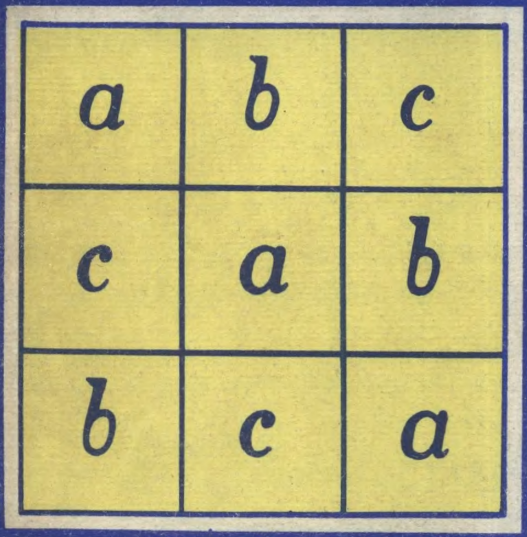
КОМБИНАТОРНО-АЛГЕБРАИЧЕСКИЕ МЕТОДЫ В ПРИКЛАДНОЙ МАТЕМАТИКЕ



МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РСФСР

ГОРЬКОВСКИЙ ГОСУДАРСТВЕННЫЙ ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ УНИВЕРСИТЕТ им. Н. И. ЛОБАЧЕВСКОГО

КОМБИНАТОРНО-АЛГЕБРАИЧЕСКИЕ МЕТОДЫ В ПРИКЛАДНОЙ МАТЕМАТИКЕ

МЕЖВУЗОВСКИЙ СБОРНИК

ИЗДАНИЕ ГГУ

ГОРЬКИЙ 1979

УДК. 519.

Комбинаторно-алгебраические методы в прикладной математике.

Межвузовский сборник. Издание Горьковского государственного университета им. Н. И. Лобачевского.

Горький, 1979, с. 124.

Решение алгоритмических вопросов, возникающих при исследовании кибернетических моделей, — одна из актуальнейших тем в современной математике. Сборник составлен из работ, в различных пропорциях сочетающих комбинаторный и алгебраический подходы к изучению дискретных систем, и представляет ряд направлений. Часть работ посвящена фундаментальным вопросам, другие имеют конкретные прикладные ориентиры: игровые модели, распознавание образов, анализ и синтез управляющих систем, целочисленное программирование и теория расписаний, передача и хранение информации.

Работы выполнены в вузах и научно-исследовательских институтах городов Горького, Красноярска, Ленинграда, Москвы, Новосибирска.

Доп. план 1979 года, позиция № 226.

Исследования в области дискретной математики занимали важное место на всех этапах развития математики. Во второй половине XX века «дискретная математика» возникла как термин, отражающий потребность в исследованиях, не укладывающихся в традиционные рамки классической математики и связанных с приложениями, в первую очередь, к кибернетическим информационным системам. Очевидно, что для эффективности развития современной дискретной математики большое значение имеет сохранение и развитие классической техники, лучшей части наследия дискретной математики прошлого, а именно таких ее разделов, как алгебра, комбинаторный анализ, математическая логика. Название настоящего сборника подчеркивает это обстоятельство: преемственность, с одной стороны, и прикладную направленность, с другой. Это обстоятельство будет служить ориентиром при формировании тематики сборников.

Не случаен выпуск сборника по дискретной математике Горьковским университетом. Работа по дискретной математике в Горьком ведется уже более 20 лет. Начальным толчком и стимулирующим фактором в дальнейшем было активное влияние московской школы математической кибернетики С. В. Яблонского. Традиционной для сложившегося сейчас в Горьком коллектива стала тематика, связанная с анализом информационных систем, теорией кодирования и дискретной оптимизацией.

Первым, кто стал пропагандировать современную идеологию дискретной математики среди горьковских математиков, был Ю. В. Глебский, трагически погибший в 1977 году. Авторы настоящего первого выпуска сборника посвящают свои работы его памяти.

