

Лекция 20. Схемы из функциональных элементов (СФЭ). Сложность схемы для умножения n -разрядных двоичных чисел по методу Карацубы.

Лектор — Селезнева Светлана Николаевна
selezn@cs.msu.ru

Факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте <https://mk.cs.msu.ru>

Арифметические операции

Рассмотрим, с какой сложностью можно построить схему для *умножения n -разрядных чисел*.

Числа в двоичной системе счисления

Пусть $n \in \mathbb{N}$.

Если $(x_1, \dots, x_n) \in E_2^n$, где $E_2 = \{0, 1\}$, то положим

$$(x_1, \dots, x_n)_2 = \sum_{i=1}^n x_i \cdot 2^{n-i}.$$

Т.е. $(x_1, \dots, x_n)_2$ обозначает число, которое в двоичной системе счисления записывается как $x_1 x_2 \dots x_n$.

Отметим, что

$$0 \leq (x_1, \dots, x_n)_2 \leq 2^n - 1.$$

Числа в двоичной системе счисления

Заметим, что

$$0 \leq (x_1, \dots, x_n)_2 < 2^n,$$

$$0 \leq (y_1, \dots, y_n)_2 < 2^n,$$

поэтому

$$0 \leq (x_1, \dots, x_n)_2 \cdot (y_1, \dots, y_n)_2 < 2^{2n}.$$

Умножитель

Умножителем M_n порядка n , $n \geq 1$, называется такая СФЭ с $2n$ входами $x_1, \dots, x_n, y_1, \dots, y_n$ и $2n$ выходами z_1, \dots, z_{2n} , что

$$(z_1, \dots, z_{2n})_2 = (x_1, \dots, x_n)_2 \cdot (y_1, \dots, y_n)_2.$$

Т.е. умножитель M_n на своих выходах вычисляет произведение двух n -разрядных чисел, которые подаются на его входы.

Умножитель M_n также называется n -разрядным умножителем.

Умножитель M_1

Пример. Построим одноразрядный умножитель $M_1(x, y; z)$.

Умножитель M_1

Пример. Построим одноступенчатый умножитель $M_1(x, y; z)$.

Найдем функцию $z(x, y)$:

x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

Умножитель M_1

Пример. Построим одноразрядный умножитель $M_1(x, y; z)$.

Найдем функцию $z(x, y)$:

x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

Поэтому

$$z = x \cdot y.$$

Умножитель M_1

Пример. Построим одноразрядный умножитель $M_1(x, y; z)$.

Найдем функцию $z(x, y)$:

x	y	z
0	0	0
0	1	0
1	0	0
1	1	1

Поэтому

$$z = x \cdot y.$$

Значит, в базисе B_0 можно построить умножитель M_1 со сложностью 1.

Сложность умножителя

С какой сложностью можно построить умножитель M_n , $n \geq 1$?

Сложность умножителя

С какой сложностью можно построить умножитель M_n , $n \geq 1$?

Можно применить алгоритм умножения n -разрядных чисел «в столбик».

При этом надо вычислить произведения вида $x_i \cdot y_j$ для всех $i, j = 1, \dots, n$.

А затем еще $n - 1$ раз сложить $2n$ -разрядные числа.

Поэтому сложность построенного таким образом n -разрядного умножителя окажется равной $O(n^2)$.

Сложность умножителя

Мы покажем, что можно построить n -разрядный умножитель с меньшей по порядку сложностью.

Сначала рассмотрим несколько вспомогательных лемм.

Умножение n -разрядного числа на разряд

Пусть M'_n обозначает СФЭ с $n + 1$ входами x_1, \dots, x_n, y и n выходами z_1, \dots, z_n , которая вычисляет **умножение n -разрядного числа $(x_1, \dots, x_n)_2$ на разряд y** , т. е.

$$(z_1, \dots, z_n)_2 = (x_1, \dots, x_n)_2 \cdot y.$$

Умножение n -разрядного числа на разряд

Лемма 20.1. В базисе $B_0 = \{x \cdot y, x \vee y, \bar{x}\}$ можно построить схему M'_n со сложностью n .

