Вестник
МОСКОВСКОГО УНИВЕРСИТЕТА

Серия I

МАТЕМАТИКА, МЕХАНИКА

4

Отдельный оттиск

1 9 6 5

Вестник
МОСКОВСКОГО УНИВЕРСИТЕТА
№ 4—1965

УДК 517.862

Б. М. КЛОСС, В. А. МАЛЫШЕВ

ОЦЕНКИ СЛОЖНОСТИ НЕКОТОРЫХ КЛАССОВ ФУНКЦИЙ

В работе [1] было определено понятие сложности реализации дискретной функции на конечном автомате. С другой стороны, всякая дискретная функция может быть реализована суперпозициями базисных функций, иначе говоря, на автомате без обратных связей. Можно поставить вопрос, существуют ли функции, реализация которых на автоматах с обратными связями проще, чем без обратных связей. В связи с этим возникает задача об уменьшении объема автомата, реализующего данную дискретную функцию, за счет увеличения времени его работы. Решение этих вопросов, вообще говоря, различно для разных классов схем. В настоящей работе приводится несколько отличное от [1] определение алгоритмической сложности дискретных функций. Суть отличия заключается в том, что схемы без обратных связей, по нашему определению, работают один такт времени. Этому условию удовлетворяют, например, полупроводниковые и электронные схемы (см. [2], стр. 146). Надо отметить, что приводящееся ниже определение алгоритмической сложности по своим оценкам «сильнее», чем определение, данное в [1], так как для любой пары (N, T) в смысле [1] найдется пара (N', T') в нашем смысле (для той же функции), такая, что $N' \leqslant N$, $T' \leqslant T$. Возвращаясь к поставленным выше задачам, отметим, что первый вопрос решается одинаково для обоих определений сложности, а второй лишь для формулируемого нами определения.

Несколько слов о возникновении данной работы. Пример функции, проще реализуемой схемами с обратными связями (определитель порядка n), был получен В. А. Малышевым весной 1963 г. Затем Б. М. Клосс улучшил и получил новые оценки снизу для рассматриваемого класса функций. Авторы согласились объединить свои результаты в одну работу.

§ 1. Определение алгоритмической сложности дискретных функций

1. Без ущерба для общности мы ограничимся рассмотрением двоичных дискретных функций, то есть отображений множества D_n двоичных последовательностей длины n в D_m. Автоматы, с помощью которых будут реализовываться функции данного типа, будут предполагаться состоящими из M ячеек, каждая из которых может находиться в двух состояниях — 0 и 1. Выделяются два упорядоченных подмножества (возможно пересекающиеся) из n входных и m выходных ячеек. Уравнение, описывающее работу автомата, можно задать с помощью M функций алгебры логики:

$$z_i(t+1) = f_i(z_1(t), \ldots, z_M(t)), \qquad i = 1, \ldots, M,$$

где $z_i(t)$ — состояние i-той ячейки в момент t. Мы скажем, что дискретная функция реализуется на данном автомате за время T, если записанное в начальный момент во входных ячейках значение аргумента даст через T тактов в выходных ячейках значение функции.

Определим теперь понятие сложности реализации системы функций алгебры логики с помощью суперпозиций функций от двух переменных. Пусть задана система из m булевых функций от n переменных (то есть дискретная функция типа $D_n \to D_m$). Запишем эти функции в виде формул, состоящих из символов всевозможных функций от двух переменных, самих переменных, скобок и запятых). Сопоставим этим m формулам ориентированный граф, вершинами которого являются вхождения символов переменных и функций. Условимся, что две вершины соединяет ребро, когда одна из вершин есть символ функции от двух переменных и одним из этих аргументов является другая вершина (в этом случае будем говорить, что вторая вершина подчинена первой). Таким образом, полученный граф естественным образом превращается в частично упорядоченное множество.

Подграфы с наибольшим элементом, содержащие вместе с каждой вершиной и все подчиненные ей вершины, назовем допустимыми. Графы с приписанными вершинам символами переменных и функций называются изоморфными, если при изоморфизме графов соответствующим вершинам приписаны одинаковые символы. Отождествляя изоморфные допустимые подграфы, получим *канонический граф* данной реализации системы функций (формально можно считать вершинами канонического графа классы всех изоморфных допустимых подграфов). Легко видеть, что таким образом получилась обычная алгебраическая «фактор-конструкция».

