ДОКЛАДЫ

АКАДЕМИИ НАУК СССР

1967

том 172, № 3

Доклады Академии наук СССР
1967. Том 172, № 3

УДК 519.95

КИБЕРНЕТИКА И ТЕОРИЯ РЕГУЛИРОВАНИЯ

Б. М. КЛОСС, В. А. МАЛЫШЕВ

ОПРЕДЕЛЕНИЕ РЕГУЛЯРНОСТИ АВТОМАТА ПО ЕГО КАНОНИЧЕСКИМ УРАВНЕНИЯМ

(Представлено академиком А. Н. Колмогоровым 19 III 1966)

Будем рассматривать автономные автоматы с конечным множеством состояний Ω, содержащим N элементов. Каждый такой автомат $\mathfrak{A}$ можно представить себе как некоторое преобразование множества Ω в себя. Условимся называть автомат регулярным, если он осуществляет взаимно однозначное преобразование Ω. Нас будет интересовать задача, как по уравнениям автомата узнать, является ли данный автомат регулярным или нет. Решение этой задачи, а также оценку ее сложности будем производить в определенном классе методов. В основе их заложена следующая идея. Понятно, что для проверки регулярности автомата $\mathfrak{A}$ достаточно для соответствующего преобразования подсчитать мощность прообраза каждого элемента из Ω. Будем говорить, что автомат $\mathfrak{A}$ сохраняет вес множества $A \subset \Omega$, если число элементов в A равно числу элементов в прообразе этого множества при отображении $\mathfrak{A}$. Обобщая указанное выше правило, мы приходим к рассмотрению систем множеств из Ω, обладающих тем свойством, что если автомат $\mathfrak{A}$ сохраняет вес любого из множеств данной системы, то автомат $\mathfrak{A}$ должен быть регулярным. Такие системы множеств будем называть определяющими.

Пусть множества $A_1, \ldots, A_s$ образуют определяющую систему в пространстве Ω. Обозначим через x_i число элементов в прообразе i-й точки для автомата $\mathfrak{A}$. В предположении, что автомат $\mathfrak{A}$ сохраняет вес данных множеств, имеем

$$\sum_{j=1}^{N} a_{ij}x_j = \sum_{j=1}^{N} a_{ij}, \quad i = 1, \ldots, s; \quad \sum_{j=1}^{N} x_j = N, \tag{1}$$

где $a_{ij} = 1$, если j-я точка входит в A_i, $a_{ij} = 0$ в противоположном случае.

Лемма 1. *Множества $\{A_1, \ldots, A_s\}$ образуют определяющую систему тогда и только тогда, когда уравнения* (1) *имеют в области $\{x_i \geqslant 0, i = 1, \ldots, N\}$ единственное целочисленное решение.*

Мы будем заниматься задачей по выбору определяющих систем множеств и оценки минимального числа множеств в таких системах.

Параллельно наши рассмотрения будут вестись еще и в следующем аспекте. Скажем, что автомат $\mathfrak{A}$ сохраняет четность множества A, если число элементов в A по четности равно числу элементов в прообразе этого множества. Назовем систему множеств четно определяющей, если из сохранения автоматом $\mathfrak{A}$ четности любого множества данной системы следует его регулярность.

Лемма 2. *Для того чтобы множества $\{A_1, \ldots, A_s\}$ образовывали четно определяющую систему, необходимо и достаточно, чтобы уравнения* (1) *в поле сложения целых чисел по модулю 2 имели единственное решение.*

Из лемм 1 и 2 следует

Лемма 3. *Свойство определимости (четной определимости) системы множеств не изменится, если некоторые из этих множеств заменить на их дополнения.*

Из леммы 2 также следует

Теорема 1. *Число множеств в минимальной четно определяющей системе равно* $N-1$. *Более того, множества* $A_1, \ldots, A_{N-1}$ *образуют четно определяющую систему тогда и только тогда, когда определитель системы* (1) (*в поле сложения целых чисел по модулю* 2) *равен единице.*

Замечание. Четно определяющая система является одновременно и определяющей системой.

Обозначим через $T(N)$ число множеств в минимальной определяющей системе (пространство Ω состоит из N элементов).

Следствие. $T(N) \leqslant N-1$.