МЕТОДЫ ИНДЕКСАЦИИ

В. Е. Алексеев, А. П. Клевцов, Ал. А. Марков

Задавая конечное множество списком его элементов, мы делаем это в форме $\{a_1, a_2, \ldots a_N\}$, считая вполне естественным описывать общий член, элемент множества буквой с индексом из множества натуральных чисел: x_i. Тем самым сразу делаем допущение о том, что множество некоторым образом линейно упорядочено. Это вполне приемлемо, когда речь идет о множествах произвольной природы, но если мы имеем дело с конкретным множеством, то от того, как именно оно упорядочено, т. е. как по элементу найти соответствующий индекс, зависит, насколько ясно мы представляем себе устройство множества, взаимоотношения между его элементами. При обработке данных на ЭВМ или передаче их по каналу связи от того, насколько множество данных обозримо, зависит возможность сжатия или более рационального представления информации, оптимизации поиска информации по ключу, признаку. Например, если имеется произвольно организованный массив, т. е. такой массив, в котором адрес каждой записи функционально связан с ключом этой записи, то поиск записи по ключу сводится к поиску по адресу и тем самым реализуется одно из главных преимуществ памяти прямого доступа — возможность быстрого извлечения или обновления информации. Современные системы программирования предусматривают средства для обращения с произвольно организованными массивами данных, однако способ индексации (адресации) остается прерогативой программиста, причем ответственность программиста за выбор способа индексации считается существенным недостатком произвольной организации.

В литературе описано немало конкретных методов индексации, применяемых на практике, но до сих пор «выбор подходящей функции относится скорее к области искусства, чем науки» [1]. Аналогична ситуация и с приемами сжатия информации. Таким образом, все говорит о том, что недостаточна математическая база, теория индексации.

В настоящей статье излагается весьма общая точка зрения на проблему индексации. Предлагаемая схема позволяет систематизировать известные методы индексации и рекомендовать новые. В разделах 1, 2 уточняется математическая постановка задачи и разъясняется принцип вложения, приводятся примеры. В разделе 3 охарактеризованы методы рандомизации. В разделе 4 разъясняется принцип аппроксимации, предлагается одна из реализаций этого принципа, установлены некоторые характеристики соответствующего метода индексации и приводятся результаты экспериментального сравнения одного из статистически оптимальных методов рандомизации, известного метода индексации, использующего информацию о массиве и предлагаемого метода, отмечается возможность усовершенствования последнего.

1. МАТЕМАТИЧЕСКАЯ ПОСТАНОВКА ЗАДАЧИ

Индексацией множества K будем называть любое отображение K в множество натуральных чисел N. Пусть U — некоторое множество, Γ — семейство подмножеств U. Под методом индексации для семейства Γ будем понимать алгоритм, который по каждой паре $<K, x>$, где где $K \in \Gamma$, $x \in K$, определяет натуральное число $i_K(x)$-индекс элемента x в множестве K. Таким образом, метод индексации для каждого $K \in \Gamma$ эффективно задает некоторую индексацию. Будем рассматривать методы индексации для множеств слов над конечным алфавитом.

Формулируя ниже некоторые критерии для оценки методов индексации, имеем в виду вполне определенный ориентир — организацию массивов данных в ЭВМ на запоминающих устройствах прямого доступа. При такой интерпретации K есть множество идентификаторов (ключей) элементов массива (записей), U — множество значений, которые могут принимать ключи, $i_K(x)$ — адрес, по которому размещается запись с ключом x. Критерии вытекают из общего требования экономии вычислительных ресурсов: время и память, необходимые для вычисления индекса, должны быть невелики. Если индексация не является взимно однозначной, то она порождает на множестве K нетривиальное отношение синонимии $S = S(i, K)$:

$$(x_1, x_2) \in S \qquad i_K(x_1) = i_K(x_2).$$

При организации массива в памяти ЭВМ наличие синонимии вынуждает предусматривать специальные мероприятия по размещению синонимов. Этой стороны проблемы касаться не будем, только отметим, что в любом случае наличие синонимии увеличивает время поиска информации в массиве, и этот фактор необходимо учитывать при сравнении методов индексации. Один из наиболее распространенных (а по экспериментальным данным [2] — и наиболее эффективных) способов размещения синонимов — ассоциативная организация массива, при которой индекс указывает адрес начала списка синонимичных записей. Подробности можно найти в [3], для нас здесь существенно то, что в устроенном так массиве для нахождения записи требуется время, пропорциональное длине списка синонимов, предшествующих этой записи. Следовательно, среднее время поиска элементов массива пропорционально величине

$$\tau(K, i) = \frac{1}{|K|} \sum_{n \in N} m^2_{K,i}(n),$$

где $m_{K,i}(n) = |\{x \mid x \in K,\ i_K(x) = n\}|$.

