности $O(n \log n)$ и глубины $\log_\varphi n + O(1)$.*

2 Метод Храпченко

Метод В. М. Храпченко показывает, что на самом деле глубина сложения n-разрядных чисел составляет асимптотически $\log_2 n$.

Пусть $n = k_1 + \ldots + k_r$, а $m_i = k_{i+1} + \ldots + k_r$. Итерируя формулу леммы 2, получаем формулу

$$F_n = F_{k_1}(m_1) + x_{n-1} \cdot \ldots \cdot x_{m_1} \cdot \\ \cdot (\ldots (F_{k_{r-1}}(m_{r-1}) + x_{m_{r-2}-1} \cdot \ldots \cdot x_{m_{r-1}} F_{k_r}) \ldots), \qquad (\star)$$

и далее, раскрывая скобки:

$$F_n = F_{k_1}(m_1) + x_{n-1} \cdot \ldots \cdot x_{m_1} F_{k_2}(m_2) + \ldots \ldots \\ \ldots \ldots + x_{n-1} \cdot \ldots \cdot x_{m_{r-2}} F_{k_{r-1}}(m_{r-1}) + x_{n-1} \cdot \ldots \cdot x_{m_{r-1}} F_{k_r}. \quad (*)$$

Лемма 5. *Пусть $C_l^2 < m \leq C_{l+1}^2$. Тогда*

$$D(F_{2^m}) \leq m + l + 1.$$

Доказательство. Докажем неравенство $D(F_{2^{C_l^2}}) \leq C_{l+1}^2$, очевидно справедливое при $l = 2$. Для индуктивного перехода применяется формула $(*)$ с параметрами $n = 2^{C_{l+1}^2}$, $r = 2^l$ и $k_1 = \ldots = k_r = 2^{C_l^2}$. Слагаемые формулы $(*)$ реализуются с глубиной $C_{l+1}^2 + 1$, т.к. $D(F_{k_j}) \leq C_{l+1}^2$ по предположению, а для оценки глубины конъюнкции $k_1 + \ldots + k_j$ переменных используется неравенство $\log_2(k_1 + \ldots + k_j) < C_l^2 + l = C_{l+1}^2$, где $j = 1, \ldots, r$. Следовательно, функция F_n, представленная в виде суммы 2^l слагаемых, вычисляется на глубине $C_{l+1}^2 + 1 + l = C_{l+2}^2$.

Теперь, для $n = 2^m$, где $C_l^2 < m \leq C_{l+1}^2$, используем $(*)$ с параметрами $r = 2^{m - C_l^2}$ и $k_1 = \ldots = k_r = 2^{C_l^2}$. Лемма доказана.

Следствие 3.
$$D(F_n) < \log_2 n + \sqrt{2\log_2 n} + 3.$$

Доказательство. Заметим, что из условия $C_l^2 < m \le C_{l+1}^2$ следует, что $l = \lceil (\sqrt{1+8m} - 1)/2 \rceil$. Тогда

$$D(F_n) \le \lceil \log_2 n \rceil + \left\lceil \frac{\sqrt{1 + 8\lceil \log_2 n \rceil} - 1}{2} \right\rceil + 1 \le$$
$$\le \lceil \log_2 n \rceil + \left\lceil \sqrt{2\log_2 n} \right\rceil + 1 < \log_2 n + \sqrt{2\log_2 n} + 3.$$

При переходе используется справедливое при $x \ge 2$ неравенство:

$$\sqrt{1 + 8\lceil x \rceil} - 1 < \sqrt{9 + 8x} - 1 \le 2\sqrt{2x},$$

а при $n = 2, 3$ соотношение проверяется непосредственно.

Таким образом, можно построить n-разрядный сумматор глубины $\log_2 n + \sqrt{2\log_2 n} + O(1)$. Можно показать, что сложность такого сумматора составляет $O\left(c^{\sqrt{\log_2 n}} n\right)$.

3 Линеаризация сложности

Пусть $n \le rk$. Положим в формуле $(\star)$ все $k_i = k$. Для $i = 0, \ldots, r-1$ введем обозначения:

$$Y_i = F_k(y_{(i+1)k-1}, \ldots, y_{ik}), \qquad X_i = x_{(i+1)k-1} \cdot \ldots \cdot x_{ik}.$$

Тогда $(\star)$ переписывается как

$$F_n(y_{n-1}, \ldots, y_0) = Y_{r-1} + X_{r-1}(Y_{r-2} + X_{r-2}(\ldots(Y_1 + X_1 Y_0)\ldots)) =$$
$$= F_r(Y_{r-1}, \ldots, Y_0).$$

(Если $i \ge n$, то полагается $x_i = 1$ и $y_i = 0$.)