Число вершин канонического графа, отличных от минимальных (которым сопоставлены символы переменных), называется сложностью данной реализации системы функций с помощью суперпозиций функций от двух переменных.

Будем говорить, что дискретная функция f вычисляется с параметрами (N, T), если система булевых функций, соответствующая уравнению автомата, на котором f реализуется за T тактов, имеет сложность N. Обозначим через $N_f(T)$ минимальную сложность автомата, реализующего функцию f за время T.

2. Для получения оценок снизу величины $N(T)$ может оказаться полезной следующая простая теорема, которая позволяет сводить эту задачу к задаче оценки сложности реализации функции в виде суперпозиций функций от двух переменных.

Теорема 1. *Если функция реализуется с параметрами (N, T), то она реализуется и с параметрами $(N_1, 1)$, где*

$$N_1 \leqslant NT.$$

Доказательство. Утверждение теоремы следует из того факта, что работу автомата в течение T тактов можно представить себе как T-тую итерацию системы булевых функций, описывающих этот автомат.

3. Можно рассматривать автоматы с остановкой, зависящей от начального состояния. Именно, в автомате помимо входных и выходных ячеек выделяется еще одна так называемая «стоп»-ячейка. Автомат работает до тех пор, пока в «стоп»-ячейке не появится число 1. Назовем средним временем вычисления функции типа $D_n \to D_m$ величину $T_{\text{ср}} = \frac{1}{2^n} \sum_x T_x$, где T_x — время вычисления значения функции для аргумента x. Легко видеть, что если функция вычисляется со средним временем $T_{\text{ср}}$, то по крайней мере для половины аргументов этой функции

$T_x < 2T_{\text{ср}}$. Небезынтересно отметить, что если функция типа $D_n \to D_m$ реализуется с параметрами $(N, \{T_x\})$, то она реализуется и с параметрами $(N+2m+1, \max_x T_x)$.

§ 2. Оценки снизу сложности некоторых классов схем без обратных связей

1. В силу данного выше определения схемы без обратных связей совпадают с классом схем, работающих $T=1$ тактов. В этом параграфе мы будем заниматься исключительно такими схемами, поэтому вместо $N_f(1)$ будем писать просто N_f. Отметим сначала несколько общих свойств этих схем.

2. Легко видеть, во-первых, что если булева функция g получается из функции f перестановкой переменных и взятием отрицания у некоторых переменных, то $N_g = N_f$. Поскольку такие функции принадлежат к одному типу, то можно, следовательно, заключить, что *все функции одного типа обладают одинаковой сложностью.*

К этому следует добавить еще одно полезное замечание: *если функция g получается из функции f путем замены значений f их отрицанием, то $N_g = N_f$.*

3. Рассмотрим так называемые R-графы (на интуитивном языке соответствующие графам, реализующим функции алгебры логики). Это ориентированные связные графы без петель, в каждую вершину которых может входить не более двух ветвей. Вершины, в которые не входит ни одна ветвь, назовем входными, остальные — внутренними. Кроме того, потребуем, чтобы в R-графе существовала равно одна вершина, из которой не выходит ни одна ветвь, — такую вершину назовем выходной (она, очевидно, является внутренней). Будем также говорить, что α является вершиной типа i, если из α выходит i ветвей.

Лемма 1. *Пусть R-граф содержит k_i входных и K_i внутренних вершин типа i $(i=1, 2, \ldots)$. Тогда число N внутренних вершин в этом графе удовлетворяет неравенству*

$$N \geqslant k_1 + 2k_2 + \ldots + N \cdot k_N + K_2 + 2K_3 + \ldots + (N-1) K_N - 1. \tag{1}$$

Доказательство. Число всех ветвей в данном графе, очевидно, не превосходит $2N$. С другой стороны, оно складывается из числа ветвей, выходящих из входных вершин, их как раз $k_1 + 2k_2 + \ldots + Nk_N$, и из числа ветвей, выходящих из внутренних вершин, — их всего $N + K_2 + 2K_3 + \ldots + (N-1)K_N - 1$ (из одной вершины не выходит ветвей). Отсюда и следует неравенство (1).