В основе следующих критериев лежит требование рационального использования памяти. С этой точки зрения представляет интерес, во-первых, «коэффициент расширения»

$$\mu(K, i_K) = \frac{1}{|K|} \max_{x \in K} i_K(x),$$

и, во-вторых, «коэффициент компактности», или «неплотность», т. е. количество «пустых» адресов σ

$$\sigma(K, i_K) = \left(\mu(K, i_K) - \frac{|i_K(K)|}{|K|} \right).$$

Почти все известные методы адресации распадаются на два класса. К первому, наиболее популярному, относятся методы, основанные на идее рандомизации, когда информация о массиве не используется совсем (т. е. $i_K(x)$ не зависит от K), а ко второму — методы, предполагающие, что массив полностью известен и хорошо устроен. Естественно,

что область применения последних весьма ограничена. Кроме того, методы второго класса, хотя и обеспечивают идеальные характеристики $\tau=\mu=1$, $\sigma=0$, связаны обычно с использованием сложных функций. Тем не менее методы второго класса могут быть положены в основу разработки простых методов индексации, учитывающих полезную информацию о массиве, в дальнейшем мы развиваем этот подход.

2. ПРИНЦИП ВЛОЖЕНИЯ

Пусть L — отношение линейного порядка на U и $K\subseteq U$. В этом случае K оказывается также линейно упорядоченным отношением L, и в качестве индекса $i_K(x)$ в K можно взять номер x в K по возрастанию относительно L на K. Если нумерацию считать с нуля, то $i_K(x)$ равен количеству предшественников x в $<K, L>$:

$$i_K(x)=|\{y|y\in K,\ (y,x)\in L\}|.$$

В выборе такой индексации и состоит принцип вложения, возможность варьировать выбор L на U оставляет при его применении значительный произвол. Рассмотрим несколько примеров.

Пусть $U=A^n$, где $A=\{0,1,...,m-1\}$, L — лексикографический порядок на U (старшие разряды слева). Формула для вычисления индекса получена в [4] в виде

$$i_K(x_1,...,x_n)=\sum_{j=1}^{n}\sum_{l=0}^{x_j-1}\nu_K(x_1,...,x_{j-1},l), \tag{1}$$

где $\nu_K(x_1,...,x_j)$ — число слов в K, имеющих префикс $x_1,...,x_j$. Для двоичного случая $m=|A|=2$ формула (1) будет иметь вид

$$i_K(x_1,...,x_n)=\sum_{j=1}^{n}x_j\nu_K(x_1,...,x_{j-1},0). \tag{2}$$

При этом сложность индексации, очевидно, зависит от сложности вычисления системы функций $\{\nu_K(x_1,...,x_j)\,|\,1\leqslant j\leqslant n\}$. Так, если $K\subseteq A^n$ — множество всех перестановок, то

$$\nu_K(x_1,...,x_j)=\begin{cases}\dfrac{(m-j)!}{(m-n)!}, & \text{если } x_1,...,x_j \text{ все различны,}\\ 0 & \text{в противном случае.}\end{cases}$$

Поэтому если положить $r_j=|\{0,1,...,x_j-1\}\cap\{x_1,...,x_{j-1}\}|$, то будем иметь

$$i_K(x_1,...,x_n)=\sum_{j=1}^{n}(x_j-r_j)\cdot\frac{(m-j)!}{(m-n)!}.$$

Аналогично, для $K=E_w^n$ (множество всех двоичных последовательностей длины n и веса w, т. е. содержащих ровно w вхождений единицы) получаем, как в [5],

$$i_K(x_1,...,x_n)=\sum_{j=1}^{n}x_j\binom{n-j}{w-x_1-\cdots-x_j}.$$

Принцип вложения может дать и сплошную нумерацию натуральными числами бесконечного множества [6]. Пусть, например, $A=N$,

$$K=\{<\kappa_1,...,\kappa_n>\,|\,\kappa_1>\cdots>\kappa_n\geqslant 1\},$$

$\varphi(a,b)$ — число монотонно убывающих последовательностей длины b, у которых максимум не превосходит a. Из очевидной рекуррентности

$$\varphi(a,b)=\sum_{j=1}^{a-b+1}\varphi(a-j,b-1)$$

и тождества

$$\sum_{s=b-1}^{a-1}\binom{s}{b-1}=\binom{a}{b}$$

по индукции получаем, что $\varphi(a,b)=\binom{a}{b}$. Тогда

$$\nu_K(x_1,\ldots,x_i)=\varphi(x_i-1,n-i)=\binom{x_i-1}{n-i}$$

и, следовательно, $i_K(x_1,\ldots,x_n)=\sum_{i=1}^{n}\binom{x_i-1}{n-i}$.

