СЛОЖНОСТЬ СУММИРОВАНИЯ.

Кудряшов Ю., Скопенков А.
при участии Никокошева И.

Посвящается столетию А. Н. Колмогорова

Вводные задачи.

Задача 1. Пусть имеется набор вещественных чисел $x_1, \dots, x_{99}$. Разрешается складывать два из уже имеющихся чисел и запоминать полученный результат. За какое наименьшее количество сложений можно найти

(a) их сумму $x_1 + \dots + x_{99}$?

(b) $x_1 + \ldots + x_{66}$ и $x_{34} + \ldots + x_{99}$?

Обозначим через $\mathbb{Z}_2$ множество $\{0, 1\}$. Введем на этом множестве операцию сложения (по модулю 2) формулами

$$0 + 0 = 1 + 1 = 0, \quad 1 + 0 = 0 + 1 = 1.$$

Далее будут рассматриваться только переменные из $\mathbb{Z}_2$ (кроме задачи 3).

Пусть имеется набор переменных $x_1, \dots, x_n$ из $\mathbb{Z}_2$. Разрешается складывать (по модулю 2) два из уже имеющихся выражений и запоминать полученный результат.

Задача 2. За какое наименьшее количество сложений можно найти

(a) сумму $x_1 + \dots + x_{99}$?

(b) $x_1 + \ldots + x_{66}$ и $x_{34} + \ldots + x_{99}$?

Задача 3. Придумайте набор сумм такой, что число сложений, необходимое для его вычисления, если переменные действительные, больше, чем минимальное число сложений, необходимое для его вычисления, если переменные из $\mathbb{Z}_2$.

Задача 4. (a) Докажите, что любую пару сумм $x_{i_1} + \dots + x_{i_p}$ и $x_{j_1} + \dots + x_{j_q}$ от переменных $x_1, \dots, x_n$, можно найти не более чем за $n - 1$ суммирований.

(b) Докажите, что любую тройку сумм $x_{i_1} + \dots + x_{i_p}$, $x_{j_1} + \dots + x_{j_q}$ и $x_{k_1} + \dots + x_{k_r}$ от переменных $x_1, \dots, x_n$, можно найти не более чем за $n + 1$ суммирований.

Задача 5. Докажите, что любой набор сумм вида $x_{i_1} + \dots + x_{i_p}$ от переменных $x_1, \dots, x_n$, можно найти не более чем за $2^n - (n + 1)$ суммирований.

Задача 6. Пусть любой набор из m сумм от n переменных можно найти за l сложений.

(a) Докажите, что любой набор из km сумм от тех же n переменных можно найти не более, чем за kl сложений.

(b) Докажите, что любой набор из m сумм от kn переменных $x_1, \dots, x_{kn}$ можно найти не более, чем за $k(l + m)$ суммирований.

Задача 7. (a) Докажите, что при достаточно больших m, n любой набор из m сумм от n переменных можно найти не более чем за

$$\frac{mn}{100}$$

суммирований.

(b) Докажите, что любой набор из m сумм от n переменных можно найти не более, чем за

$$2m \left\lceil \frac{n}{[\log_2 m]} \right\rceil$$

суммирований. Здесь $[x]$ — целая часть числа x, то есть наибольшее целое число, не превосходящее x, $\lceil x \rceil$ — верхняя целая часть числа x, то есть наименьшее целое число, не меньшее x.

Последовательность суммирований можно представлять себе следующим образом. У нас есть набор элементов («сумматоров») с двумя входами и одним выходом, равным сумме по модулю 2 входов. Необходимо собрать схему из сумматоров, реализующую данный набор сумм.

При этом количество суммирований равно числу использованных сумматоров. Это число называется *сложностью схемы*.

Минимальная сложность схемы, реализующей данный набор M сумм называется *сложностью этого набора сумм* и обозначается $\mathrm{L}(M)$.