Доказательство. Действительно, достаточно заметить, что $z_i = x_i \cdot y$ для всех $i = 1, \dots, n$.

□

Умножение n -разрядного числа на степень двойки

Пусть $M''_{n,m}$ обозначает СФЭ с n входами x_1, \dots, x_n и $n + m$ выходами z_1, \dots, z_{n+m} , которая вычисляет **умножение n -разрядного числа $(x_1, \dots, x_n)_2$ на число 2^m** , т. е.

$$(z_1, \dots, z_{n+m})_2 = (x_1, \dots, x_n)_2 \cdot 2^m.$$

Умножение n -разрядного числа на степень двойки

Лемма 20.2. В базисе $B_0 = \{x \cdot y, x \vee y, \bar{x}\}$ можно построить схему $M''_{n,m}$ с константной сложностью.

Доказательство. Действительно, достаточно заметить, что $z_i = x_i$ для всех $i = 1, \dots, n$, а

$$z_{n+1} = \dots = z_{n+m} = 0.$$

Поэтому сложность схемы можно оценить сложностью вычисления константы 0, а эта сложность — константна.

□

Умножение $(n + 1)$ -разрядных чисел

Лемма 20.3. В базисе $B_0 = \{x \cdot y, x \vee y, \bar{x}\}$ для каждого $n \geq 1$ и любого умножителя M_n можно построить такой умножитель M_{n+1} , что

$$L(M_{n+1}) \leq L(M_n) + C_1 n,$$

где $C_1 > 0$ — некоторое действительное число, не зависящее от n .

Доказательство. Пусть $n \geq 1$. Рассмотрим произвольный умножитель M_n .

Покажем, как построить такой умножитель M_{n+1} , что

$$L(M_{n+1}) \leq L(M_n) + C_1 n,$$

где $C_1 > 0$ — некоторое действительное число, не зависящее от n .

Умножение $(n + 1)$ -разрядных чисел

Доказательство. Пусть на входы умножителя M_{n+1} подаются числа:

$$x = (x_0, x_1, \dots, x_n)_2, \quad y = (y_0, y_1, \dots, y_n)_2.$$

Введем обозначения:

$$x' = (x_1, \dots, x_n)_2, \quad y' = (y_1, \dots, y_n)_2.$$

Тогда:

$$\begin{aligned} x &= (x_0, x_1, \dots, x_n)_2 = x_0 \cdot 2^n + (x_1, \dots, x_n)_2 = x_0 \cdot 2^n + x', \\ y &= (y_0, y_1, \dots, y_n)_2 = y_0 \cdot 2^n + (y_1, \dots, y_n)_2 = y_0 \cdot 2^n + y'. \end{aligned}$$

Умножение $(n + 1)$ -разрядных чисел

Доказательство. Получаем:

$$\begin{aligned}x \cdot y &= (x_0 \cdot 2^n + x')(y_0 \cdot 2^n + y') = \\ &= x_0 \cdot y_0 \cdot 2^{2n} + (x_0 \cdot y' + x' \cdot y_0) \cdot 2^n + x' \cdot y'.\end{aligned}$$

Значит, для умножения $(n + 1)$ -разрядных чисел можно умножить n -разрядные числа и выполнить дополнительные вычисления.

При этом сложность этих дополнительных вычислений не превосходит $C_1 \cdot n$, где $C_1 > 0$ — действительное число, не зависящее от n (по леммам 20.1, 20.2 и по теореме о сложности сумматора).



Умножение $(n + 1)$ -разрядных чисел

Лемма 20.3 содержательно утверждает следующее:

умножать $(n + 1)$ -разрядные числа можно со сложностью, которая на линейное слагаемое отличается от сложности умножения n -разрядных чисел.