3. РАНДОМИЗАЦИЯ

Применение принципа вложения дает возможность учесть информацию о структуре массива с такой степенью подробности, какая необходима для получения взаимно однозначной и сплошной индексации. Проанализируем теперь другой крайний случай, когда информация о K совсем не используется. Термин «рандомизация», принятый в литературе для таких методов, отражает их ориентацию на массивы, строение которых хаотично или неизвестно (такие массивы можно рассматривать как сформировавшиеся в результате случайного выбора). Эффективность методов рандомизации естественно оценивать по усредненным характеристикам

$$\bar{\tau}=\frac{1}{|\Gamma|}\sum_{K\in\Gamma}\tau(K)\quad\text{и}\quad\bar{\sigma}=\frac{1}{|\Gamma|}\sum_{K\in\Gamma}\sigma(K).$$

Дальнейшие рассуждения проводим в предположении, что $\Gamma=\Gamma_\alpha$ — семейство всех α-элементных подмножеств U. Положим $|U|=t$, $\max_{x\in U} i(x)=\beta$, $U_j=\{x\,|\,x\in U,\ i(x)=j\}$ и $|U_j|=t_j$. Число таких $K\in\Gamma_\alpha$, для которых $|K\cap U_j|=s$ равно $\binom{t_j}{s}\binom{t-t_j}{\alpha-s}$, следовательно,

$$\bar{\tau}=\frac{1}{\alpha\binom{t}{\alpha}}\sum_{j=1}^{\beta}\sum_{s=0}^{t_j}s^2\binom{t_j}{s}\binom{t-t_j}{\alpha-s}.$$

Применяя тождество

$$\sum_{s=0}^{c}s^2\binom{a}{s}\binom{b}{c-s}=a(a-1)\binom{a+b-2}{c-2}+a\binom{a+b-1}{c-1},$$

получаем

$$\bar{\tau}=\frac{t-\alpha}{t-1}+\frac{\alpha-1}{t(t-1)}\sum_{j=1}^{\beta}t_j^2.$$

Минимум этого выражения по всем наборам $\langle t_1,\ldots,t_\beta\rangle$ таким, что $\sum_{i=1}^{\beta}t_i=t$, достигается при $t_1=\cdots=t_\beta=\frac{t}{\beta}$ и равен

$$\bar{\tau}_0=\frac{t-\alpha}{t-1}+\frac{(\alpha-1)t}{\beta(t-1)}.\qquad(3)$$

Рассмотрим теперь среднюю «неплотность»

$$\bar{\sigma}=\frac{1}{\alpha\binom{t}{\alpha}}\sum_{j=1}^{\beta}\sum_{K\in\Gamma_\alpha}t_{j,K},$$

где $t_{j,K}=\begin{cases}1, & \text{если } K\cap U_j=\varnothing,\\ 0, & \text{в противном случае.}\end{cases}$

Учитывая, что число таких $K\in\Gamma_\alpha$, для которых $K\cap U_j=\varnothing$, равно $\binom{t-t_j}{\alpha}$, получаем

$$\bar{\sigma}=\frac{1}{\alpha\binom{t}{\alpha}}\sum_{j=1}^{\beta}\binom{t-t_j}{\alpha}.$$

Так как функция $\binom{t-x}{\alpha}$ выпукла относительно x, то

$$\sum_{j=1}^{\beta}\binom{t-t_j}{\alpha}\geqslant\beta\binom{t-\frac{1}{\beta}\sum_{j=1}^{\beta}t_j}{\alpha}=\beta\binom{t\left(1-\frac{1}{\beta}\right)}{\alpha}$$

и равенство достигается при $t_1=\cdots=t_\beta=\frac{t}{\beta}$. Отсюда следует, что минимальное значение $\bar{\sigma}$ есть

$$\bar{\sigma}_0=\frac{\beta}{\alpha\binom{t}{\alpha}}\binom{t\left(1-\frac{1}{\beta}\right)}{\alpha} \tag{4}$$

и, как и $\bar{\tau}_0$, достигается при равномерном распределении. Равенства (3) и (4) уточняют хорошо известные приближенные оценки $\bar{\tau}_0\approx 1+\frac{\alpha}{\beta}$ и $\bar{\sigma}_0\approx\frac{\beta}{\alpha}e^{-\frac{\alpha}{\beta}}$, которые получаются из вероятностных соображений.

Итак, статистически оптимальным методом рандомизации является любой, при котором множества U_j, $j=\overline{1,\beta}$, равномощны. Отметим, что некоторые из популярных методов этого свойства не имеют (см. [1—3]), например, метод середины квадрата. Из оптимальных упомянем, как достаточно простой, метод деления с остатком, он показал наилучшие результаты и по итогам эксперимента [2].

