Московский государственный университет им. М.В. Ломоносова
Механико-математический факультет

МАТЕРИАЛЫ

ЧЕТВЕРТОЙ МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

МГУ 2000

УДК 519.7

М34 Материалы четвертой молодежной научной школы по дискретной математике и ее приложениям (Москва, 18-23 сентября 2000г.). — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2000. — 96 с.

Сборник содержит материалы четвертой молодежной научной школы по дискретной математике и ее приложениям. Школа проводилась на механико-математическом факультете Московского государственного университета им. М.В. Ломоносова с 18 по 23 сентября 2000г. при поддержке Федеральной целевой программы "Интеграция" (проект 474). Издание осуществлено при финансовой поддержке ФЦП "Интеграция". Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Без объявл.

Научное издание

МАТЕРИАЛЫ
ЧЕТВЕРТОЙ МОЛОДЕЖНОЙ НАУЧНОЙ ШКОЛЫ
ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЕ ПРИЛОЖЕНИЯМ

Под общей редакцией чл.-корр. РАН О.Б. Лупанова

Ответственный за выпуск А.В. Чашкин

Н/К
ЛР № 040746 от 12.03.96. Подписано к печати 24.10.00. Формат 60 × 90/16. Бумага типогр. №1. Гарнитура "Computer Modern". Печать РИЗО. Печ. л. 4. Тираж 120 экз.

Издательство центра прикладных исследований при механико-математическом факультете МГУ.
Отпечатано на типографском оборудовании механико-математического факультета МГУ и Франко-русского центра им. А.М. Ляпунова.

Без объявл.

СОДЕРЖАНИЕ

О 3–РАСКРАСКЕ ПЛОСКОГО ГРАФА С ОТОЖДЕСТВЛЕННОЙ ПАРОЙ ВЕРШИН

В. А. Аксенов*, О. В. Бородин**, А. Н. Глебов**

Первым важнейшим результатом по проблеме раскраски вершин плоского графа в 3 цвета является доказанная Грецшем [1] в 1958 г. теорема о том, что если плоский граф не содержит циклов длины 3, то его вершины можно правильно раскрасить в 3 цвета. Грюнбаум [2] в 1963 г. сформулировал следующее усиление теоремы Грецша: если плоский граф содержит не более трех 3-циклов, то он является 3-раскрашиваемым. Полное доказательство этого факта было дано Аксеновым в [3]. При доказательстве использовалась техника продолжения раскраски, заданной на грани, на весь граф. В 1997 г. Бородин [4] дал новое, более простое, доказательство теоремы Грюнбаума, основывающееся на перераспределении эйлеровых вкладов в плоском графе и так называемой порционной раскраске.

Основываясь на идеях, развитых в [3] и [4], мы доказали следующий факт, относящийся к 3-раскраске уже неплоских графов:

Теорема 1. *Если G плоский граф без 3-циклов, то граф, получающийся из G отождествлением любой пары несмежных вершин, является 3-раскрашиваемым.*

Иначе говоря, теорема утверждает, что существует такая раскраска вершин плоского графа без 3-циклов в три цвета, в которой заданные две вершины имеют один цвет. Данная теорема является неулучшаемой в том смысле, что она перестает быть верной при наличии в G хотя бы одного 3-цикла; это подтверждается соответствующим примером.

При доказательстве теоремы сначала рассматривается случай, когда в предполагаемом контрпримере G отсутствуют разделяющие 4- и 5-циклы; в этом случае перераспеределение вкладов в G приводит к противоречию с формулой Эйлера. При наличии в G разделяющих 4- или 5-циклов рассмотрение переносится со всего графа G на специально выбранный подграф, ограниченный одним из таких циклов.

Работа поддержана грантом РФФИ (№ 00-01-00916), а также грантом Университеты России (№ 1792) — программа фундаментальных исследований.

ЛИТЕРАТУРА

[1] H. Grötzsch (1958/1959) Ein Dreifarbensatz für dreikreisfreie Netze auf der Kugel. // Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe, **8**, 109–119.

[2] B. Grünbaum (1963). Grötzsch's theorem on 3-coloring. // Michigan Math. J., **10**, 303–310.

[3] В. А. Аксенов (1974). О продолжении 3-раскраски планарных графов. // Дискретный анализ, **26**, 3–19.

[4] O.V. Borodin (1997). A new proof of Grünbaum's 3-color theorem. // Discrete Math., **169**, 177–183.

*630090, Новосибирск, Новосибирский государственный университет, ул. Пирогова 4

**630090, Новосибирск, Институт математики им. С.Л. Соболева СО РАН, пр. Академика Коптюга 4, e-mail: brdnoleg@math.nsc.ru

О МАТРИЦАХ С ПОПАРНО РАЗЛИЧНЫМИ СТРОКАМИ И СТОЛБЦАМИ

М. А. Алексеев*

Пусть ${\mathbb{Z}_p}^{n\times m}$ — множество всех матриц размера $n \times m$ над кольцом $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. В статье рассматривается те матрицы из ${\mathbb{Z}_p}^{n\times m}$, у которых все столбцы и все строки попарно различны. Благодаря установленной связи со связными графами, получена явная формула общего числа таких матриц. Найденные комбинаторные характеристики связных графов могут представлять самостоятельный интерес.

Пусть ${\mathbb{Z}_p}^{n\times m}$ — множество всех матриц размера $n \times m$ над кольцом $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$. В данной статье рассматривается задача о нахождении числа $M(p; n, m)$ — тех матриц из ${\mathbb{Z}_p}^{n\times m}$, у которых все столбцы и все строки попарно различны.

Определение 1. [1] *Коэффициентным оператором* $[x^s]$ *называется отображение, определенное на множестве (формальных) степенных рядов по формуле*

$$[x^s] \sum_i a_i x^i \stackrel{\text{def}}{=} a_s .$$

Аналогичным образом коэффициентные операторы определяются на формальных степенных рядах нескольких переменных.

Для дальнейшего нам понадобятся производящие функции

$$G_n(x) = \sum_{k=0}^{\infty} g(n,k)x^k,$$

где $g(n,k)$ — число связных графов с n помеченными вершинами и k ребрами.

Определение 2. *Пусть* Γ *— граф с* n *вершинами, у которого компонентами связности являются* γ_1 *одновершинных графов,* γ_2 *— двувершинных, ...,* γ_n *— n-вершинных. Тогда набор чисел* $(\gamma_1, \gamma_2, \ldots, \gamma_n)$*, который удовлетворяет равенству* $\gamma_1 + 2\gamma_2 + \ldots + n\gamma_n = n$*, будем называть* характеристикой (связности) *графа* Γ*.*

Непосредственно из определения следует

Лемма 1. *Число графов с* n *вершинами и* s *ребрами, имеющих характеристику* $(s_1, s_2, \ldots, s_n)$*, равно*

$$[x^s]\ \frac{n!}{1!^{s_1}s_1!2!^{s_2}s_2!\ldots n!^{s_n}s_n!}G_1(x)^{s_1}G_2(x)^{s_2}\ldots G_n(x)^{s_n} \qquad (1)$$
$$= [x^s]\ n!\prod_{t=1}^{n}\left(\frac{G_t(x)}{t!}\right)^{s_t}\frac{1}{s_t!}.$$

Особый интерес для нас будет представлять число $G_n(-1)$, равное разности между количествами связных n-вершинных графов с четным и нечетным числом ребер.

Лемма 2. $G_n(-1) = (-1)^{n-1}(n-1)!$.

Доказательство. Найдем число векторов из $\mathbb{Z}_p^n$, у каждого из которых все координаты попарно различны. Нетрудно понять, что оно равно числу размещений $p^{\underline{n}} = \frac{p!}{(p-n)!}$. С другой стороны, попытаемся вычислить его же, используя принцип включения–исключения.

Пусть $B = \{(i,j) \mid 1 \le i < j \le n\}$ — множество свойств, которыми могут обладать или не обладать векторы из $\mathbb{Z}_p^n$. Здесь под свойством (i,j) понимается тот факт, что у вектора i-я и j-я координаты равны. Понятно, что все координаты у вектора различные

тогда и только тогда, когда этот вектор не обладает ни одним из свойств из множества B. По формуле включения–исключения число векторов, не обладающих ни одним из свойств из B, равно

$$\sum_{S\subset B}(-1)^{|S|}f_{\geq}(S), \tag{2}$$

где $f_{\geq}(S)$ равно количеству векторов, обладающих всеми свойствами из S.

Пусть S произвольное подмножество свойств мощности $|S|=s$. Поставим ему в соответствие граф $\Gamma(S)$ с n помеченными вершинами и s ребрами, у которого i-я вершина соединена ребром с j-ой $(i<j)$ тогда и только тогда, когда $(i,j)\in S$.

Пусть $\Gamma(S)$ имеет характеристику $(s_1,s_2,\ldots,s_n)$. Понятно, что вектор удовлетворяет всем свойствам из S тогда и только тогда, когда его координаты на каждой из компонент связности $\Gamma(S)$ одинаковы. Поэтому

$$f_{\geq}(S)=p^{s_1+s_2+\ldots+s_n}.$$

Теперь, используя (1), формулу (2) можно переписать в виде

$$\sum_{s=0}^{\infty}(-1)^s\ \ [x^s]\ F_n(x), \tag{3}$$

где

$$F_n(x)\stackrel{\text{def}}{=}n!\sum_{s_1+2s_2+\ldots+ns_n=n}\prod_{t=1}^{n}\left(\frac{G_t(x)p}{t!}\right)^{s_t}\frac{1}{s_t!}.$$

Следуя [2], получаем, что выражение (3) равно $F_n(-1)$. Сравнивая результаты двух способов подсчета, заключаем, что

$$F_n(-1)=p^{\underline{n}}=\binom{p}{n}n!. \tag{4}$$

Рассмотрим экспоненциальную производящую функцию для $F_n(x)$

$$\tilde{F}(x,y)\stackrel{\text{def}}{=}\sum_{n=0}^{\infty}F_n(x)\tfrac{y^n}{n!}=\sum_{n=0}^{\infty}y^n\sum_{s_1+2s_2+\ldots+ns_n=n}\prod_{t=1}^{n}\left(\tfrac{G_t(x)p}{t!}\right)^{s_t}\tfrac{1}{s_t!}=$$
$$=\sum_{n=0}^{\infty}\sum_{s_1+2s_2+\ldots+ns_n=n}\prod_{t=1}^{n}\left(\tfrac{G_t(x)py^t}{t!}\right)^{s_t}\tfrac{1}{s_t!}=\prod_{t=1}^{\infty}\sum_{i=0}^{\infty}\left(\tfrac{G_t(x)py^t}{t!}\right)^{i}\tfrac{1}{i!}=$$
$$=\prod_{t=1}^{\infty}\exp\left(\tfrac{G_t(x)py^t}{t!}\right)=\exp\left(p\sum_{t=1}^{\infty}\tfrac{G_t(x)y^t}{t!}\right),$$

откуда

$$\sum_{t=1}^{\infty} \frac{G_t(x)\,y^t}{t!} = \frac{1}{p} \ln \tilde{F}(x,y). \tag{5}$$

Рассмотрим полученное тождество при $x = -1$. Благодаря (4), значение $\tilde{F}(-1,y)$ легко вычислить

$$\tilde{F}(-1,y) = \sum_{n=0}^{\infty} F_n(-1)\frac{y^n}{n!} = \sum_{n=0}^{\infty} p^{\underline{n}}\frac{y^n}{n!} = \sum_{n=0}^{\infty} \binom{p}{n} y^n = (1+y)^p.$$

Поэтому подстановка $x = -1$ в (5) дает

$$\sum_{t=1}^{\infty} \frac{G_t(-1)y^t}{t!} = \frac{1}{p} \ln \tilde{F}(-1,y) = \frac{1}{p} \ln(1+y)^p = \ln(1+y) = \sum_{t=1}^{\infty} \frac{(-1)^{t-1}y^t}{t}.$$

Откуда немедленно следует, что $G_t(-1) = (-1)^{t-1}(t-1)!$.

Определение 3. *Числами Стирлинга 1-го рода со знаком* $\left[{n \atop i}\right]$ *называются коэффициенты разложения* $x^{\underline{n}}$ *по степеням* x*:*

$$x^{\underline{n}} = \sum_{i=0}^{n} \left[{n \atop i}\right] x^i. \tag{6}$$

Замечание 1. [3] *Справедлива явная формула*

$$\left[{n \atop i}\right] = (-1)^{n-i} \sum_{\substack{s_1+s_2+\ldots+s_n=i \\ s_1+2s_2+\ldots+ns_n=n}} \frac{n!}{1^{s_1}s_1!2^{s_2}s_2!\ldots n^{s_n}s_n!}. \tag{7}$$

Теорема 1.

$$M(p;n,m) = \sum_{i=0}^{n}\sum_{j=0}^{m} \left[{n \atop i}\right]\left[{m \atop j}\right] p^{ij}. \tag{8}$$

Доказательство. Аналогично доказательству леммы рассмотрим два множества свойств

$$B = \{(i,j) \mid 1 \le i < j \le n\} \quad \text{и} \quad C = \{(k,l) \mid 1 \le k < l \le m\},$$

которыми могут обладать или не обладать матрицы из ${\mathbb{Z}_p}^{n\times m}$. Здесь свойство $(i,j)\in B$ означает равенство i-ой и j-ой строк, а свойство $(k,l)\in C$ — равенство k-ого и l-ого столбцов. Каждая матрица с попарно различными строками и столбцами не обладает ни одним из этих свойств и наоборот. По формуле включения–исключения число матриц, не обладающих ни одним из этих свойств, равно

$$\sum_{S\subset B, T\subset C}(-1)^{|S\cup T|}f_{\geq}(S\cup T). \tag{9}$$

Рассмотрим произвольные подмножества $S\subset B$ и $T\subset C$. Пусть $|S|=s,\ |T|=t$, а графы $\Gamma(S)$ и $\Gamma(T)$ имеют соответственно характеристики $(s_1,s_2,\ldots,s_n)$ и $(t_1,t_2,\ldots,t_m)$. Тогда нетрудно понять, что

$$f_{\geq}(S\cup T)=p^{(s_1+s_2+\ldots+s_n)(t_1+t_2+\ldots+t_m)}.$$

В полной аналогии с доказательством леммы формулу (9) можно переписать в виде

$$\begin{aligned}
&\sum\nolimits_{s=0}^{\infty}\sum_{t=0}^{\infty}(-1)^{s+t}\ [x^s y^t]n!m!\sum_{\substack{s_1+\ldots+ns_n=n\\ t_1+\ldots+mt_m=m}}\sum p^{(s_1+\ldots+s_n)(t_1+\ldots+t_m)}\\
&\quad\prod_{i=1}^{n}\left(\frac{G_i(x)}{i!}\right)^{s_i}\frac{1}{s_i!}\prod_{j=1}^{m}\left(\frac{G_j(y)}{j!}\right)^{t_j}\frac{1}{t_j!}\\
&=n!m!\sum_{\substack{s_1+\ldots+ns_n=n\\ t_1+\ldots+mt_m=m}}\sum p^{(s_1+\ldots+s_n)(t_1+\ldots+t_m)}\\
&\quad\prod_{i=1}^{n}\left(\frac{G_i(-1)}{i!}\right)^{s_i}\frac{1}{s_i!}\prod_{j=1}^{m}\left(\frac{G_j(-1)}{j!}\right)^{t_j}\frac{1}{t_j!}\\
&=n!m!\sum_{\substack{s_1+\ldots+ns_n=n\\ t_1+\ldots+mt_m=m}}\sum p^{(s_1+\ldots+s_n)(t_1+\ldots+t_m)}\prod_{i=1}^{n}\left(\frac{(-1)^{i-1}}{i}\right)^{s_i}\frac{1}{s_i!}\\
&\quad\prod_{j=1}^{m}\left(\frac{(-1)^{j-1}}{j}\right)^{t_j}\frac{1}{t_j!}\\
&=\sum_{\substack{s_1+\ldots+ns_n=n\\ t_1+\ldots+mt_m=m}}\sum\frac{n!\ (-1)^{n-s_1-\ldots-s_n}}{1^{s_1}s_1!2^{s_2}s_2!\ldots n^{s_n}s_n!}\frac{m!\ (-1)^{m-t_1-\ldots-t_m}}{1^{t_1}t_1!2^{t_2}t_2!\ldots m^{t_m}t_m!}
\end{aligned}$$

$$\cdot\, p^{(s_1+\ldots+s_n)(t_1+\ldots+t_m)}.$$

Теперь, вводя обозначения $i = s_1 + s_2 + \ldots + s_n$ и $j = t_1 + t_2 + \ldots + t_m$ и используя (7), получаем утверждение теоремы.

Следствие 1. *Учитывая* (6), *формулу* (8) *можно преобразовать*

$$M(p;n,m) = \sum_{i=0}^{n}\sum_{j=0}^{m} \begin{bmatrix} n \\ i \end{bmatrix} \begin{bmatrix} m \\ j \end{bmatrix} p^{ij} = \sum_{i=0}^{n} \begin{bmatrix} n \\ i \end{bmatrix} (p^i)_{\underline{m}} = \sum_{j=0}^{m} \begin{bmatrix} m \\ j \end{bmatrix} (p^j)_{\underline{n}}, \tag{10}$$

откуда, в частности, следует, что $M(p;n,m) = 0$ *при* $n > p^m$ *или* $m > p^n$.

Формула (10) позволяет существенно сократить вычислительные затраты.

Теорема 2. *При наличии достаточного объема памяти для вычисления* $M(p;n,m)$ *по формуле* (10) *требуется* $O(nm)$ *операций.*

В заключение приведем два утверждения без доказательства.

Теорема 3. *Обозначим через* $M_0(p;n,m)$ *число матриц размера* $n \times m$ *с попарно различными ненулевыми строками и столбцами. Тогда справедливо рекуррентное соотношение* $(n,m > 1)$

$$\begin{aligned} M_0(p;n,m) = M(p;n,m) &- nM_0(p;n-1,m) - \\ &- mM_0(p;n,m-1) + nmM_0(p;n-1,m-1) \end{aligned}$$

с начальными условиями

$$\begin{gathered} M_0(p;0,0) = 1; \\ M_0(p;n,0) = M_0(p;0,m) = 0 \text{ при } n,m > 0. \end{gathered}$$

Теорема 4. *Число* d*-мерных матриц с элементами из* $\mathbb{Z}_p$ *размера* $n_1 \times n_2 \times \ldots \times n_d$, *у которых все* $(d-1)$*-мерные "срезы", получаемые фиксированием одной из координат, различны, равно*

$$M(p;n_1,n_2,\ldots,n_d) = \sum_{i_1=0}^{n_1}\sum_{i_2=0}^{n_2}\cdots\sum_{i_d=0}^{n_d} \begin{bmatrix} n_1 \\ i_1 \end{bmatrix} \begin{bmatrix} n_2 \\ i_2 \end{bmatrix} \cdots \begin{bmatrix} n_d \\ i_d \end{bmatrix} p^{i_1 i_2 \ldots i_d}.$$

ЛИТЕРАТУРА

[1] Гульден Я., Джексон Д. Перечислительная комбинаторика: Пер. с англ. М.: Наука, 1990.

[2] Егорычев Г. П. Интегральное представление и вычисление комбинаторных сумм. Наука, 1977.

[3] Стенли Р. Перечислительная комбинаторика: Пер. с англ. М.: Мир, 1990.

*Нижегородский государственный университет им. Н. И. Лобачевского

ВЕРХНИЕ ОЦЕНКИ НЕНАДЕЖНОСТИ СХЕМ В БАЗИСАХ ИЗ ДВУХВХОДОВЫХ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ ПРИ ОДНОТИПНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина*

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в базисах из двухвходовых функциональных элементов [1]. Схема реализует функцию $f(x_1, \ldots, x_n)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, \ldots, a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$. Все элементы схемы независимо друг от друга с вероятностью γ ($\gamma < 1/2$) подвержены однотипным константным неисправностям на выходах элементов. Неисправности типа 0 на выходах элементов характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию, а в неисправном — константу 0. Аналогично определяются неисправности типа 1 на выходах функциональных элементов.

Пусть $P_{\overline{f}(\tilde{a})}(S, \tilde{a})$ – вероятность появления значения $\overline{f}(\tilde{a})$ на выходе схемы S, реализующей $f(\tilde{x})$, при входном наборе $\tilde{a}$. Ненадежность P(S) схемы S определяется как максимальное из различных чисел $P_{\overline{f}(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах $\tilde{a}$. Надежность схемы, следовательно, равна $1 - P(S)$.

Построить абсолютно надежную схему ($P(S) \to 0$) при данных неисправностях для произвольной функции невозможно [2]. Возникает вопрос, какой максимальной надежности можно добиться при

использовании ненадежных элементов, подверженных однотипным константным неисправностям на выходах? Ответ на него зависит от базиса и типа неисправностей.

Известно, что произвольный базис в пространстве булевых функций, содержащий функции двух переменных, отличный от приведенных ниже базисов, получается добавлением одной или нескольких функций к некоторому базису из списка [3].

$B_1 = \{/\}, B_2 = \{\downarrow\}, B_3 = \{\not\to, \sim\}, B_4 = \{\not\leftarrow, \sim\}, B_5 = \{\not\to, \bar{}\},$
$B_6 = \{\not\leftarrow, \bar{}\}, B_7 = \{\to, \not\to\}, B_8 = \{\leftarrow, \not\leftarrow\}, B_9 = \{\&, \bar{}\}, B_{10} = \{\sim, \&, \oplus\},$
$B_{11} = \{\not\leftarrow, 1\}, B_{12} = \{\oplus, \&, 1\}, B_{13} = \{\sim, \&, 0\}, B_{14} = \{\not\to, 1\},$
$B_{15} = \{\to, \bar{}\}, B_{16} = \{\leftarrow, \bar{}\}, B_{17} = \{\to, \oplus\}, B_{18} = \{\leftarrow, \oplus\},$
$B_{19} = \{\vee, \bar{}\}, B_{20} = \{\sim, \vee, \oplus\}, B_{21} = \{\to, 0\}, B_{22} = \{\sim, \vee, 0\},$
$B_{23} = \{\leftarrow, 0\}, B_{24} = \{\leftarrow, \not\to\}, B_{25} = \{\to, \not\leftarrow\}, B_{26} = \{\oplus, \vee, 1\}.$

Используемые при перечислении базисов обозначения функций приведены ниже:

$x/y = \bar{x} \vee \bar{y}$, $x \downarrow y = \bar{x}\&\bar{y}$,
$x \sim y = x\&y \vee \bar{x}\&\bar{y}$, $x \oplus y = x\&\bar{y} \vee \bar{x}\&y$,
$x \to y = \bar{x} \vee y$, $x \leftarrow y = x \vee \bar{y}$,
$x \not\to y = x\&\bar{y}$, $x \not\leftarrow y = \bar{x}\&y$.

В работе [4] показано, что утверждение, доказанное для функции в некотором базисе при неисправностях типа 0 (1), справедливо для двойственной функции в двойственном базисе при неисправностях типа 1 (0). Поэтому далее будем предполагать, что базисные элементы подвержены неисправностям типа 0 на выходах.

1. Для базиса $B_1 = \{x/y\}$ в [4] показано, что:

1) любую функцию можно реализовать схемой S такой, что при $\gamma \leq 1/50$ верно $P(S) \leq 2\gamma + 8\gamma^2 + 157\gamma^3$;

2) для любой функции $f(x_1, \ldots, x_n)$, не равной константе, не представимой в виде $f(\tilde{x}) = \bar{x_k} \vee g(\tilde{x}), k \in \{1, \ldots, n\}$, для реализации которой требуется не менее трех функциональных элементов, и любой схемы S, ее реализующей, при $\gamma \leq 1/3$ верно $P(S) \geq 2\gamma - 3\gamma^2 + \gamma^3$.

Таким образом, при $\gamma \to 0$ почти все функции можно реализовать схемами, ненадежность которых асимптотически равна 2γ. С точки зрения надежности функционирования эти схемы будут асимптотически наилучшими.

2. Для $B_2 = \{x \downarrow y\}$ в [4] показано, что:

1) любую функцию можно реализовать схемой S такой, что при $\gamma \le 1/50$ верно $P(S) \le \gamma + 2\gamma^2 + 35\gamma^3$;

2) для любой функции f, не равной константе, и любой схемы S, ее реализующей, при $\gamma \le 1/2$ верно $P(S) \ge \gamma$.

Таким образом, при $\gamma \to 0$ все функции, кроме константы 0, можно реализовать схемами, ненадежность которых асимптотически равна γ. С точки зрения надежности функционирования эти схемы будут асимптотически наилучшими.

3. В базисе $B_3 = \{\not\to, \sim\}$ построим схему A, реализующую $x \downarrow y$, моделируя формулу $(x \sim y) \not\to y$. Вычислим вероятности ошибок для схемы A:

$P_0 = 2\gamma - \gamma^2$ при входном наборе (00),

$P_1 = 0$ при входных наборах (01), (10), (11).

Схема A имеет тот же набор вероятностей ошибок, что и функциональный элемент $x \downarrow y$, переходящий в неисправное состояние с вероятностью $2\gamma - \gamma^2$. Поэтому применимо утверждение 1) п.2, согласно которому при $\gamma \le 1/100$ любую функцию можно реализовать схемой S, для которой верно $P(S) \le 2\gamma + 7\gamma^2 + 268\gamma^3$.

4. В базисе $B_4 = \{\not\leftarrow, \sim\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $(x \not\leftarrow (x \sim y)$. Вероятности ошибок на выходе этой схемы такие же, как у схемы A. Поэтому, повторяя рассуждения п.3, получаем, что при $\gamma \le 1/100$ любую функцию можно реализовать схемой S, для которой верно $P(S) \le 2\gamma + 7\gamma^2 + 268\gamma^3$.

5. В базисе $B_5 = \{\not\to, \bar{}\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $\bar{x} \not\to y$. Вероятности ошибок для нее те же, что для схемы A, поэтому при $\gamma \le 1/100$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \le 2\gamma + 7\gamma^2 + 268\gamma^3$.

6. В базисе $B_6 = \{\not\leftarrow, \bar{}\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $x \not\leftarrow \bar{y}$. Вероятности ошибок для нее те же, что для схемы A, поэтому при $\gamma \le 1/100$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \le 2\gamma + 7\gamma^2 + 268\gamma^3$.

7. В базисе $B_7 = \{\to, \not\to\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $(x \to (x \not\to x)) \not\to y$. Вероятности ошибок для нее те же, что для схемы A, поэтому при $\gamma \le 1/100$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \le 2\gamma + 7\gamma^2 + 268\gamma^3$.

8. В базисе $B_8 = \{\leftarrow, \not\leftarrow\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $x \not\leftarrow ((x \not\leftarrow x) \leftarrow y)$. Вероятности ошибок для

нее те же, что для схемы A, поэтому при $\gamma \leq 1/100$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 2\gamma + 7\gamma^2 + 268\gamma^3$.

9. В базисе $B_9 = \{\&, \bar{}\}$

1) построим схему B, реализующую $x \downarrow y$, моделируя формулу $\bar{x}\&\bar{y}$. Вычислим вероятности ошибок для схемы B:

$P_0 = 3\gamma - 3\gamma^2 + \gamma^3$ при входном наборе (00),

$P_1 = 0$ при входных наборах (01), (10), (11).

Схема B имеет тот же набор вероятностей ошибок, что и функциональный элемент $x \downarrow y$, переходящий в неисправное состояние с вероятностью $3\gamma - 3\gamma^2 + \gamma^3$. Поэтому применимо утверждение 1) п.2, согласно которому при $\gamma \leq 1/150$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 3\gamma + 15\gamma^2 + 910\gamma^3$.