В этих обозначениях в задаче 2 требовалось найти $\mathrm{L}(\{x_1 + \dots + x_{99}\})$ и $\mathrm{L}(\{x_1 + \ldots + x_{66}, x_{34} + \ldots + x_{99}\}$.

Минимальное число l такое, что любой набор из m сумм от переменных $x_1, \ldots, x_n$ можно найти за l суммирований называется *сложностью упорядоченной пары* (m, n) и обозначается $\mathrm{L}(m, n)$.

В этих обозначениях задача 4 утверждает, что $\mathrm{L}(2, n) \leqslant n - 1$ и $\mathrm{L}(3, n) \leqslant n + 1$, а задача 7(b) утверждает, что

$$\mathrm{L}(m, n) \leqslant 2m \left\lceil \frac{n}{[\log_2 m]} \right\rceil .$$

Набор из m сумм от n переменных можно обозначать матрицей M размера $m \times n$, где на пересечении i-й строки и j-о столбца стоит 1, если j-я переменная входит в i-ю сумму и 0 в противном случае. При этом i-я сумма будет записываться очень просто:

$$s_i = \sum_{j=1}^{n} M_{ij} x_j .$$

В этих обозначениях наборы сумм из задачи 2 выглядят следующим образом:

$$\begin{pmatrix} 1 & \ldots & 1 \end{pmatrix}, \begin{pmatrix} 1 & \ldots & 1 & 1 & \ldots & 1 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 1 & \ldots & 1 & 1 & \ldots & 1 \end{pmatrix},$$

Рассмотрим набор из m сумм, составленных из переменных $x_0, \ldots, x_{2^m - 1}$, в который все переменные входят по-разному. Пусть B_m — соответствующая матрица. Столбцы этой матрицы — это двоичные представления целых чисел от 0 до $2^m - 1$. Формально, обозначим $j = b_{m-1,j} 2^{m-1} + \cdots + b_{0,j} 2^0$ двоичную запись числа $j < 2^m$. Тогда $B_m = (b_{i,j})$. Например,

$$B_1 = \begin{pmatrix} 0 & 1 \end{pmatrix}, B_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, B_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Задача 8. Докажите, что $\mathrm{L}(B_m) < 2^{m+1}$.

Задача 9. Докажите, что $\mathrm{L}(m, n) < n + 2^{m+1}$.

Задача 10. Докажите, что при достаточно больших n выполнено неравенство

$$\mathrm{L}(n, n) < \frac{n^2}{0,9 \log_2 n} .$$

СЛОЖНОСТЬ СУММИРОВАНИЯ. (Кудряшов Ю., Скопенков А.)

Задачи, предложенные после промежуточного финиша.

Задача 11. (a) Докажите, что существует не более, чем $(n+k)^{m+2k}$ схем из k сумматоров с n входами и m выходами.

(b) Если $k = \mathrm{L}(m,n)$, то $mn \leqslant (m+2k)\log_2(n+k)$.

(c) При достаточно больших n выполнено неравенство $\mathrm{L}(n,n) \geqslant \frac{n^2}{5\log_2 n}$.

Указание. Если $k = \mathrm{L}(n,n) < \frac{n^2}{5\log_2 n}$, то $n^2 \leqslant (n + \frac{2n^2}{5\log_2 n})\log_2(n + \frac{n^2}{5\log_2 n})$, что неверно при достаточно больших n.

(d) Для любого $\varepsilon > 0$ при достаточно больших n выполнено неравенство

$$\mathrm{L}(n,n) \geqslant \frac{n^2}{(4+\varepsilon)\log_2 n}$$

Для формулироки последующих результатов нам потребуются некоторые асимптотические обозначения.

Говорят, что последовательность $a_n > 0$ асимптотически *не больше* последовательности $b_n > 0$, если для любого $\varepsilon > 0$ найдётся лишь конечное множество индексов k таких, что $a_n > (1+\varepsilon)b_n$. Обозначение: $a_n \lesssim b_n$.