4. ПРИНЦИП АППРОКСИМАЦИИ

Как было отмечено, единственный, но очень серьезный недостаток методов индексации, основанных на применении принципа вложения, состоит в необходимости вычисления сложных функций. Рандомизация преодолевает этот недостаток слишком большой ценой, так как задачи не носят массового характера, и поэтому даже хорошие средние значения не могут позволить считать вопрос исчерпанным. Необходим компромисс, который мы видим в применении ослабленного принципа вложения — принципа аппроксимации. Применение этого принципа включает два этапа: во-первых, принятие за основу некоторого вложения K в $<U, L>$ и, во-вторых, если вычислительная формула для индекса $i_K(x)$ оказывается слишком сложной, приближение функций, фигурирующих в исходной формуле, функциями какого-либо класса ограниченной сложности вычисления.

Рассмотрим одну из возможных реализаций для двоичного случая: $U=A^n$, $A=\{0,1\}$, L—лексикографический порядок на U, $K\subseteq<U,L>$. Согласно (2),

$$i_K(x_1,\ldots,x_n)=\sum_{j=1}^{n}x_j\cdot v_K(x_1,\ldots,x_{j-1},0),$$

определяет взаимно однозначное отображение $K \longrightarrow \{0, 1, ..., |K|-1\}$, но функции $\{\nu_K(x_1, ..., x_j) \mid j=\overline{1,n}\}$, как правило, слишком сложны (отсутствие аналитического задания и громоздкое табличное).

Возьмем следующее приближение. Пусть

$$\eta_K(j, w) = \binom{j-1}{w} \sum_{x_1+\cdots+x_{j-1}=w} \nu_K(x_1, ..., x_{j-1}, 0), \tag{5}$$

— среднее значение функции $\nu_K(x_1, ..., x_{j-1}, 0)$ на наборах веса w. Положим

$$i_K^*(x_1, ..., x_n) = \sum_{j=1}^{n} x_j \eta_K(j, x_1+\cdots+x_{j-1}), \tag{6}$$

и $i_K(x) = [i_K^*(x)]$.

Если $K_1 \cap K_2 = \varnothing$, то, очевидно,

$$\eta_{K_1 \cup K_2}(j, w) = \eta_{K_1}(j, w) + \eta_{K_2}(j, w), \tag{7}$$

и, следовательно,

$$i^*_{K_1 \cup K_2}(x) = i^*_{K_1}(x) + i^*_{K_2}(x).$$

Вычисление функций $\eta_K(j, w)$, $j=\overline{1,n}$, выполняется после однократного просмотра массива (т. е. в линейное по сравнению с объемом исходной информации время), причем таблица, ввиду (7), может заполняться последовательно, с просмотром строк и суммированием (предполагая, что биномиальные коэффициенты для усреднения вычислены заранее). Приемлем следующий алгоритм.

Пусть массив K представлен в виде двумерной таблицы $K = \|k_{ij}\|$, $i=\overline{1,t}$, $j=\overline{1,n}$, $k_{ij} \in \{0, 1\}$, строки которой суть слова из K.

1) Образуем таблицу $M = \|m_{ij}\|$, $i=\overline{1,t}$, $j=\overline{0,n-1}$, полагая $m_{i,0}=0$ для всех $i=\overline{1,t}$ и вычисляя последовательно элементы остальных столбцов по правилу

$$m_{i,j+1} = m_{i,j} + k_{i,j+1}, \quad j=\overline{0,n-1}.$$

Если $k_{i,j+1}=0$, то вычисленный элемент $m_{i,j+1}$ таблицы M помечаем.

2) Для любых $j=\overline{1,n}$ и $w=\overline{0,n-1}$ значение $\binom{j-1}{w} \cdot \eta_K(j, w)$ равно числу помеченных элементов w в j-м столбце таблицы M. С помощью таблицы биномиальных коэффициентов находим табличное задание функции η_K.

Проиллюстрируем действие алгоритма на примере (помеченные элементы обведены кружком): см. стр. 11.

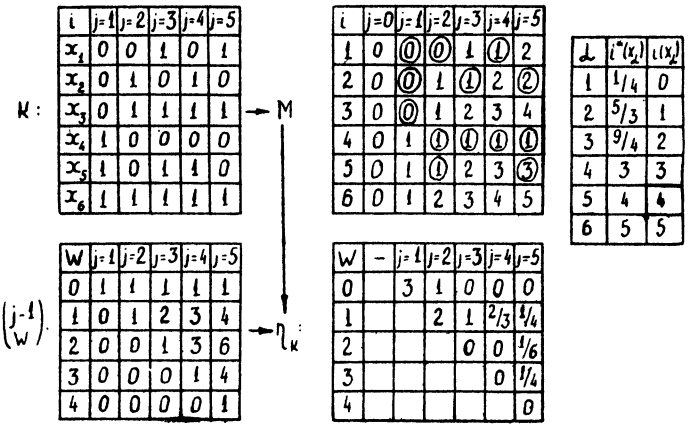
Как видим, в данном случае получились идеальные характеристики индексации: $\mu=\tau=1$, $\sigma=0$.