Замечание. Если в R-графе к каждой внутренней вершине подходят две ветви, то неравенство (1) превращается в равенство.

4. В качестве следствия из леммы 1 можно получить, что *для функций, существенно зависящих от n переменных, имеет место соотношение $N_f \geqslant n-1$.* Эту оценку будем называть тривиальной. Нашей задачей будет получение нетривиальных оценок.

5. Будем говорить, что наборы $(\alpha_1, \ldots, \alpha_k)$ и $(\beta_1, \ldots, \beta_k)$ значений аргументов $x_1, \ldots, x_k$ функции $f(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n)$ разделяются, если существуют такие значения остальных аргументов $x_{k+1} = c_{k+1}, \ldots, x_n = c_n$, что

$$f(\alpha_1, \ldots, \alpha_k, c_{k+1}, \ldots, c_n) \neq f(\beta_1, \ldots, \beta_k, c_{k+1}, \ldots, c_n).$$

Назовем функцию f *парно-разделимой*, если для любой ее пары аргументов x_i и x_j разделяются наборы $\{(\alpha, 0), (\alpha, 1), \alpha = 0, 1\}$ и $\{(0, 0),$

$(1,1)\}$ (возможен и другой вариант определения, когда последняя пара наборов заменяется на пару $\{(0,1),\ (1,0)\}$, — в этом случае последующие рассуждения также остаются в силе).

Теорема 2. *Если функция $f(x_1, \ldots, x_n)$ парно-разделима, то*

$$N_f \geqslant 1{,}1n.$$

Доказательство. Рассмотрим канонический граф Г, реализующий функцию f. Очевидно, функция f существенно зависит от всех n аргументов, поэтому в графе Г имеется n входных вершин. Пусть среди них имеется p вершин типа 1. Поскольку функция f парно-разделима, то никакая внутренняя вершина не может подчинять себе сразу две входные вершины типа 1. Следовательно, существует хотя бы одна входная вершина типа $\geqslant 2$, и p не может равняться n.

Назовем внутреннюю вершину отмеченной, если ей подчинена входная вершина типа 1. Отмеченных вершин всего p, пусть среди них l являются вершинами типа 1. Из леммы 1 следует, что

$$N_f \geqslant p + 2(n-p) + p - l = 2n - l.$$

Докажем, что, кроме того, $N_f \geqslant 1{,}25\, l$, откуда и будет следовать искомая оценка.

Разберемся сначала в расположении отмеченных вершин. Пусть отмеченная вершина типа 1, которой соответствует функция $\psi(x_1, u)$, подчинена отмеченной вершине, которой соответствует функция $\varphi(x_2, \psi)$. Если функция φ, записанная в виде приведенного многочлена, нелинейна, то найдется такое значение $x_2 = c$, что φ не будет зависеть от второго аргумента, и тогда для переменных x_1 и x_2 не будут разделяться наборы значений $(0, c)$ и $(1, c)$, что противоречит условию парной разделимости функции f. Следовательно, функция φ должна быть линейной. При этом следует заметить, что функция ψ не может быть также линейной, так как в этом случае для тех же переменных не будут разделяться наборы $(0,0)$ и $(1,1)$. Таким образом, отмеченная вершина (ψ) типа 1 может подчиняться отмеченной вершине (φ) лишь в том случае, когда функция φ линейна, а функция ψ нелинейна. Отсюда следует, что если отмеченная вершина типа 1 подчинена некоторой отмеченной вершине, то ей в свою очередь не может быть подчинена никакая отмеченная вершина типа 1.