В этих обозначениях задача 11(d) примет следующий вид: $\mathrm{L}(n,n) \gtrsim \frac{n^2}{4\log_2 n}$.

Говорят, что $a_n \sim b_n$, если $a_n/b_n \to 1$ при $n \to \infty$.

Говорят, что $a_n \ll b_n$, если $a_n/b_n \to 0$ при $n \to \infty$.

Задача 12. (a) Докажите, что если $a_n \lesssim b_n$ и $b_n \lesssim c_n$, то $a_n \lesssim c_n$.

(b) Докажите, что $a_n \sim b_n$ тогда и только тогда, когда $a_n \lesssim b_n$ и $b_n \lesssim a_n$.

Задача 13. Докажите, что если $\log_2 n \ll f(n) \ll 2^n$, то

$$\frac{nf(n)}{2\log_2(nf(n))} \lesssim \mathrm{L}(f(n),n).$$

Задача 14. Докажите, что при $\log_2 n \ll f(n) \ll 2^n$

$$\mathrm{L}(f(n),n) \lesssim \frac{nf(n)}{\log_2 f(n)}.$$

Задача 15. Докажите, что при $\log_2 n \ll f(n) \ll 2^n$

$$\mathrm{L}(f(n),n) \lesssim \frac{nf(n)}{\log_2 n}.$$

Из задач 13, 14 и 15 следует, что при $\log_2 n \ll f(n) \ll 2^n$ выполнено асимптотическое неравенство

$$\frac{nf(n)}{2\log_2(nf(n))} \lesssim \mathrm{L}(f(n),n) \lesssim \frac{nf(n)}{\max(\log_2 n, \log_2 f(n))}.$$

Задача 16. (a) Рассмотрим матрицу A размера $m \times n$, в которой нет нулевых строк и нет нулевых столбцов. Верно ли, что $\mathrm{L}(A) + m = \mathrm{L}(A^t) + n$, где A^t — матрица A транспонированная?

(b) Верно ли, что $\mathrm{L}(m,n) + m = \mathrm{L}(n,m) + n$?

(c) Найдите $\mathrm{L}(B_m)$.

Задача 17. Рассмотрим набор переменных $x_{\alpha_1,\dots,\alpha_n}$, занумерованных вершинами n-мерного единичного куба $\mathbb{Z}_2^n$. Требуется найти суммы во всех гранях, содержащих вершину $(0,\dots,0)$. Другими словами, для каждого набора $(\alpha_1,\dots,\alpha_n) \in \mathbb{Z}_2^n$ требуется найти $\sum\limits_{\forall i:\beta_i \leqslant \alpha_i} x_{\beta_1\dots\beta_n}$. За какое наименьшее число суммирований (mod2) это можно сделать?

Задача 18. Попробуйте получить аналогичные результаты для переменных из $\mathbb{R}$ в следующих случаях:

(a) Требуется найти набор сумм. Есть только сумматоры.

(b) Требуется найти набор сумм. Есть два вида элементов: сумматоры и разности.

(c) Требуется найти набор линейных комбинаций с целыми коэффициентами. Есть два вида элементов: сумматоры и умножатели на целую константу (быть может, разную для разных умножателей).

СЛОЖНОСТЬ СУММИРОВАНИЯ.

Кудряшов Ю., Скопенков А. (при участии Никокошева И.)

РЕШЕНИЯ.

Задача 1. (a) Ответ: 98. Очевидно, что сумму $x_1 + \dots + x_{99}$ можно найти за 98 суммирований. Допустим, у нас есть схема из a сумматоров, реализующая нашу сумму. Рассмотрим граф, в котором 99 вершин $P_1, \dots, P_{99}$ и для каждого сумматора с суммой на первом входе $x_{i_1} + \dots + x_{i_p}$ и суммой на втором входе $x_{j_1} + \dots + x_{j_q}$ проводится ребро из вершины P_{i_1} в вершину P_{j_1}. Ясно, что в каждый момент вершины, соответствующие переменным, входящим в одну из уже вычисленных сумм, лежат в одной компоненте связности. Следовательно, конечный граф связен, а значит в нём не менее 98 рёбер, т.е. $a \geqslant 98$.