2) В работе [4] показано, что если схема S реализует функцию $f(x_1, \ldots, x_n)$, не представимую ни в одном из видов $f(\tilde{x}) = x_k \& g(\tilde{x})$ или $f(\tilde{x}) = x_m \& \bar{h}(\tilde{x}), k, m \in \{1, \ldots, n\}$, и при $\gamma \leq 1/150$ верно $P(S) \leq 3\gamma + 15\gamma^2 + 910\gamma^3$, то $P(S) \geq (3\gamma - 3\gamma^2 + \gamma^3)(1-\gamma)^2$.

Таким образом, при $\gamma \to 0$ почти все функции можно реализовать схемами, ненадежность которых асимптотически равна 3γ. С точки зрения надежности функционирования эти схемы будут асимптотически наилучшими.

10. В базисе $B_{10} = \{\sim, \&, \oplus\}$ построим схему из четырех функциональных элементов, реализующую $x \downarrow y$, моделируя формулу $(x \sim (x \oplus x))\&(y \sim (x \oplus x))$.

Построенная схема имеет тот же набор вероятностей ошибок, что и схема B, реализующая $x \downarrow y$. Поэтому при $\gamma \leq 1/150$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 3\gamma + 15\gamma^2 + 910\gamma^3$.

11. В базисе $B_{11} = \{\not\leftarrow, 1\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $x \not\leftarrow (y \not\leftarrow 1)$.

Построенная схема имеет тот же набор вероятностей ошибок, что и схема B, реализующая $x \downarrow y$. Поэтому при $\gamma \leq 1/150$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 3\gamma + 15\gamma^2 + 910\gamma^3$.

12. В базисе $B_{12} = \{\oplus, \&, 1\}$ построим схему из 5 функциональных элементов, реализующую $x \downarrow y$, моделируя формулу $(x \oplus 1)\&(1\&(y \oplus 1))$. Вычислим вероятности ошибок для построенной схемы:

$P_0 = 5\gamma - 10\gamma^2 + 10\gamma^3 - 5\gamma^4 + \gamma^5$ при входном наборе (00),
$P_1 = 0$ при входных наборах (01), (10), (11).

Эта схема имеет тот же набор вероятностей ошибок, что и функциональный элемент $x \downarrow y$, переходящий в неисправное состояние с вероятностью $5\gamma - 10\gamma^2 + 10\gamma^3 - 5\gamma^4 + \gamma^5$. Поэтому применимо утверждение 1) п.2, согласно которому при $\gamma \leq 1/250$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 5\gamma + 40\gamma^2 + 4185\gamma^3 \leq 5\gamma + 57\gamma^2$.

13. В базисе $B_{13} = \{\sim, \&, 0\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $(x \sim 0)\&(y \sim 0)$.

Построенная схема имеет тот же набор вероятностей ошибок, что и схема B, реализующая $x \downarrow y$. Поэтому при $\gamma \leq 1/150$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 3\gamma + 15\gamma^2 + 910\gamma^3$.

14. В базисе $B_{14} = \{\not\to, 1\}$ построим схему, реализующую $x \downarrow y$, моделируя формулу $(1 \not\to x) \not\to y$.

Построенная схема имеет тот же набор вероятностей ошибок, что и схема B, реализующая $x \downarrow y$. Поэтому при $\gamma \leq 1/150$ любую функцию можно реализовать схемой S, ненадежность которой $P(S) \leq 3\gamma + 15\gamma^2 + 910\gamma^3$.

Прежде чем рассмотреть остальные базисы, докажем несколько вспомогательных утверждений.

Пусть схема C реализует функцию x/y и имеет вероятности ошибок $P_0(C,(00)) = \alpha, P_0(C,(01)) = \beta, P_0(C,(10)) = \delta, P_1(C,(11)) = 0$. Обозначим $P(C) = \mu$.

Пусть схема S реализует функцию f с ненадежностью $P(S)$. Возьмем четыре экземпляра схемы S, соединим их выходы со входами двух схем C, а выходы полученной схемы снова соединим со входами 3-го экземпляра схемы C. Обозначим построенную схему S^*.

Лемма 1. *Если* $18\mu^2 \leq \alpha$, *то* $P(S^*) \leq 2\alpha + 2(\beta+\delta)P(S) + 2(P(S))^2$.

Для доказательства достаточно вычислить и оценить сверху вероятности ошибок на выходе схемы S^*.

Лемма 2. *Если* $\mu \leq 1/70$, *то любую функцию можно реализовать схемой* S, *ненадежность которой* $P(S) \leq 3\mu$.

Доказательство такое же как в [4].

Из лемм 1 и 2 следует

Теорема 1. *Если* $\mu \le 1/70$, $18\mu^2 \le \alpha$, *схема* S *реализует функцию* f *с ненадежностью* $P(S) \le 3\mu$, *то* $P(S^*) \le 2\alpha + 6(\beta+\delta)\mu + 18(\mu)^2$.

15.В базисе $B_{15} = \{\to, \bar{}\}$ построим схему С, реализующую x/y, моделируя формулу $x \to \bar{y}$. Вычислим вероятности ошибок для схемы С:

$P_0(C,(00)) = \gamma, P_0(C,(01)) = \gamma,$

$P_0(C,(10)) = 2\gamma - \gamma^2, P_1(C,(11)) = 0.$

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема С удовлетворяет условиям теоремы 1 ($\alpha = \gamma, \beta = \gamma, \delta = 2\gamma - \gamma^2, \mu = 2\gamma - \gamma^2$.) Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 108\gamma^2$.

16. В базисе $B_{16} = \{\leftarrow, \bar{}\}$ построим схему С, реализующую x/y, моделируя формулу $\bar{x} \leftarrow y$. Вычислим вероятности ошибок для схемы С:

$P_0(C,(00)) = \gamma, P_0(C,(01)) = 2\gamma - \gamma^2,$

$P_0(C,(10)) = \gamma, P_1(C,(11)) = 0.$

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема С удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 108\gamma^2$.

17. В базисе $B_{17} = \{\to, \oplus\}$ построим схему С, реализующую x/y, моделируя формулу $x \to (y \to (y \oplus y))$. Вычислим вероятности ошибок для схемы С:

$P_0(C,(00)) = \gamma, P_0(C,(01)) = \gamma,$

$P_0(C,(10)) = 2\gamma - \gamma^2, P_1(C,(11)) = 0.$

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема С удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 108\gamma^2$.

18. В базисе $B_{18} = \{\leftarrow, \oplus\}$ построим схему С, реализующую x/y, моделируя формулу $((x \oplus x) \leftarrow x) \leftarrow y$. Вычислим вероятности ошибок для схемы С:

$P_0(C,(00)) = \gamma, P_0(C,(01)) = 2\gamma - \gamma^2,$

$P_0(C,(10)) = \gamma, P_1(C,(11)) = 0.$

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема С удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 108\gamma^2$.

19. В базисе $B_{19} = \{\vee, \bar{}\}$ построим схему С, реализующую x/y, моделируя формулу $\bar{x} \vee \bar{y}$. Вычислим вероятности ошибок для схемы С:

$P_0(C,(00)) = \gamma + \gamma^2 - \gamma^3$, $P_0(C,(01)) = 2\gamma - \gamma^2$,
$P_0(C,(10)) = 2\gamma - \gamma^2$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 122\gamma^2 - 2\gamma^3$.

20. В базисе $B_{20} = \{\sim, \vee, \oplus\}$ построим схему C из 4 элементов, реализующую x/y, моделируя формулу $(x \sim (x \oplus x)) \vee (y \sim (x \oplus x))$. Вычислим вероятности ошибок для схемы C:
$P_0(C,(00)) = \gamma + \gamma^2 - \gamma^3$, $P_0(C,(01)) = 2\gamma - \gamma^2$,
$P_0(C,(10)) = 2\gamma - \gamma^2$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 122\gamma^2 - 2\gamma^3$.

21. В базисе $B_{21} = \{\to, 0\}$ построим схему C из 3 элементов, реализующую x/y, моделируя формулу $x \to (y \to 0)$. Вычислим вероятности ошибок для схемы C:
$P_0(C,(00)) = \gamma + \gamma^2 - \gamma^3$, $P_0(C,(01)) = \gamma$,
$P_0(C,(10)) = 2\gamma - \gamma^2$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 110\gamma^2 - 2\gamma^3$.

22. В базисе $B_{22} = \{\sim, \vee, 0\}$ построим схему C, реализующую x/y, моделируя формулу $(x \sim 0) \vee (y \sim 0)$. Вычислим вероятности ошибок для схемы C:
$P_0(C,(00)) = \gamma + \gamma^2 - \gamma^3$, $P_0(C,(01)) = 2\gamma - \gamma^2$,
$P_0(C,(10)) = 2\gamma - \gamma^2$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 122\gamma^2 - 2\gamma^3$.

23. В базисе $B_{23} = \{\leftarrow, 0\}$ построим схему C, реализующую x/y, моделируя формулу $(0 \leftarrow x) \leftarrow y$. Вычислим вероятности ошибок для схемы C:
$P_0(C,(00)) = \gamma + \gamma^2 - \gamma^3$, $P_0(C,(01)) = 2\gamma - \gamma^2$,
$P_0(C,(10)) = \gamma$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 110\gamma^2 - 2\gamma^3$.

24. В базисе $B_{24} = \{\leftarrow, \not\rightarrow\}$ построим схему C, реализующую x/y, моделируя формулу $((x \not\rightarrow x) \leftarrow x) \leftarrow y$. Вычислим вероятности ошибок для схемы C:

$P_0(C,(00)) = \gamma$, $P_0(C,(01)) = 2\gamma - \gamma^2$,

$P_0(C,(10)) = \gamma$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 108\gamma^2$.

25. В базисе $B_{25} = \{\rightarrow, \not\leftarrow\}$ построим схему C, реализующую x/y, моделируя формулу $x \rightarrow (y \rightarrow (y \not\leftarrow y))$. Вычислим вероятности ошибок для схемы C:

$P_0(C,(00)) = \gamma$, $P_0(C,(01)) = \gamma$,

$P_0(C,(10)) = 2\gamma - \gamma^2$, $P_1(C,(11)) = 0$.

При $\gamma \le 1/140$ условие $18\mu^2 \le \alpha$ выполняется, схема C удовлетворяет условиям теоремы 1. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \le 2\gamma + 108\gamma^2$.

26. В базисе $B_{26} = \{\oplus, \vee, 1\}$ построим схему E из 4 элементов, реализующую x/y, моделируя формулу $(x \oplus 1) \vee (y \oplus 1)$. Вычислим вероятности ошибок для схемы E:

$P_0(E,(00)) = 2\gamma - 2\gamma^3 + \gamma^4$, $P_0(E,(01)) = 2\gamma - \gamma^2$,

$P_0(E,(10)) = 2\gamma - \gamma^2$, $P_1(E,(11)) = \gamma - \gamma^2 - \gamma^3 + \gamma^4$.

Лемма 3. *Пусть схема E реализует x/y с вероятностями ошибок $P_0(C,(00)) = \alpha, P_0(C,(01)) = \beta, P_0(C,(10)) = \delta, P_1(C,(11)) = \tau$. Схема S реализует булеву функцию f, схема S^* построена по схеме S как в лемме 1 с заменой C на E. Тогда $P(S^*) \le \max\{2\alpha + \tau + 2(\beta + \delta)P(S) + 2(P(S))^2, \alpha + (\beta + \delta)(\tau + P(S)) + (\tau + 2P(S))^2\}$.*

Для доказательства достаточно вычислить вероятности ошибок на выходе схемы S^*.

Лемма 4. *Если $\mu \le 1/240$, то любую функцию можно реализовать схемой S, ненадежность которой $P(S) \le 6\mu$.*

Доказательство такое же как в [4].

Из лемм 3 и 4 следует

Теорема 2. *Если $\mu \le 1/240$, $18\mu^2 \le \alpha + \tau(1 - \beta - \delta - \tau - 12\mu)$, схема S реализует функцию f с ненадежностью $P(S) \le 6\mu$, то схема S^* реализует f, причем $P(S^*) \le 2\alpha + \tau + 12(\beta + \delta)\mu + 72(\mu)^2$.*

При $\gamma \leq 1/480$ условие $18\mu^2 \leq \alpha+\tau(1-\beta-\delta-\tau-12\mu)$ выполняется, схема E удовлетворяет условиям теоремы 2. Следовательно, любую функцию можно реализовать схемой D с ненадежностью $P(D) \leq 5\gamma + 384\gamma^2$.

Итак, в каждом из 26 базисов из двухвходовых функциональных элементов при однотипных константных неисправностях можно построить схему, реализующую произвольную булеву функцию с максимальной вероятностью ошибки на выходе сравнимой с ненадежностью одного функционального элемента.

В заключение автор благодарит профессора МГУ им.М.В. Ломоносова Н.П.Редькина за постановку задачи и внимание к работе. Работа выполнена при поддержке Российского фонда фундаментальных исследований, номер проекта 98-01-00049

ЛИТЕРАТУРА

[1] Лупанов О. Б. Асимптотические оценки сложности управляющих систем. М.: Изд-во МГУ, 1984.

[2] Тарасов В. В. К синтезу надежных схем из ненадежных элементов. Матем. заметки, 1976, т.20, № 3, С.391-400.

[3] Горбатов В. А. Основы высшей математики. М.: Высшая школа, 1986.

[4] Алехина М. А. О надежности схем из ненадежных функциональных элементов при однотипных константных неисправностях на выходах элементов. //Дискретная математика, 1993, т.5, вып.2, с.59-74.

* Пензенский государственный университет

ОПРЕДЕЛЕНИЕ ВСЕХ БЕЗГРАНИЧНО ДЕЛИМЫХ МЕР НА РЕШЕТКАХ

Л. Б. Бейненсон*

1. Пример. Пусть U — некоторое конечное или счетное множество, $L = 2^U$ — множество всех подмножеств множества U.

Обозначим $\mathcal{P}$ семейство неотрицательных действительных функций F на L, обладающих следующим свойством:

для любых конечных подмножеств A и B множества U, удовлетворяющих включению $A \subset B$, выполняется неравенство

$$\sum_{A \subset C \subset B} (-1)^{|C|-|B|} F(C) \geq 0.$$

Задача состоит в том, чтобы описать все функции F такие, что для любого положительного числа t функция F^t будет принадлежать семейству функций $\mathcal{P}$, т. е. выяснить, при каких условиях на функцию F для любого положительного числа t и для любых конечных подмножеств A и B множества U, удовлетворяющих включению $A \subset B$, выполняется неравенство

$$\sum_{A \subset C \subset B} (-1)^{|C|-|B|} F^t(C) \geq 0.$$

Справедливо следующее утверждение:

функция F^t будет принадлежать семейству функций $\mathcal{P}$ для любого положительного числа t в том и только в том случае, когда выполняются следующие два условия:

1) для любых подмножеств A и B множества U если $F(A) \neq 0$ и $F(B) \neq 0$, то

$$F(A \cap B) \neq 0;$$

2) существует такая функция G из $\mathcal{P}$, что для любого подмножества A множества U, если $F(A) \neq 0$, то

$$F(A) = F(U) e^{G(A)-G(U)}.$$

В докладе дается обобщение этого утверждения.

2. Некоторые определения. Частично упорядоченным множеством (ЧУМ) называется множество, на котором введено бинарное отношение порядка $\leq$, удовлетворяющее условиям рефлексивности, антисимметричности и транзитивности.

Подмножество ЧУМ будем называть фильтром, если вместе с каждым элементом в него входят все элементы большие его, и подмножество ЧУМ будем называть идеалом, если вместе с каждым элементом в него входят все элементы меньшие его.

Для любого элемента a из ЧУМ обозначим I_a главный идеал для элемента a, то есть минимальный идеал, содержащий элемент a, и,

аналогично, для любого элемента a из ЧУМ обозначим $\mathcal{F}_a$ главный фильтр для элемента a, то есть минимальный фильтр, содержащий элемент a.

Очевидно, что

$$I_a = \{a' : \ a' \le a\}, \quad \mathcal{F}_a = \{a' : \ a' \ge a\}.$$

Решеткой называется такое частично упорядоченное множество, в котором пересечение двух любых главных идеалов есть главный идеал, а пересечение двух любых главных фильтров есть главный фильтр.

Как следует из этого определения, на решетке можно ввести две бинарные операции $\wedge$ и $\vee$, полагая, что для любых элементов решетки a и b элементы $a \wedge b$ и $a \vee b$ определяются следующими соотношениями:

$$\mathcal{F}_a \cap \mathcal{F}_b = \mathcal{F}_{a \vee b}, \qquad I_a \cap I_b = I_{a \wedge b}.$$

Приведем примеры наиболее часто используемых и простых решеток.

Пусть U — некоторое множество, 2^U — множество всех подмножеств U. Определим на 2^U порядок по отношению включения. Тогда рассмотренное в п.1 частично упорядоченное множество 2^U будет решеткой, при этом операции $\wedge$ и $\vee$ будут совпадать с операциями пересечения и объединения множеств, то есть для любых подмножеств A и B множества U будут выполняться соотношения

$$A \vee B = A \cup B, \qquad A \wedge B = A \cap B.$$

Пусть n — некоторое натуральное число. Тогда на множествах $\mathbf{R}^n$ и $\mathbf{Z}^n$ можем ввести отношение порядка следующим образом: для любых элементов $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$ отношение $a \le b$ выполняется тогда и только тогда, когда $a_i \le b_i$ для всех $i = 1, \ldots n$. Эти частично упорядоченные множества также являются решетками, при этом выполняются следующие соотношения

$$a \vee b = \Big(\max(a_1, b_1), \max(a_2, b_2), \ldots, \max(a_n, b_n)\Big),$$

$$a \wedge b = \Big(\min(a_1, b_1), \min(a_2, b_2), \ldots, \min(a_n, b_n)\Big).$$

3. Формулировка задачи и результатов. Пусть L — некоторая решетка, Σ — сигма-алгебра, порожденная главными идеалами

решетки L, а $\mathcal{M}$ — множество всех вероятностных мер на сигма-алгебре Σ.

Для любой меры μ из $\mathcal{M}$ функцией распределения F_μ меры μ будем называть неотрицательную функцию на L, определенную следующим образом: для любого элемента a из L

$$F_\mu(a) = \mu(I_a).$$

Так как сигма-алгебра Σ порождена главными идеалами решетки L, то функция распределения F_μ однозначно определяет меру μ из $\mathcal{M}$.

Для любого случайного элемента ξ со значениями в L однозначно определим отвечающую ему меру μ из $\mathcal{M}$, полагая для любого множества A из Σ

$$\mu(A) = \mathbf{P}\Big(\xi \in A\Big)$$

(здесь обозначаем $\mathbf{P}(\mathcal{E})$ вероятность события $\mathcal{E}$).

Очевидно, что решеточная операция $\wedge : L \times L \longrightarrow L$ является измеримой относительно сигма-алгебры Σ. Поэтому для любых двух случайных элементов ξ_1 и ξ_2 со значениями в L можно определить случайный элемент ξ на L, полагая $\xi = \xi_1 \wedge \xi_2$. Если при этом случайные элементы ξ_1 и ξ_2 независимы, а μ_1, μ_2 и μ — меры из $\mathcal{M}$, отвечающие случайным элементам ξ_1, ξ_2 и ξ соответственно, то будет выполняться соотношение

$$F_\mu = F_{\mu_1} F_{\mu_2}.$$

Определение: Случайный элемент ξ называется безгранично делимым, если для любого натурального n существуют такие одинаково распределенные случайные независимые элементы $\xi_{1n}, \ldots, \xi_{nn}$, что

$$\xi = \xi_{1n} \wedge \ldots \wedge \xi_{nn}.$$

Соответственно, мера μ из $\mathcal{M}$ называется безгранично делимой в том и только в том случае, когда для любого натурального n функция $F_\mu^{1/n}$ является функцией распределения некоторой меры из $\mathcal{M}$.

В работе [1] построен обширный класс безгранично делимых распределений на дистрибутивных решетках.

Безгранично делимые случайные элементы решетки являются аналогом безгранично делимых случайных величин с вещественными значениями (вещественная случайная величина ξ называется без-

гранично делимой, если для любого натурального n существуют такие одинаково распределенные независимые случайные величины $\xi_{1n}, \ldots, \xi_{nn}$, что $\xi = \xi_{1n} + \ldots + \xi_{nn}$).

Для определения множества всех безгранично делимых случайных величин в теории вероятностей служит теорема Леви-Хинчина.

Приводимая ниже теорема является решеточным аналогом теоремы Леви-Хинчина.

Теорема 1. *Неотрицательная функция F на L является функцией распределения безгранично делимой меры в том и только в том случае, когда*

1) *для любых элементов a и b из L, если $F(a) \neq 0$ и $F(b) \neq 0$, то $F(a \wedge b) \neq 0$;*

2) *существует такая неотрицательная сигма-аддитивная (возможно, неограниченная) мера β на сигма-алгебре Σ, что для любого элемента a из L если, $F(a) \neq 0$, то выполняется соотношение*

$$F(a) = e^{-\beta(L \setminus I_a)}.$$

Для конечных решеток это утверждение было получено в неопубликованной дипломной работе А.А. Бетиным.

В случае, когда решетка L конечна, условие 1 этой теоремы эквивалентно следующему:

1′) существует такой элемент a_0 из L, что неравенство $F(a) \neq 0$ выполняется для тех и только тех элементов a из L, для которых выполняется неравенство $a \geq a_0$.

ЛИТЕРАТУРА

[1] Антонец М.А., Шерешевский И.А. Безгранично делимые распределения вероятностей на решетках. // Алгебра и анализ, т. 5 (1993 г.), вып. 6.

[2] Биркгоф Г. Теория решеток. Пер. с англ. М.: Наука, 1984.

[3] А.Н. Колмогоров, С.В. Фомин. Элементы теории функций и функционального анализа. М: Наука, 1972.

*Нижний Новгород

ОБ ОДНОМ СТРУКТУРНОМ СВОЙСТВЕ ПЛОСКИХ ГРАФОВ

О. В. Бородин*, А. Н. Глебов*

Если в плоском графе ребро инцидентно двум треугольным граням, то оно называется *слабым*, а если только одной треугольной грани, то *полуслабым*. *Вес* ребра есть сумма степеней его концевых вершин.

Бородин [1] доказал, что любой непустой плоский граф содержит либо слабое ребро веса не более 13, либо полуслабое ребро веса не более 10, либо ребро веса не более 8, причем все границы достижимы. В [2] был доказан другой похожий факт: каждый связный плоский граф не менее чем с двумя вершинами содержит либо две вершины с суммой степеней не более 5, либо две вершины на расстоянии 2 с суммой степеней не более 7, либо слабое ребро веса не более 11, либо полуслабое ребро веса не более 9, либо ребро веса не более 7. Данная структурная теорема использовалась в [2] для доказательства того, что из любого плоского графа удалением не более 5 ребер можно получить граф, обладающий нетривиальным автоморфизмом. Однако сама эта структурная теорема не является неулучшаемой в том смысле, что не все указанные в ней оценки достижимы. Нами доказан следующий усиленный вариант данной теоремы с неулучшаемыми оценками.

Теорема 1. *Каждый связный плоский граф не менее чем с двумя вершинами содержит один из следующих фрагментов*:

а) *две вершины с суммой степеней не более* 4;

б) *две вершины степени* 3 *на расстоянии* 2;

в) *слабое ребро веса не более* 11;

г) *полуслабое ребро веса не более* 9;

д) *ребро веса не более* 7.

Все оценки неулучшаемы.

Доказательство основано на технике перераспределения эйлеровых вкладов. Для того чтобы убедиться, что все оценки достигаются, построены примеры следующих плоских графов: для случая а) все полные двудольные графы $K_{2,n}$ при $n \geq 6$; для случая б) триангуляция, получаемая добавлением в каждую из граней икосаэдра

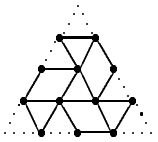

Рис. 1

вершины степени 3; для случая в) триангуляция, получаемая добавлением в каждую из граней икосаэдра треугольной решетки; для случая г) граф, получаемый заменой каждой грани октаэдра на конфигурацию, показанную на рис. 1; для случая д) четыреангуляция, получаемая добавлением в каждую из граней куба четырехугольной решетки.

Работа поддержана грантом РФФИ (№ 00-01-00916), а также грантом Университеты России (№ 1792) — программа фундаментальных исследований.

ЛИТЕРАТУРА

[1] O. V. Borodin (1992). Joint extension of two Kotzig's theorems on 3-polytopes. // Combinatorica, **13**, 121–130.

[2] V. A. Aksenov, O. V. Borodin, L. S. Mel'nikov, G. Sabidussi, M. Stiebitz, B. Toft (1999). Deeply asymmetric planar graphs. // Journal of Combinatorial Theory B, submitted.

* 630090, Новосибирск, Институт математики им. С.Л. Соболева СО РАН, пр. Академика Коптюга 4, e-mail: brdnoleg@math.nsc.ru

О КОЛИЧЕСТВЕ МНОГОМЕРНЫХ ОТОБРАЖЕНИЙ, УДОВЛЕТВОРЯЮЩИХ ЧАСТИ АКСИОМ ЗАМЫКАНИЯ

А.А. Вороненко*

Ранее (см. [1]) была изучена связь между задачами о числе монотонных булевых функций, о числе систем подмножеств, замкнутых относительно пересечений, и рядом задач, связанных с моделями зависимости для баз данных. В [1] была получена асимптотика логарифма числа систем подмножеств, замкнутых относительно пересечения, и, как следствие, для числа всех возможных операций замыкания на n-элементном множестве.

Замыканием $[\ ]$ на множестве M называется отображение 2^M в себя, удовлетворяющее трем условиям: 1) если $A \subseteq B$, то $[A] \subseteq [B]$; для всех A выполняется 2) $A \subseteq [A]$, 3) $[[A]] = [A]$. Если $\mathbf{x}$ — вектор

принадлежности элементов подмножества множеству M (характеристическая функция подмножества), а $\varphi(\mathbf{x})$ — вектор принадлежности элементов замыкания подмножества множеству M, то условия 1)–3) соответственно эквивалентны условиям:

$$\forall\mathbf{x}\forall\mathbf{y} \qquad \mathbf{x} \geq \mathbf{y} \Longrightarrow \varphi(\mathbf{x}) \geq \varphi(\mathbf{y}) \qquad \text{(монотонность)} \tag{1}$$

$$\forall\mathbf{x} \qquad \varphi(\mathbf{x}) \geq \mathbf{x} \qquad \text{(экстенсивность)} \tag{2}$$

$$\forall\mathbf{x} \qquad \varphi(\varphi(\mathbf{x})) = \varphi(\mathbf{x}) \qquad \text{(замкнутость)} \tag{3}$$

Если учитывать кратные или нечеткие вхождения элементов, то возникает задача о подсчете многозначных отображений, удовлетворяющих соответствующим условиям.

Через $V_n^{i,j}(\geq)$ будем обозначать множество отображений n-й декартовой степени частичного порядка $\geq$ в себя, удовлетворяющих условиям i, j.