Умножение $2n$ -разрядных чисел

Лемма 20.4 (основная). В базисе $B_0 = \{x \cdot y, x \vee y, \bar{x}\}$ для каждого $n \geq 1$ и любого умножителя M_n можно построить такой умножитель M_{2n} , что

$$L(M_{2n}) \leq 3L(M_n) + C_2n,$$

где $C_2 > 0$ — некоторое действительное число, не зависящее от n .

Доказательство. Пусть $n \geq 1$. Рассмотрим произвольный умножитель M_n .

Покажем, как построить такой умножитель M_{2n} , что

$$L(M_{2n}) \leq 3L(M_n) + C_2n,$$

где $C_2 > 0$ — некоторое действительное число, не зависящее от n .

Умножение $2n$ -разрядных чисел

Доказательство. Пусть на входы умножителя M_{2n} подаются числа:

$$x = (x_1, \dots, x_n, x_{n+1}, \dots, x_{2n})_2, \quad y = (y_1, \dots, y_n, y_{n+1}, \dots, y_{2n})_2.$$

Введем обозначения:

$$\begin{aligned} x' &= (x_1, \dots, x_n)_2, & x'' &= (x_{n+1}, \dots, x_{2n})_2, \\ y' &= (y_1, \dots, y_n)_2, & y'' &= (y_{n+1}, \dots, y_{2n})_2. \end{aligned}$$

Тогда:

$$\begin{aligned} x &= x' \cdot 2^n + x'', \\ y &= y' \cdot 2^n + y''. \end{aligned}$$

Умножение $2n$ -разрядных чисел

Доказательство. Получаем:

$$\begin{aligned}x \cdot y &= (x' \cdot 2^n + x'')(y' \cdot 2^n + y'') = \\ &= x' \cdot y' \cdot 2^{2n} + (x' \cdot y'' + x'' \cdot y') \cdot 2^n + x'' \cdot y''.\end{aligned}$$

Умножение $2n$ -разрядных чисел

Доказательство. Получаем:

$$\begin{aligned}x \cdot y &= (x' \cdot 2^n + x'')(y' \cdot 2^n + y'') = \\ &= x' \cdot y' \cdot 2^{2n} + (x' \cdot y'' + x'' \cdot y') \cdot 2^n + x'' \cdot y''.\end{aligned}$$

Рассмотрим тождество:

$$x' \cdot y'' + x'' \cdot y' = (x' + x'') \cdot (y' + y'') - x' \cdot y' - x'' \cdot y''.$$

Умножение $2n$ -разрядных чисел

Доказательство. Получаем:

$$\begin{aligned}x \cdot y &= (x' \cdot 2^n + x'')(y' \cdot 2^n + y'') = \\ &= x' \cdot y' \cdot 2^{2n} + (x' \cdot y'' + x'' \cdot y') \cdot 2^n + x'' \cdot y''.\end{aligned}$$

Рассмотрим тождество:

$$x' \cdot y'' + x'' \cdot y' = (x' + x'') \cdot (y' + y'') - x' \cdot y' - x'' \cdot y''.$$

Значит,

$$\begin{aligned}x \cdot y &= x' \cdot y' \cdot 2^{2n} + \\ &+ ((x' + x'') \cdot (y' + y'') - x' \cdot y' - x'' \cdot y'') \cdot 2^n + \\ &+ x'' \cdot y''.\end{aligned}$$

Умножение $2n$ -разрядных чисел

Доказательство. Итак,

$$\begin{aligned}x \cdot y &= x' \cdot y' \cdot 2^{2n} + \\ &+ ((x' + x'') \cdot (y' + y'') - x' \cdot y' - x'' \cdot y'') \cdot 2^n + \\ &+ x'' \cdot y''.\end{aligned}$$

Значит, с учетом леммы 20.3, для умножения $2n$ -разрядных чисел можно трижды умножить n -разрядные числа и выполнить дополнительные вычисления.