Подсчитаем, сколько отмеченных вершин типа 1 непосредственно подчинено неотмеченным вершинам. Так как каждая отмеченная вершина типа $\geqslant 2$ может в принципе подчинять себе одну отмеченную вершину типа 1, то $k = p - l$ таких вершин типа 1 лишаются возможности подчиняться неотмеченным вершинам. Следовательно, число отмеченных вершин типа 1, которые подчинены неотмеченным вершинам, равно по меньшей мере $\frac{l-k}{2}$. Поскольку одной вершине может быть подчинено не более двух вершин, то число неотмеченных вершин будет $\frac{l-k}{4}$. Отсюда следует, что число внутренних вершин графа Г будет

$$\geqslant \frac{5}{4} l + \frac{3}{4} k \geqslant \frac{5}{4} l.$$

6. Будем говорить, что функция f дважды парно-разделима, если при подстановке вместо любого аргумента произвольной константы получившаяся функция является парно-разделимой. Аналогично определим, что функция f *m раз парно-разделима*, если при подстановке вместо любых $m-1$ аргументов произвольных констант получившаяся функция снова парно-разделима.

7. Теорема 3. *Если функция $f(x_1, ..., x_n)$ является трижды парно-разделимой, то*

$$N_f \geqslant \frac{8}{7} n.$$

Доказательство. Сохраним терминологию, введенную при доказательстве теоремы 2. Пусть отмеченная вершина типа 1 подчинена другой отмеченной вершине типа 1, тогда такую пару вершин мы назовем конфигурацией. Из условия, что исходная функция трижды парно-разделима, следует, как легко проверить, что неотмеченная вершина не может подчинять себе две конфигурации. Следовательно, неотмеченная вершина может подчинять себе максимум три отмеченные вершины типа 1. Поэтому число неотмеченных вершин равно по меньшей мере $\frac{l-k}{3}$. Следовательно, число внутренних вершин канонического графа оценивается снизу величиной $\frac{l-k}{3} + l + k \geqslant \frac{4}{3} l$, откуда и следует искомая оценка.

8. Теорема 4. *Если функция $f(x_1, ..., x_n)$ является m раз парно-разделимой, то*

$$N_f \geqslant n + m - 1.$$

Доказательство. Пусть в каноническом графе имеется $n-l$ входных вершин типа 1. Если $l \geqslant m$, то теорема доказана; если $l<m$, то подставим на место переменных, соответствующих этим вершинам, некоторые константы. Тогда все вершины графа разделятся на вершины, которым соответствует функция-константа, и на вершины с непостоянной функцией. Рассмотрим канонический граф, полученный отбрасыванием вершин с постоянной функцией и с функциями от одного аргумента с соответствующими заменами функций у других вершин, чтобы этот граф реализовал полученную функцию от $n-l$ переменных. Так как у этого графа должно быть столько внутренних вершин типа $\geqslant 2$, чтобы сумма их типов минус их число была $\geqslant m-l$ (по индуктивному предположению), то теорема следует из неравенства (1).

Замечание. Теорема будет верна, если в определении кратной парной разделимости потребовать, чтобы парная разделимость сохранялась лишь при подстановке некоторых констант.

9. Ниже мы рассмотрим несколько примеров функций со свойством разделимости.

Лемма 2. *Функция*

$$C_2(x_1, \dots, x_n) = \sum_{i<j} x_i x_j$$

(сумма понимается по модулю 2) является $n-2$ раза парно-разделимой.

Доказательство. Проверим свойство разделимости в отношении наборов $(0, \alpha_2, ..., \alpha_{n-1})$ и $(1, \alpha_2, ..., \alpha_{n-1})$, подставленных вместо аргументов $x_1, x_2, ..., x_{n-1}$ (чем всегда можно ограничиться в силу симметрии функции C_2). Надо доказать, что

$$C_2(0, \alpha_2, \dots, \alpha_{n-1}, x_n) + C_2(1, \alpha_2, \dots, \alpha_{n-1}, x_n) \not\equiv 0.$$

Имеем

$$C_2(0, \alpha_2, \dots, \alpha_{n-1}, x_n) + C_2(1, \alpha_2, \dots, \alpha_{n-1}, x_n) =$$
$$= \alpha_2 + \dots + \alpha_{n-1} + x_n \not\equiv 0.$$