В настоящей работе установлены следующие результаты:

$$\log_k |V_n^1(\geq)| \sim \log_k |V_n^{1,3}(\geq)| \sim \Theta_1(\geq) k^n \sqrt{n} \text{ при } n \to \infty,$$

$$\log_k |V_n^{1,2}(\geq)| \sim \Theta_2(\geq) k^n \sqrt{n} \text{ при } n \to \infty, (\Theta_1 > \Theta_2 \geq 0),$$

$$\log_k |V_n^2(\geq)| \sim \log_k |V_n^{2,3}(\geq)| \sim \Theta_3(\geq) k^n n \text{ при } n \to \infty.$$

Значения констант Θ вычислены точно. Кроме этого установлен критерий равенства $\Theta_2 = 0$: необходимым и достаточным условием выполнения этого соотношения является отсутствие такой константы a в E_k, что среди бóльших ее в смысле частичного порядка $\geq$ есть наименьшая.

Работа выполнена при поддержке РФФИ (код проекта 00-01-00351)

ЛИТЕРАТУРА

[1] Алексеев В.Б. О числе семейств подмножеств, замкнутых относительно пересечения. // Дискретная математика. Т. 1, Вып. 2, 1989. С. 129–136.

*Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики

ОПИСАНИЕ МНОЖЕСТВА f-ВЕКТОРОВ ТРИАНГУЛЯЦИЙ 4-МЕРНОГО КУБА

Д. В. Груздев*

В докладе найдено множество всех f-векторов триангуляций 4-мерного куба.

Мы будем изучать триангуляции d-мерного куба P^d. Минимальное число симплексов в триангуляции P^d обозначим через $\nu(d)$. Оценки для $\nu(d)$ изучались в [3, 10, 11]. Первый нетривиальный результат $\nu(3) = 5$ установлен в [9]. Полностью множество триангуляций P^3 было описано в [8]. Несколько авторов [4, 10] доказали, что $\nu(4) = 16$. В [10, 11] установлено, что $60 \leq \nu(5) \leq 67$. После этого было доказано [6], что $\nu(5) = 67$. Введем f-вектор триангуляции, компоненты которого есть количество граней триангуляции различных размерностей. Для P^d можно поставить несколько задач: нахождение $\nu(d)$, описание множества всех f-векторов триангуляций P^d, описание множества всех триангуляций P^d, заметив, что каждая следующая решает предыдущую. Здесь решена задача описания множества всех f-векторов триангуляций P^4.

Рассмотрим d-мерный выпуклый многогранник M, который будем называть *политопом*. Через $\Gamma_i(M)$ обозначим множество i-мерных граней политопа M и положим $f_i^M = |\Gamma_i(M)|$, $i = 0, \ldots, d$. Пусть $\Gamma(M) = \bigcup_{i=0}^{d} \Gamma_i(M)$ — множество всех граней политопа M. Если $|\Gamma_0(M)| = d + 1$, то M будем называть *d-мерным симплексом*.

Множество точек $A = \{a^1, \ldots, a^n\}$, $a^i \in R^d$, $i = 1, \ldots, n$, выпуклую оболочку которого обозначим через $[A]$, назовем *d-мерной точечной конфигурацией*, если $[A]$ — d-мерный политоп.

Триангуляцией $T(A)$ d-мерной точечной конфигурации A назовем множество $T(A) = \{S_1, \ldots, S_t\}$ d-мерных симплексов $S_1, \ldots, S_t$ такое, что:

(C_1) $[A] = \bigcup_{\tau=1}^{t} S_\tau$,

(C_2) $\Gamma_0(S_\tau) \subset A$, $\tau = 1, \ldots, t$,

(C_3) $S_\tau \cap S_\sigma = [\Gamma_0(S_\tau) \cap \Gamma_0(S_\sigma)]$, $\tau, \sigma = 1, \ldots, t$.

Если $A = \Gamma_0([A])$, то триангуляцию $T(A)$ назовем триангуляцией политопа $[A]$.

Пусть $\Gamma_i(T(A)) = \bigcup_{\tau=1}^{t} \Gamma_i(S_\tau)$ — множество i-мерных граней триангуляции $T(A)$, $f_i^{T(A)} = |\Gamma_i(T(A))|$ — количество i-мерных гра-

ней триангуляции $T(A)$, $i = 0, \ldots, d$. Пусть $\Gamma(T(A)) = \bigcup_{i=0}^{d} \Gamma_i(T(A))$ — множество всех граней триангуляции $T(A)$. Справедливы следующие леммы:

Лемма 1. $\forall F_1, F_2 \in \Gamma(T(A)) \quad F_1 \cap F_2 = [\Gamma_0(F_1) \cap \Gamma_0(F_2)]$.

Лемма 2. *Для любой точки* $a \in \Gamma([A])$ *существует единственная грань* $F \in \Gamma(T(A))$ *триангуляци* $T(A)$, *содержащая точку* $a \in int(F)$ *внутри себя.*

Грань F триангуляции $T(A)$ назовем *внутренней*, если она имеет внутренние точки из $[A]$, в противном случае ее назовем *внешней*. Пусть $G_i(T(A)) = \{F \,/\, F \in \Gamma_i(T(A))$ и $F \not\subset [A] \backslash int[A]\}$ — множество i-мерных внутренних граней триангуляции $T(A)$, $g_i^{T(A)} = |G_i(T(A))|$ — количество i-мерных внутренних граней триангуляции $T(A)$, $i = 0, \ldots, d$. Таким образом $g_d^{T(A)} = f_d^{T(A)}$, и если $A \subset [A] \backslash int([A])$, то $g_0^{T(A)} = 0$, .

Вектор $f^{T(A)} = (f_0^{T(A)}, \ldots, f_d^{T(A)})$ назовем *f-вектором* триангуляции $T(A)$, поставив ему в соответствие *f-полином* $f^{T(A)}(\lambda) = \sum_{i=0}^{d+1} f_{i-1}^{T(A)} \lambda^i$, где $f_{-1}^{T(A)} = 1$. Вектор $g^{T(A)} = (g_0^{T(A)}, \ldots, g_d^{T(A)})$ назовем *g-вектором* триангуляции $T(A)$, поставив ему в соответствие *g-полином* $g^{T(A)}(\lambda) = \sum_{i=1}^{d+1} g_{i-1}^{T(A)} \lambda^i$.

Множество всех триангуляций точечной конфигурации A обозначим через $\mathcal{T}(A)$. Полагая $F(A) = \{f^{T(A)} \,/\, T(A) \in \mathcal{T}(A)\}$, определим множество $F(A)$ всех f-векторов триангуляций точечной конфигурации A, которому поставим во взаимно-однозначное соответствие множество $\mathcal{F}(A) = \{f^{T(A)}(\lambda) \,/\, T(A) \in \mathcal{T}\ (A)\}$.

Пусть $\psi_{d,i}(\lambda) = \lambda^i (1+\lambda)^{d+1-i}$, $\varphi_{d,2i} = \psi_{d,i}(\lambda) = \lambda^i (1+\lambda)^{d+1-i}$, $\varphi_{d,2i-1} = \psi_{d+1,i}(\lambda) - \psi_{d+1,d+2-i}(\lambda) = \lambda^i (1+\lambda)^{d+2-i} - \lambda^{d+2-i}(1+\lambda)^i$. Тогда для произвольной триангуляции $T(A)$ d-мерной точечной конфигурации A из [1, 2] следует

$$g^{T(A)}(\lambda) = (-1)^{d+1} f^{T(A)}(-1-\lambda) \tag{2}$$

Лемма 3. *Существуют, единственны и являются целыми неотрицательными числа* $\alpha_i^{T(A)}$, $i = 0, \ldots, d$, *такие, что* $f^{T(A)}(\lambda) = \sum_{i=0}^{d} \alpha_i^{T(A)} \varphi_{d,i}(\lambda)$, *причем* $\alpha_0^{T(A)} = 1$.

Следствие 1. $\alpha_1^{T(A)} = g_0^{T(A)}$, *и если* $d \geq 3$ *и* $\alpha_1^{T(A)} = 0$, *то* $\alpha_3^{T(A)} = g_1^{T(A)}$.

Вектор $\alpha^{T(A)} = (\alpha_0^{T(A)}, \ldots, \alpha_d^{T(A)})$ назовем *α-вектором* триангуляции $T(A)$ и определим множество $\mathcal{A}(A) = \{\alpha^{T(A)} \,/\, T(A) \in \mathcal{T}(A)\}$. Таким образом лемма 3 ставит во взаимно однозначное соответствие f-полином $f^{T(A)}(\lambda)$ и α-вектор $\alpha^{T(A)}$, множества $\mathcal{F}(A)$ и $\mathcal{A}(A)$.

Точечную конфигурацию A^d назовем точечной конфигурацией, соответствующей d-мерному кубу, если в некоторой декартовой системе координат $A^d = \{0,1\}^d$. Сам же d-мерный куб определим как $P^d = [A^d]$ и поставим задачу описания множества $\mathcal{F}(A^4)$.

Порядком ребра $e = [u,v] \in \Gamma(T(A^d))$ триангуляции $T(A^d)$, где $u = (u_1, \ldots, u_d) \in A^d$ и $v = (v_1, \ldots, v_d) \in A^d$, назовем число $d(e) = d(u,v) = \sum_{i=1}^{d} |u_i - v_i|$. Пусть $E_i(T(A^d)) = \{e \in \Gamma_1(T(A^d)) \,/\, d(e) = i\}$ — множество ребер порядка i в триангуляции $T(A^d)$ и $e_i^{T(A^d)} = |E_i(T(A^d))|$ — количество ребер порядка i в триангуляции $T(A^d)$. Имеют место следующие утверждения.

$$G_1(T(A^d)) = E_d(T(A^d)),\ g_1^{T(A^d)} = e_d^{T(A^d)}. \tag{3}$$

Лемма 4. $e_3^{T(A^4)} \in \{0, \ldots 8\}$, $g_1^{T(A^4)} \in \{0,1\}$.

Лемма 5. $\alpha^{T(A^4)} = (1, 0, 11, g_1^{T(A^4)}, 2 + e_3^{T(A^4)})$.

Таким образом, ранее лемма 3 свела задачу описания $\mathcal{F}(A^4)$ к описанию $\mathcal{A}(A^4)$, теперь задача описания $\mathcal{A}(A^4)$ сводится к задаче отыскания всех возможных значений вектора $(g_1^{T(A^4)}, e_3^{T(A^4)})$ из диапазона, приведенного в лемме 4.

Точку $c = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ назовем центром 4-мерного куба и рассмотрим триангуляцию $T^0(A^4)$ без внутренних ребер ($g_1^{T^0(A^4)} = 0$). Грань $F_c^0 \in \Gamma(T^0(A^4))$, содержащую точку $c \in int(F_c^0)$ внутри себя, назовем центральной гранью триангуляции $T^0(A^4)$. Основная идея всего рассуждения заключена в том, чтобы установить, что центральная грань триангуляции $T^0(A^4)$ имеет не менее 4 ребер порядка 3, из чего следует:

Лемма 6. *Если* $g_1^{T(A^4)} = 0$, *то* $e_3^{T(A^4)} \geq 4$.

Теперь представим способ получения так называемых *регулярных* триангуляций точечных конфигураций. Пусть $A = \{a^1, \ldots, a^n\}$ — d-мерная точечная конфигурация, $a^j \in R^d$, и вектор весов $\omega =$

$(\omega_1,\ldots,\omega_n)$, $\omega_j \in R$, $j = 1,\ldots,n$. Составим точечную конфигурацию $\mathcal{A} = \{\binom{a^1}{\omega_1},\ldots,\binom{a^n}{\omega_n}\}$ и рассмотрим политоп $[\mathcal{A}]$ как $(d+1)$-мерный. Множество его гиперграней $\Gamma_d([\mathcal{A}]) = \{F_1,\ldots,F_m\}$ и $[\mathcal{A}] = \{x \in R^d \;/\; (b^i,x) \geq \beta_i, i = 1,\ldots,m\}$, где b^i — нормаль к грани F_i. Пусть $S(F_i) = [\{a^j \in A \;/\; \binom{a^j}{\omega_j} \in \Gamma_0(F_i)\}]$, $i = 1,\ldots,m$, и $\Phi(A,\omega,k) = \{F_i \;/\; kb^i_{d+1} > 0\}$, $k = -1,+1$. Фиксируя $k = -1,+1$, утверждаем, что если для любой $F \in \Phi(A,\omega,k)$ $\Gamma_0(F) = d+1$, то $T(A,\omega,k) = \{S(F) \;/\; F \in \Phi(A,\omega,k)\}$ есть триангуляция точечной конфигурации A. Заметим, что $T(A,\omega,-k) = T(A,-\omega,k)$, и положим $T(A,\omega) = T(A,\omega,+1)$.

Пусть $A^4 = \{a^1,\ldots,a^{16}\}$, где a^j — двоичный вектор, соответствующий двоичной записи числа $j-1$. Введем векторы весов ω^i_j:
$w^0_4 = -(13,19,21,7,30,6,23,30,16,39,1,15,18,16,38,7)$,
$w^0_5 = -(27,11,3,25,11,35,6,10,21,38,6,6,10,7,23,19)$,
$w^0_6 = (4,0,1,7,3,3,5,2,1,2,0,7,3,7,6,5)$, $w^0_7 = -w^0_6$,
$w^0_8 = -(0,6,3,0,7,8,9,9,0,4,6,2,8,1,2,0)$,
$w^1_0 = (23,6,14,12,15,21,23,9,1,18,8,1,13,6,2,19)$,
$w^1_1 = -(5,3,3,7,0,6,8,0,3,9,4,4,7,0,6,8)$, $w^1_2 = -w^1_0$,
$w^1_3 = -(26,8,23,29,14,26,24,0,4,4,15,0,17,0,23,19)$, $w^1_4 = -w^0_4$,
$w^1_5 = -(31,3,16,33,29,13,37,16,24,3,37,15,32,7,1,12)$, $w^1_6 = -w^1_5$,
$w^1_7 = (0,0,17,4,5,13,6,3,7,8,1,9,1,16,1,5)$, $w^1_8 = -w^1_7$.

Следующая теорема решает поставленную задачу.

Теорема 1.

$$\mathcal{F}(A^4) = \{\ \varphi_{4,0}(\lambda) + 11\varphi_{4,2}(\lambda) + \alpha_3\varphi_{4,3}(\lambda) + \alpha_4\varphi_{4,4}(\lambda) \mid (\alpha_3,\alpha_4) \in (\{0\} * \{6,\ldots,10\}) \bigcup (\{1\} * \{2,\ldots,10\})\ \}.$$

Доказательство. Используя леммы 4 и 6, заключаем, что для произвольной триангуляции $T(A^4)$ вектор $(g_1^{T(A^4)}, e_3^{T(A^4)}) \in M = (\{0\} * \{4,\ldots,8\}) \bigcup (\{1\} * \{0,\ldots,8\})$. Непосредственной проверкой убеждаемся, что для каждого вектора $(i,j) \in M$ существует соответствующая ему триангуляция $T^i_j(A^4) = T(A^4,\omega^i_j)$ такая, что $(g_1^{T^i_j(A^4)}, e_3^{T^i_j(A^4)}) = (i,j)$. Применение лемм 3 и 5 завершает доказательство теоремы.

Следствие 2.

$$F(A^4) = \{(16,56,82,55,14) + \alpha(0,1,3,3,1) + \beta(0,1,4,5,2) \mid (\alpha,\beta) \in (\{4,\ldots,8\} * \{0\}) \bigcup (\{0,\ldots,8\} * \{1\})\}.$$

ЛИТЕРАТУРА

[1] Шевченко В.Н. О разбиении выпуклого политопа на симплексы без новых вершин. // Известия ВУЗ, Математика, N12, 1997, с.89–99.

[2] Шевченко В.Н. Триангуляции точечных конфигураций и их f-векторы. // Проблемы теоретической кибернетики. Тезисы докладов XII международной конференции. Часть II. Москва: изд-во мех.-мат. ф-та МГУ, 1999, с.255.

[3] Шевченко В.Н. Качественные вопросы целочисленного программирования. Наука, Физматлит, Москва, 1995, с.35.

[4] R.W. Cottle. Minimal triangulations of the 4-cube. // Discrete Math. 40(1982) 25-29.

[5] R.B. Hughes. Minimum-cardinality triangulations of the d-cube for d=5 and d=6. // Discrete Math. 118(1993) 75-118.

[6] J. A. de Loera. Nonregular triangulations of products of simplices. // Discrete Comput Geom. 15 (1996) 253-264.

[7] P. S. Mara. Triangulations of the cube. // J. Combin. Theory Ser. A 20 (1976) 170-177.

[8] J. F. Sallee. A triangulation of the n-cube. // Discrete Math. 40 (1982) 81-86.

[9] J. F. Sallee. A note on minimal triangulations of an n-cube. // Discrete Appl. Math. 4 (1982) 211-215.

*Нижегородский государственный университет им. Н.И. Лобачевского

ОБ АЛГОРИТМИЧЕСКОЙ ТРУДНОСТИ ОДНОЙ ЗАДАЧИ, СВЯЗАННОЙ С ПРОБЛЕММОЙ ФОЛОВ В РЭНДЗЮ

М.А. Елисейкин

Описание правил игры рэндзю

Имеется клетчатая доска (игровое поле) размером $N \times N$ (в классическом варианте рэндзю 15×15) линий и шашки двух цветов: черные и белые. Ход производится выставлением шашки на пересечение линий. Пересечения линий называются пунктами (или точками). Число шашек ничем не ограничено. Игру начинают черные ходом в центр доски. Оба игрока ставят шашки по очереди, стараясь первым построить ряд из пяти своих шашек (по горизонтали, вертикали или диагонали). Цель игры - построить такой ряд из пяти своих шашек. Если ни один из игроков уже не сможет построить ряд из пяти своих шашек (при этом не обязательно должны быть выставлены все шашки), то партия заканчивается вничью.

Расположение пяти шашек одного цвета подряд есть пятерка. Ряд из четырех шашек, который может быть одним ходом превращен в пятерку, называется четверкой. Если данная четверка может быть достроена до пятерки с двух сторон, то такую четверку мы называем открытой. Тройкой называется ряд из трех шашек, который можно одним ходом достроить до открытой четверки. Тройки могут быть двух видов: сплошные и с интервалом. Построение одиночной тройки или четверки, которая не является открытой, в принципе, не опасно. Мы всегда сможем устранить эту угрозу за один ход. Более опасным является тот случай, когда результатом хода соперника становится появление на доске двух или большего числа троек или четверок. Еще хуже создание комбинаций троек или четверок (пересекающихся в пункте появления шашки), так как тогда соперник попадает в совсем трудное положение и единственное, на что он может надеется — успешная контратака. Такие комбинации принято называть вилками. Вилка, состоящая из двух рядов-троек: вилка 3×3, из двух рядов-четверок: вилка 4×4. Наконец, вилка, состоящая из одного ряда- тройки и одного ряда-четверки, называется вилкой 3×4.

Черным запрещается создание одним ходом любых вилок, содержащих две и большее число троек или две и большее число четве-

рок, а также построение длинного ряда из шести или большего числа шашек. Образование одной из таких вилок называется фолом. Вилка состоящая из рядов, один из которых — четверка, а другой — тройка, не запрещена, как и вилки, возникающие в тот момент, когда черные объявляют мат (выставляют пять шашек своего цвета в ряд).

Построение некоторых необходимых вспомогательных объектов

Определение. Пусть ходом в некоторую точку образуется k троек и m четверок. Точку, в которую этот ход делается, назовем обобщенной вилкой, а число $N = k + m$ назовем степенью обобщенной вилки (или просто обобщенной степенью этой точки).

Замечание 1. Буквой S с цифрой-индексом будем обозначать подозрительные на фол точки, обобщенная степень которых может быть выше, чем это следует из рисунка или схемы. Такое может произойти в силу того, что на каждом этапе нами будет рассматриваться лишь некоторый фрагмент игровой позиции, а проверяемая точка (фол она, или не фол?) может быть связана (и в большинстве случаев связана) с другими частями позиции через комбинации «тройка». Если точка не помечена описанным выше образом, то ее обобщенная степень в точность равна той, которая следует из рисунка.

Замечание 2. На прилагаемых рисунках черным кружочком будем обозначать точки, занятые черными шашками, белым кружочком — точки, занятые белыми шашками, крестиком будут обозначаться точки, не занятые в данный момент. Точки, никак не обозначенные на рисунке, предполагаются не занятыми, хотя если в них также находятся шашки не в коей мере не влияет на ход наших рассуждений. Нетрудно заметить, что на рассматриваемых частях игрового поля количество черных шашек превышает количество белых. Для того, чтобы обсуждаемая позиция была формально достижимой в реальной игре, будем считать, что недостающие белые шашки находятся некоторой области игрового поля, достаточно удаленной от рассматриваемых фрагментов доски.

Блок 1: *Эквивалентность.*

На Рис. 1 представлен кусок позиции, определяющий блок данного вида, а на Рис. 2 можно видеть его схематическое изображение.

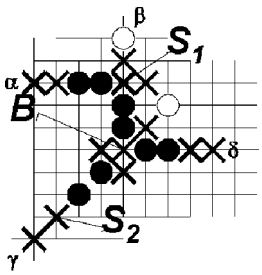

Рис. 1

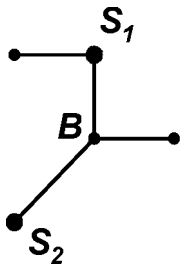

Рис. 2

Чаще нам будет удобнее работать именно со схематическими изображениями блоков. Предположим, что нами тестируется точка S_1 на предмет того, является ли ход в нее фолом для черных (начинающих) или нет. Тогда исходя из правил рэндзю, относительно определения фолов, S_1 фол тогда и только тогда, когда сделав ход в S_1, мы затем сможем пойти в обоих доступных направлениях до построения открытой четверки. В направлении α это возможно всегда. Поэтому все зависит от направления β. В этом направлении построение открытой четверки невозможно без участия точки B. Следовательно, S_1 — фол тогда и только тогда, когда B не фол. То есть, пойдя в B, мы потом должны быть не в состоянии пойти в направлении γ или в направлении δ. В направлении δ мы сможем играть при любых условиях. Поэтому B не фол, только если невозможно построение открытой четверки в направлении γ. А это имеет место тогда и только тогда, когда ход в точку S_2 невозможен, то есть когда S_2 — фол. Хотя из Рис. 1 вроде бы должно следовать, что S_2 — не фол, в силу замечания 1, обобщенная степень S_2 может быть равной не единице, а например, трем, и тогда S_2 может оказаться фолом. Получена следующая зависимость между S_2 и S_1: S_1 — фол тогда и только тогда, когда S_2 — фол.

Определение. Вершины на схематическом изображении некоторой части игровой позиции, отмеченные жирным кружочком, будем называть помеченными. Остальные вершины схемы будем называть непомеченными.

Блок 2: *Конъюнктивность.*

На Рис. 3 изображена часть позиции, соответствующая блоку дан-

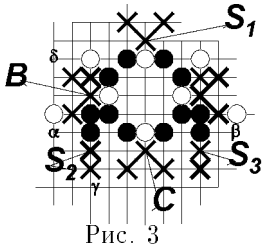

Рис. 3

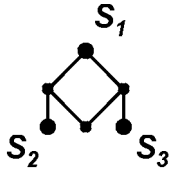

Рис. 4

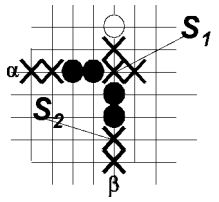

Рис. 5

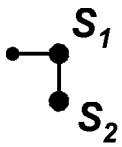

Рис. 6

ного вида, а на Рис. 4 представлено схематическое изображение блока. Описанным выше способом проверяем, является ли ход в точку S_1 фолом или нет. В итоге имеем: S_1 – фол тогда и только тогда, когда S_2 – фол и S_3 – фол.

Блок 3: *Отрицание.*

На Рис. 5 показана часть позиции, соответствующая данному виду блоков, а на Рис. 6 ее схематическое представление. Для определения того, является ли ход в точку S_1 фолом, необходимо проверить, действительно ли мы имеем дело с вилкой 3×3 и не является ли одна из троек на самом деле псевдотройкой. По поводу тройки в направлении α никаких сомнений не возникает, это действительно тройка. Рассмотрим направление β. В этом направлении возможно построение открытой четверки (и тогда S_1 — фол), только если S_2 не является фолом. Таким образом, S_1 — фол тогда и только тогда, когда S_2 — не фол.

Блок 4: *Дизъюнктивность.*

На Рис. 7 изображено схематическое представление блока. Вывод, который можно сделать здесь: S_1 — фол тогда и только тогда,

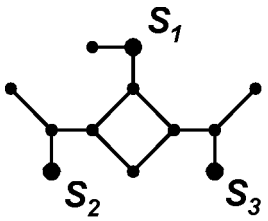

Рис. 7

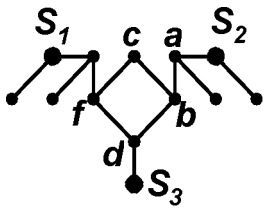

Рис. 8

когда S_2 — фол или S_3 — фол. Данное утверждение получается, если провести рассуждения, подобные тем, что мы проводили выше, или же, согласно известного правила двузначной логики, применив схему «отрицание» к схеме «конъюнктивность».

Блок 5: *Объединение.*

На Рис. 8 представлена схема блока типа «объединение». Покажем механизм действия этого блока. Точка S_2 является фолом тогда и только тогда, когда точка a не фол. Но a не фол, только если b будет фолом. Точка b является фолом, если и c, и d вместе не фолы. Ход в c всегда не фол (вилка 4×3 разрешена), поэтому должно быть, что d не фол. Ход в точку d не фол тогда и только тогда, когда или f фол, или S_3 фол. Точка f не может быть фолом, так как ход в c (после хода в f) всегда запрещен (вилка 4×4). Следовательно, остается только одна возможность: S_3 обязано быть фолом. Итак, мы получили, что S_2 — фол тогда и только тогда, когда S_3 — фол. Аналогично получается такое же утверждение про S_1 и S_3.

Блок 6: *Перекрестие.*

На Рис. 9 можно видеть схематическое изображение этого блока. Здесь имеют место две «эквивалентности»: S_1 — фол тогда и только тогда, когда S_2 — фол, S_3 — фол тогда и только тогда, когда S_4 — фол. Положительный момент этой конструкции в том, что меняется очередность следования рассматриваемых цепочек, происходит пересечение их траекторий без нарушения эквивалентности переходов.

Замечание 3. Блок «эквивалентность», представленный схемой на Рис. 2, очевидно, может быть устроен и другими способами. Для этого достаточно несколько иначе взаимно расположить комбинации шашек по рассматриваемым направлениям. Примеры схем, соответствующих некоторым возможным вариантам, показаны на Рис. 10.

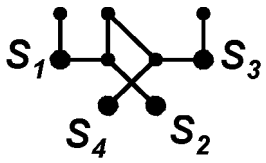

Рис. 9

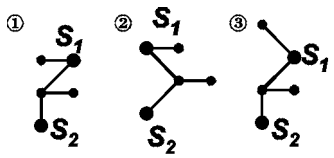

Рис. 10

NP-трудность одной задачи о фолах

Задача. Рассматриваем класс позиций при игре в рэндзю, имеющих некоторую общую для всех них область (часть позиции) с выделенной точкой в этой области. Спрашивается, существует ли позиция, принадлежащая данному классу, что ход в эту выделенную точку будет фолом.

Примечание. Другими словами, мы задаемся вопросом, влияет ли то, что находится за пределами указанной области (внешние условия), на возможность черным сделать ход в некоторую точку этой выделенной области, и если влияет, то насколько. Может ли конкретная точка при одних внешних условиях быть фолом, а при других не фолом.