При этом сложность этих дополнительных вычислений не превосходит $C_2 \cdot n$, где $C_2 > 0$ — действительное число, не зависящее от n (по леммам 20.2, 20.3 и по теоремам о сложности сумматора и вычитателя).



Умножение $2n$ -разрядных чисел

Лемма 20.4 содержательно утверждает следующее:

умножать $2n$ -разрядные числа можно со сложностью, которая на линейное слагаемое отличается от утроенной сложности умножения n -разрядных чисел.

Сложность умножителя M_n

Теорема 20.1 (Карацубы). В базисе $B_0 = \{x \cdot y, x \vee y, \bar{x}\}$ можно построить умножитель M_n со сложностью $O(n^{\log_2 3})$.

Сложность умножителя M_n

Доказательство. 1. Сначала рассмотрим случай $n = 2^k$, где $k \in \mathbb{N}$.

Применяя лемму 20.4, получаем:

$$\begin{aligned} L(M_{2^k}) &\leq 3L(M_{2^{k-1}}) + C_2 \cdot 2^{k-1} \leq \\ &\leq 3(3L(M_{2^{k-2}}) + C_2 \cdot 2^{k-2}) + C_2 \cdot 2^{k-1} = \\ &= 3^2 L(M_{2^{k-2}}) + C_2 \cdot (3 \cdot 2^{k-2} + 2^{k-1}) \leq \dots \leq \\ &\leq 3^k L(M_{2^0}) + C_2 \cdot (3^{k-1} + \dots + 3 \cdot 2^{k-2} + 2^{k-1}). \end{aligned}$$

Заметим, что $L(M_1) = 1$. Кроме того,

$$\begin{aligned} 3^{k-1} + \dots + 3 \cdot 2^{k-2} + 2^{k-1} &= 3^{k-1} \cdot \left(1 + \dots + \left(\frac{2}{3}\right)^{k-1}\right) \leq \\ &\leq 3^{k-1} \cdot \frac{1}{1-\frac{2}{3}} = 3^k. \end{aligned}$$

Сложность умножителя M_n

Доказательство. Поэтому:

$$L(M_{2^k}) \leq 3^k + C_2 \cdot 3^k \leq C_3 \cdot 3^k,$$

где $C_3 = C_2 + 1 > 0$ — некоторое действительное число.

Но $n = 2^k$, значит,

$$L(M_n) \leq C_3 \cdot 3^k = C_3 \cdot 2^{k \log_2 3} = C_3 \cdot n^{\log_2 3} = O(n^{\log_2 3}).$$

Сложность умножителя M_n

Доказательство. 2. Теперь рассмотрим случай $2^{k-1} < n < 2^k$, где $k \in \mathbb{N}$.

Добавим к n -разрядным числам нули слева, чтобы получились 2^k -разрядные числа. Тогда:

$$\begin{aligned} L(M_n) &\leq L(M_{2^k}) \leq C_3 \cdot 2^{k \log_2 3} = \\ &= (C_3 \cdot 2^{\log_2 3}) \cdot 2^{(k-1) \log_2 3} \leq C \cdot n^{\log_2 3}, \end{aligned}$$

где $C = C_3 \cdot 2^{\log_2 3} > 0$ — некоторое действительное число.

Значит,

$$L(M_n) \leq C \cdot n^{\log_2 3} = O(n^{\log_2 3}).$$



Сложность умножения n -разрядных чисел

Известен алгоритм Шенхаге-Штрассена, который n -разрядные числа позволяет умножать со сложностью $O(n \cdot \log n \cdot \log \log n)$.

Задачи для самостоятельного решения

1. Оцените сверху константы C_1 , C_2 , C_3 и C из лемм 20.3, 20.4 и теоремы 20.1.

Литература к лекции

1. Алексеев В. Б. Лекции по дискретной математике. М.: Инфра-М, 2012. С. 66–70.
2. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004. Гл. X 1.1.