Теперь проверим разделимость наборов $(0, 0, \alpha_3, ..., \alpha_{n-1})$ и $(1, 1, \alpha_3, ..., \alpha_{n-1})$. Имеем

$$C_2(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_{n-1}, x_n) + C_2(\beta_1, \beta_2, \alpha_3, \dots, \alpha_{n-1}, x_n) =$$

$$= \alpha_1\alpha_2 + (\alpha_1 + \alpha_2)(\alpha_3 + \ldots + \alpha_{n-1} + x_n) + \beta_1\beta_2 +$$
$$+ (\beta_1 + \beta_2)(\alpha_3 + \ldots + \alpha_{n-1} + x_n),$$

что после подстановки $\alpha_1=\alpha_2=0$, $\beta_1=\beta_2=1$ даст нам тождественную единицу.

Теорема 5. *Для функции $C_2(x_1, ..., x_n)$ имеет место соотношение*

$$N_{C_2} \geqslant 2(n-1).$$

Доказательство. Теорема 4 дает нам, что $N_{C_2} \geqslant 2(n-2)$. Уточненную оценку получим по индукции. Для $n=3$ функция $C_2(x_1, x_2, x_3)$ реализуется с помощью четырех суперпозиций. Например, $C_2(x_1, x_2, x_3) = \varphi_1(x_3, \varphi_2, (\varphi_3(x_1, x_3), \varphi_4(x_2, x_3)))$, где $\varphi_1(x, y) = x+y$, $\varphi_2(x, y) = xy$, $\varphi_3(x, y) = x+y$, $\varphi_4(x, y) = x+y$. Нетрудно показать (хотя бы перебором вариантов), что на меньшем числе элементов функцию $C_2(x_1, x_2, x_3)$ реализовать невозможно. Таким образом, уточненная оценка для $n=3$ справедлива. Теперь шаг индукции довольно легко проследить, если положить один из аргументов равным нулю (именно тот, для которого соответствующая входная вершина канонического графа имеет тип больший, чем 2).

10. Аналогичными приемами доказывается также, что *функция*

$$C_k(x_1, \ldots, x_n) = \sum_{i_1<\ldots<i_k} x_{i_1} \ldots x_{i_k}$$

является $n-k-1$ раз парно-разделимой и, следовательно,

$$N_{C_k} \geqslant 2(n-1) - k.$$

11. Функция $V_k(x_1, ..., x_n)$ называется функцией уровня k, если она обращается в единицу на тех наборах, число единиц в которых $\geqslant k$. *Если $2 \leqslant k \leqslant n-2$, то*, как легко видеть, *функция уровня V_k $n-2$ раза парно-разделима в слабом смысле* (в смысле замечания 1 к теореме 4) *и, следовательно, $N_{V_k} \geqslant 2n-3$.*

12. Функцию $f(x_1, ..., x_n)$ назовем *m-разделимой*, если для нее разделяются произвольные значения любых $m<n$ аргументов.

Лемма 3. *Функция $\pi(x_1, \ldots, x_n) = \sum_{i=1}^{n} (x_i x_{i+1} + x_i x_{i+5})$, $n > 15$, где индексы $i+k>n$ надо понимать по $\mathrm{mod}\, n$, является трижды разделимой.*

Доказательство. Рассмотрим некоторые три индекса i_1, i_2, i_3 и две системы значений переменных: $(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3})$ и $(\beta_{i_1}, \beta_{i_2}, \beta_{i_3})$. Для одного из индексов, например, i_1, $\alpha_{i_1} \neq \beta_{i_1}$. После подстановки этих двух систем значений получим два приведенных многочлена Жегалкина. Тогда нетрудно убедиться в том, что одно из переменных $x_{i_1-5}, x_{i_1-1}, x_{i_1+1}, x_{i_1+5}$ будет присутствовать как слагаемое в одном и отсутствовать в другом приведенном многочлене. Таким образом, найдутся i_1 и значения остальных переменных такие, что эти два многочлена не будут равны.