Рассмотрим классическую задача ВЫПОЛНИМОСТЬ, алгоритмическая трудность которой известна, принадлежащую классу NP-полных задач. По произвольной формуле F (F — конъюнктивная нормальная форма) от n переменных строится некоторый класс позиций в рэндзю. Этот класс определяется общим куском игрового поля, присутствующим в каждой из позиций, и выделенной точкой S, принадлежащей этому куску, подозрительной на фол (подозрительность на фол означает, что обобщенная степень точки не ниже двух). Построение проходит в четыре этапа. На первом этапе реализуются все конъюнкции, входящие в формулу. В итоге получается, что некоторая точка S позиции эквивалентна конъюнкции других k точек (то есть S — фол тогда и только тогда, когда эти k точек фолы одновременно; здесь k — количество дизъюнктивных скобок в формуле F). На втором этапе к уже построенным k точкам «приклеиваются» снизу блоки, реализующие дизъюнкции; новые точки помечаются значками переменных или их отрицаний. На третьем

— к точкам, помеченным отрицанием переменных, «навешиваются» блоки типа «отрицание» (иначе используются блоки «эквивалентность») и новые точки помечаются той же переменной, но уже без отрицания. Получается «эквивалентность» точки S некоторому количеству точек позиции, согласованная с формулой F. На четвертом этапе происходит объединение в смысле использования блока «объединение» точек, помеченных одинаково в точку, помеченную той же переменной. При этом иногда возникает необходимость применения «перекрестия», если между этими точками находятся точки, помеченные иначе. Роль вспомогательных построений на всех этапах (для того, чтобы использовать любой из блоков, необходимо, чтобы точки находились на одной горизонтали и расстояние между ними на этой горизонтали было строго определенным (для каждого блока оно свое)) исполняют блоки «эквивалентность» в различных модификациях. В итоге, получается конструкция позиции, отвечающей условиям задачи, такая, что найдутся некоторые внешние условия (определяющие являются ли фолами помеченные концевые вершины схемы), что выделенная точка S будет фолом, тогда и только тогда, когда выполнима формула F. Это означает, что рассматриваемая задача является NP-полной.

Работа выполнена при финансовой поддержке РФФИ (проект 99–01–01175), Программы поддержки ведущих научных школ РФФИ (проект 00–15–96103), Программы «Университеты России» (проект 992206) и ФЦП «Интеграция» (объединенный проект АО110).

*Московский государственный университет им. М.В. Ломоносова, механико-математический факультет

О ВРЕМЕНИ ПАРАЛЛЕЛЬНОГО СЛОЖЕНИЯ НЕСКОЛЬКИХ ЧИСЕЛ

Д. А. Жуков*

Рассматривается следующая задача. Дан набор из N чисел, каждое из которых записано в позиционной системе счисления с основанием k и имеет длину n:

$$A_j = \sum_{i=0}^{n-1} a_{i,j} k^i,$$

$$a_{i,j} \in \{0, 1, \ldots, k-1\}, \quad j = 1 \ldots N, \quad i = 0 \ldots n-1.$$

Требуется, используя функции k-значной логики, найти их сумму.

В работах [1, 3] эта задача рассматривается в булевом случае $k = 2$ применительно к построению схем для умножения. Предложенные Храпченко [1] схемы умножения двух чисел длины n состоят из трёх частей: сначала произведение представляется, как в "школьном" алгоритме умножения в столбик, в виде суммы n чисел (эта подсхема имеет не зависящую от n глубину $O(1)$), затем происходит $(n, 2)$-преобразование ((n_1, n_2)–*преобразованием* называется преобразование группы из n_1 слагаемых в группу из n_2 слагаемых с той же суммой [1]). Решающую роль играет то, что глубина (n_1, n_2)-преобразования не зависит от длины слагаемых. Наконец, последняя подсхема вычисляет сумму двух оставшихся чисел (это можно сделать за время $\log_2 n$ [2]), и на её выходе мы получаем искомое произведение. Наилучшая полученная таким методом верхняя оценка глубины $(n, 2)$-преобразования составляет $3.57 \log_2 n$ ([3]). В данной работе показано, что в случае k-значной логики мультипликативную постоянную перед знаком логарифма можно уменьшить.

Теорема 1. *В базисе всех двуместных функций k-значной логики можно построить схему S, которая для всякого набора $\{A_j\}$ из N штук n-значных k-ичных чисел получает пару k-ичных чисел B и C с той же суммой: $B + C = \sum A_j$. При этом глубина этой схемы $D(S)$ не превосходит числа*

$$D(S) \leq \frac{]\log_2(k+1)[+]\log_2]\log_2(k+1)[[}{\log_2(k+1) - 1} \cdot \log_2 N + O(\log_2 k).$$

Доказательство. Будем строить схему S над набором $\{\oplus, \&\}$ двуместных функций из P_k, где через $\oplus$ и $\&$ обозначены сложение по модулю k и возможный перенос соответственно: при $x, y \in \{0, 1, \ldots, k-1\}$

$$x \oplus y = x + y \pmod{k},$$

$$x \& y = \begin{cases} 1, & \text{если } x + y \geq k, \\ 0, & \text{иначе.} \end{cases}$$

Для этого потребуется вспомогательная подсхема R_{k+1} — полный сумматор.

Схема R_{k+1} имеет $k+1$ входов $z_1, \ldots, z_{k+1}$ и два выхода x и y. Она получает на входе k-ичные цифры и вычисляет их сумму в k-ичном позиционном представлении: x и y — это младший и старший разряды суммы входов $\sum_{i=1}^{k+1} z_i$. Подсхема вычисления младшего разряда — это бинарное дерево с вершинами–функциональными элементами. Оно, очевидно, имеет глубину $]\log_2(k+1)[$, и уменьшить её нельзя. Синтез подсхемы вычисления старшего разряда осуществляется по схеме младшего по следующему правилу: если a и b — вершины некоторой глубины t из подсхемы младшего разряда и c — $\oplus$-вершина глубины $t+1$ в подсхеме младшего разряда (в ней реализуется функция $a \oplus b$), то в подсхеме старшего разряда имеется соответствующая &-вершина глубины $t+1$, реализующая функцию $a\&b$. Эта вершина учитывает возможный перенос в следующий разряд. На следующем шаге переносы складываются, и т.д. В тот момент, когда младший разряд получен, дерево вычисления старшего разряда имеет $]\log_2(k+1)[$ вершин поддеревьев глубины $]\log_2(k+1)[$. На сложение этих чисел требуется ещё $]\log_2]\log_2(k+1)[[$ единиц времени. Окончательно, схема R_{k+1} имеет глубину не более

$$D(R_{k+1}) \leq]\log_2(k+1)[+]\log_2]\log_2(k+1)[[.$$

Схема R_{k+1} имеет асимптотически оптимальную глубину (с ростом k). Это позволяет построить имеющую асимптотически оптимальную глубину схему S следующим образом.

Из соответсвующего количества соединённых параллельно схем R_{k+1} можно построить схему Q_{k+1}, входы которой разбиты на $k+1$ групп, выходы — на две группы. Блок Q_{k+1} заменяет группу из $k+1$ слагаемых (k-ичных чисел) группой из двух слагаемых с той же суммой, осуществляя $(k+1,2)$–преобразование. Первое слагаемое представляет собой набор младших разрядов поразрядных сумм цифр входных чисел, второе — набор старших разрядов этих сумм. Очевидно, глубина схемы Q_{k+1} не зависит от числа разрядов k-ичных чисел на её входах и совпадает с глубиной схемы R_{k+1}: $D(Q_{k+1}) = D(R_{k+1})$.

Дальнейшая процедура не отличается от изложенной в [1]. Реализуемое схемой S $(N,2)$–преобразование выполняется по шагам, каждый из которых сводится к выполнению совокупности более простых $(k+1,2)$-преобразований, реализуемых блоками Q_{k+1}. Обозначим через n_j число слагаемых на шаге с номером j, тогда легко видеть (см.

[1]), что $n_j < N\left(\frac{2}{k+1}\right)^j + \frac{(k+1)^2}{k-1}$. Взяв d – наименьшее целое решение неравенства $N\left(\frac{2}{k+1}\right)^d \le 1$, то есть $d =]\log_{\frac{k+1}{2}} N[$, получим $n_d < k+4$ при $k \ge 2$, и $n_d \le k+1$ при $k \ge 5$.

Общая глубина схемы S есть произведение (постоянной) глубины каждого шага на число шагов:

$$\begin{aligned} D(S) &\le D(Q_{k+1}) \cdot (d+2) \\ &\le (]\log_2(k+1)[+]\log_2]\log_2(k+1)[[) \cdot (]\log_{\frac{k+1}{2}} N[+2) \\ &\le \frac{]\log_2(k+1)[+]\log_2]\log_2(k+1)[[}{\log_2(k+1)-1}\log_2 N \\ &\quad + 3(]\log_2(k+1)[+]\log_2]\log_2(k+1)[[) \\ &\le \left(1 + \frac{\log_2\log_2(k+1)+4}{\log_2(k+1)-1}\right) \cdot \log_2 N + O(\log_2 k). \end{aligned}$$

Теорема доказана.

Другой пример схемы для быстрого $(N,2)$-преобразования даёт следующая

Теорема 2. *Пусть $k = 2^r+1$, $r \ge 1$. Тогда в базисе из двуместных функций k-значной логики можно построить схему $S_{k,N}$, при $N \to \infty$ осуществляющую $(N,2)$-преобразование за время*

$$D(S_{k,N}) \le \frac{1}{1-\log_2\alpha}\log_2 N \cdot (1+o(1)),$$

где α — наибольший из модулей корней многочлена $x^{r+1} - x^r - 1$.

В частности, $D(S_{3,N}) \le 3.27\log_2 N$, $D(S_{9,N}) \le 1.87\log_2 N$.

Доказательство основано на том, что при сложении k-ичных чисел возможный перенос из разряда в разряд всегда не больше единицы. Поэтому переносы можно складывать друг с другом без переполнения разрядов.

Итак, $k = 2^r + 1$; схемы, как и при доказательстве теоремы 1, строим из функциональных элементов, реализующих функции $\oplus$ и $\&$ из P_k.

Назовём число x *δ-числом*, если все его цифры x_i удовлетворяют неравенству

$$\forall i \quad 0 \le x_i \le \delta.$$

Алгоритм построения схемы $(N, 2)$-преобразования выполняется пошагово. Обозначим через $M_i(t)$ количество 2^i-чисел на шаге t, $i = 0, \ldots, r$. На каждом шаге выполняются две процедуры:

1) Складывая всякие два $(k-1)$-числа, получаем одно $(k-1)$-число и одно 1-число. А именно, если

$$X = \sum_{i=0}^{n} x_i k^i, \qquad Y = \sum_{i=0}^{n} y_i k^i,$$

где $0 \le x_i, y_i \le k-1$, то

$$x_i + y_i = w_i + t_i,$$

где $w_i = x_i \oplus y_i$, $t_i = x_{i-1} \& y_{i-1}$, причём $0 \le w_i \le k-1$ и $0 \le t_i \le 1$. Получаем

$$X + Y = W + T,$$

где $W = \sum_{i=0}^{n} w_i k^i$ — $(k-1)$-число, $T = \sum_{i=0}^{n+1} t_i k^i$ — 1-число.

2) Если $\delta \le \frac{k-1}{2}$, то складывая два δ-числа получаем одно 2δ-число (аналогичное рассуждение).

Полезно ввести ещё одно определение. Пусть $\mathbf{m} = \{m_0, \ldots, m_r\}$, $\mathbf{m}' = \{m'_0, \ldots, m'_r\}$. Назовём $(\mathbf{m}, \mathbf{m}')$-*преобразованием* такое $(m_0 + m_1 + \ldots + m_r, m'_0 + m'_1 + \ldots + m'_r)$-преобразование, что m_i — количество 2^i-чисел в сумме до преобразования, а m'_i — после. Тогда на каждом шаге t алгоритм 1) – 2), складывая друг с другом максимальное возможное количество 2^i-чисел, $i = 0 \ldots r$, строит подсхему, совершающую $(\{M_0(t-1), \ldots, M_r(t-1)\}, \{M_0(t), \ldots, M_r(t)\})$ – преобразование, где

$$\left\{ \begin{array}{lcl} M_0(t) & = & [\frac{M_r(t-1)}{2}] + \delta\left(M_0(t-1)\right), \\ M_1(t) & = & [\frac{M_0(t-1)}{2}] + \delta\left(M_1(t-1)\right), \\ & \ldots & \\ M_{r-1}(t) & = & [\frac{M_{r-2}(t-1)}{2}] + \delta\left(M_{r-1}(t-1)\right), \\ M_r(t) & = & [\frac{M_{r-1}(t-1)}{2}] + \left]\frac{M_r(t-1)}{2}\right[, \end{array} \right. \tag{1}$$

для сокращения обозначено

$$\delta(n) = \left]\frac{n}{2}\right[- \left[\frac{n}{2}\right] = \left\{ \begin{array}{ll} 0, & \text{если } n \text{ четное}, \\ 1, & \text{если } n \text{ нечетное}. \end{array} \right.$$

Глубина подсхемы, очевидно, равна 1. На первом шаге $M_0(0) = M_1(0) = \ldots = M_{r-1}(0) = 0$, $M_r(0) = N$. Алгоритм заканчивает работу, когда $\sum_{i=0}^{r} M_i(t) = 2$.

Оценим теперь глубину полученной схемы. Пусть $N = 2^n$, тогда при $1 \le t \le n$:

$$\begin{array}{lcl} M_0(t) & = & M_r(t-1)/2, \\ M_1(t) & = & M_0(t-1)/2, \\ & \ldots & \\ M_{r-1}(t) & = & M_{r-2}(t-1)/2, \\ M_r(t) & = & M_r(t-1)/2 + M_{r-1}(t-1)/2. \end{array} \tag{2}$$

Обозначим $N_i(t) = \frac{M_i(t)}{N} 2^t = M_i(t) 2^{t-n}$. Из (2), очевидно, следует, что

$$N_0(t) = N_r(t-1), \quad N_1(t) = N_0(t-1), \quad \ldots \quad N_{r-1}(t) = N_{r-2}(t-1),$$

$$N_r(t) = N_r(t-1) + N_{r-1}(t-1) = N_r(t-1) + N_{r-2}(t-2) = \ldots =$$
$$= N_r(t-1) + N_0(t-r) = N_r(t-1) + N_r(t-r-1).$$

Получили рекуррентное соотношение

$$\begin{cases} N_r(t) - N_r(t-1) - N_r(t-r-1) = 0, \\ N_r(0) = N_r(1) = \ldots = N_r(r) = 1. \end{cases} \tag{3}$$

с характеристическим уравнением

$$x^{r+1} - x^r - 1 = 0.$$

Пусть α — наибольший модуль (комплексных) корней многочлена $x^{r+1} - x^r - 1$. Тогда для решения $N_r(t)$ рекуррентного сотношения (3) справедливо неравенство

$$N_r(t) \le c_1 \alpha^t (1 + c_2 \beta^t),$$

где $0 < \beta < 1$, c_1 и c_2 — некоторые постоянные. В частности,

$$M_r(n) = N_r(n) \le c_1 \alpha^n (1 + c_2 \beta^n). \tag{4}$$

Эта оценка относится к первым n шагам алгоритма, осуществляющим $(\{0, 0, \ldots, 0, N\}, \{M_0(n), M_1(n), \ldots, M_r(n)\})$ – преобразование. Чтобы оценить глубину всей схемы, полезно произвести некоторые упрощения. Это позволит избежать громоздких выкладок.

Во-первых, т.к. $\beta < 1$, при достаточно больших n можно считать, что $M_r(n) \le c\alpha^n$, где c — постоянная. Во-вторых, несколько огрубляя оценку (что, впрочем, не сказывается на окончательном результате), можно считать, что первые n шагов алгоритма осуществляют $(\{0,0,\ldots,0,N\},\{0,0,\ldots,0,(r+1)M_r(n)\})$ – преобразование (вытекает из очевидных неравенств $M_i(t) \le M_r(t)$, $i = 0,\ldots,r-1$; $t = 0,\ldots,n$) — ведь всякое δ-число является и γ-числом при $\gamma > \delta$.

Итак, получено $(2^n, m)$-пребразование глубины n, причём

$$m \le c(r+1)\alpha^n \le 2^{b+n\log_2\alpha},$$

$$b \le \log_2 c(r+1) + 1 = \mathrm{const},$$

т.к. ближайшая сверху к числу $c(r+1)\alpha^n$ степень двойки имеет показатель $]\log_2 c(r+1)\alpha^n[$. Применяя его индуктивно для разных n, можно говорить о последовательности $(2^{d_j}, 2^{d_{j+1}})$-преобразований: сначала из $2^n = 2^{d_0}$ k-ичных чисел получаем не более чем 2^{d_1} k-ичных чисел; применяя к ним подобное преобразование, получаем не более чем 2^{d_2} k-ичных чисел, и т.д. Числа d_j подчиняются рекуррентному соотношению

$$\begin{cases} d_{j+1} = b + d_j \log_2\alpha, \\ d_0 = n, \end{cases}$$

общий член которого, как легко видеть, есть

$$d_j = n\,(\log_2\alpha)^j + b\frac{1-\log_2^{j+1}\alpha}{1-\log_2\alpha} \le n\,(\log_2\alpha)^j + \frac{b}{1-\log_2\alpha}.$$

Глубина подсхемы, реализующей $(2^{d_j}, 2^{d_{j+1}})$-преобразование, равна d_j. Глубина схемы, построенной алгоритмом 1) – 2), по построению не превосходит общей глубины всех $(2^{d_j}, 2^{d_{j+1}})$-преобразований, т.е. величины $\sum d_j$. Точнее, для всякого $m \ge 0$ справедлива следующая оценка.

$$\begin{aligned} D(S_{k,2^n}) &\le \sum_{j=0}^{m} d_j + D_m \\ &\le n\sum_{j=0}^{m}\log_2^j\alpha + \frac{bm}{1-\log_2\alpha} + D_m \\ &\le \frac{n}{1-\log_2\alpha} + \frac{bm}{1-\log_2\alpha} + D_m. \end{aligned}$$

Здесь через D_m обозначена глубина $(2^{d_{m+1}}, 2)$-преобразования. Выберем m как наименьшее целое решение неравенства $n\,(\log_2 \alpha)^m = b/(1-\log_2 \alpha)$, то есть

$$m = -\left]\log_{\log_2 \alpha} \frac{n(1-\log_2 \alpha)}{b}\right[\sim -\frac{\log_2 n}{\log_2 \log_2 \alpha}.$$

В этом случае

$$d_{m+1} \le \frac{2b}{1-\log_2 \alpha} \le \frac{2\log_2 c(r+1)+1}{1-\log_2 \alpha} = \mathrm{const}$$

— не зависит от n. Поэтому $D_m = O(1)$.

Окончательно, если $N = 2^n$, то

$$D(S_{k,N}) \le \frac{n}{1-\log_2 \alpha} + O(\log_2 n) = \frac{n}{1-\log_2 \alpha} \cdot (1+o(1)).$$

Если же N не есть степень двойки, то

$$D(S_{k,N}) \le D(S_{k,2^{]\log_2 n[}}) \le \left(\frac{\log_2 N}{1-\log_2 \alpha} + O(1)\right) \cdot (1+o(1))$$

при $N \to \infty$.

Для $r = 1$ и $r = 3$ численное нахождение комплексных корней многочлена $x^{r+1} - x^r - 1$ даёт $\alpha = 1.6180...$ и $\alpha = 1.3802...$ соответственно. Отсюда следуют оценки $D(S_{3,N}) \le 3.27 \log_2 N$ и $D(S_{9,N}) \le 1.87 \log_2 N$. Эта иллюстрация завершает доказательство теоремы.

В заключение приведём одно полезное следствие результатов Храпченко.

Теорема 3. *В базисе двуместных функций k-значной логики можно построить схему Σ_n сложения двух чисел длины n, имеющую асимптотически оптимальную глубину*

$$D(\Sigma_n) \sim \log_2 n.$$

Доказательство дословно повторяет рассуждения Храпченко [2, с.109-112]. Меняются лишь несущественные детали: перенос w_i из

$(i+1)$-го разряда в i-й разряд подчиняется прежнему рекуррентному соотношению

$$w_{i-1} = u_i \vee w_i \& v_i,$$

где $u_i = x_i \& y_i$, $v_i = x_i \oplus y_i$, но в этом соотношении функциональные связки имеют уже новый смысл. За исключением дизъюнкции "$\vee$" это — вышеописанные функции k-значной логики. Поэтому полностью доказательство теоремы 3 мы здесь не приводим.

Следствие 1. *Если имеется алгоритм для построения схемы, реализующей k-ичное $(n,2)$-прeбразование с глубиной не более $c \cdot \log_2 n \cdot (1+o(1))$, то существует схема умножения двух k-ичных чисел длины n глубины не более $(1+c) \cdot \log_2 n \cdot (1+o(1))$.*

В частности, для $k = 9$ можно построить схему умножения с глубиной $\leq 2.87 \log_2 n \cdot (1+o(1))$.

Работа выполнена при финансовой поддержке РФФИ (проект 99–01–01175), Программы поддержки ведущих научных школ РФФИ (проект 00–15–96103), Программы «Университеты России» (проект 992206) и ФЦП «Интеграция» (объединенный проект АО110).

ЛИТЕРАТУРА

[1] Храпченко В.М. Некоторые оценки для времени умножения. // Проблемы кибернетики. 1978. вып. 33, с. 221-227.

[2] Храпченко В.М. Об асимптотической оценке времени сложения параллельного сумматора. // Проблемы кибернетики. 1967. вып. 19, с. 107-122.

[3] Paterson M.S., Pippenger N., Zwick U. Optimal carry save networks. In "Boolean Function Complexity", M.S. Paterson, editor, London Mathematical Society Lecture Note Series 169, Cambrige Univ. Press, 1992, pp. 174-201.

*Московский государственный университет им. М.В. Ломоносова, механико-математический факультет

ПОРОГОВЫЕ ФУНКЦИИ, ЗАВИСЯЩИЕ ОТ ДВУХ ПЕРЕМЕННЫХ: СЛОЖНОСТЬ РАСШИФРОВКИ И МОЩНОСТЬ РАЗРЕШАЮЩЕГО МНОЖЕСТВА

Н. Ю. Золотых*

Предлагается алгоритм расшифровки пороговой функции двух переменных, использующий не более $6\log(k-1)+4$ обращений к оракулу и $O(\log^2 k)$ арифметических операций. Приведена схема доказательства того, что тупиковое разрешающее множество пороговой функции двух переменных состоит либо из трех, либо из четырех точек.

Введение

Функция k-значной логики n переменных, принимающая два значения 0, 1 называется *пороговой*, если существует гиперплоскость, разделяющая ее множество нулей и единиц (точек, в которых функция равна 0 и 1 соответственно).

Пусть с каждой пороговой функцией связан *оракул*, позволяющий по произвольной точке из области определения установить значение функции в этой точке. Под расшифровкой заранее не известной пороговой функции понимается определение коэффициентов разделяющей гиперплоскости с помощью вопросов оракулу [1].

В [2] предложен алгоритм расшифровки пороговой функции, при любом фиксированном n использующий не более $O(\log^n k)$ обращений к оракулу и полиномиальное от $\log k$ число арифметических операций (здесь и далее все асимптотические оценки рассматриваются при $k \to \infty$ и фиксированном $n \geq 2$).

Разрешающим множеством пороговой функции f называется такое подмножество T области определения, что для любой отличной от f функции g найдется $x \in T$, для которого $f(x) \neq g(x)$. Разрешающее множество минимальной мощности называется *минимальным* разрешающим множеством функции f. Разрешающее множество, для которого никакое его собственное подмножество не является разрешающим, называется *тупиковым* разрешающим множеством функции f.

В [4, 5] доказана единственность тупикового (и, следовательно, минимального) разрешающего множества любой пороговой функции.

В [6] показано, что мощность минимального разрешающего множества не превосходит $O(\log^{n-1} k)$. В [4, 5] для любых n, k установлено существование пороговых функций с минимальным разрешающим множеством мощности $\Omega(\log^{n-2} k)$ и тем самым доказана невозможность алгоритма расшифровки, использующего менее $\Omega(\log^{n-2} k)$ вопросов оракулу. Структура минимального разрешающего множества булевой ($k = 2$) пороговой функции рассматривается в [7].

В [8] предложен алгоритм расшифровки пороговой функции двух переменных ($n = 2$), использующий не более $O(\log^2 k)$ обращений к оракулу и полиномиальное от $\log k$ число арифметических операций. В [9] этот алгоритм улучшен, верхняя оценка числа обращений к оракулу снижена до $O(\log k)$, а верхняя оценка числа арифметических операций — до $O(\log^2 k)$. Предложенный в [10] алгоритм расшифровки пороговой функции двух переменных использует не более $6 \log k + 33 \log\log k - 26$ обращений к оракулу и полиномиальное от $\log k$ число арифметических операций.

Работа состоит из двух разделов. В первом предлагается алгоритм расшифровки пороговой функции двух переменных, использующий не более $6 \log(k-1) + 4$ обращений к оракулу и $O(\log^2 k)$ арифметических операций. Во втором разделе приведена схема доказательства того, что тупиковое разрешающее множество пороговой функции двух переменных состоит либо из трех, либо из четырех точек. Результаты были анонсированы также в [4]. Связь задачи расшифровки пороговой функции с задачей нахождения наилучшего диофантового приближения рассмотрена в [11].

Алгоритм расшифровки пороговой функции двух переменных

Пусть $k \geq 2$, $n \geq 2$, $B(k) = \{0, 1, \ldots, k-1\}^2$, $f : B(k) \to \{0, 1\}$. Обозначим через $M_0(f)$, $M_1(f)$ множество нулей и соответственно множество единиц функции f, т.е.

$$M_\nu(f) = \{x \in B(k) : f(x) = \nu\} \quad (\nu = 0, 1).$$

Функция f называется *пороговой*, если существуют a_0, a_1, a_2 такие, что

$$M_0(f) = \{x \in B(k) : a_1 x_1 + a_2 x_2 \leq a_0\}. \tag{11}$$

Множество всех пороговых функций, заданных на множестве $B(k)$, обозначим через $F_\pi(k)$. Предположим, что с каждой функцией f из $F_\pi(k)$ связан *оракул*, позволяющий по произвольному $x \in B(k)$ определить $f(x)$. Под *расшифровкой* заранее не известной функции f понимается нахождение с помощью оракула целых чисел a_0, a_1, a_2, при которых выполняется (11). Пусть алгоритм $\mathcal{A}$ для расшифровки функции f использует $\tau(\mathcal{A}, k, f)$ обращений к оракулу и $\rho(\mathcal{A}, k, f)$ арифметических операций над целыми числами. Введем обозначения:

$$\tau(\mathcal{A}, k) = \max_{f \in F_\pi(k)} \tau(\mathcal{A}, k, f); \quad \rho(\mathcal{A}, k) = \max_{f \in F_\pi(k)} \rho(\mathcal{A}, k, f).$$

Теорема 1. 1) *Для любого алгоритма $\mathcal{A}$ расшифровки пороговой функции двух переменных справедливо асимптотическое неравенство*

$$\tau(\mathcal{A}, k) \gtrsim 4 \log k.$$

2) *Существует алгоритм $\mathcal{A}_1$ расшифровки пороговой функции двух переменных, для которого*

$$\tau(\mathcal{A}_1, k) \le 6 \log(k-1) + 4; \quad \rho(\mathcal{A}_1, k) = O(\log^2 k).$$

Первое утверждение теоремы 1 является следствием оценки $|F_\pi(k)| \asymp k^4$ из [12].