(b) Ответ: 98. Доказательство аналогично п. (a).

Задача 2. Решение дословно повторяет решение задачи 1.

Задача 3. Подходит, например, следующий набор:

$$\{\ x_1 + x_2,\ x_1 + x_2 + x_3,\ x_1 + x_2 + x_3 + x_4,\ x_2 + x_3 + x_4\ \}.$$

Действительно, в случае $\mathbb{Z}_2$ мы можем вычислить эти суммы в указанном порядке без вычисления вспомогательных сумм, а в случае $\mathbb{R}$ нам придётся вычислять хотя бы одну вспомогательную сумму.

Задача 4. (a) Обозначим через $S(A)$ сумму всех переменных, индексированных элементами множества A. Пусть $S(A_1)$ и $S(A_2)$ — искомые суммы. Если все множества $B_1 := A_1 \setminus A_2$, $B_2 := A_1 \cap A_2$ и $B_3 := A_2 \setminus A_1$ непусты, то вычислим сумму в каждом из этих множеств, потратив на это не более

$$|B_1| - 1 + |B_2| - 1 + |B_3| - 1 = |A_1 \cup A_2| - 3 \leqslant n - 3$$

суммирований. Осталось найти $S(A_1) = S(B_1) + S(B_2)$ и $S_2 = S(B_2) + S(B_3)$. Для этого достаточно двух суммирований.

Можно несложно (например, перебором) убедиться, что в случае, когда одно из множеств пусто требуется не больше суммирований, чем в этом случае.

(b) Аналогично п. (a).

Задача 5. Несложно видеть, что $2^n - (n+1)$ — это число всех сумм от n переменных, имеющих хотя бы два слагаемых. Эти суммы мы можем последовательно вычислять: сначала суммы с двумя слагаемыми, потом суммы с тремя слагаемыми, … , потом сумму с n слагаемыми. В результате этого процесса мы вычислим все суммы от переменных $x_1, \dots, x_n$.

Задача 6. (a) Набор из km сумм можно воспринимать как k наборов из m сумм. Реализуя каждый такой набор по отдельности, получаем требуемую оценку.

(b) «Разрежем» вертикальными разрезами матрицу, соответствующую нашему набору из m сумм от kn переменных на k матриц размера $m \times n$. Сначала при помощи kl сумматоров реализуем все полученные матрицы $m \times n$. Тогда каждая искомая сумма является суммой не более чем $k-1$ уже найденных сумм. Следовательно, искомый набор сумм можно реализовать не более, чем за $kl + m(k-1) < k(l+m)$ суммирований.

СЛОЖНОСТЬ СУММИРОВАНИЯ.

Кудряшов Ю., Скопенков А. (при участии Никокошева И.)

РЕШЕНИЯ (ЧАСТЬ 2).

Задача 7. (a) Из задачи 5 при $n = 500$ получим, что любой набор из m сумм от 500 переменных можно вычислить не более, чем за $l = 2^{500}$ суммирований. Следовательно, по задаче 6(b), любой набор из m сумм от $500k$ переменных можно вычислить не более, чем за $k(l+m)$ сложений. Таким образом, любой набор из m сумм от n переменных можно вычислить не более, чем за

$$\left\lceil \frac{n}{500} \right\rceil (l+m)$$

суммирований. Ясно, что при достаточно больших m и n это меньше, чем $mn/100$.