13. Лемма 4. *Определитель $\det(n)$ порядка n является $(n-1)$-разделимой функцией от n^2 аргументов.*

Доказательство. Теорему докажем по индукции. Для $n=2$ она проверяется непосредственно. Теперь пусть $\det_a(n)$ есть определитель порядка n, в котором некоторые $n-1$ элементов замещены числами $a_1, ..., a_{n-1}$, а $\det_b(n)$ — определитель, в котором те же элементы замещены числами $b_1, ..., b_{n-1}$. Мы считаем, что векторы $(a_1, ..., a_{n-1})$ и $(b_1, ..., b_{n-1})$ различны. Нужно доказать, что $\det_a(n) + \det_b(n) \not\equiv 0$. Легко видеть, что в $\det_a(n)$ существует столбец, не содержащий ни одно из чисел $a_1, ..., a_{n-1}$. Пусть это будет первый столбец. Теперь могут возникнуть два случая. Первый случай, когда существует строка (пусть это будет первая строка), содержащая хотя бы одно из чисел a_i, причем в определителе, оставшемся после вычеркивания этой строки и первого столбца, найдется хотя бы одно из чисел a_j, для которого соответствующее b_j было бы равно его отрицанию: $b_j = \bar{a}_j$. Положим $x_{11} = 1$, а остальные элементы первого столбца приравняем нулю, тогда

$$\det_a(n) + \det_b(n) = \det_a(n-1) + \det_b(n-1) \not\equiv 0,$$

по предположению индукции. Остается второй случай, когда все числа $a_1, ..., a_{n-1}$ расположены в одной строке. Тогда, поменяв местами строки и столбцы, придем к первому случаю.

§ 3. Уменьшение нижней границы алгоритмической сложности введением обратной связи

1. *Функция* $\pi(x_1, \ldots, x_n) = \sum (x_i x_{i+1} + x_i x_{i+5})$ (см. лемму 3) *реализуется с параметрами* (N_π, n), *где*

$$N_\pi \leqslant n + 3.$$

Действительно, можно построить реализующий автомат, состоящий из $n+1$ ячеек (n входных: $z_1, \ldots, z_n$ и одна выходная z_{n+1}). Его уравнения суть: $z_{i+1}(t+1) = z_i(t)$ при $1 \leqslant i < n$, $z_1(t+1) = z_n(t)$, $z_{n+1}(t+1) = z_{n+1}(t) + z_1(t) z_2(t) + z_1(t) z_6(t)$.

2. Теорема 6. *Определитель порядка* n *в поле из двух элементов* $\det_n(a_{ij})$, $i, j = 1, \ldots, n$, *реализуется с параметрами* $(N_{\det_n}, 2n^2)$, *где*

$$N_{\det_n} < n^2 + Cn.$$

Доказательство. Реализующий автомат будет состоять из n^2 входных ячеек a_{ij}, одной выходной x, $2p = 2([\log n] + 1)$ дополнительных $c_1, \ldots, c_p, d_1, \ldots, d_p$. Уравнения его записываются так:

$$a_{ij}(t+1) = a_{i,j+1}(t), \quad 2 \leqslant i < n,$$

$$a_{ij}(t+1) = \begin{cases} a_{1j}(t), \text{ если: } & 1.\ y(t) = 0,\ a_{11}(t) = 1. \\ & 2.\ y(t) = 0,\ a_{11}(t) = 0,\ a_{21}(t) = 0. \\ a_{2j}(t), \text{ если: } & 1.\ y(t) = 0,\ a_{11}(t) = 0,\ a_{21}(t) = 1. \\ & 2.\ y(t) = 1. \end{cases}$$

$$a_{nj}(t+1) = \begin{cases} 0, \text{ если } y(t) = 1, \\ a_{2j}(t), \text{ если } y(t) = 0,\ a_{11}(t) = 0,\ a_{21}(t) = 0, \\ a_{1j}(t), \text{ если } y(t) = 0,\ a_{11}(t) = 0,\ a_{21}(t) = 1, \\ a_{2,j+1}(t),\ j < n, \text{ если } y(t) = 0,\ a_{11}(t) = 1,\ a_{21}(t) = 0, \\ 0,\ j = n, \\ a_{1,j+1}(t) + a_{2,j+1}(t),\ j < n, \text{ если } y(t) = 0,\ a_{11}(t) = 1,\ a_{21}(t) = 1, \\ 0,\ j = n. \end{cases}$$