Пусть в параллелограмме Φ с целочисленными вершинами R_0, R_1, R_2, R_3 стороны R_0R_1 и R_2R_3 кроме концов не содержат других целочисленных точек:

$$\begin{gathered} R_i \in \mathbf{Z}^2 \ (i = 0, \ldots, 3), \\ [R_0, R_1] \cap \mathbf{Z}^2 = \{R_0, R_1\}, \\ [R_2, R_3] \cap \mathbf{Z}^2 = \{R_2, R_3\}. \end{gathered} \tag{12}$$

Назовем неравенство

$$\alpha_1 x_1 + \alpha_2 x_2 \le \alpha_0 \tag{13}$$

отсечением вершины R_i $(i = 0, \ldots, 3)$ параллелограмма Φ, если оно не выполняется для координат точки R_i. Будем говорить, что отсечение проходит через точку (x_1, x_2), если $\alpha_1 x_1 + \alpha_2 x_2 = \alpha_0$. Отсечение (13) вершины R_i называется *правильным*, если выполняются

следующие условия: 1) неравенство (13) справедливо для всех целочисленных точек из Φ кроме R_i; 2) отсечение (13) проходит через вершину R', соседнюю с R_i по ребру R_0R_1 или R_2R_3; 3) отсечение (13) проходит по крайней мере еще через одну точку из $\Phi \cap \mathbf{Z}^2$.

Доказательство теоремы 1 основано на следующих вспомогательных утверждениях.

Лемма 1. *Существует алгоритм $\mathcal{A}'$, который для любого параллелограмма $\Phi = R_0R_1R_2R_3 \subseteq B(k)$, обладающего свойством 12 и заданного своими вершинами, за линейное от $\log k$ время строит правильное отсечение вершины R_0.*

Лемма 2. *Пусть параллелограмм $\Phi = R_0R_1R_2R_3$ обладает свойством (12) и кроме вершин содержит еще хотя бы одну целочисленную точку. Тогда либо правильное отсечение вершины R_0, либо правильное отсечение вершины R_1 содержит не менее 3 точек множества $\Phi \cap \mathbf{Z}^2$.*

Перейдем теперь к пошаговому описанию алгоритма $\mathcal{A}_1$.

Шаг 0. Определим $f(x)$ в вершинах прямоугольника $B(k)$ и обозначим через S_ν $(\nu = 0, 1)$ множество тех из них, для которых $f(x) = \nu$. Если при $\nu = 0$ или при $\nu = 1$ множество S_ν пусто, то расшифровка закончена, так как в этом случае $M_\nu(f) = \emptyset$ и $f \equiv 1 - \nu$.

Шаг 1. Пусть L_i $(i = 0, 1)$ — сторона прямоугольника $B(k)$, в концах которой функция f принимает различные значения. Дихотомией на каждой из сторон L_0, L_1 найдем пару соседних целочисленных точек R_0, R_1 и R_2, R_3 соответственно, так, чтобы $f(R_0) = f(R_3) = \nu$, $f(R_1) = f(R_2) = 1 - \nu$ $(\nu = 0, 1)$. Присоединим R_0, R_3 к S_ν, а R_1, R_2 к $S_{1-\nu}$. Для целочисленных точек из $\operatorname{Conv} S_\nu$ $(\nu = 0, 1)$ имеем $f(x) = \nu$. Если L_0 и L_1 — противоположные стороны прямоугольника $B(k)$, тогда $R_0 - R_1 = R_3 - R_2$, следовательно, $R_0R_1R_2R_3$ — параллелограмм. В противном случае, когда L_0, L_1 — смежные, обозначим через R их общую вершину и рассмотрим ту пару точек R_{2i}, R_{2i+1}, которая расположена дальше от R. Пусть $j \in \{1, 2\}$ и $\nu \in \{0, 1\}$ выбраны так, что R_{2i}, R_{2i+1} являются соседями по координате j и $R_{2i+\nu}$ расположена дальше от R, чем $R_{2i+1-\nu}$. Заменим $R_{2i+\nu}$ точкой $R'_{2i+\nu}$, соседней с $R_{2i+1-\nu}$ по координате $3-j$. Очевидно, что $f(R'_{2i+\nu}) = f(R_{2i+\nu})$. Положим $R_{2i+\nu} := R'_{2i+\nu}$. Возможен случай, когда до замены обе пары R_0, R_1 и R_2, R_3 были равноудалены от R, тогда, очевидно, $\Phi = R_0R_1R_2R_3$ не содержит внут-

ренних целочисленных точек и $M_\nu(f) = \operatorname{Conv} S_\nu \cap B(k)$ $(\nu = 0, 1)$ — расшифровка завершена.

Шаг 2. Алгоритмом $\mathcal{A}'$ построим правильные отсечения вершин R_0 и R_1 и выберем из них отсечение, проходящее через бóльшее число точек из $\Phi \cap B(k)$, где $\Phi = R_0R_1R_2R_3$. Пусть i — номер соответствующей выбранному отсечению вершины. Если на отсечении нет ни одной целочисленной внутренней точки области Φ, то Φ вообще не содержит внутренних целочисленных точек, $M_\nu(f) = \operatorname{Conv} S_\nu \cap B(k)$ $(\nu = 0, 1)$ — расшифровка завершена. В противном случае дихотомией найдем две соседние целочисленные точки R'_0, R'_1, лежащие на построенном отсечении, такие, что $f(R'_0) \neq f(R'_1)$. Аналогичную процедуру проведем с отсечением вершины R_{3-i}: дихотомией найдем лежащие на этом отсечении соседние целочисленные точки R'_2, R'_3, такие, что $f(R'_0) = f(R'_3)$, $f(R'_1) = f(R'_2)$.

Шаг 3. Для всех $i = 0, \ldots, 3$ положим $R_i := R'_i$. Добавим R_0 и R_3 к S_ν, а R_1 и R_2 к $S_{1-\nu}$, где $\nu = f(R_0)$. Перейдем на шаг 2.

Очевидно, что за конечное число шагов алгоритм $\mathcal{A}_1$ остановится, при этом $M_\nu(f) = \operatorname{Conv} S_\nu \cap \mathbf{Z}^2$ — функция f расшифрована.

Созданная автором программа, реализующая алгоритм $\mathcal{A}_1$, находится в Internet по адресу `http://www.uic.nnov.ru/~zny`.

Мощность тупикового разрешающего множества пороговой функции двух переменных

Множество $T \subseteq B(k)$ называется *разрешающим* для функции $f \in F_\pi(k)$, если для любой другой функции $g \in F_\pi(k)$ найдется $x \in T$, для которого $f(x) \neq g(x)$. Разрешающее множество функции f называется *тупиковым*, если никакое его собственное подмножество не является разрешающим для функции f.

Теорема 2. *Для любой пороговой функции двух переменных тупиковое разрешающее множество единственно и состоит либо из* 3*, либо из* 4 *точек.*

Доказательство теоремы 2 основано на следующей лемме, являющейся частным случаем теоремы из [5].

Лемма 3. *Тупиковое разрешающее множество пороговой функции f состоит из тех и только тех точек x, для каждой из которых найдется отличная от f пороговая функция g такая, что $f(x) \neq g(x)$ и $f(y) = g(y)$ для всех $y \neq x$.*

Работа поддержана грантом РФФИ, код проекта 0001-00599.

ЛИТЕРАТУРА

[1] Шевченко В.Н. О расшифровке пороговых функции многозначной логики. // Комбинаторно–алгебраические методы в прикладной математике. Горький: Горьк. гос. ун-т, 1987. С. 155–163.

[2] Золотых Н. Ю., Шевченко В. Н. Расшифровка пороговых функций k-значной логики. // Дискретный анализ и исследование операций. 1995. Т. 2 № 3. С. 18–23.

[3] Hegedüs T. Generalized teaching dimensions and the query complexity of learning. // Proc. 8 annual conf. on computational learning theory (COLT'95). New York: ACM Press, 1995. pp. 108–117.

[4] Шевченко В. Н., Золотых Н. Ю. О сложности расшифровки пороговых функций k-значной логики. // Доклады Академии наук. 1998. Т.362, № 5. С.606–608.

[5] Золотых Н. Ю., Шевченко В.Н. О нижней оценке сложности расшифровки пороговых функций k-значной логики. // Журнал вычислительной математики и математической физики. 1999. Т.39, №2. С.346–352.

[6] Hegedüs T. Geometrical concept learning and convex polytopes. // Proc. 7 annual conf. on computational learning theory (COLT'94). New York: ACM Press, 1994. pp. 228–236.

[7] Anthony, M., Brightwell, G., Shawe-Taylor, J. On specifying Boolean functions by labelled examples. // Discrete Applied Mathematics N.61 (1), 1995. pp. 1–25

[8] Золотых Н. Ю. Алгоритм расшифровки пороговой функции на плоскости с трудоемкостью $O(\log^2 k)$. Нижний Новгород: Нижегородский гос. ун-т, 1994 / Деп. ВИНИТИ 28.04.94. № 1062-В94. 11 с.

[9] Золотых Н. Ю. Алгоритм расшифровки пороговой функции k-значной логики на плоскости с числом обращений к оракулу $O(\log k)$. // Труды Первой Международной конференции "Математические алгоритмы". Н. Новгород: Изд-во Нижегородского ун-та, 1995. С. 21–26.

[10] Bultman W. J., Maass W. Fast identification of geometric objects with membership queries. // Information and computation. 1995. V. 118, N. 1, April. pp. 48–64.

[11] Золотых Н. Ю., Шевченко В. Н. Расшифровка пороговых функций и диофантовы приближения. // Вестник Нижегородского государственного университета. Математическое моделирование и оптимальное управление. 1998. Вып. 1 (18). С. 199–207.

[12] Шевченко В. Н.Качественные вопросы целочисленного программирования. М.: Физматлит, 1995. 192 с.

*Нижегородский государственный университет им. Н. И. Лобачевского, e-mail: zny@uic.nnov.ru

ПОИСК КОРРЕЛЯЦИОННО-ИММУННЫХ ФУНКЦИЙ

П. С. Королев*

1. Основные определения

Определение. Функция f называется уравновешенной, если количество наборов, на которых она принимает значение 0, равно количеству наборов, на которых она принимает значение 1.

Определение. Функция $f(x_1, \ldots, x_n) : \mathbb{B}^n \to \mathbb{B}$ называется корреляционно-иммунной порядка k, если $\forall\ 1 \le i_1 < \cdots < i_k \le n$ и $\forall\ \alpha_1, \ldots, \alpha_k \in \mathbb{B}$

$$\sum_{x_{i_1}=\alpha_1, \ldots, x_{i_k}=\alpha_k} f(\tilde{x}) = \mu = \text{const}.$$

Замечание. Для уравновешенных корреляционно-иммунных функций порядка k от n переменных $\mu = 2^{n-k-1}$.

Функцию f можно представлять различными способами, как таблицей значений, так и формулами в различных базисах.

Определение. Полиномом Жегалкина функции f называется ее представление в базисе $\{1, \wedge, \oplus\}$. Такое представление единственно с точностью до перестановки слагаемых, множителей и замены $x_i x_i \leftrightarrow x_i$.

Определение. Степенью вхождения переменной x_i в функцию $f(x_1, \ldots, x_n)$ будем называть максимальную степень одночлена, содержащего x_i в полиноме Жегалкина функции f. Обозначать мы ее будем $\deg_f x_i$.

Определение. Степенью многочлена Жегалкина функции f будем называть $\deg f = \max\limits_i \deg_f x_i$.

2. Связь корреляционно-иммунности и линейности

Теорема 1. [2] *Для любого натурального k существует неотрицательное целое число $p'(k)$, такое что для любого $n > k$ любая функция $f(x_1, \ldots, x_n)$, корреляционно-иммунная порядка $n-k$, может зависеть нелинейно не более чем от $p'(k)$ переменных.*

Теорема 2. (Неравенство Зигенталера) [1]. *Если булева функция $f(x_1, \ldots, x_n)$ — корреляционно-иммунная порядка k, то* $\deg f \leq n-k$.

Если при этом функция f уравновешенная и $n-k \geq 2$, то $\deg f \leq n-k-1$.

Поскольку нас не интересуют функции, содержащие переменные, входящие фиктивно или линейно ($\deg_f x_i = 0$ или 1), то мы будем рассматривать среди оставшихся самые простые — квадратичные: $\deg_f x_i = 2$.

Квадратичные функции можно записывать по-разному: и в виде списка значений, и в виде многочлена, и в виде таблицы коэффициентов многочлена и даже рисовать в виде графа, в котором вершинам соответствуют переменные, ребрам — одночлены $x_i x_j$, а петлям — одночлены x_k.

3. Таблица результатов

Целью работы был поиск всех квадратичных уравновешенных корреляционно-иммунных функций порядка k от n переменных при небольших значениях k и n, и, в первую очередь, в пограничных случаях — когда при изменении k или n на единицу число таких функций становилось равным нулю.

В результате была получена следующая таблица:

Количества квадратичных корреляционно-иммунных функций

k \ n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	-	-	4	13	+	+	+	+	+	+
1	-	-	-	1	9	147	+	+	+	+
2	-	-	-	-	-	2	23	+	+	+
3	-	-	-	-	-	-	-	6	+	+
4	-	-	-	-	-	-	-	-	-	+

Каждой клетке этой таблицы, в которой записано число, соответствует конкретный список функций. Причем среди этих функций не попадаются эквивалентные с точностью до перестановки индексов, и, видимо, поэтому для чисел в таблице не наблюдается какимх-либо очевидных закономерностей.

Таблица при этом имеет ступенчатый вид, поскольку функция, корреляционно-иммунная порядка k является корреляционно-иммунной порядков $k-1, k-2, \ldots, 0$. Также подстановкой константы вместо одной из переменной мы получаем из CI-k (корреляционно-иммунной порядка k) функции от n переменных CI-$(k-1)$ функцию от $n-1$ переменной.

Интерес представляет выяснение "угла наклона ступенек". Вполне возможно, что он равен $\frac{1}{2}$ и что не существует функций с $n < 2k+2$.

4. Методы получения функций

Представления функций. Поскольку в компьютере есть возможность производить побитовые операции параллельно, то имеет смысл использовать это преимущество, задавая строку значений не в виде массива *логических* переменных, а в виде `int`, `long` или массива таких *числовых* переменных.

1) Результат сложения двух функций $f_1 \oplus f_2$ вычисляется за 2^{n-5} операций, если f_1 и f_2 представлены в виде массивов `long` (32 бита).

2) Проверка на уравновешенность осуществляется за $\sim 2^{n-1}$ операций, если f представлена в виде массива `long`[1].

[1] Делая переход $N \mapsto (N-1)\,\&\,N$ ("&" — побитовая конъюнкция двоичных записей), мы убираем последнюю единицу, и количество операций получается равным количеству единиц, а не количеству бит.

Поскольку нас интересуют только квадратичные функции с точностью до прибавления 1, то $f(\tilde{x})$ представима в виде:

$$f(x_1, \ldots, x_n) = \bigoplus_{1 \le i \le j \le n} a_{ij} x_i x_j.$$

1) Функцию, получающуюся в результате подстановки констант вместо k переменных можно получить, убирая соответствующие строчку и столбцы и при необходимости изменяя диагональные элементы, поэтому сложность можно оценить как $(n-k)^2$.

2) Перевод в строчную запись осуществляется суммированием заранее вычисленных функций, соответствующих одночленам $x_i x_j$ и x_k. Сложность в худшем случае $\sim \frac{n(n+1)}{2} 2^{n-5} \sim n^2 2^{n-6}$.

3) Проверка на уравновешенность заключается в переводе в строчную запись и проверки в строчной записи. Сложность $\sim n^2 2^{n-6} 2^{n-1} = n^2 2^{2n-7}$.

"Лобовой" перебор. Всего надо рассмотреть $2^{\frac{n(n+1)}{2}}$ матриц, в каждой из них надо в каждой из C_n^k выборок переменных подставить 2^k вариантов значений, уменьшив за $(n-k)^2$ операций матрицу, переведя за $k^2 2^{k-6}$ операций ее в строчку и проверив эту строчку на уравновешенность за 2^{k-1} операций. Итого получается

$$\textit{Сложность} = 2^{\frac{n(n+1)}{2}} C_n^k 2^k \left((n-k)^2 + k^2 2^{k-6} + 2^{k-1} \right).$$

При $n = 9$, $k = 2$ получается сложность приблизительно 10^{18} операций, что, конечно, нереально воплотить в нормальное время. Даже если учитывать, что это — сложность в худшем случае, и что она не учитывает прекращения рассмотрения функций, у которых хотя бы одна подфункция оказалась неуравновешенной. Приходится изыскивать другие способы нахождения корреляционно-иммунных функций.

Добавление переменной. Поскольку при подстановке в CI-k функцию от n переменных вместо любой переменной константы получается CI-$(k-1)$ функция от $n-1$ переменной, то можно искать все CI-k функции от n переменных, добавляя переменную.

Пусть имеется CI-$(k-1)$ функция

$$f'(x_1,\ldots,x_{n-1}) = \bigoplus_{1\le i\le j\le n-1} a_{ij}x_ix_j.$$

Введем функцию f, полагая

$$f(x_1,\ldots,x_{n-1},x_n) := f'(x_1,\ldots,x_{n-1}) \oplus \bigoplus_{i=1}^{n} a_{in}x_ix_n.$$

Для того, чтобы проверить ее на CI-k, необходимо перебрать все возможные подстановки k констант вместо первых $n-1$ переменных. Вместо последней переменной подставлять константы не надо, потому что тогда получится проверка f' на CI-$(k-1)$. Таким образом, для проверки одного расширения f' получается

$$\textit{Сложность} = C_{n-1}^k 2^k \left((n-k)^2 + k^2 2^{k-6} + 2^{k-1}\right).$$

Если нам известны все CI-$(k-1)$ функции от $n-1$ переменной, и их $\mathcal{A}$ штук, то для нахождения всех CI-k функций от n переменных получается

$$\textit{Сложность} = \mathcal{A}2^n C_{n-1}^k 2^k \left((n-k)^2 + k^2 2^{k-6} + 2^{k-1}\right).$$

При $n=9$, $k=4$ эта сложность получается $\sim 10^8$, что вполне реально перебрать. Правда, для этого необходимо сначала вычислить все функции с $(n=5,k=0)$, $(n=6,k=1)$, $(n=7,k=2)$, $(n=8,k=3)$, но это тоже не занимает много времени.

Исключение повторов. При работе с помощью метода добавления переменных важно, чтобы рассматривалось как можно меньше функций предыдущего уровня. Хотя мы не можем изменить общее число таких функций, можно исключить из рассмотрения функциив эквивалентные с точностью до перестановки индексов переменных. То есть нас будет инересовать скорее не матрица коэффициентов, а граф на ненумерованных вершинах, который представляет данную функцию.

При этом необязательно перебирать все $n!$ перестановок, достаточно лишь рассмотреть перестановки внутри подмножеств, в которых $(a_{ii}, \sum\limits_{j=1}^{n} a_{ij}) = \text{const}$, то есть среди вершин, у которых есть или нет петли и заданная степень.

ЛИТЕРАТУРА

[1] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications. // IEEE Transactions on Information theory, V. IT-30, № 5, 1984, p. 776–780.

[2] Yu. Tarannikov. On the structure and numbers of higher order correlation-immune functions. // Proceedings of 2000 IEEE International Symposium on Information Theory ISIT2000, Sorrento, Italy, June 25–30, 2000, p. 185.

*Московский государственный университет им. М.В. Ломоносова, механико-математический факультет

РАСШИРЕНИЕ ДЛЯ НЕКОТОРЫХ ЗАМКНУТЫХ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ КЛАССА КОНСТАНТНЫХ НЕИСПРАВНОСТЕЙ С СОХРАНЕНИЕМ ЭФФЕКТИВНОСТИ ДИАГНОСТИКИ

А. М. Мошкова*

В работе рассматривается реализация булевых функций из замкнутых классов [3] схемами из функциональных элементов и изучается возможность расширения класса K константных неисправностей схем из функциональных элементов с сохранением эффективности диагностики.

Под расширением класса неисправностей будем понимать следующее. Пусть в случае константных неисправностей элемент, реализующий в исправном состоянии функцию f, в неисправном состоянии может реализовать любую функцию из множества $K(f)$, а в случае расширенного класса неисправностей — любую функцию из множества $X(f)$. Тогда $K(f) \subseteq X(f)$.

Пусть B — непустое конечное множество булевых функций и пусть S — схема из функциональных элементов над B, имеющая один выход. Число функциональных элементов в схеме S будем обозначать $L(S)$. Минимальную глубину дерева решений [2], решающего задачу диагностики схемы S относительно неисправностей некоторого класса X, будем обозначать $h_X(S)$. Схему из функциональных элементов будем называть *бесповторной*, если из каждого ее

элемента и из каждого входа выходит не более одной дуги, и входам приписаны попарно различные переменные.

Булеву функцию $f(x_1, \ldots, x_n)$ будем называть *квазимонотонной*, если существуют числа $\sigma_1, \ldots, \sigma_n \in E_2$ и монотонная булева функция $g(x_1, \ldots, x_n)$ такая, что $f(x_1, \ldots, x_n) = g(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n})$, где $x^\sigma = x$, если $\sigma = 1$, и $x^\sigma = \neg x$, если $\sigma = 0$. Константы 0 и 1, по определению, являются квазимонотонными функциями.

Непустое конечное множество булевых функций B будем называть *квазимонотонным*, если оно состоит только из квазимонотонных функций.

Непустое конечное множество булевых функций B будем называть *квазипримитивным*, если оно удовлетворяет хотя бы одному из следующих условий:

а) все функции множества B являются линейными функциями;

б) все функции множества B являются квазимонотонными функциями.

Пусть φ — формула над B, реализующая функцию $f \in U$. Тогда по формуле φ строится схема S над B, которая удовлетворяет следующим условиям:

а) схема S реализует функцию f;

б) $L(S) = L(\varphi)$, где $L(\varphi)$ — число функциональных символов в формуле φ;

в) из любого элемента схемы S выходит не более одной дуги.

Такую схему S будем называть схемой формульного типа.

В дополнение к обычному режиму работы схемы S рассматривается диагностический режим, при котором входы схемы S "расщепляются" и она становится бесповторной схемой $\tilde{S}$.

Пусть B — квазипримитивное множество. В [4] было показано, что существует константа c такая, что для любой бесповторной схемы из функциональных элементов S над B справедливо неравенство $h_K(S) \leq cL(S)$.

Предположим, что множество B не является квазипримитивным. В [4] было показано, что в этом случае существуют бесконечная последовательность $S_1, S_2, \ldots$ бесповторных схем из функциональных элементов над B и константа $c > 0$ такие, что $L(S_1) < L(S_2) < \ldots$ и для $i = 1, 2, \ldots$ справедливо неравенство $h_K(S_i) \geq 2^{cL(S_i)}$.

Далее мы будем рассматривать только реализацию булевых функций при помощи схем формульного типа над квазипримитивными

множествами и диагностику бесповторных схем из функциональных элементов.

Для квазипримитивного множества B булевых функций обозначим $\mathcal{C}_K(B)$ минимальное неотрицательное целое c такое, что для любой бесповторной схемы из функциональных элементов S над B справедливо неравенство $h_K(S) \leq cL(S)$.

В [4] было показано, что для любого замкнутого класса булевых функций U существует квазипримитивный базис B. Обозначим $\mathcal{C}_K(U) = \min \mathcal{C}_K(B)$, где минимум берется по всевозможным квазипримитивным базисам B класса U.

Базис B класса U будем называть *оптимальным базисом класса U относительно константных неисправностей*, если B — квазипримитивный базис и $\mathcal{C}_K(B) = \mathcal{C}_K(U)$.

Пусть U — замкнутый класс булевых функций и B — оптимальный относительно константных неисправностей базис класса U. Этот базис может быть использован для построения схем, которые реализуют функции из U и для которых существуют эффективные алгоритмы диагностики константных неисправностей на входах элементов.

Для бесповторной схемы $\tilde{S}$, полученной из схемы формульного типа S при помощи "расщепления" входов, справедливо отношение $h_K(\tilde{S}) \leq \mathcal{C}_K(U)L(\tilde{S}) = \mathcal{C}_K(U)L(\varphi)$.

В [5] показано, что если U — замкнутый класс булевых функций порядка $\rho \in \{2, 3\}$ и B — квазипримитивный базис порядка ρ класса U, состоящий из функций, существенно зависящих от всех своих переменных, то $\mathcal{C}_K(U) = \rho + 1$ и B — оптимальный базис класса U относительно константных неисправностей.

На основании этого результата в [5] оптимальные базисы были найдены для 40 замкнутых классов булевых функций. Не исследованными остались вырожденные классы, не содержащие функций, существенно зависящих от двух или более переменных (для таких классов задача построения оптимального базиса не представляет интереса), и классы F_i^μ, $i = 1, \ldots, 8$, $\mu = 3, 4, \ldots$.

Основной задачей, рассмотренной в данной работе, было изучение возможностей расширения класса константных неисправностей с сохранением эффективности диагностики. Получены следующие результаты. Пусть U — замкнутый класс булевых функций, имеющий квазимонотонный базис B (такие базисы существуют для всех

замкнутых классов булевых функций, кроме невырожденных классов, состоящих только из линейных функций). Обозначим Q класс квазимонотонных неисправностей, определяемый следующим образом. Функциональный элемент, реализующий в исправном состоянии квазимонотонную функцию $f(x_1,\ldots,x_n) = g(x_1^{\sigma_1},\ldots,x_n^{\sigma_n})$, где $g(x_1,\ldots,x_n)$ — монотонная функция, в неисправном состоянии может реализовать функцию $f'(x_1,\ldots,x_n) = g'(x_1^{\sigma_1},\ldots,x_n^{\sigma_n})$, где $g'(x_1,\ldots,x_n)$ — произвольная монотонная функция от n переменных.

Теорема 1. *Пусть B — непустое конечное множество квазимонотонных функций. Тогда существует константа c такая, что для любой бесповторной схемы из функциональных элементов S над B справедливо неравенство $h_Q(S) \le cL(S)$.*

Для квазимонотонного множества B обозначим $\mathcal{C}_Q(B)$ минимальное неотрицательное целое c такое, что для любой бесповторной схемы из функциональных элементов S над B справедливо неравенство $h_Q(S) \le cL(S)$. Для замкнутого класса U, для которого существует квазимонотонный базис, обозначим $\mathcal{C}_Q(U) = \min\mathcal{C}_Q(B)$, где минимум берется по всевозможным квазимонотонным базисам B класса U.

Базис B класса U будем называть *оптимальным базисом класса U относительно квазимонотонных неисправностей*, если B — квазимонотонный базис и $\mathcal{C}_Q(B) = \mathcal{C}_Q(U)$. Следующий результат получен с использованием работы [1].

Теорема 2. *Пусть U — замкнутый класс булевых функций порядка $\rho = 2$ ($\rho = 3$) и B — квазимонотонный базис порядка ρ класса U, состоящий из функций, существенно зависящих от всех своих переменных. Тогда $\mathcal{C}_Q(U) = 3$ ($\mathcal{C}_Q(U) = 6$) и B — оптимальный базис класса U.*

Разработан полиномиальный алгоритм, позволяющий по известным условным тестам, диагностирующим одноэлементные схемы в некотором квазимонотонном базисе, и произвольной бесповторной схеме в этом базисе построить за полиномиальное время выполняемый путь в условном тесте, диагностирующем квазимонотонные неисправности элементов рассматриваемой схемы.