Заметим, что для любого $x = x_1 x_2 \ldots x_n$ имеет место

$$i^*_{\{x\}}(x) = \sum_{j=1}^{n} x_j \eta_K(j, x_1+\cdots+x_{j-1}) = 0.$$

Следующая теорема устанавливает верхнюю границу для $\mu(K, i)$.

Теорема. Пусть $\mu_0 = \frac{4}{3} + \frac{2\pi}{9\sqrt{3}} \approx 1{,}74$. Тогда $\mu(K, i) < \mu_0$ для любого K и $\lim\limits_{n\to\infty} \max\limits_{K \subseteq A^n} \mu(K, i) = \mu_0$.



Доказательство. Оценим наибольшее значение, которое может принимать индекс, вычисляемый по формулам (5) и (6). Пусть x^0 таково, что $\max\limits_{x\in K} i_K(x) = i_K(x^0)$. Представим это слово в виде

$$x^0 = 0^{p_0}1^{q_1}0^{p_1}1^{q_2}\ldots 0^{p_{s-1}}1^{q_s}0^{p_s},$$

где $p_0,\ p_s \geqslant 0,\ p_1, \ldots, p_{s-1} > 0,\ q_1, \ldots, q_s > 0$, и обозначим $P_j = p_1 + \cdots + p_j$, $Q_j = q_1 + \cdots + q_j$, $Q_0 = 0$. Тогда

$$i_K^*(x^0) = \sum_{j=0}^{s-1} \sum_{w=0}^{q_{j+1}-1} \eta_K(P_j+Q_j+w+1,\ Q_j+w) =$$

$$= \sum_{j=0}^{s-1} \sum_{w=0}^{q_{j+1}-1} \binom{P_j+Q_j+w}{Q_j+w}^{-1} |K(P_j+Q_j+w+1,\ Q_j+w)|,$$

где $K(l, v)$ — множество тех x из K, у которых $x_l = 0$ и префикс длины $l-1$ имеет вес v. Легко убедиться в справедливости неравенства

$$\binom{a+b}{a} \geqslant \binom{2c}{c}, \tag{8}$$

где $c = \min(a, b)$, а так как $\binom{2c}{c}$ возрастает с ростом c, то (8) справедливо также при $c < \min(a, b)$. Учитывая еще, что $P_j \geqslant j$, $Q_j \geqslant j$, получаем

$$i_K^*(x^0) \leqslant \sum_{j=0}^{s-1} \binom{2j}{j}^{-1} \sum_{w=0}^{q_{j+1}-1} |K(P_j+Q_j+w+1,\ Q_j+w)|. \tag{9}$$

Множества $K(l, v)$ и $K(l+u, v+u)$ при $u > 0$ не пересекаются. Действительно, если x — общий элемент этих множеств, то $x_1 + \cdots + x_{l-1} = v$, $x_1 + \cdots + x_{l+u-1} = v+u$, откуда $x_l + x_{l+1} + \cdots + x_{l+u-1} = u$, а это возможно, только тогда, когда каждое слагаемое равно единице, но по условию $x_l = 0$. Отсюда следует, что каждая из внутренних сумм в (9) не превосходит $|K|-1$, т. е.

$$i_K(x^0) \leqslant (|K|-1) \sum_{j=0}^{s-1} \binom{2j}{j}^{-1}.$$

Следовательно, верхней границей для $\mu(K, i)$ является

$$\mu < \mu_0 = \sum_{j=0}^{\infty} \binom{2j}{j}^{-1}.$$

исленное значение можно получить, рассматривая ряд

$$F(x)=\sum_{j=0}^{\infty}\binom{2j}{j}^{-1}(2x)^{2j},$$

сходящийся при $|x|<1$. $F(x)$ удовлетворяет уравнению

$$x(x^2-1)F'+(2x^2+1)F-1=0$$

и начальному условию $F'(0)=0$. Интегрируя, находим

$$F(x)=\frac{1}{1-x^2}+\frac{x}{(1-x^2)^{3/2}}\arcsin x$$

и окончательно получаем

$$\mu_0=F\left(\frac{1}{2}\right)=\frac{4}{3}+\frac{2\pi}{9\sqrt{3}}\approx 1{,}74.$$