$$c_1(t+1) = \begin{cases} 0, \text{ если: } & 1.\ y(t) = 1. \\ & 2.\ y(t) = 0,\ c_1(t) = 1. \\ 1, \text{ если: } & 1.\ y(t) = 0,\ c_1(t) = 0,\ \bar{c}_2(t) \ldots \bar{c}_p(t) = 0. \\ & 2.\ y(t) = 0,\ a_{11}(t) = 1,\ \bar{c}_1(t) \ldots \bar{c}_p(t) = 1. \end{cases}$$

$$c_k(t+1)=\begin{cases} 0, \text{ если: } & 1.\ y(t)=1. \\ & 2.\ y(t)=0,\ c_1(t)\dots c_{k-1}(t)=0,\ c_k(t)=0. \\ & 3.\ y(t)=0,\ c_1(t)\dots c_k(t)=1. \\ 1 \text{ в остальных случаях}, \end{cases} \quad 2\leqslant k\leqslant p$$

$$\text{где } y(t)=c_1^{\alpha_1}(t)\dots c_p^{\alpha_p}(t),\ \sum_{k=0}^{p-1}2^k\cdot\alpha_{k+1}=n-1.$$

$$d_k(t+1)=\begin{cases} d_k(t), \text{ если: } y(t)=0, \\ 0, \text{ если: } & 1.\ y(t)=1,\ d_1(t)\dots d_k(t)=1. \\ & 2.\ y(t)=1,\ d_1(t)\dots d_{k-1}(t)=0,\ d_k(t)=0. \\ 1 \text{ в остальных случаях}. \end{cases}$$

$$x(1)=0,$$

$$x(t+1)=\begin{cases} x(t), \text{ если: } & 1.\ x(t)=0,\ d_1^{\alpha_1}(t)\dots d_p^{\alpha_p}(t)=0. \\ & 2.\ x(t)=1. \\ a_{11}(t), \text{ если } x(t)=0,\ d_1^{\alpha_1}(t)\dots d_p^{\alpha_p}(t)=1. \end{cases}$$

Сделаем некоторые необходимые пояснения. Идея состоит в том, чтобы функции более чем от двух переменных в канонических уравнениях были только для числа ячеек порядка Cn. Для этого информация устраивается непрерывно циркулирующей снизу вверх по матрице (a_{ij}). Все необходимые преобразования совершаются в первой и последней строках. Сначала переставляются строки до тех пор, пока в a_{11} не появится 1; тогда начинается работа счетчика тактов (ячейки $c_1, \dots, c_p$), то есть в течение того времени, когда складываются строки. При сложении строк результат помещается в последнюю строку со сдвигом так, что к концу работы этого счетчика на месте определителя оказывается минор элемента a_{11}. Этим заканчивается первый этап. Второй счетчик тактов отмечает пройденные этапы. Если на некотором этапе в первом столбце все нули, то сдвигов не происходит.

ЛИТЕРАТУРА

1. Офман Ю. Об алгоритмической сложности дискретных функций. ДАН СССР, 145, № 1, 48—51, 1962.
2. Кобринский Н. Е., Трахтенброт Б. А. Введение в теорию конечных автоматов. ГИФМЛ, М., 1962.

Поступила в редакцию
4. 2 1964 г.

Кафедра
теории вероятностей

B. M. Kloss, V. A. Malyshev

VALUATIONS OF COMPLEXITY OF SEVERAL CLASSES OF FUNCTIONS

The Boolean functions for which nonlinear (with respect to the number of their arguments) estimates from below of complexity of their realization in a class of formulas have been obtained (by Kritchevsky, Subbotovskaya, Markov) possess linear complexity in a class of schemes of functional elements. In this paper linear estimates from below of complexity in the latter class have been derived for classes of functions with «separability» properties.

The determinant of order n is proved to be more easily realized if the realizing automaton works for $T>1$ units of time.