Теперь пусть U — замкнутый класс, включающий в себя только линейные функции. Обозначим L класс линейных неисправностей,

определяемый следующим образом. Функциональный элемент, реализующий в исправном состоянии линейную функцию $f(x_1, \ldots, x_n)$, в неисправном состоянии может реализовать произвольную линейную функцию $g(x_1, \ldots, x_n)$.

Теорема 3. *Пусть B — непустое конечное множество линейных функций. Тогда существует константа c такая, что для любой бесповторной схемы из функциональных элементов S над B справедливо неравенство $h_L(S) \leq cL(S)$.*

Для множества B линейных функций обозначим $\mathcal{C}_L(B)$ минимальное неотрицательное целое c такое, что для любой бесповторной схемы из функциональных элементов S над B справедливо неравенство $h_L(S) \leq cL(S)$. Для замкнутого класса U, состоящего из линейных функций, обозначим $\mathcal{C}_L(U) = \min \mathcal{C}_L(B)$, где минимум берется по всевозможным базисам B класса U.

Базис B класса U, состоящего только из линейных функций, будем называть *оптимальным базисом класса U относительно линейных неисправностей*, если $\mathcal{C}_L(B) = \mathcal{C}_L(U)$.

Теорема 4. *Пусть U — замкнутый класс булевых функций порядка $\rho \in \{2, 3\}$, состоящий только из линейных функций, и B — базис порядка ρ класса U, состоящий из функций, существенно зависящих от всех своих переменных. Тогда $\mathcal{C}_L(U) = \rho + 1$ и B — оптимальный базис класса U.*

Таким образом, для замкнутых классов булевых функций, имеющих базисы, состоящие только из квазимонотонных функций, мы можем, сохраняя эффективность диагностики, расширить класс константных неисправностей, допуская реализацию неисправными элементами произвольных квазимонотонных функций от того же числа переменных со следующим ограничением: набор $\sigma_1, \ldots, \sigma_n \in E_2^n$, определяющий наличие отрицаний над переменными $x_1, \ldots, x_n$ исходной функции, должен сохраняться неизменным и для новой функции. Для замкнутых классов булевых функций, включающих в себя только линейные функции, мы можем расширить класс константных неисправностей, добавив возможность замены исходной функции, реализуемой элементом, на произвольную линейную функцию, зависящую от тех же переменных.

Используя утверждения теорем 4 и 5, можно показать, что базисы замкнутых классов, приведенные в [5], являются оптимальными

и относительно рассматриваемых расширений класса константных неисправностей.

В настоящее время проверяется гипотеза о том, что дальнейшее расширение таких классов неисправностей с сохранением эффективности диагностики невозможно.

Работа выполнена при финансовой поддержке ФЦП "Интеграция" (проект АО110), РФФИ (проект 99-01-00820) и программы "Университеты России" (проект 015.04.01.76).

ЛИТЕРАТУРА

[1] Ансель Ж. О числе монотонных булевых функций n переменных. // Кибернетический сборник. Новая серия. Выпуск 5. Москва: изд-во "Мир", 1968. С. 53-57.

[2] Мошков М. Ю. Деревья решений. Теория и приложения. Нижний Новгород: изд-во ННГУ, 1994.

[3] Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. М.: Наука, 1966.

[4] Moshkov M. Diagnosis of constant faults of circuits. // Proceedings of Fourth International Workshop on Rough Sets, Fuzzy Sets and Machine Discovery. Tokyo, Japan, 1996. P. 325-327.

[5] Moshkov M., Moshkova A. Optimal bases for some closed classes of Boolean functions. // Proceedings of the Fifth European Congress on Intelligent Techniques and Soft Computing. Aachen, Germany, 1997. P. 1643-1647.

*Нижегородский государственный университет им. Н.И. Лобачевского

О МИНИМАЛЬНЫХ ЕДИНИЧНЫХ ДИАГНОСТИЧЕСКИХ ТЕСТАХ ДЛЯ НЕКОТОРЫХ КЛАССОВ КОНТАКТНЫХ СХЕМ

Д. С. Романов

В работах [2, 3] С. А. Ложкиным и Д. С. Романовым предложен метод построения единичных диагностических тестов для некоторых

классов блочных контактных схем. В настоящей работе формулируется результат, развивающий применение данного метода.

В работе рассматриваются двухполюсные блочные КС, которые строятся путем "последовательного присоединения" друг к другу базовых схем, называемых блоками (множество всех различных блоков образует базис) и применения операции "усечения", заключающейся в выделении одного входа и одного выхода схемы и удалении тех контактов схемы, которые не принадлежат ни одной проводящей цепи, ведущей от выделенного входа к выделенному выходу. Блочная КС называется периодической, если последовательность типов ее блоков периодическая без предпериода (этот термин также будет применяться к блочным КС, полученным как "усечение" периодических). Блочная КС S называется каскадной блочной контактной схемой (КБКС), если каждый ее блок управляется одной переменной, разные блоки управляются разными переменными, всякий контакт блока соединяет какой-то вход блока с каким-то выходом, и каждому входу блока инцидентны либо два противоположных контакта, либо один контакт.

"Сдвиговым" $2d$-полюсным блоком H_d^{ε} называется КС с d входами и d выходами, пронумерованными числами от 0 до $d-1$, управляемая своей переменной x и такая, что всякий вход i соединен с выходом i размыкающим контактом переменной x, т. е. контактом вида $\bar{x}$, и всякий вход i соединен с выходом $i+\varepsilon \pmod d$ $(\varepsilon \in \{1,\dots,d-1\})$ замыкающим контактом переменной x, т. е. контактом вида x (при этом величина ε называется сдвигом блока H_d^{ε}).

Пусть A, B, T — натуральные постоянные. Обозначим через $\Sigma(A,B,T)$ класс периодических двухполюсных КБКС из "сдвиговых" блоков такой, что

- длина периода каждой из схем не превышает T,
- если основной период Π_d схемы имеет вид $H_d^{\varepsilon_1}, H_d^{\varepsilon_2}, \dots, H_d^{\varepsilon_\tau}$, то выполнено соотношение

$$\min_{\substack{(\varepsilon_{i_1},\varepsilon_{i_2},\dots,\varepsilon_{i_k}),\\ 1\le i_1\le i_2\le\dots\le i_k\le\tau,\\ k=\overline{1,A}}} НОД\left(\sum_{\nu=1}^{k}\varepsilon_{i_\nu};d\right)\le B.$$

Длину минимального диагностического теста для схемы S и источника неисправностей, допускающего одно размыкание, будем обо-

значать через $l^p(S)$, а длину минимального диагностического теста для схемы S и источника неисправностей, допускающего одно замыкание, будем обозначать через $l^3(S)$.

Используя полученные С. М. Вартаняном [1] нижние оценки длин тестов, можно сформулировать следующую теорему.

Теорема. *Пусть $\hat{S}_n(\Pi_d)$ — двухполюсная периодическая КБКС с базисом из "сдвиговых" $2d$-полюсных блоков, принадлежащая классу $\Sigma(A, B, T)$. Тогда при $n \to \infty$ и d таком, что $\log_2 d = O\left(\sqrt{\log_2 n}\right)$, имеют место соотношения:*

$$l^p(\hat{S}_n(\Pi_d)) \asymp \frac{d \log_2 n}{\log_2 d}, \qquad l^3(\hat{S}_n(\Pi_d)) \asymp \frac{d \log_2 n}{\log_2 d}.$$

Работа поддержана грантом РФФИ № 99-01-01111.

ЛИТЕРАТУРА

[1] Вартанян С. М. Единичные диагностические тесты для последовательных блочных схем. Дисс. на соиск. уч. ст. к. ф.-м. н. М.: МГУ, 1987 г. 114 с.

[2] С. А. Ложкин, Д. С. Романов. Об одном методе построения единичных диагностических тестов для некоторого класса блочных контактных схем. // Труды IV Международной конференции "Дискретные модели в теории управляющих систем" (19–25 июня 2000 г.). М.: "МАКС-Пресс", 2000. С. 114–116.

[3] Романов Д. С. Построение тестов и оценка их параметров для некоторых классов контактных схем. Дисс. на соиск. уч. ст. к. ф.-м. н. М.: МГУ, 2000 г. 114 с.

*Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики

О ГЛУБИНЕ И СЛОЖНОСТИ ФОРМУЛ В НЕКОТОРЫХ КЛАССАХ k-ЗНАЧНОЙ ЛОГИКИ

Р. Ф. Сафин*

Пусть $\mathfrak{A}$ — конечная система функций из P_k, $k \geq 2$, Φ — формула над $\mathfrak{A}$. Обозначим через $L(\Phi)$ число символов переменных и констант, входящих в Φ. Будем называть $L(\Phi)$ *сложностью формулы* Φ. *Глубину формулы* $D(\Phi)$ определим рекуррентно: $D(\Phi) = 0$, если Φ состоит из одного символа (константы или переменной); $D(\Phi) = 1 + \max\limits_{1 \leq i \leq k} D(\Phi_i)$, если формула Φ имеет вид $\varphi(\Phi_1, \Phi_2, \ldots, \Phi_k)$, где $\varphi \in \mathfrak{A}$. Через $[\mathfrak{A}]$ обозначим замыкание системы $\mathfrak{A}$ относительно операции суперпозиции. Пусть f — функция из $[\mathfrak{A}]$. Положим $L_{\mathfrak{A}}(f) = \min L(\Phi)$, $D_{\mathfrak{A}}(f) = \min D(\Phi)$, где минимум берется по всем формулам Φ над $\mathfrak{A}$, которые реализуют функцию f. Систему $\mathfrak{A}$ назовем *равномерной*, если существуют такие константы c и d (зависящие только от системы $\mathfrak{A}$), что для всех функций f из $[\mathfrak{A}]$ выполнено неравенство

$$D_{\mathfrak{A}}(f) \leq c \log_2 L_{\mathfrak{A}}(f) + d.$$

Известно, что любая полная в P_2 конечная система функций равномерна (см., например, [1]). В [2] доказано, что любая конечная система функций из P_2 равномерна. Аналогичный результат для всех конечных систем функций из P_k, где $k \geq 3$, уже не имеет места (см. [2]). Автором аналогичный результат доказан для конечных систем функций, являющихся порождающими для некоторых предполных классов k-значной логики.

Все предполные классы в P_3 описаны в [3], все семейства предполных классов в P_k — в [4] (см. также [5]). Будем пользоваться обозначениями из [5], согласно которым в P_k имеются следующие семейства предполных классов: 1) классы самодвойственных функций — классы типа $\mathbb{P}$; 2) классы монотонных функций — классы типа $\mathbb{O}$; 3) классы линейных функций — классы типа $\mathbb{L}$; 4) классы функций, сохраняющих разбиения множества E_k, — классы типа $\mathbb{E}$; 5) классы функций, сохраняющих центральные отношения, — классы типа $\mathbb{C}$; 6) классы функций, сохраняющих сильно гомоморфные прообразы h-адических элементарных отношений, — классы типа $\mathbb{B}$. Через A_ρ будем обозначать класс функций, сохраняющих отношение ρ. Если ρ — отношение частичного порядка на E_k, такое, что су-

ществуют единственный максимальный и единственный минимальный элементы и для любых двух элементов a и b из E_k существуют $\sup(a,b)$ и $\inf(a,b)$ относительно порядка ρ, то будем говорить, что A_ρ — *класс типа* $\mathbb{O}^*$. Нетрудно показать, что наименьшее число k, для которого в P_k существует класс типа $\mathbb{O}$, не являющийся классом типа $\mathbb{O}^*$, равно 6. Будем называть A_τ *классом типа* $\mathbb{C}_2$, если τ — бинарное центральное отношение. Будем называть A_σ *классом типа* $\mathbb{C}_1$, если σ — унарное центральное отношение (т.е. унарное отношение, отличное от E_k и $\emptyset$).

Основным результатом является следующая теорема.

Теорема 1. *Пусть* $\mathfrak{A}$ — *конечная система функций из* P_k $(k \geq 3)$ *и* $[\mathfrak{A}]$ *принадлежит одному из семейств:* $\mathbb{E}$, $\mathbb{B}$, $\mathbb{O}^*$, $\mathbb{L}$, $\mathbb{P}$, $\mathbb{C}_1$, $\mathbb{C}_2$. *Тогда* $\mathfrak{A}$ — *равномерная система.*

Следствие 1. (см. также [6]). *Пусть* $\mathfrak{A}$ — *конечная система функций из* P_3 *и* $[\mathfrak{A}]$ — *предполный класс в* P_3. *Тогда* $\mathfrak{A}$ — *равномерная система.*

Замечание. Используя двойственность некоторых предполных классов, нетрудно проверить, что для доказательства аналогичного факта для P_4 остается доказать равномерность порождающих систем для классоа A_ρ, где матрица $M(\rho)$ отношения ρ имеет следующий вид

$$M(\rho) = \begin{pmatrix} 1 & 2 & 2 & 3 & 3 & 1 \\ 2 & 1 & 3 & 2 & 1 & 3 \\ 3 & 3 & 1 & 1 & 2 & 2 \end{pmatrix}^T$$

(строками матрицы $M(\rho)$ являются наборы из ρ).

В заключение автор выражает искреннюю благодарность профессору А.Б. Угольникову за постановку задачи и обсуждение результатов работы.

ЛИТЕРАТУРА

[1] Pratt V.R. The effect of basis on size of Boolean expressions. // 16th Ann. Symp. Found. Comput. Sci. 1975. New York. N.Y., 1975. 119–121. (Рус. пер.: *Пратт В. П.* Влияние базиса на сложность булевых формул. // Кибернет. сб. (новая серия). Вып. 17. М.: Мир, 1980. 114–123.)

[2] Угольников А. Б. О глубине и полиномиальной эквивалентности формул для замкнутых классов двузначной логики. // Матем. заметки. 1987. **42**, №4. 603–612.

[3] Яблонский С. В. Функциональные построения в k-значной логике. // Тр. Матем. ин-та РАН имени В. А. Стеклова. 1958. **51**. 3–142.

[4] Rosenberg I. Über die funktionale Vollständigkeit in den mehrvertigen Logiken. // Rozpravy Československě Academie věd. Rada matematickych a přirodnich věd. Praha, 1970, Ročnik 80, Sešit 4. 3–93.

[5] Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. М.: Изд-во МЭИ, 1997.

[6] Ахметова Л. И. О глубине формул для предполных классов трехзначной логики. // Методы и системы технической диагностики. Вып. 18. Саратов: Изд-во Саратовского ун-та, 1993. 19–20.

*Московский государственный университет им. М.В. Ломоносова, механико-математический факультет, e-mail: rin@au.ru

ПОЛИНОМИАЛЬНЫЙ АЛГОРИТМ ДЛЯ РАСПОЗНАВАНИЯ ПРИНАДЛЕЖНОСТИ ПРЕДСТАВЛЕННОЙ ПОЛИНОМОМ ФУНКЦИИ k-ЗНАЧНОЙ ЛОГИКИ ПРЕДПОЛНЫМ КЛАССАМ ЛИНЕЙНЫХ ФУНКЦИЙ

С. Н. Селезнева

1. Введение

В настоящей заметке представлен результат о существовании алгоритма с полиномиальной временной сложностью для решения задачи распознавания принадлежности функции k-значной логики, представленной полиномом, предполным классам линейных функций.

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$. Функцию $f(x_1, \ldots, x_n)$, определенную на E_k^n и принимающую значения из E_k, назовем функцией

k-значной логики. Множество всех функций k-значной логики обозначим через P_k.

Множество P_k рассматривается как функциональная система с операцией суперпозиции [1]. Пусть $M \subseteq P_k$. Множество M называется полным, если каждая функция k-значной логики может быть получена суперпозицей из функций множества M. По критерию полноты [2] множество M полно, если и только если оно целиком не содержится ни в одном из конечного числа предполных классов. Следовательно, задача распознавания полноты множества M сводится к конечному числу задач распознавания принадлежности функций множества M предполным классам. Все предполные классы конструктивно описаны [1, 3 – 7]. Они разделены на 6 семейств: предполные классы монотонных, самодвойственных, линейных функций, функций, сохраняющих разбиение, типа B и типа C.

Алгоритмическая сложность решения задачи распознавания полноты конечных множеств функций k-значной логики зависит от способа представления функций. Если функции представлены в виде формул в общем случае и даже в виде определенных форм (конъюнктивных или дизъюнктивных нормальных форм), то уже в двузначной логике задача оказывается NP-полной [8]. Заметим, что при перечисленных представлениях функций двузначной логики NP-полной является и задача распознавания нелинейности функции. Автором было доказано [9, 10], что при представлении функций k-значных логик полиномами задачи распознавания принадлежности функции четырем семействам предполных классов, а именно классам монотонных, самодвойственных функций, функций, сохраняющих разбиение, и классам типа B, имеют полиномиальное решение. В настоящей заметке представлен аналогичный результат для предполных классов линейных функций.

2. О предполных классах линейных функций

Предполный класс линейных функций двузначной логики был определен Э. Постом [3]. В k-значной логике часть предполных классов линейных функций была описана С. В. Яблонским [1], окончательно все предполные классы линейных функций k-значной логики описал Ло Чжу-Кай [5].

Пусть на множестве E_k задана абелева группа $G =< E_k, \oplus >$ с нулем 0. Пусть $\ominus a$ обозначает элемент группы G, обратный к элементу a ($a \in E_k$) Будем говорить, что функция k-значной логики $f(x_1, \ldots, x_n)$ *линейна по отношению к группе* G, если верно тождество

$$f(x_1 \oplus y_1, \ldots, x_n \oplus y_n) = f(x_1, \ldots, x_n) \oplus f(y_1, \ldots, y_n) \ominus f(0, \ldots, 0).$$

Обозначим посредством L_G множество всех линейных по отношению к группе G функций.

Пусть теперь $k = p^h$, где p — простое число, $h \geq 1$, и в группе G каждый ненулевой элемент имеет порядок p. В этом случае к операции сложения $\oplus$ в группе G можно так добавить операцию умножения $\otimes$, что множество E_k относительно них образует поле $F =< E_k, \oplus, \otimes >$. Верны следующие теоремы 1 и 2.

Теорема 1. [11] *Пусть $k = p^h$, где p — простое число, $h \geq 1$, $G =< E_k, \oplus >$ — абелева группа над множеством E_k, каждый ненулевой элемент которой имеет порядок p. Тогда множество L_G — предполный класс.*

Теорема 2. [11] *Пусть $k = p^h$, где p — простое число, $h \geq 1$, $F =< E_k, \oplus, \otimes >$ — поле над множеством E_k. Функция k-значной логики $f(x_1, \ldots, x_n)$ линейна по отношению к группе $G =< E_k, \oplus >$, если и только если она представима в виде*

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{i=1}^{n} \bigoplus_{j=0}^{h-1} a_{ij} \otimes x_i^{p^j}.$$

В теореме 1 определяются все возможные предполные классы линейных функций k-значной логики. Теоремой 2 описывается явный вид полиномов (относительно операций поля F $\oplus$ и $\otimes$) функций k-значной логики, принадлежащих определенному предполному классу линейных функций.

3. О представлении функций k-значной логики полиномами

Зададим способ представления функций k-значной логики.

Функции k-значной логики будем записывать полиномами, т. е. в виде $\sum_{i=1}^{l} c_i \cdot x_{i_1}^{m_{i_1}} \cdot \ldots \cdot x_{i_{r_i}}^{m_{r_i}}$. Каждую функцию k-значной логики можно представить полиномом и однозначно (с точностью до порядка слагаемых и сомножителей в слагаемых) если и только если $k = p^h$, где p — простое число, $h \geq 1$ (ссылка в [12]). При таких значениях k на множестве E_k можно ввести двуместные операции $+$ и $\cdot$, относительно которых E_k образует поле $\hat{F} = (E_k, +, \cdot)$. Полиномы, представляющие функции k-значной логики, являются полиномами относительно операций поля $\hat{F}$. Таким образом, и требование представления функции k-значной логики полиномом, и требование существования предполных классов линейных функций накладывают одно и то же ограничение на значность логики, а именно $k = p^h$, где p — простое число, $h \geq 1$.

4. О сложности распознавания принадлежности полинома функции k-значной логики предполным классам линейных функций

Задача состоит в следующем. Задана функция k-значной логики, представленная полиномом. Требуется выяснить, с какой временной сложностью можно распознать, принадлежит ли она определенному предполному классу линейных функций.

В качестве формальной алгоритмической модели будем рассматривать многоленточные детерминированные машины Тьюринга (МТ).

Пусть $A = \{x, 0, 1, \ldots, k-1, \uparrow, +, \cdot\}$ — алфавит символов МТ. Функцию k-значной логики $f(x_1, \ldots, x_n)$ перепишем словом α_f в алфавите A, внеся следующие изменения в ее полином: индексы переменных запишем числами в системе счисления по основанию k, перед показателями степени укажем символ $\uparrow$, все надстрочные и подстрочные символы напишем в строчку. Под длиной слова α в алфавите A будем понимать число символов в нем.

Теорема 3. *Пусть $k = p^h$, где p — простое число, $h \geq 1$, $F =< E_k, \oplus, \otimes >$ — поле над множеством E_k. Существует детерминированная МТ, которая для каждого слова α_f в алфавите A с полиномиальной временной сложностью определяет, функция $f(x_1, \ldots, x_n)$ является линейной по отношению к группе $G =< E_k, \oplus >$ или нет.*

Работа поддержана грантом РФФИ, код проекта 00-01-00351.

ЛИТЕРАТУРА

[1] Яблонский С. В. Функциональные построения в k-значной логике. // Труды Матем. института им. В. А. Стеклова АН СССР (1958) 51. С. 5–142.

[2] Кузнецов А. В. О проблемах тождества и функциональной полноты алгебраических систем. В кн. Труды 3-го всесоюзного матем. съезда, т.2. М., издательство АН СССР, 1956. С. 145–146.

[3] Post E. Introduction to a General Theory of ElementaryPropositions. Amer. Journ. Mathem. (1921) 43, pp. 163–185.

[4] Мартынюк В. В. Исследование некоторых классов в многозначных логиках. // Проблемы кибернетики (1960) 3. С. 49–60.

[5] Lo Czu Kai. Precompleteness of a Set and Rings of Linear Functions. // Acta bf. natur Univ. Jilinensis (1963) 2.

[6] Rosenberg I. La structur des fonctions de plusieurs variables sur un Ensemble fini. // Comptes Rendus, de l'Academ. Paris (1965) 260, Pp. 3817–3819.

[7] Rozenberg I. Über die funktionale Vollständigkeit in der mehrvertigen Logiken. // Rozpravy Česko-slovenskě Academie vď. Rada matematickych a přirodnich věd. Praga, 1970, ročnic 80, Sešit 4, 3–93.

[8] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М., Мир, 1982.

[9] Селезнева С. Н. Полиномиальный алгоритм для распознавания принадлежности реализованной полиномом функции k-значной логики предполным классам самодвойственных функций. // Дискретная математика (1998) 10, № 3. С. 64–72.

[10] Селезнева С. Н. О сложности распознавания функций многозначных логик, сохраняющих некоторые предикаты. // Труды IV Международной конференции "Дискретные модели в теории управляющих систем" (Красновидово, 2000). М., МАКС Пресс. С. 119–122.

[11] Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. М., МЭИ, 1997.

[12] Лидл Р., Нидеррайтер Г. Конечные поля. М., Мир, 1988.

*Московский государственный университет им. М.В. Ломоносова, факультет вычислительной математики и кибернетики

АЛГОРИТМ ПРОВЕРКИ РАЗРЕШИМОСТИ СИСТЕМ ЭЛЕМЕНТАРНЫХ НЕРАВЕНСТВ

Е. С. Смирнова*, Н. К. Косовский*

Введение

Во многих областях науки приходится иметь дело с различными системами равенств или неравенств. Зачастую исследователя не столько интересует конкретное решение данной системы, сколько сам факт ее разрешимости или неразрешимости. Такой подход используется, например, для проверки совместности набора условий или выявления факта одновременного выполнения ряда событий. Одним из классических примеров является задача о наличии общих точек у двух и более кривых или поверхностей — не всегда нужно знать конкретные точки, зачастую бывает достаточно установить тот факт, что кривые или поверхности вообще не пересекаются или общие точки все же существуют.

Говоря о системах равенств или неравенств, можно заметить, что наиболее распространенными и известными среди них являются линейные системы. Авторы предлагают рассмотреть один из простейших, но также нередко используемых частных случаев линейных систем, когда все неравенства имеют вид $\alpha \prec \beta$, где в роли α и β могут выступать константы или переменные (возможно со знаком), а знак сравнения $\prec$ является строгим или нестрогим неравенством . В силу простого вида, назовем такие системы *"линейными системами элементарных неравенств"*.

Настоящая статья предлагает один из методов установления совместности или несовместности систем такого вида. Решение задачи, столь простой на первый взгляд, усложняется с ростом количества неравенств, участвующих в системе, а также за счет ряда дополнительных условий, накладываемых на систему. В качестве примера использования таких систем можно привести задачу проверки упорядоченности множества объектов, где в качестве критерия упорядоченности могут выступать одновременно несколько параметров. Также свое применение системы элементарных неравенств и задача об их неразрешимости нашли в областях искусственного интеллекта и многоуровневых логиках, обрабатывающих нечеткие данные [1].

Простота исходной системы позволила получить эффективный алгоритм проверки ее совместности. Добавим также, что к настоящему моменту первым автором доклада создан машинный алгоритм, реализующий предложенный метод и выполняющий проверку за полиномиальное время (Теорема 2 из [2]). Программа алгоритма написана в двух вариантах (консольного и оконного) и предназначена для работы в операционных системах DOS и Windows соответственно.

Описание метода установления неразрешимости систем

Теперь непосредственно опишем сам метод. Пусть дана система элементарных неравенств S:

$$\begin{cases} x_{11} & \prec_1 x_{12}, \\ & \dots \\ x_{i1} & \prec_i x_{i2}, \\ & \dots \\ x_{n1} & \prec_n x_{n2}, \end{cases}$$

где x_{ij} для $i = \{1, 2, ...n\}, j = \{1, 2\}$ является переменной (возможно со знаком) или константой, а знак сравнения $\prec_i \in \{<, \leq\}$.

Иногда бывает полезно рассматривать эту систему не на всей числовой оси, а на заданном интервале [**a**,**b**]. В качестве частного случая могут быть рассмотрены только целые или рациональные числа из этого промежутка. Тогда обозначим множество $[\mathbf{a}, \mathbf{b}] \cap \mathbf{Z}(\mathbf{Q})$ как **D** (домен интерпретаций) и будем исследовать разрешимость системы S на этом множестве. (Условимся, что если промежуток $[\mathbf{a}, \mathbf{b}]$ не задан, то множество **D** неограниченно и представляет все целые или рациональные числа).

1. На первом шаге алгоритма исходная система S трансформируется в симметричную, что в дальнейшем позволит получить наиболее эффективную процедуру ее обработки. Преобразование происходит по следующей схеме:

1.1. Если задан интервал [**a**,**b**], то он переводиться в симметричный относительно нуля отрезок [-**k**,**k**], где $\mathbf{k} = (\mathbf{b} - \mathbf{a})/2$. Также пересчитываются все константы исходной системы S — производиться сдвиг на $(\mathbf{a} + \mathbf{b})/2$ в результате чего мы получим систему S_1. (Очевидно, на неразрешимость системы параллельный перенос значений

ее констант и переменных не влияет, следовательно, если разрешима система S, то разрешима и новая система S_1 и наоборот). Если же интервал $[\mathbf{a}, \mathbf{b}]$ не задан, то такое преобразование не выполняется.