С другой стороны, из того факта, что для каждой пары точек из Ω должно найтись в определяющей системе множество, которое их «разделяет», следует, что $T(N) \geqslant \log N$.

Лемма 4. $T(N-1) \leqslant T(N) \leqslant T(N-1)+1$.

Определим множество векторов, на которых обращается в 1 булева функция f, как носитель функции f. Число элементов в носителе называется весом функции и обозначается $\|f\|$. Теперь приведем некоторые примеры четно определяющих систем в случае, когда $N=2^n$.

Теорема 2. *Носители всевозможных элементарных конъюнкций* $x_{i_1} \ldots x_{i_k}$, $1 \leqslant k \leqslant n$, *образуют четно определяющую* (*следовательно, и определяющую*) *систему множеств в пространстве n-мерных булевых векторов.*

Следствие 1. *Носители всевозможных элементарных дизъюнкций* $x_{i_1} \vee \ldots \vee x_{i_k}$, $1 \leqslant k \leqslant n$, *образуют четно определяющую* (*определяющую*) *систему множеств в пространстве n-мерных булевых векторов.*

Следствие 2. *Система булевых уравнений*

$$y_i = f_i(x_1, \ldots, x_n), \quad i = 1, \ldots, n, \tag{2}$$

разрешима при любых значениях левых частей тогда и только тогда, когда $\|f_{i_1} \ldots f_{i_k}\| = 2^{n-k}$, $1 \leqslant k \leqslant n$.

Следствие 3. *Система булевых уравнений* (2) *разрешима при любых значениях левых частей тогда и только тогда, когда*

$$\|f_{i_1} \vee \ldots \vee f_{i_k}\| = 2^n - 2^{n-k}, \quad 1 \leqslant k \leqslant n.$$

Следствие 4 (Д. Хаффмен [1]). *Для того чтобы система уравнений* (2) *была разрешима при любых значениях левых частей, необходимо и достаточно, чтобы функции* $f_{i_1} \ldots f_{i_k}$, $1 \leqslant k \leqslant n-1$, *записанные в виде полиномов Жегалкина, не содержали произведения* $x_1 x_2 \ldots x_n$, *а функция* $f_1 \ldots f_n$ *его содержала.*

Теорема 3. *Носители всевозможных линейных функций* $x_{i_1} \oplus \ldots \oplus x_{i_k}$, $1 \leqslant k \leqslant n$ ($\oplus$ *означает сложение по модулю* 2), *образуют в пространстве n-мерных булевых векторов определяющую систему, не являющуюся четно определяющей.*

Доказательство. Рассмотрим матрицу соответствующей системы (1). Один столбец в ней состоит из всех нулей и одной единицы (соответствующей строке из одних единиц), поэтому откинем этот столбец и последнюю строку,— приходим к некоторой матрице C порядка 2^n-1. Заметим, что носитель каждой линейной функции содержит 2^{n-1} элементов, а носитель произведения двух различных функций содержит 2^{n-2} элементов. Поэтому произведение матрицы C на транспонированную дает матрицу $2^{n-2}\begin{pmatrix} 2 & 1 & \ldots & 1 \\ 1 & 2 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 2 \end{pmatrix}$, которая является невырожденной. Определимость системы следует тогда из леммы 1. В то же время в поле сложения целых чисел по модулю 2 матрица C является вырожденной (так как в каждой строке этой матрицы имеется четное число единиц), следовательно, по теореме 1, данная система не является четно определяющей.

Следствие. *Система булевых уравнений* (2) *разрешима при любых значениях левых частей тогда и только тогда, когда*

$$\|f_{i_1} \oplus \ldots \oplus f_{i_k}\| = 2^{n-1}, \quad 1 \leqslant k \leqslant n.$$

Теорема 4. *Пусть* Ω *есть множество* n*-мерных булевых векторов. Если определяющая система состоит из носителей линейных функций, то число множеств в такой системе равно* $2^n - 1$.

Доказательство. Предположим, что данная система включает носители не всех линейных функций; например, пусть индикаторная строка $a_1, \ldots, a_N$, соответствующая носителю некоторой линейной функции, не входит в матрицу системы (1) (берем лишь линейно независимые строки). Тогда, учитывая замечания, сделанные при доказательстве предыдущей теоремы, приходим к тому, что система (1) имеет дополнительное решение, равное $x_1 = 2a_1, \ldots, x_N = 2a_N$.