(b) Из задачи 5 получим, что любой набор из m сумм от $\lfloor \log_2 m \rfloor$ переменных можно вычислить не более, чем за $l = 2^{\lfloor \log_2 m \rfloor} < m$ суммирований. Следовательно, по задаче 6(b), любой набор из m сумм от $\lfloor \log_2 m \rfloor k$ переменных можно вычислить не более, чем за $k(l+m) < 2km$ сложений. Таким образом, любой набор из m сумм от n переменных можно вычислить не более, чем за

$$2m \left\lceil \frac{n}{\lfloor \log_2 m \rfloor} \right\rceil$$

суммирований.

Задача 9. Рассмотрим произвольную матрицу A размера $m \times n$. Если в этой матрице все столбцы различны, то сложность этой матрицы не превосходит $\mathrm{L}(B_m)$. Если же есть два совпадающих столбца, то, вычислив сначала сумму соответствующих этим столбцам переменных, мы сводим задачу к реализации матрицы $m \times (n-1)$. Следовательно, $\mathrm{L}(m,n) \leqslant \mathrm{L}(B_m) + n < n + 2^{m+1}$.

Задача 10. При достаточно больших n выполнена цепочка неравенств

$$\mathrm{L}(n,n) < \left\lceil \frac{n}{\lfloor 0.95 \log_2 n \rfloor} \right\rceil \mathrm{L}(\lfloor 0.95 \log_2 n \rfloor, n) < \frac{n}{0.94 \log_2 n} \mathrm{L}(\lfloor 0.95 \log_2 n \rfloor, n) <$$
$$< \frac{n}{0.94 \log_2 n}(n + 2 \cdot 2^{\lfloor 0.95 \log_2 n \rfloor}) < \frac{n}{0.94 \log_2 n}(n + 2n^{0.95}) < \frac{n}{0.9 \log_2 n}.$$

Задача 11. (a) Назовём *началами проводов* входы схемы и выходы сумматоров (всего $n+k$), *концами проводов* выходы схемы и входы сумматоров (всего $m+2k$). Пронумеруем все начала и концы проводов. Сопоставим каждой схеме информацию о том, какие начала проводов подсоединены к каким концам проводов. Понятно, что эта информация однозначно определяет схему. Поэтому искомое число схем не больше, чем число различных вариантов подсоединить к каждому из $m+2k$ концов проводов какое-то из $n+k$ начал проводов, которое равно $(n+k)^{m+2k}$.

(b) Так как число различных схем из $\mathrm{L}(m,n)$ элементов с n входами и m выходами не меньше числа матриц размера $m \times n$ с коэффициентами из $\mathbb{Z}_2$, то $2^{mn} \leqslant (n+k)^{m+2k}$. Логарифмируя это неравенство, получаем утверждение задачи.

(c) Если $k = \mathrm{L}(n,n) < \frac{n^2}{5 \log_2 n}$, то $n^2 \leqslant (n + \frac{2n^2}{5 \log_2 n}) \log_2(n + \frac{n^2}{5 \log_2 n})$. Докажем, что это неравенство неверно при достаточно больших n. Действительно,

$$\lim_{n\to\infty} \frac{1}{n^2}(n + \frac{2n^2}{5 \log_2 n}) \log_2(n + \frac{n^2}{5 \log_2 n}) = \lim_{n\to\infty} \frac{\log_2 n}{n^2}(n + \frac{2n^2}{5 \log_2 n}) \cdot \lim_{n\to\infty} \frac{1}{\log_2 n} \log_2(n + \frac{n^2}{5 \log_2 n}) = \frac{2}{5} \cdot 2 = \frac{4}{5}.$$

Осталось воспользоваться определением предела.

(d) Этот пункт полностью аналогичен предыдущему.

Задача 12. (a) Заметим, что если $a_n < b_n\sqrt{1+\varepsilon}$ и $b_n < c_n\sqrt{1+\varepsilon}$, то $a_n < (1+\varepsilon)c_n$. Осталось воспользоваться определением.

(b) Утверждение задачи сразу следует из определения символов «$\sim$»и «$\lesssim$».