1.2. Если необходимо учесть тот факт, что множество $\mathbf{D}$ ограниченно, и разрешимость системы S_1 рассматривается на множестве [-$\mathbf{k}$,$\mathbf{k}$], то для каждой переменной x системы S_1 добавляется ограничительное двойное неравенство $-\mathbf{k} \leq x \leq \mathbf{k}$. В противном случае (множество $\mathbf{D}$ неограниченно) этот пункт также пропускается.

1.3. И, независимо от граничных условий, для каждого неравенства $x \prec y$ добавляется противоположное ему неравенство $-y \prec -x$, в результате чего получается система S', эквивалентная исходной.

Таким образом система S' имеет вид:

$$\begin{cases} x'_{11} \prec_1 x'_{12}, & -x'_{12} \prec_1 -x'_{11}, \\ \quad \ldots\ldots\ldots & \quad \ldots\ldots\ldots \\ x'_{i1} \prec_i x'_{i2}, & -x'_{i2} \prec_i -x'_{i1}, \\ \quad \ldots\ldots\ldots & \quad \ldots\ldots\ldots \\ x'_{n'1} \prec_{n'} x'_{n'2}, & -x'_{n'2} \prec_{n'} -x'_{n'1}, \end{cases}$$

где x'_{ij} для $i = \{1, 2, \ldots n'\}, j = \{1, 2\}$ по-прежнему являются переменными (возможно со знаком) или константами, а знак сравнения $\prec_i \in \{<, \leq\}$.

2. Следующим шагом алгоритма будет преобразование построенной симметричной системы в нагруженный ориентированных граф $G_{S'}$ по следующему принципу:

В качестве вершин графа $G_{S'}$ рассматриваются все переменные и константы, встречающиеся в системе S' (x и $-x$ представляют различные вершины), а дуга между вершинами α и β добавляется, если система S' содержит неравенство $\alpha \prec \beta$, и дуга (α, β) помечается знаком соответствующего неравенства.

3. Далее построенный по системе S' граф $G_{S'}$ тестируется на наличие в нем всевозможных противоречий с целью выявления неразрешимости исходной системы неравенств. Ниже приведены случаи, позволяющие установить несовместность системы S':

3.1. В графе $G_{S'}$ обнаружен цикл, одна из дуг которого помечена знаком строгого неравенства.

Пример: $a \leq b \leq c < a$. Очевидно, что наличие такого цикла влечет несовместность системы S'.

3.2. Граф $G_{S'}$ содержит цикл с двумя различными константами.

Пример: $a \leq 3 \leq b \leq 4 \leq a$. Присутствие такого цикла также выявляет неразрешимость S'.

3.3. Если в графе $G_{S'}$ есть цикл, содержащий две противоположные переменные и ненулевую константу, несовместность также очевидна.

Пример: $-x \leq 5 \leq x \leq -x$.

3.4. Граф $G_{S'}$ содержит путь между двумя константами, такими, что значение константы в начале пути больше значения на конце.

Пример: $8 \leq a < b < 3$.

3.5. Это условие рассматривается только для целочисленных значений констант и переменных (когда $\mathbf{D} \subseteq \mathbf{Z}$):

$G_{S'}$ содержит путь между двумя константами, разность между которыми меньше длины пути, измеренной в количестве дуг, помеченных знаком строгого неравенства.

Пример: $1 \leq a < b < 3$, не существует два различных целых числа, которые бы можно было расположить между 1 и 3.

Во всех перечисленных выше случаях описаны ситуации, позволяющие сразу установить несовместность рассматриваемой системы элементарных неравенств. Следующие три не выявляют неразрешимость, но позволяют упростить исходную систему, удалив из нее все циклы, не отвечающих условиям 1-3:

3.6.1. Если в графе обнаружен цикл, не содержащий строгих неравенств и констант, отличных от нуля, но имеющий две противоположные переменные или константу 0, то весь этот цикл удаляется из графа и замещается единственной вершиной, содержащей ноль. (Одновременно из системы удаляются все соответствующие циклу неравенства, а все участвующие в них переменные заменяются нулем).

Например циклы $a \leq -x \leq b \leq x \leq a$ и $a \leq b \leq 0 \leq c \leq a$ будут заменены на единственную вершину, содержащую 0, что позволит сократить систему сразу на 4 неравенства.

3.6.2. Если в графе обнаружен цикл, не содержащий строгих неравенств и противоположных переменных, но имеющий единственную константу, отличную от нуля, то весь этот цикл заменяется единственной вершиной, содержащей эту константу. (Аналогично предыдущему случаю из системы удаляются все неравенства, соответствующие циклу, а все встречающиеся в них переменные заме-

няются этой константой).

К примеру цикл $a \leq b \leq 5 \leq a$ будет заменен на вершину, содержащую константу 5, а переменные a и b, встречающиеся в системе S', также будут замещены этим значением. При этом размер системы сократиться не на 3, а сразу на 6 неравенств, так как в силу симметрии системы граф также должен содержать цикл $-a \leq -5 \leq -b \leq -a$, который также следует заменить вершиной -5.

3.6.3. Если граф содержит цикл, в котором все дуги помечены нестрогим неравенством, и нет ни констант, ни пар противоположных переменных, то весь цикл замещается одной вершиной, содержащей новую переменную, а симметричный ему цикл заменяется на противоположную переменную.

Пример: цикл $a \leq b \leq c \leq a$ будет замещен новой уникальной переменной New, а симметричный цикл $-a \leq -c \leq -b \leq -a$ преобразуется в вершину с переменной $-New$. А в системе S' вместо переменных a, b, c проявиться их единый "заменитель" — переменная New. То же произойдет и с членами $-a, -b, -c$, которые будут удалены из S', а вместо них появиться новый член $-New$.

В целом процедура исследования графа выглядит так:

• Вначале в нем выявляются все циклы (для большей эффективности можно обрабатывать компоненты сильной связности[2]), если в каком-то из обнаруженных циклов выполняется одно из условий 3.1–3.3, то очевидно выявлено противоречие, и система S' несовместна.

• Если же ни один из циклов не удовлетворяет условиям 3.1–3.3, то в нем имеет место одна из схем 3.6.1–3.6.3, что позволит сокращать граф и систему до тех пор, пока в нем не останется ни одного цикла.

• На следующем этапе исследуется ациклический граф на предмет обнаружения в нем "противоречивых" путей между двумя константами. Для общего случая это пункт 3.4, а для целочисленного 3.4 и 3.5. Если противоречие выявлено, то система, очевидно, неразрешима.

• Если же ни одного противоречия не выявлено, то согласно Теореме 1 из [2], система имеет как минимум одно решение. Таким образом, рассмотренные случаи являются необходимым и достаточным условием для неразрешимости системы S', а в силу ее эквивалентности системе S, то и неразрешимости самой S.

Некоторые частные случаи домена интерпретаций D

Отдельного внимания достойны частные случаи множества, на котором рассматривается разрешимость системы S. Некоторые из них уже были рассмотрены (случай неограниченного домена $\mathbf{D}$, сужение на заданный интервал $[\mathbf{a}, \mathbf{b}]$, сужение на симметричный относительно нуля интервал [-$\mathbf{k}$,$\mathbf{k}$], а также целочисленный случай).

Интересен и еще один вариант домена $\mathbf{D}$, когда рассматривается симметричное относительно нуля множество, но сам ноль в него не входит. Такой подход используется при описании некоторых практических и прикладных задач, когда равенство нулю переменных недопустимо. Таким образом, $\mathbf{D}$ будет иметь вид $\mathbf{Z}(\mathbf{Q})/\{0\}$ или $[-\mathbf{k}, \mathbf{k}] \cap \mathbf{Z}(\mathbf{Q})/\{0\}$.

Отсутствие нуля в домене интерпретаций накладывает дополнительные условия на алгоритм проверки неразрешимости системы, что иногда позволяет ускорить процесс выявления несовместности системы. Напомним, что пункт 3.6.1, выявляющий в графе нестрогий цикл с двумя противоположными переменными, позволял всего лишь сократить систему, тогда как в данном случае он сразу выявит неразрешимость. Например, если граф содержит цикл $a \leq b \leq -a \leq \mathrm{c} \leq a$, то единственная возможность для переменных a, b и c — это быть равными нулю, чего не может быть в силу отсутствия нуля в домене интерпретаций $\mathbf{D}$. Аналогичный результат получается и при обнаружении цикла, содержащего единственную константу ноль — такой цикл замене на ноль не подлежит, а значит и исходная система неразрешима.

Непринадлежность нуля ко множеству $\mathbf{D}$ отражается и на целочисленном случае — в условии 3.5 будет учитываться отсутствие нуля в пути между разнознаковыми константами. Например, для цепочки неравенств $-2 < a < b < 1$ в целочисленном случае с нулем есть решение: $a = -1, b = 0$, а без нуля — решений нет. Таким образом, условие 3.5 преобразуется в следующее:

3.5′. Если граф $G_{S'}$ содержит путь между двумя константами A и B и длина этого пути, измеренная в количестве знаков ¡, не превосходит их разности, в случае, когда A и B — противоположных знаков и строго меньше $B - A$, в противном случае, тогда система S' не имеет решений.

К описанному выше случаю непринадлежности нуля к множеству $\mathbf{D}$ сводиться и случай целочисленных переменных из асимметрично-

го промежутка [**a**,**b**], когда разность $\mathbf{b}-\mathbf{a}$ нечетная. В этом случае нельзя параллельно перенести отрезок $[\mathbf{a},\mathbf{b}]$ на симметричный относительно нуля интервал $[-\mathbf{k},\mathbf{k}]$ с сохранением целочисленности переменных и констант. Например, отрезок [**a**,**b**]= $[0,1]$ не получиться преобразовать в промежуток [-**k**,**k**], так как в случае целых чисел $[\mathbf{a},\mathbf{b}]$ содержит всего два значения 0 и 1. Но если же мы рассмотрим симметричное относительно нуля множество $[-1,1]/\{0\}$, то его целые числа взаимно однозначно отобразятся на исходное множество $[\mathbf{a},\mathbf{b}]\cap\mathbf{Z}$.

Таким образом, преобразование домена интерпретаций $\mathbf{D}=[\mathbf{a},\mathbf{b}]\cap\mathbf{Z}$ производиться следующим образом:

Вычисляется граница множества: $\mathbf{k}=[(\mathbf{b}-\mathbf{a}+\mathbf{1})/\mathbf{2}]$ и тогда новый домен

$$\mathbf{D}'=\begin{cases}[-\mathbf{k},\mathbf{k}], & \text{если } (\mathbf{b}-\mathbf{a}) \text{ — четное,}\\ [-\mathbf{k},\mathbf{k}]/\{0\}, & \text{в противном случае.}\end{cases}$$

Константы и переменные системы пересчитываются по формуле

$$c'=c-(a+b)/2-0.5*sign(c-(a+b)/2).$$

где c — старое значение переменной или константы, а c' — новое.

Например для множества $\mathbf{D}=[3,8]\cap\mathbf{Z}$ новый домен интерпретаций $\mathbf{D}'=[-2,2]/\{0\}$, и константе c=4 будет соответствовать новое значение $c'=4-(3+8)/2-0.5*sign(4-(3+8)/2)=4-5.5+0.5=-1$, а для $d=7$ $d'=7-5.5-0.5=1$.

Таким образом, случай целых чисел для асимметричного интервала всегда может быть преобразован в целочисленный симметричный, и в зависимости от наличия в новом домене $\mathbf{D}'$ нуля, система будет обработана тем или иным способом.

ЛИТЕРАТУРА

[1] Н.К. Косовский, А.В. Тишков. Полиномиальные алгоритмы установления совместимости в рациональных и целых числах систем строгих и нестрогих линейных неравенств. // Актуальные проблемы современной математики Т.3 (1996), с. 95–100.

[2] D. Beauquier, N. Kossovski, E. Smirnova. An algorithm for solvability testing of elementary linear inequalities systems. // 6th

IMACS International Conference on Applications of Computer Algebra. IMACS ACA 2000, pp.59–61.

*С.-Петербургский государственный университет

ОБЛАСТЬ ЗНАЧЕНИЙ ЭНТРОПИИ СЕКЦИОННЫХ КЛАССОВ ЦВЕТНЫХ ГРАФОВ

С. В. Сорочан*

Настоящая работа продолжает исследование наследственных классов цветных графов, начатое в [5], и обобщает некоторые результаты, полученные в [1] и [2] для наследственных классов обыкновенных графов.

В [5] было введено понятие *цветного графа*, или *q-графа*. Этот граф возникает в результате раскрашивания ребер обыкновенного полного графа в q цветов. Более строго, если $Q = \{1, 2, \ldots, q\}$ — множество цветов, то *q-графом* с множеством вершин V называется пара $G = (V, g)$, где $g : V^{(2)} \to Q$, $V^{(2)}$ — множество всех неупорядоченных пар различных элементов множества V. Если $g(x, y) = \alpha$, то пару (x, y) будем называть ребром цвета α.

Обыкновенный граф можно рассматривать как 2-граф. Некоторые термины, применяемые для обыкновенных графов, естественным образом распространяются и на цветные графы. Это относится, в частности, к понятиям изоморфизма, порожденного подграфа и наследственного класса.

Подграф G' цветного графа G называется *порожденным подграфом*, если он получен посредством удаления из G произвольного числа вершин (и всех возникающих при этом "висячих" раскрашенных ребер).

Класс q-графов $\mathcal{X}^{\langle q \rangle}$ называется *наследственным* (или *фрагментно замкнутым*), если он содержит всякий q-граф G', изоморфный порожденному подграфу графа G из $\mathcal{X}^{\langle q \rangle}$.

Пусть $\mathcal{X}_n^{\langle q \rangle}$ — совокупность всех q-графов с множеством вершин $\{1, \ldots, n\}$ из класса $\mathcal{X}^{\langle q \rangle}$. Рассмотрим последовательность

$$h_n\left(\mathcal{X}^{\langle q \rangle}\right) = \log_q \left|\mathcal{X}_n^{\langle q \rangle}\right| / \binom{n}{2}.$$

Из [5] известно, что для любого наследственного класса q-графов существует предел $h_n\left(\mathcal{X}^{\langle q\rangle}\right)$ при $n\to\infty$. Этот предел называется *энтропией* цветного класса $\mathcal{X}^{\langle q\rangle}$ и обозначается $h\left(\mathcal{X}^{\langle q\rangle}\right)$:

$$h\left(\mathcal{X}^{\langle q\rangle}\right)=\lim_{n\to\infty}h_n\left(\mathcal{X}^{\langle q\rangle}\right)=\lim_{n\to\infty}\frac{2\log_q\left|\mathcal{X}_n^{\langle q\rangle}\right|}{n^2}.$$

Также в [5] было введено понятие двудольного цветного графа. Именно, если V и U — непересекающиеся множества, то *двудольным q-графом* с долями V и U называется тройка (V,U,g), где $g: V\times U\to Q$ (при этом функция g не определена на множествах $V^{(2)}$ и $U^{(2)}$, т.е. *двудольный цветной граф* формально не имеет право называться *цветным графом*). Для непустого $P\subseteq Q$ множество всех двудольных q-графов с $g(V\times U)\subseteq P$ будем обозначать $\mathcal{B}^{\langle q\rangle}(P)$. Определения изоморфизма, порожденного подграфа и наследственного класса распространяются на двудольные цветные графы очевидным образом.

Пусть $\mathcal{Y}^{\langle q\rangle}$ — множество двудольных q-графов. Через $\mathcal{Y}_n^{\langle q\rangle}$ обозначим множество всех графов из $\mathcal{Y}^{\langle q\rangle}$, в которых $V=\{1,2,\ldots,n\}$, $U=\{n+1,n+2,\ldots,2n\}$. В [3] (в несколько иной терминологии) доказано, что для каждого наследственного класса двудольных q-графов существует энтропия, определяемая следующим образом:

$$h_{\mathcal{B}}(\mathcal{Y}^{\langle q\rangle})=\lim_{n\to\infty}\frac{\log_q|\mathcal{Y}_n^{\langle q\rangle}|}{n^2}.$$

Пополнением двудольного q-графа $G=(V,U,g)$ называется любой q-граф $H=(V\cup U,h)$, такой, что h совпадает с g на $V\times U$. Для непустых множеств $M_1,M_2\subseteq Q$ пополнение, в котором $h(x,y)\in M_1$ для всех $(x,y)\in V^{(2)}$ и $h(x,y)\in M_2$ для всех $(x,y)\in U^{(2)}$, назовем (M_1,M_2)-пополнением двудольного цветного графа.

В [5] удалось показать, что

— для конечного фрагментно замкнутого класса q-графов $h\left(\mathcal{X}^{\langle q\rangle}\right)=-\infty$, а для бесконечного $0\le h\left(\mathcal{X}^{\langle q\rangle}\right)\le 1$;

– существует q минимальных (по включению) наследственных классов q-графов, на которых достигается значение $h=0$: ими являются *одноцветные классы* $\mathcal{O}_\alpha^{\langle q\rangle}$ всех q-графов, каждое ребро которых имеет цвет α, $\alpha=1,2,\ldots,q$;

– область значений энтропии бесконечных фрагментно замкнутых классов q-графов является разрывным множеством: $h\left(\mathcal{X}^{\langle q\rangle}\right) = 0$, либо $1/(2\log_2 q) \le h\left(\mathcal{X}^{\langle q\rangle}\right) \le 1$;
– в слое наследственных классов q-графов с энтропией $h = 1/(2\log_2 q)$ имеется в точности $\binom{q+1}{2}\binom{q}{2}$ минимальных (по включению) элементов; этими элементами являются классы $\mathcal{B}^{\langle q\rangle}(\{\alpha\},\{\beta\};\{\gamma,\delta\})$ всех $(\{\alpha\},\{\beta\})$-пополнений двудольных q-графов из $\mathcal{B}^{\langle q\rangle}(\{\gamma,\delta\})$, где $\alpha \le \beta, \gamma < \delta$, $\alpha,\beta,\gamma,\delta = 1,2,\ldots,q$.

Для произвольного непустого неупорядоченного множества $M \subseteq Q$, $|M| = m$ обозначим через $\mathcal{O}^{\langle q\rangle}(M)$ класс всех q-графов, цвет каждого ребра которых есть число из M. Очевидно, что

$$h\left(\mathcal{O}^{\langle q\rangle}(M)\right) = \log_q m\,.$$

Пусть $\mathcal{B}^{\langle q\rangle}(P)$ — некоторый класс двудольных q-графов, где $P \ne \emptyset, P \subseteq Q, |P| = p$. Нетрудно видеть, что

$$h_{\mathcal{B}}\left(\mathcal{B}^{\langle q\rangle}(P)\right) = \log_q p.$$

Определим понятие секционного класса цветных графов следующим образом. Пусть $\mathcal{E}^{\langle q,k\rangle} = \left\|\mathcal{E}_{ij}^{\langle q\rangle}\right\|_{i,j=1}^{k}$ – симметрическая матрица, в которой

$$\mathcal{E}_{ii}^{\langle q\rangle} = \mathcal{O}^{\langle q\rangle}(M_{ii}), \quad \text{а} \quad \mathcal{E}_{ij}^{\langle q\rangle} = \mathcal{B}^{\langle q\rangle}(M_{ij})$$

для некоторых непустых множеств $M_{ii}, M_{ij} \subseteq Q$, $i \ne j$, $i,j = 1,2,\ldots,k$.

Под *k-секционным (k-дольным) классом q-графов*, задаваемым симметрической матрицей $\mathcal{E}^{\langle q,k\rangle}$ $(k \ge 2)$, будем понимать совокупность всех q-графов, допускающих разбиение множества вершин на k секций, i-я из которых порождает подграф из класса $\mathcal{E}_{ii}^{\langle q\rangle}$, а подграф, порожденный вершинами i-й и j-й секций, является (M_{ii}, M_{jj})-пополнением двудольного цветного графа, принадлежащего классу $\mathcal{E}_{ij}^{\langle q\rangle}$, $i \ne j$, $i,j = 1,2,\ldots,k$.

С каждым секционным классом $\mathcal{E}^{\langle q,k\rangle}$ свяжем также симметрическую числовую матрицу $\mathrm{H}^{\langle q,k\rangle} \equiv \mathrm{H} = \left\|h_{ij}^{\langle q\rangle}\right\|_{i,j=1}^{k}$, в которой

$$h_{ii}^{\langle q\rangle} = h\left(\mathcal{E}_{ii}^{\langle q\rangle}\right), \quad h_{ij}^{\langle q\rangle} = h_{\mathcal{B}}\left(\mathcal{E}_{ij}^{\langle q\rangle}\right),$$

при $i \neq j,\ i,j = 1,2,\ldots,k$.

Матрица $\mathrm{H} = \mathrm{H}^{\langle q,k\rangle}$ называется *матрицей энтропий* секционного класса $\mathcal{E}^{\langle q,k\rangle}$. Элементами $\mathrm{H}^{\langle q,k\rangle}$ являются числа из множества $\{0 = \log_q 1, \log_q 2, \ldots, \log_q(q-1), \log_q q = 1\}$.

Заметим, что матрицы $\mathcal{E}^{\langle q,k\rangle}$ и $\mathrm{H}^{\langle q,k\rangle}$ определяются с точностью до перестановок строчек и столбцов, т. е. с точностью до нумерации секций.

Секционный класс цветных графов $\mathcal{E}^{\langle q,k\rangle}$ назовем *регулярным*, если для его матрицы энтропий H выполнены *требование максимальности*:

$\langle 1\rangle$ матрица $\mathrm{Q}^{\top}\mathrm{H}\,\mathrm{Q}$ является отрицательно определенной (Q — $k \times (k-1)$-матрица, в столбцах которой записаны базисные векторы подпространства решений уравнения $\tilde{1}^{\top}\tilde{\mathbf{u}} = 0$),

и *условие внутренней допустимости*:

$\langle 2\rangle$ $\mathrm{H}^{-1}\tilde{1} > \tilde{0}$ (здесь $\tilde{1} = \{1,1,\ldots,1\}^{\top}$, $\tilde{0} = \{0,0,\ldots,0\}^{\top}$, а неравенство понимается покомпонентно).

Доказано, что проблема вычисления энтропии всякого секционного класса цветных графов сводится к следующей задаче поиска максимума квадратичной формы с линейным ограничением при условии неотрицательности переменных:

$$h\left(\mathcal{E}^{\langle q,k\rangle}\right) = \max\left\{F(\tilde{\mathbf{u}}) = \tilde{\mathbf{u}}^{\top}\mathrm{H}\tilde{\mathbf{u}} \,\middle|\, \tilde{1}^{\top}\tilde{\mathbf{u}} = 1, \tilde{\mathbf{u}} \geq \tilde{0}\right\}.$$

Решая эту задачу, приходим к следующему результату.

Теорема 1. *Энтропия всякого регулярного секционного класса цветных графов вычисляется по формуле*

$$h\left(\mathcal{E}^{\langle q,k\rangle}\right) = \frac{1}{\tilde{1}^{\top}\mathrm{H}^{-1}\tilde{1}}.$$

Энтропия любого нерегулярного класса равна максимальной энтропии в нем целиком содержащегося многодольного класса с меньшим количеством секций.

Уместен вопрос о том, как много имеется наследственных классов цветных графов с нулевой и ненулевой энтропией. Ответ содержится в следующей теореме.

Теорема 2. *Множество фрагментно замкнутых классов q-графов с нулевой энтропией континуально. Кроме того, если* H *— матрица энтропий k-дольного регулярного секционного класса, то имеется*

континуальное семейство наследственных классов q-графов с энтропией, равной $\dfrac{1}{\tilde{1}^{\top}\mathrm{H}^{-1}\tilde{1}}$.

Среди $(k-1)$-дольных классов, содержащихся в произвольном регулярном k-секционном классе $\mathcal{E}^{\langle q,k\rangle}$, не все обязаны быть регулярными. Тем не менее справедлива следующая

Теорема 3. *В любом k-дольном регулярном классе цветных графов имеется хотя бы один $(k-1)$-дольный регулярный класс.*

Пусть $\left\{\mathcal{X}^{\langle q,1\rangle}, \mathcal{X}^{\langle q,2\rangle}, \ldots, \mathcal{X}^{\langle q,k-1\rangle}, \mathcal{X}^{\langle q,k\rangle}, \mathcal{X}^{\langle q,k+1\rangle}, \ldots\right\}$ — некоторое семейство наследственных классов q-графов. Фрагментно замкнутый класс $\mathcal{X}_*^{\langle q\rangle} = \bigcup\limits_{k=1}^{\infty} \mathcal{X}^{\langle q,k\rangle}$ назовем *минимальной верхней границей* для последовательности $\mathcal{X}^{\langle q,1\rangle}, \mathcal{X}^{\langle q,2\rangle}, \ldots, \mathcal{X}^{\langle q,k\rangle}, \ldots$

Будем говорить, что последовательность $\left\{\mathcal{X}^{\langle q,k\rangle}, k \in \mathbf{N}\right\}$ фрагментно замкнутых классов *монотонно возрастает*, если

$$\mathcal{X}^{\langle q,1\rangle} \subset \mathcal{X}^{\langle q,2\rangle} \subset \cdots \subset \mathcal{X}^{\langle q,k-1\rangle} \subset \mathcal{X}^{\langle q,k\rangle} \subset \mathcal{X}^{\langle q,k+1\rangle} \subset \ldots$$

Минимальную верхнюю границу $\mathcal{X}_*^{\langle q\rangle}$ назовем *нетривиальной*, если для нее существует монотонно возрастающая последовательность наследственных классов $\left\{\mathcal{X}^{\langle q,k\rangle}, k \in \mathbf{N}\right\}$ такая, что

$$h\left(\mathcal{X}^{\langle q,1\rangle}\right) < h\left(\mathcal{X}^{\langle q,2\rangle}\right) < \cdots < h\left(\mathcal{X}^{\langle q,k\rangle}\right) < \cdots < h\left(\mathcal{X}_*^{\langle q\rangle}\right).$$

Пусть монотонно возрастающая последовательность значений энтропий классов $\mathcal{X}^{\langle q,1\rangle}, \mathcal{X}^{\langle q,2\rangle}, \ldots, \mathcal{X}^{\langle q,k\rangle}, \ldots$ сходится. Значение $h^* = h(\mathcal{X}_*^{\langle q\rangle})$ энтропии нетривиальной минимальной верхней границы $\mathcal{X}_*^{\langle q\rangle}$ назовем *точкой сгущения*, если оно совпадает с пределом последовательности $h\left(\mathcal{X}^{\langle q,k\rangle}\right)$ при $k \to \infty$: $h\left(\mathcal{X}_*^{\langle q\rangle}\right) = \lim\limits_{k\to\infty} h\left(\mathcal{X}^{\langle q,k\rangle}\right)$.

Пусть $\widetilde{\mathcal{E}}^{\langle q\rangle}$ и $\widetilde{\mathcal{E}}_{\mathrm{reg}}^{\langle q\rangle}$ — соответственно множество всех *секционных* и *регулярных секционных* классов q-графов. Очевидно, что $\widetilde{\mathcal{E}}_{\mathrm{reg}}^{\langle q\rangle} \subseteq \widetilde{\mathcal{E}}^{\langle q\rangle}$, причем из основного результата работы [4] следует, что равенство имеет место только при $q = 2$.