Теорема 5. *Пусть* Ω *есть множество* n*-мерных булевых векторов. Если определяющая система состоит из носителей конъюнкций* $x_{i_1} \ldots x_{i_k}$, $k \leqslant n$, *то число множеств в такой системе равно* $2^n - 1$.

Теорема 6. *Если определяющая система состоит из носителей конъюнкций ранга* n, *то число множеств в такой системе равно* $2^n - 1$.

С другой стороны, как показывает следующий пример, указанные выше оценки не всегда имеют место.

Теорема 7. *В множестве* n*-мерных булевых векторов* ($n \geqslant 3$) *существует определяющая система, в которой число множеств равно* $2^n - 2$.

Доказательство. В качестве множеств $A_1, \ldots, A_{2^n-3}$ выберем носители некоторых $2^n - 3$ линейных функций. Соответствующую им систему (1) после очевидной замены переменных приведем к однородной системе, а решения будем искать в области $\{x_i \geqslant -1\}$. Пусть две строки, соответствующие двум недостающим линейным функциям, имеют вид: $a_1 = \ldots = a_{2^{n-1}} = 1$, $a_{2^{n-1}+1} = \ldots = a_{2^n} = 0$; $b_1 = \ldots = b_{2^n-2} = 0$, $b_{2^n-2+1} = \ldots = b_{3\cdot 2^{n-2}} = 1$, $b_{3\cdot 2^{n-2}+1} = \ldots = b_{2^n} = 0$. Однородной системе удовлетворяют два линейно независимых решения: $x_1^1 = \ldots = x_{2^{n-1}}^1 = 1$, $x_{2^{n-1}+1}^1 = \ldots = x_{2^n}^1 = -1$; $x_1^2 = \ldots = x_{2^n-2}^2 = -1$, $x_{2^n-2+1}^2 = \ldots = x_{3\cdot 2^{n-2}}^2 = 1$, $x_{3\cdot 2^{n-2}+1}^2 = \ldots = x_{2^n}^2 = -1$, и два решения, являющиеся их линейными комбинациями: $x_1^3 = \ldots = x_{2^n-2}^3 = 0$, $x_{2^n-2+1}^3 = \ldots = x_{2^{n-1}}^3 = 1$, $x_{2^{n-1}+1}^3 = \ldots = x_{3\cdot 2^{n-2}}^3 = 0$, $x_{3\cdot 2^{n-2}+1}^3 = \ldots = x_{2^n}^3 = -1$; $x_1^4 = \ldots = x_{2^n-2}^4 = 1$, $x_{2^n-2+1}^4 = \ldots = x_{2^{n-1}}^4 = 0$, $x_{2^{n-1}+1}^4 = \ldots = x_{3\cdot 2^{n-2}}^4 = -1$, $x_{3\cdot 2^{n-2}}^4 = \ldots = x_{2^n}^4 = 0$. Других решений, кроме нулевого, не имеется. Если теперь $2^{n-2} \geqslant 2$, то мы выберем множество A_{2^n-2}, которому отвечает строка $c_1, \ldots, c_{2^n}$, у которой $c_1 = c_2 = c_{2^{n-1}} = 1$, а остальные $c_i = 0$. Указанные выше четыре решения уравнению $c_1x_1 + \ldots + c_{2^n}x_{2^n} = 0$ не удовлетворяют, поэтому, если его присоединить к первоначальной однородной системе, то новая система будет иметь в области $\{x_i \geqslant -1\}$ единственное решение.

Замечание. Более того, какое бы ни было целое $C_0 > 0$, найдется такое $N_0 = N_0(C_0)$, что для всех $N > N_0$ будет $T(N) \leqslant N - C_0$.

В качестве примера на применение полученных выше критериев рассмотрим различные регистровые схемы, уравнения которых после несложных преобразований приводятся к треугольному виду:

$$y_i = f_i(x_1, x_2, \ldots, x_i), \quad i = 1, 2, \ldots, n. \tag{3}$$

Система типа (3) определяет регулярный автомат, как легко следует из сказанного выше, в том и только том случае, если функции f_i имеют вид $f_i(x_1, \ldots, x_{i-1}, x_i) = f_i'(x_1, \ldots, x_{i-1}) \oplus x_i$.