Задача 13. Будем обозначать $m = f(n)$. Если $k = \mathrm{L}(m,n) < \frac{mn}{(2+\varepsilon)\log_2(mn)}$, то

$$mn \leqslant (m + \frac{2mn}{(2+\varepsilon)\log_2(mn)}) \log_2(n + \frac{mn}{2 \log_2(mn)}).$$

Докажем, что это неравенство неверно при достаточно больших n. Действительно,

$$\lim_{n\to\infty}\frac{1}{mn}(m+\frac{2mn}{(2+\varepsilon)\log_2(mn)})\log_2(n+\frac{mn}{(2+\varepsilon)\log_2(mn)}) =$$
$$= \lim_{n\to\infty}\frac{\log_2(mn)}{mn}(n+\frac{2mn}{(2+\varepsilon)\log_2(mn)})\cdot\lim_{n\to\infty}\frac{1}{\log_2(mn)}\log_2(n+\frac{mn}{(2+\varepsilon)\log_2(mn)}) =$$
$$= \frac{2}{2+\varepsilon}\cdot 2 = \frac{4}{2+\varepsilon}.$$

Осталось воспользоваться определением предела.

Задача 14. Разобьём реализуемую матрицу A на подматрицы ширины $\lfloor\log_2\frac{m}{k}\rfloor$. Каждую подматрицу можно реализовать за $\frac{m}{k}$ суммирований. Следовательно, все подматрицы вместе можно реализовать за $\left\lceil\frac{n}{\lfloor\log_2\frac{m}{k}\rfloor}\right\rceil\cdot\frac{m}{k}$ сложений, а саму матрицу A — за $\left\lceil\frac{n}{\lfloor\log_2\frac{m}{k}\rfloor}\right\rceil\cdot\frac{m}{k}+m\left\lceil\frac{n}{\lfloor\log_2\frac{m}{k}\rfloor}\right\rceil\lesssim\frac{k+1}{k}\frac{nm}{\log_2 m}$. Следовательно, для любого k выполнено асимптотическое неравенство $\mathrm{L}(m,n)\lesssim\frac{k+1}{k}\frac{mn}{\log_2 m}$. Следовательно, $\mathrm{L}(m,n)\lesssim\frac{mn}{\log_2 m}$, ч.т.д.

Задача 15. Аналогично задаче 10, можно доказать, что для любого $\varepsilon\in(0,1)$ при достаточно больших n выполнено неравенство $\mathrm{L}(m,n)\leqslant\frac{mn}{\alpha\log_2 n}$, что и требуется в задаче.

Задача 16. (a) Представим схему в виде ориентированного графа, у которого есть вершины четырёх видов:

- входы схемы (у них нет входов, один выход),
- сумматоры (у них два входа, один выход),
- размножатели (у них один вход, два выхода),
- выходы схемы (у них один вход, нет выходов).

Как несложно видеть, элемент a_{ij} равен числу путей из j-го входа в i-й выход (по модулю 2). Рассмотрим новый граф, в котором все рёбра направлены в противоположную сторону и соответствующую ему схему. Несложно видеть, что эта схема реализует матрицу A^t. Обозначим l_1 сложность первой схемы, а l_2 — второй. Найдём число рёбер нашего графа двумя способами: как число начал рёбер первого графа и как число начал рёбер второго графа. В первом случае получим $n+l_1+2l_2$, а во втором случае получим $m+l_2+2l_1$. Следовательно, $n+l_2=m+l_1$. Так как $l_1=\mathrm{L}(A)$, то $\mathrm{L}(A^t)\leqslant m-n+\mathrm{L}(A)$. Осталось воспользоваться тем, что $(A^t)^t=A$.

(b) Следует из (a).

(c) Выбросим из матрицы B_m нулевой столбец и обозначим полученную матрицу B'_m. Тогда $(B'_m)^t$ — это матрица, соответствующая набору всех сумм от m переменных. Сложность этого набора сумм мы уже знаем. Используя пункт (a), получаем $\mathrm{L}(B_m)=2^{m+1}-2m-2$.