Теорема 4. *Всякий наследственный класс, являющийся минимальной верхней границей для произвольной монотонно возрастающей последовательности секционных классов, либо сам принадлежит множеству $\widetilde{\mathcal{E}}_{\mathrm{reg}}^{\langle q\rangle}$, либо содержит в себе целиком некоторый регулярный*

многодольный класс из $\widetilde{\mathcal{E}}_{\mathrm{reg}}^{\langle q\rangle}$ *с таким же, как у него, значением энтропии.*

Интересным представляется вопрос о количестве минимальных верхних границ и точек сгущения энтропии наследственных классов q-графов. Справедлива следующая

Теорема 5. *При* $q > 2$ *количество минимальных верхних границ последовательностей фрагментно замкнутых классов* q*-графов бесконечно; соответственно, в области значений энтропии наследственных классов* q*-графов имеется бесконечно много точек сгущения.*

Работа выполнена при финансовой поддержке РФФИ, код проекта 00-01-00601.

ЛИТЕРАТУРА

[1] Алексеев В. Е. Наследственные классы и кодирование графов. // Проблемы кибернетики. Вып. 39. 1982. С. 151–164.

[2] Алексеев В. Е. Об энтропии фрагментно замкнутых классов графов. // Комбинаторно-алгебраические методы в прикладной математике. Горький, 1986. С. 3–12.

[3] Алексеев В. Е. Об энтропии двумерных фрагментно замкнутых языков. // Комбинаторно-алгебраические методы и их применения. Горький, 1987. С. 5–13.

[4] Алексеев В. Е. Область значений энтропии наследственных классов графов. // Дискретная математика. 1992. Т. 4, вып. 2. С. 148–157.

[5] Алексеев В. Е., Сорочан С. В. Об энтропии наследственных классов цветных графов. // Дискретная математика. 2000. Т. 12, вып. 2. С. 99–102.

*Нижегородский государственный университет им. Н. И. Лобачевского

О ТЕХНИКЕ РЕШЕНИЯ ЗАДАЧИ СИНТЕЗА ИГРОВЫХ ПРОГРАММ

Р. В. Хелемендик*

1. Введение

Значительным шагом в развитии математической теории программирования является создание А.А.Ляпуновым и Ю.И.Яновым модели программ. В работе [1] изложена теория операторных схем Янова — формального исчисления, в котором полностью решалась задача распознавания эквивалентностей моделей программ и строилась система независимых преобразований программы в любую, ей эквивалентную. Основными объектами этой теории являются преобразователи (функции), распознаватели (предикаты), конфигурации ("состояния выполнения" программы).

В то же время следует заметить, что теория операторных схем создавалась в годы, когда программы были прежде всего вычислительными, тогда как в последние два десятилетия значительно увеличилось число интерактивных. Такие программы можно рассматривать как игровые, т.е. как взаимодействие с пользователем, роботом, другой программой. Участника такого взаимодействия в дальнейшем будем называть партнером. Основное требование, предъявляемое к игровым программам, — корректная работа в зависимости от целей программы и действий партнера. Мы рассматриваем такое взаимодействие, при котором переменные могут изменяться как программой, так и партнером и принимают конечное число значений.

Сначала для описания ситуаций взаимодействия автором применялись схемы Янова, одна из которых была построена как решение шахматного этюда в [2], т.е. как игровая программа, выполняющая поставленную задачу при любой игре соперника. Однако роль распознавателей в получающихся схемах программ сводится лишь к учету каждого из действий партнера. Поэтому в игровых программах распознаватели заменены на внешние преобразователи — конечные наборы функций (действий партнера). Такая модель в случае отсутствия циклов имеет аналогии со схемами из функциональных элементов в k-значной логике в базисе, заданном зафиксированными

в условии функциями, причем у некоторых функциональных элементов имеется несколько выходов. Рассмотренный выше пример иллюстрирует важный подкласс игровых программ, соответствующих модели взаимодействия, в которой изменения переменных программой и партнером происходят по очереди, а также возможность использования игровой программы в качестве решения игры.

Каждая игровая программа должна удовлетворять некоторым свойствам (целям), зависящим от ситуации взаимодействия. Эти свойства мы будем записывать на языке логики ветвящегося времени (CTL — Computating Time Logic, [3,4]). Выбор именно этого языка для записи целей игровой программы вызван интерпретацией момента времени как "состояния выполнения" игровой программы, а возможность альтернативных изменений соответствует различным ответам партнера.

Итак, условием для игровой программы является конечное число переменных; конечное число их значений; начальные значения переменных; конечное множество преобразований переменных, осуществляемых программой; конечное множество преобразований переменных, осуществляемых партнером; конечное множество целей в программе; выбранный тип взаимодействия. Задача синтеза состоит в ответе на вопрос о существовании для заданного условия игровой программы и в случае существования — ее построения.

Предлагаемая ниже техника решения задачи синтеза игровых программ состоит в 1) построении по условию для игровой программы формулы логики ветвящегося времени, выполнимость которой равносильна существованию игровой программы; 2) выборе алгоритма распознавания выполнимости формулы логики ветвящегося времени; 3) построении в случае выполнимости по результатам работы алгоритма некоторой игровой программы.

2. Логика ветвящегося времени

В логике ветвящегося времени используются идеи Г.В. Лейбница о семантике возможных миров. В каждом мире (моменте времени) верны все законы классической логики высказываний, а значения высказываний могут изменяться при переходе от одного мира к другому. Таким образом, логика ветвящегося времени является расширением логики высказываний, при котором добавляются но-

вые операторы, связывающие один мир с другим и кванторы по этим операторам.

Определим понятие формулы логики ветвящегося времени.

• Каждая пропозициональная переменная P есть основная формула.

• Если Φ, Ψ — основные формулы, то $(\Phi \wedge \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \to \Psi)$, $\neg\Phi$ тоже основные формулы.

• Если Φ, Ψ — основные формулы, то $\bigcirc\Phi$, $\Box\Phi$, $\Diamond\Phi$, $(\Phi \mho \Psi)$ временные формулы.

• Если Φ — временная формула, то $\forall\Phi$, $\exists\Phi$ — основные формулы.

• Основная формула есть формула. Других формул нет.

Модель — это пара $M = \langle \tau, L \rangle$, где $\tau = \langle U, R \rangle$ — бесконечное дерево – связный ориентированный граф без циклов с корнем u_0, множеством вершин U и множеством дуг R, а L — оценка (функция означивания), сопоставляющая каждой вершине множество истинных в ней пропозициональных переменных.

Истинность формулы Φ в модели M в вершине (мире) u_i (обозначим это $M, u_i \models \Phi$) и истинность временной формулы Φ в модели M на бесконечной последовательности $x = (u_i, u_{i+1}, u_{i+2}, \ldots)$ (обозначим это $M, x \models \Phi$), где $(u_{i+j}, u_{i+j+1}) \in R$ для любого $j \geq 0$, определяется индуктивно.

• $M, u_i \models \Phi \iff \Phi \in L(u_i)$, когда Φ есть пропозициональная переменная

• $M, u_i \models (\Phi \wedge \Psi) \iff M, u_i \models \Phi$ и $M, u_i \models \Psi$

• $M, u_i \models (\Phi \vee \Psi) \iff M, u_i \models \Phi$ или $M, u_i \models \Psi$

• $M, u_i \models (\Phi \to \Psi) \iff M, u_i \models \Psi$ или $M, u_i \not\models \Phi$ (неверно $M, u_i \models \Phi$)

• $M, u_i \models \neg\Phi \iff M, u_i \not\models \Phi$

• $M, x \models \bigcirc\Phi \iff M, u_{i+1} \models \Phi$

• $M, x \models \Box\Phi \iff \forall j \geq i \;\; M, u_j \models \Phi$

• $M, x \models \Diamond\Phi \iff \exists j \geq i \;\; M, u_j \models \Phi$

• $M, x \models (\Phi \mho \Psi) \iff \exists j \geq i \;\; M, u_j \models \Psi$ и $\forall k (i \leq k < j$ влечет $M, u_k \models \Phi)$

• $M, u_i \models \exists\Phi \iff$ существует последовательность $x = (u_i, u_{i+1}, \ldots)$ такая, что $(u_{i+j}, u_{i+j+1}) \in R$ для любого $j \geq 0$ и $M, x \models \Phi$

• $M, u_i \models \forall\Phi \iff M, x \models \Phi$ для любой последовательности $x = (u_i, u_{i+1}, u_{i+2}, \ldots)$ такой, что $(u_{i+j}, u_{i+j+1}) \in R$ для любого $j \geq 0$.

Формула Φ общезначима, если $M, u_0 \models \Phi$ для каждой модели M.

Формула Φ выполнима, если $M, u_0 \models \Phi$ на некоторой модели M.

3. Понятие игровой программы. Задача синтеза

Структура игровой программы. Пусть $Y = \{y_1, \ldots, y_n\}$ — конечное непустое множество переменных, $\overline{y} = (y_1, \ldots, y_n)$ — набор переменных $y_1, \ldots, y_n$. Пусть $\mathrm{A} = \{\alpha_1, \ldots, \alpha_\mathrm{m}\}$ — конечная непустая область значений переменных из множества Y. Тогда преобразователем будем называть n-мерную функцию $f\colon \mathcal{A} \to \mathrm{A}^\mathrm{n}$, где $\mathcal{A} \subseteq \mathrm{A}^\mathrm{n}$, $\mathcal{A} \neq \emptyset$, а преобразованием набора $\overline{y}$ — выражение $\overline{y} := f(\overline{y})$, где $\overline{y}$ в левой части есть значение $f(\overline{y})$. Внешним преобразователем будем называть конечное множество $G(\overline{y}) = \{g_1(\overline{y}), \ldots, g_k(\overline{y})\}$ n-мерных функций g_i, определенных на одном и том же множестве $\mathcal{A} \subseteq \mathrm{A}^\mathrm{n}$, $\mathcal{A} \neq \emptyset$, а внешним преобразованием набора $\overline{y}$ — выражение $\overline{y} := G(\overline{y}) = \{g_1(\overline{y}), \ldots, g_k(\overline{y})\}$, где $\overline{y}$ в левой части есть значение некоторой функции $g_i(\overline{y})$, $1 \leq i \leq k$.

Игровая программа есть связный конечный размеченный ориентированный граф следующего вида. Каждой вершине приписано либо преобразование (это вершина-преобразователь), либо внешнее преобразование (это вершина-партнер), либо ничего не приписано (это финальная вершина). Из вершины-преобразователя $\overline{y} := f(\overline{y})$ выходит одна дуга, она помечена символом $f(\overline{y})$. Из вершины-партнера $\overline{y} := G(\overline{y}) = \{g_1(\overline{y}), \ldots, g_k(\overline{y})\}$ выходит k дуг, помеченных соответственно символами $g_1(\overline{y}), \ldots, g_k(\overline{y})$. Из финальной вершины не выходит ни одной дуги. В графе выделена вершина v_0, называемая начальной.

Функционирование игровой программы. Пусть $\overline{\alpha}_0$ — начальное значение набора $\overline{y}$. Конфигурацией игровой программы называется пара $c_i = \langle v_i, \overline{\alpha}_i \rangle$, где v_i — вершина графа, $\overline{\alpha}_i$ — значение набора $\overline{y}$ в вершине v_i. Вычисление игровой программы есть последовательность π конфигураций, определяемая следующим образом. Последовательность $\pi = \langle c_0 \rangle$, где $c_0 = \langle v_0, \overline{\alpha}_0 \rangle$, есть вычисление игровой программы. Пусть последовательность $\pi = \langle c_0, \ldots, c_i \rangle$ есть вычисление игровой программы. 1) Если v_i — вершина-преобразователь $\overline{y} := f(\overline{y})$, то $\pi = \langle c_0, \ldots, c_i, c_{i+1} \rangle$, где $c_{i+1} = \langle v_{i+1}, \overline{\alpha}_{i+1} \rangle$, v_{i+1} — вершина, в которую ведет дуга из v_i, а $\overline{\alpha}_{i+1} = f(\overline{\alpha}_i)$, есть тоже вычисление игровой программы. 2) Если v_i — вершина-партнер $\overline{y} := G(\overline{y}) = \{g_1(\overline{y}), \ldots, g_k(\overline{y})\}$, то каждая

из k последовательностей $\pi_j = \langle c_0, \ldots, c_i, c_{i+1,j}\rangle$, $1 \le j \le k$, где $c_{i+1,j} = \langle v_{i+1,j}, \overline{\alpha}_{i+1,j}\rangle$, $v_{i+1,j}$ — вершина, в которую ведет дуга из v_i, помеченная символом $g_j(\overline{y})$, а $\overline{\alpha}_{i+1,j} = g_j(\overline{\alpha}_i)$, являются также вычислениями игровой программы. 3) Если v_i — финальная вершина, то вычисление π считается завершенным. Функционирование игровой программы есть множество ее вычислений.

Цели в игровой программе. Цели в игровой программе записываются в виде формул логики ветвящегося времени, где в качестве пропозициональных переменных стоят высказывания $(y_i = \alpha_j)$, а в качестве последовательности — вычисление игровой программы. Примеры целей: 1) $\forall\Diamond(y_i = \alpha_j)$ — при любом вычислении игровой программы наступит момент (найдется конфигурация), когда $y_i = \alpha_j$. 2) $\exists\Box\neg((y_{i_1} = \alpha_{j_1}) \vee (y_{i_2} = \alpha_{j_2}))$ — существует вычисление игровой программы такое, что во всякой кофигурации неверно хотя бы одно из высказываний: $(y_{i_1} = \alpha_{j_1})$ или $(y_{i_2} = \alpha_{j_2})$. 3) $\forall((y_{i_1} = \alpha_{j_1})\, \mho\, (y_{i_2} = \alpha_{j_2}))$ — при любом вычислении игровой программы найдется конфигурация, в которой $y_{i_2} = \alpha_{j_2}$, и во всякой другой конфигурации вычисления, встретившейся в последовательности перед данной, верно $y_{i_1} = \alpha_{j_1}$. Остается открытым вопрос выбора подходящей интерпретации для временных формул на конечных последовательностях конфигураций. Поэтому в дальнейшем будем рассматривать игровые программы без финальных состояний.

Тип взаимодействия. Каждое взаимодействие характеризуется порядком изменения переменных внутренними и внешними преобразованиями. Рассмотрим следующие типы взаимодействий: 1) тип игры Ω_1, когда преобразователи и внешние преобразователи изменяют переменные по очереди; 2) тип взаимодействия с приоритетом программы Ω_2, когда в случае возможности выбора для данных значений переменных как преобразователя, так и внешнего преобразователя выбирается первый; 3) тип взаимодействия с приоритетом партнера Ω_3, когда в указанной выше ситуации выбирается внешний преобразователь; 4) общий тип взаимодействия Ω_4, когда порядок выбора может быть произвольным.

Постановка задачи синтеза. Пусть для игровой программы задано условие $\mathcal{U} = \langle Y, \mathrm{A}, \overline{\alpha}_0, \mathrm{I}, \mathrm{E}, \mathcal{F}, \Omega\rangle$, где $Y = \{y_1, \ldots, y_n\}$, $\mathrm{A} = \{\alpha_1, \ldots, \alpha_{\mathrm{m}}\}$, $\overline{\alpha}_0$ — начальное значение $\overline{y}$, I, E, $\mathcal{F}$ — соответственно конечные множества преобразователей, внешних преобразователей,

целей в программе, Ω — тип взаимодействия, $\Omega \in \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\}$. Существует ли игровая программа, удовлетворяющая условию $\mathcal{U}$? Если существует, то необходимо построить хотя бы одну такую программу.

4. Техника решения задачи синтеза.

Построение формулы. По условию $\mathcal{U}$ мы будем строить формулу $\Phi_{\mathcal{U}}$ следующего вида:

$$\Phi_{\mathcal{U}} = Init \wedge Rules \wedge Aims,$$

где $Init$ записывает начальные значения $\overline{\alpha}_0$, Rules обеспечивает корректное изменение значений переменных, а $Aims$ есть конъюнкция всех целей.

Введем $n \times m$ пропозициональных переменных $p_{i,j}$, где $1 \le i \le n$, $1 \le j \le m$, и заменим каждое равенство вида $y_i = \alpha_j$ на пропозициональную переменную $p_{i,j}$. Тогда каждая из целей превращается в формулу логики ветвящегося времени в соответствии с определениями пункта 2, а формула $Init$ становится конъюнкцией n пропозициональных переменных, выбранных по начальным значениям $\overline{\alpha}_0$. Пусть $One(z_1, \ldots, z_k) = (z_1 \vee \ldots \vee z_k) \wedge [\wedge_{1 \le i < j \le k} \neg(z_i \wedge z_j)]$, что соответствует истинности ровно одной из пропозициональных переменных $z_1, \ldots, z_k$. Пусть $\overline{P}_h$ есть обозначение для конъюнкции $p_{1,i_1} \wedge \ldots \wedge p_{n,i_n}$ — h-го набора значений переменных $\overline{y}$, где $y_1 = \alpha_{i_1}$, $\ldots$, $y_n = \alpha_{i_n}$, $h = \sum_{j=1}^{n} (i_j - 1) m^{n-j}$. В этом случае будем говорить, что формула $\overline{P}_h$ получена по набору $\overline{y} = \overline{\alpha}$.

В формуле $Rules = Vars \wedge Int \wedge Ext \wedge Type$ собраны все правила изменений значений переменных. Формула $Vars = \forall\Box \wedge_{i=1}^{n} One(p_{i,1}, \ldots, p_{i,m})$ утверждает, что каждая переменная y_i в каждой конфигурации должна принимать ровно одно значение.

Выбор преобразования в конфигурации производится по формуле $Int = \forall\Box(I \rightarrow (I \wedge Ints))$, где I — пропозициональная переменная, соответствующая "очереди хода" программы, а $Ints = \vee_{h=0}^{m^n - 1} I_h$ — выбор преобразователя. Пусть $\overline{y} = \overline{\alpha}$, т.е. $y_1 = \alpha_{i_1}, \ldots, y_n = \alpha_{i_n}$ и $\{f_1(\overline{y}), \ldots, f_l(\overline{y})\} \subseteq I$ — все преобразователи, определенные на этом наборе значений с попарно различными наборами выходных значений. Тогда если $l = 0$, то выбора нет — полагаем $I_h =$

$(p_{1,1} \wedge \neg p_{1,1})$, в противном случае выбор ровно одного из преобразователей $f_1(\overline{y}), \ldots, f_l(\overline{y})$ для набора $\overline{y} = \overline{\alpha}$ записывается формулой $I_h = (\overline{P}_h \wedge One(\forall\bigcirc\overline{P}_{h_1}, \ldots, \forall\bigcirc\overline{P}_{h_l}))$, где формула $\overline{P}_h$ получена по набору $\overline{y} = \overline{\alpha}$, а формула $\overline{P}_{h_j}$ — по набору $\overline{y} = f_j(\overline{\alpha})$, где $1 \le j \le l$.

Выбор внешнего преобразования в конфигурации производится по формуле $Ext = \forall\Box(E \to (E \wedge Exts))$, где E — пропозициональная переменная, соответствующая "очереди хода" партнера, а $Exts = \vee_{h=0}^{m^n-1} E_h$ — выбор внешнего преобразователя. Пусть $\overline{y} = \overline{\alpha}$, т.е. $y_1 = \alpha_{i_1}, \ldots, y_n = \alpha_{i_n}$ и $\{G_1(\overline{y}), \ldots, G_l(\overline{y})\} \subseteq E$ — все преобразователи, определенные на этом наборе значений с попарно различными множествами наборов выходных значений. Тогда если $l = 0$, то выбора нет — полагаем $E_h = (p_{1,1} \wedge \neg p_{1,1})$, в противном случае выбор ровно одного из внешних преобразователей $G_1(\overline{y}), \ldots, G_l(\overline{y})$ для набора $\overline{y} = \overline{\alpha}$ записывается формулой $E_h = (\overline{P}_h \wedge One(EG_1, \ldots, EG_l))$, где формула $\overline{P}_h$ получена по набору $\overline{y} = \overline{\alpha}$. Пусть $G_i(y) = \{g_{i,1}(\overline{y}), \ldots, g_{i,k_i}(\overline{y})\}$. Тогда утверждение о том, что осуществлено внешнее преобразование, т.е. новым значением $\overline{y}$ является один из наборов $\overline{y} = g_{i,1}(\overline{y}), \ldots, \overline{y} = g_{i,k_i}(\overline{y})$ и никакой другой, записывается формулой $EG_i = (\forall\bigcirc(\vee_{j=1}^{k_i}\overline{P}_{h_{i,j}}) \wedge (\wedge_{j=1}^{k_i}\exists\bigcirc\overline{P}_{h_{i,j}}))$, где формула $\overline{P}_{h_{i,j}}$ получена по набору $\overline{y} = g_{i,j}(\overline{\alpha})$, где $1 \le i \le l$, $1 \le j \le k_i$.

Типу взаимодействия Ω_1, при котором начинает программа [партнер] соответствует формула $Type = (I \wedge Turn)$ $[Type = (E \wedge Turn)]$, где формула $Turn = \forall\Box(((I \wedge \neg E) \wedge \forall\bigcirc E) \vee ((\neg I \wedge E) \wedge \forall\bigcirc I))$ утверждает, что преобразования и внешние преобразования должны чередоваться. Остальным типам взаимодействия $\Omega_2, \Omega_3, \Omega_4$ поставим в соответствие формулу $Type = \forall\Box((I \wedge \neg E) \vee (\neg I \wedge E))$, утверждающую, что для каждого набора значений необходимо выбрать что-то одно: либо преобразование, либо внешнее преобразование. Различие между указанными типами взаимодействия происходит на этапе выбора алгоритма.

Формула $\Phi_{\mathcal{U}}$, моделирующая функционирование игровой программы с условием $\mathcal{U}$, построена.

Выбор алгоритма. Для логики ветвящегося времени существует табличный алгоритм распознавания выполнимости формулы, рассмотренный в [3,4] и состоящий в построении по формуле графа, вершинам которого приписаны множества формул, анализа графа и построения в случае выполнимости модели. Построение по формуле

графа, описанное в [4], носит автоматический характер и не учитывает содержание формул: оно подходит для типов взаимодействия Ω_1, Ω_4, но не позволяет различать типы Ω_2 и Ω_3. В [3] предложен другой алгоритм построения по формуле графа, в котором на каждом шаге выбирается некоторая подформула исходной формулы, причем можно фиксировать порядок выбора. Так, при выборе альтернативы $(I \wedge \neg E)$ в формуле $Type$ реализуется тип взаимодействия Ω_2; при выборе альтернативы $(\neg I \wedge E)$ — тип Ω_3; в случае произвольного выбора - тип Ω_4. Таким образом, выбор алгоритма распознавания выполнимости формул в общем случае определяется условием игровой программы.

Построение игровой программы. В случае выполнимости формулы логики ветвящегося времени табличный алгоритм предъявляет преобразованный граф, который на заключительном этапе разворачивается в бесконечную модель. Под построенной игровой программой мы понимаем именно этот конечный граф, в котором каждую вершину помечаем соответствующим ей преобразователем, либо внешним преобразователем; символами соответствующих функций помечаем исходящие из нее дуги; а вершину, содержащую формулу $\Phi_{\mathcal{U}}$, помечаем как начальную. Из истинности на модели формулы $\Phi_{\mathcal{U}}$ следует выполнение условия $\mathcal{U}$ для игровой программы, в частности, истинность формулы $Aims$ означает выполнение всех целей в построенной игровой программе.

ЛИТЕРАТУРА

[1] Янов Ю. И. О логических схемах алгоритмов. // Проблемы кибернетики. 1, М.: Физматгиз, 1958. С. 75-127.

[2] Хелемендик Р. В. Применение временных логик к анализу логических игр и головоломок. // Труды III Международной конференции "Дискретные модели в теории управляющих систем". М.: Диалог-МГУ, 1998. С. 112–114.

[3] Хелемендик Р. В. Приложение логик линейного и ветвящегося времени. Алгоритм распознавания выполнимости формул. // Вестник Нижегородского государственного университета. Математическое моделирование и оптимальное управление. Нижний Новгород. Изд-во Нижегородского ун-та, 2000. 1(22). В печати.

[4] Emerson E. A. Automated temporal reasoning about reactive systems. // Logics for concurrency. Lecture Notes in Computer Science, V. 1043. Berlin: Springer, 1996. P. 41–101.

*Москва

О ФОРМУЛЬНОЙ СЛОЖНОСТИ СИММЕТРИЧЕСКИХ БУЛЕВЫХ ФУНКЦИЙ

Д. Ю. Черухин*

Булевой функцией от n аргументов называется произвольная функция $f : \{0,1\}^n \to \{0,1\}$. Булева функция называется симметрической, если её значение не изменяется при произвольной биективной перестановке аргументов. Каждой симметрической булевой функции f от n аргументов взаимно-однозначно соответствует её характеристический набор — $(f_0, f_1, \ldots, f_n)$, в котором f_i является значением функции f на любом наборе, содержащем i единиц. Например, функция голосования Γ_n — это симметрическая функция от n аргументов (n нечётно), характеристический набор которой имеет вид $(0, \ldots, 0, 1, \ldots, 1)$, где число нулей равно числу единиц.

Пусть Б — произвольное конечное функционально полное множество булевых функций (такое множество будем называть базисом). Формулами в базисе Б называются следующие и только следующие выражения в алфавите $\text{Б} \cup \{x_1, x_2, \ldots\} \cup \{'(', ')', ','\}$:

1) c, если $c \in \text{Б} \cap \{0,1\}$;

2) $f(F_1, \ldots, F_k)$, если $f \in$ Б, f — функция от k аргументов, и любое из выражений $F_1, \ldots, F_k$ либо является формулой в базисе Б, либо принадлежит множеству переменных $\{x_1, x_2, \ldots\}$.

Сложностью формулы называется число вхождений в неё переменных. Сложностью функции f в базисе Б называется минимальная из сложностей формул в базисе Б, реализующих функцию f. Сложность функции f в базисе Б обозначим через $L_{\text{Б}}(f)$.

Теорема 1. *Для каждого натурального числа n можно построить такое множество T_n, состоящее только из симметрических функций от n аргументов, что выполнены условия*:

а) $|T_n| \sim 2^{n+1}, n \to \infty$ *(т. е. последовательность множеств T_n содержит "почти все" симметрические функции)*;

б) *если* n *нечётно, то* $\Gamma_n \in T_n$;

в) *для любого базиса* Б *существуют такие константы* A *и* B, *что для любого числа* n *и любой функции* $f \in T_n$ *выполнено неравенство*

$$L_{\text{Б}}(f) \geq An \log_2 n + B.$$

В случае, когда Б состоит только из двуместных функций, Теорема была доказана Фишером, Мейером и Патерсоном [1]. Планируется, что статья докладчика с доказательством Теоремы будет опубликована в журнале "Дискретный анализ и исследование операций", Серия 1.

Пользуясь случаем, докладчик выражает благодарность своему учителю по дискретной математике Олегу Борисовичу Лупанову.

Работа выполнена при финансовой поддержке РФФИ (проект 99–01–01175), ФЦП "Интеграция" (проект АО–110), Программы "Университеты России" (проект 992206) и Программы поддержки ведущих научных школ РФФИ (проект 00–15–96103).

ЛИТЕРАТУРА

[1] Fischer M .J., Meyer A. R., Paterson M. S. $\Omega(n \log n)$ lower bounds on length of Boolean formulas. // SIAM J. Comput. 1962. V. 11, № 3. P. 416–427.

*Московский государственный университет им. М.В. Ломоносова, механико-математический факультет