В разных конкретных случаях удобно применять тот или иной крите-

рий с разными проверочными функциями. На эти проверочные функции естественно накладываются требования к их простоте. Приведенные выше критерии (проверка четности, проверка весов с проверочными линейными функциями и конъюнкциями) имеют по существу квадратичную сложность (сложность понимается в смысле ([2])). Кроме того, теоремы 1, 4, 5 и 6 дают оценку этой сложности снизу. Представляет интерес оценить снизу сложность задачи по определению регулярности автомата для любых методов ее решения (в классе схем из функциональных элементов, реализующих произвольные функции двух переменных).

Рассмотрим произвольную нумерацию R булевых функций n переменных двоичными наборами длины 2^n (например, коэффициенты многочлена Жегалкина, табличное задание функции и др.). Нумерация R естественно порождает некоторую нумерацию систем булевых функций (2) наборами длины $n \cdot 2^n$. Рассмотрим теперь функцию Ф от $n \cdot 2^n$ переменных, равную 1 тогда и только тогда, когда система (2), соответствующая набору-аргументу, разрешима при любых значениях левых частей. Мы докажем, что сложность функции Ф оценивается снизу величиной $n(2^n - 1) - 1$, что (с учетом ([2])) будет следовать из теоремы 8.

Теорема 8. *Функция* Ф *существенно зависит по крайней мере от* $n(2^n - 1)$ *переменных.*

Доказательство. Разобьем переменные на n групп по 2^n в каждой группе — соответственно функциям из (2). Предположим, что Ф зависит несущественно от переменной z_1 первой группы. Тогда для фиксированного набора $(\sigma_2, \ldots, \sigma_{2^n})$ значений остальных переменных этой группы функции f_1^0 и f_1^1, соответствующие в данной нумерации наборам $(0, \sigma_2, \ldots, \sigma_{2^n})$ и $(1, \sigma_2, \ldots, \sigma_{2^n})$, как легко видеть, либо обе имеют вес 2^{n-1}, либо обе этим свойством не обладают. Исследуем первую возможность. Здесь могут представиться два случая: либо найдутся два набора $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$ на хеммингговском расстоянии 1 друг от друга и такие, что для одной функции, например, $f_1^0(\alpha) = f_1^0(\beta)$, а для другой $f_1^1(\alpha) \neq f_1^1(\beta)$, либо таких наборов не найдется. В этом последнем случае либо $f_1^0 \equiv f_1^1$, либо $f_1^0 = \bar{f}_1^1$. Действительно, рассмотрим произвольный набор $x = (x_1, \ldots, x_n)$ и цепочку наборов $\alpha = \alpha^0, \alpha^1, \ldots, \alpha^{k-1}, \alpha^k = x$ такую, что $\alpha^i \alpha^{i+1}$ для всех $i = 0, \ldots, k-1$ находятся друг от друга на расстоянии 1. Тогда, очевидно, равенство или неравенство функций f_1^0 и f_1^1 на одном наборе α будет распространяться на любой набор x. Поскольку все-таки функции f_1^0 и f_1^1, по определению, должны быть различны, мы приходим к выводу, что в данном случае $f_1^0 \equiv \bar{f}_1^1$.

Теперь исследуем другой случай — когда такие два набора α и β существуют (можно ограничиться случаем, когда они отличаются лишь первой координатой). Определим тогда остальные функции системы (2) так, чтобы они переводили наборы α и β в один набор $(\alpha_2, \ldots, \alpha_n)$, а в сочетании с функцией f_1^1 образовывали разрешимую систему. Это, как нетрудно видеть, всегда можно сделать, но, с другой стороны, приводит к существенности переменной z_1, что противоречит исходному предположению. Следовательно, этот случай не имеет места.

На основании изложенного можно сделать вывод, что две противоположные функции (одна является отрицанием другой) веса 2^{n-1} могут отличаться лишь первой координатой нумерующего набора, и любая другая переменная из этой же группы должна быть существенной (так как для нее могут быть проведены те же самые рассуждения).

Поступило
5 III 1966

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] D. Huffman, Trans. IRE, CT-6, Spec. Suppl., 41 (1959). [2] Б. М. Клосс, В. А. Малышев, Вестн. Моск. унив., № 4 (1965).