Остается построить последовательность множеств, на которой реализуется приближение к предельному значению μ_0. Пусть

$$K_{p,q}=(01)^p A^q \cup \{(10)^p 0^q\} \quad (n=2p+q,\ |K_{p,q}|=1+2^q).$$

Для этого массива $\eta_K(2j+1,j)=2^q\binom{2j}{j}^{-1}$, $j=\overline{0,p-1}$, $i_K^*((10)^p0^q)=$ $=2^q\sum_{j=0}^{p-1}\binom{2j}{j}^{-1}$ и легко проверить, что $\mu(K_{p,q})\longrightarrow\mu_0$ при $p,q\longrightarrow\infty$. Теорема доказана.

Замечание. Рассмотренный в доказательстве класс массивов $K_{p,q}$ показывает, что при рассматриваемом методе индексации синонимия может быть значительной. Так, в случае $p=q=3$ имеем

Таблица

x	$i^*(x)$	$i(x)$
010101000	0	0
010101001	1/28	0
010101010	3/35	0
010101011	4/35	0
010101100	1/4	0
010101101	39/140	0
010101110	43/140	0
010101111	91/280	0
101010000	40/3	13

Массивы $K_{p,q}$ интересны еще в одном отношении. Для обращенного (т. е. переписанного справа налево) массива

$$K'_{p,q}=A^q(10)^p\cup\{0^q(01)^p\}$$

индексация оказывается уже взаимно однозначной и сплошной:

$$i_{K'}(0^q(01)^p)=0,$$

$$i_{K'}(0^q(10)^p)=\left[\sum_{j=0}^{p}\binom{q+2j}{j}^{-1}\right]=1,\ \text{если } q>0 \quad (\text{так как } \binom{q+2j}{i}\geqslant$$

$\geqslant 2^j$, имеем $\sum_{j=0}^{q}\binom{q+2j}{j}^{-1}<2$), и при $\alpha\neq 0^q$

$$i_{K'}(\alpha(10)^p)=1+i^0(\alpha),$$

где $i^0(\alpha)$ —номер α в лексикографическом упорядочении слов длины q.

Таким образом, перестановка столбцов массива может значительно повысить эффективность метода индексации.

Нами был проведен вычислительный эксперимент, в котором метод, описанный в этом разделе, сравнивался с двумя другими методами индексации, описанными в литературе, и своего рода рекордными. Один из них — метод деления с остатком, лучший из известных методов рандомизации. Другой — метод, основанный на выборе разрядов ключа, в которых распределение символов наиболее близко к равномерному (подробное описание см. в [2]), один из немногого числа известных методов, учитывающих информацию о массиве. Методы тестировались на 60 массивах псевдослучайных чисел по 1000 элементов в каждом, определялись величины τ и σ. Лучшие результаты в большинстве случаев показал метод деления с остатком (типичные значения $\tau=1{,}95\div 2{,}05$, $\sigma=0{,}35\div 0{,}37$), близок к нему метод, описанный выше ($\tau=2{,}05\div 2{,}15$, $\sigma=0{,}37\div 0{,}39$), третий метод оказался значительно хуже ($\tau=2{,}85\div 3{,}0$, $\sigma=0{,}57\div 0{,}60$). Таким образом, хотя на случайных массивах лучшей является рандомизированная стратегия, методы индексации, основанные на принципах вложения и аппроксимации, оказываются с ней конкурентоспособными, приводя к гораздо лучшим результатам на массивах, обладающих регулярной структурой. Кроме встречавшихся уже примеров, рассмотренная реализация дает взаимно однозначную сплошную индексацию для всех симметричных массивов (включающих вместе с любым словом любую его перестановку), для любых подмножеств множества $\{0^i\,1\,0^{n-i-1}\mid 0\leqslant i\leqslant n-1\}\cup\{1^i\,0^{n-i}\mid 0\leqslant i\leqslant n\}$ и многих других.

ЛИТЕРАТУРА

1. Джадд Д. Р. Работа с файлами. М., Мир, 1975.
2. Zum V. Y., P. S. T. Yuen, M. Dodd. Key-to-adress transform techniques: a fundamental performance study on large existing formatted files, Commun. of the ACM, v. **14**, N 4, 1971, p. 228.
3. Кнут Д. Искусство программирования для ЭВМ, т. 3. М., Мир, 1978.
4. Cover T. M. Enumerative source encoding, IEEE Trans, v. IT-19, № 1, 1973, p. 73.
5. Мудров В. И. Алгоритм нумерации сочетаний. Журн. «Вычислит. математики и мат. физики», 5, № 4, 776 (1965).
6. Bosset P. G. A Combinatorial theorem. Canad. Math Bull. v. 9, N 4, 1966, p. 515.