Теперь допустим, что имеются два метода (условно назовем их методом A и методом B) реализации набора функций $F_1, \ldots, F_s$ вместе с соответствующими конъюнкциями $x_{i-1} \cdot \ldots \cdot x_0$, $i = 1, \ldots, s$. Построим новый метод, назовем его методом C. Обозначим $L_I(s), D_I(s)$ сложность и глубину реализации указанного набора функций методом I, где

$I \in \{A, B, C\}$. Основная идея состоит в том, что при надлежащем выборе параметров сложность метода C будет «близка» к сложности метода A, а глубина — к глубине метода B.

Метод C заключается в следующем.

1. Для всех $j = 0, \ldots, r-1$ реализуются наборы функций $F_l(y_{jk+l-1}, \ldots, y_{jk})$ и конъюнкции $x_{jk+l-1} \cdot \ldots \cdot x_{jk}$, $l = 1, \ldots, k$, методом A.

2. Для всех $j = 1, \ldots, r$ вычисляются функции

$$F_{jk}(y_{jk-1}, \ldots, y_0) = F_j(Y_{j-1}, \ldots, Y_0)$$

и вместе с ними конъюнкции $K_j = X_{j-1} \cdot \ldots \cdot X_0$ методом B.

3. Для каждого $j = 1, \ldots, r-1$ вычисляются все функции $F_{jk+l}(y_{jk+l-1}, \ldots, y_0)$, $l = 1, \ldots, k-1$, по формулам

$$F_{jk+l}(y_{jk+l-1}, \ldots, y_0) = F_l(y_{jk+l-1}, \ldots, y_{jk}) + x_{jk+l-1} \cdot \ldots \cdot x_{jk} F_{jk}(y_{jk-1}, \ldots, y_0)$$

и необходимые конъюнкции

$$x_{jk+l-1} \cdot \ldots \cdot x_0 = (x_{jk+l-1} \cdot \ldots \cdot x_{jk}) \cdot K_j.$$

Лемма 6. *Если* $(r-1)k < n \le rk$, *то*

$$L_C(n) \le rL_A(k) + L_B(r) + 3n, \qquad D_C(n) \le D_A(k) + D_B(r) + 2.$$

Доказательство. Оценки сложности и глубины построенной методом C схемы складываются из суммы сложностей и глубин реализации шагов 1–3.

Шаг 1 реализуется со сложностью $rL_A(k)$ и глубиной $D_A(k)$. Шаг 2 — со сложностью $L_B(r)$ и глубиной $D_B(r)$. Шаг 3 — со сложностью $3(r-1)(k-1) \le 3n$ и глубиной 2. Складывая оценки на всех шагах, приходим к утверждению леммы.

Применим описанный способ к построению сбалансированных по сложности и глубине сумматоров. Примем за основу стандартный метод, имеющий сложность $3(n-1)$ и глубину $2(n-1)$.

А) Выберем $k, r \sim \sqrt{n}$ и стандартный метод в качестве как метода A, так и метода B. Получим метод сложности $O(n)$ и глубины $O(\sqrt{n})$.

Б) Выберем $k \sim \log n$, только что полученный метод в качестве метода A и метод золотого сечения — в качестве метода B. Получим метод линейной сложности $O(n)$ и логарифмической глубины $\log_\varphi n + O(\sqrt{\log n})$.

B) Выберем $k \sim \sqrt{\log n}$, стандартный метод в качестве метода A и только что полученный метод — в качестве метода B. Получим метод сложности $6n + o(n)$ и глубины $\log_\varphi n + O(\sqrt{\log n})$.

Заметим, что если не вычислять конъюнкции, то оценка сложности последнего метода понизится до $5n + o(n)$. Так как для построения n-разрядного сумматора схему, вычисляющую набор функций F_i, достаточно дополнить $3n$ функциональными элементами, получаем

Следствие 4. *Можно реализовать n-разрядный сумматор схемой сложности $8n + o(n)$ и глубины $\log_\varphi n + o(\log n)$.*

Аналогичный результат можно получить и для метода Храпченко. Наилучшая известная верхняя оценка глубины схемы сложения n-разрядных чисел получена М. И. Гринчуком и составляет $\log_2 n + \log_2 \log_2 n + O(1)$.

Дополнительные вопросы

1. Показать, что глубина n-разрядного сумматора не превосходит $D(F_n) + 1$.