Горьковский государственный университет

[18/VII 1977]

О ДВОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ С ОГРАНИЧЕННОЙ АВТОКОРРЕЛЯЦИЕЙ

В. Е. Алексеев, Н. А. Маслова

Пусть $E=\{0, 1\}$. Последовательность $\alpha=(\alpha_1, \ldots, \alpha_n)\in E^n$ назовем (κ, r)-последовательностью, если выполняются условия:

1) $\sum\limits_{i=1}^{n}\alpha_i=\kappa$;

2) $\sum\limits_{i=1}^{n-t}\alpha_i\alpha_{i+t}\leqslant r$ при $t=1, 2, \ldots, n-1$.

Иначе говоря, (κ, r)-последовательности — это последовательности веса κ (т. е. содержащие ровно κ единиц), для которых значения апе-

риодической автокорреляционной функции при ненулевых сдвигах ограничены величиной r. Последовательности с такими свойствами применяются для построения сигналов, устойчивых к действию помех [1], а также некоторых классов корректирующих кодов [2]. В приложениях важно, чтобы при данных κ и r длина (κ, r)-последовательности была минимальна. Такие последовательности будем называть оптимальными. Очевидно, оптимальная (κ, r)-последовательность начинается и оканчивается единицей.

Случай $r=1$ рассматривался в ряде работ, библиографию и, по-видимому, наиболее обширную таблицу известных $(\kappa, 1)$-последовательностей можно найти в [1]. При $r>1$ о (κ, r)-последовательностях известно очень мало. В настоящей статье выводится нижняя граница длины (κ, r)-последовательностей и предлагается эвристический алгоритм построения (κ, r)-последовательностей для произвольных κ и r.

1. Множество целых чисел $A=\{a_1, \ldots, a_\kappa\}$ назовем $\Delta(\kappa, r)$-множеством, если среди разностей $a_i - a_j$ каждое натуральное число встречается не более чем r раз.

Каждой последовательности $\alpha \in E^n$ веса κ можно поставить в соответствие множество целых чисел $A(\alpha)=\{a_1, \ldots, a_\kappa\}$ номеров позиций, в которых расположены единицы последовательности α. Равенство $\sum_{i=1}^{n-t} \alpha_i \alpha_{i+t} = s$ равносильно тому, что среди разностей $a_i - a_j$ число t встречается точно s раз. Поэтому α является (κ, r)-последовательностью тогда и только тогда, когда $A(\alpha)$ есть $\Delta(\kappa, r)$-множество.

Отметим сходство определения $\Delta(\kappa, r)$-множества с определением разностного множества [3]. Легко понять, что разностное множество с параметрами (v, κ, λ) является $\Delta(\kappa, \lambda)$-множеством. Это позволяет переносить известные результаты из теории разностных множеств на (κ, r)-последовательности — обстоятельство, которому мы обязаны почти всем, что в настоящее время известно о (κ, r)-последовательностях.

Если A — конечное множество чисел, то через $l(A)$ обозначим разность между наибольшим и наименьшим элементами A. Через $L(\kappa, r)$ обозначим наименьшее n, при котором существует $\Delta(\kappa, r)$-множество A с $l(A)=n$. Из сказанного выше ясно, что $L(\kappa, r)$ на единицу меньше длины оптимальной (κ, r)-последовательности.

Пусть $A=\{a_1, \ldots, a_\kappa\}$ является $\Delta(\kappa, r)$-множеством, причем $a_i < a_j$ при $i<j$. Тогда среди разностей $a_i - a_j$, где $i>j$, каждое натуральное число от 1 до $l(A)$ встречается не более чем r раз. Отсюда следует неравенство

$$L(\kappa, r) \geqslant \frac{\kappa(\kappa-1)}{2r}.$$

Более сильную нижнюю оценку можно получить способом, который был применен для аналогичной задачи в [4]. Выберем какое-нибудь натуральное число t, $1 \leqslant t \leqslant \kappa-1$, и рассмотрим величину

$$S=\sum_{j=1}^{t} \sum_{i=1}^{\kappa-j} (a_{i+j}-a_i). \qquad (1)$$

Эта сумма состоит из $N=\frac{t(2\kappa-t-1)}{2}$ слагаемых, причем каждое натуральное число входит в качестве слагаемого не более чем r раз. Поэтому

$$S \geqslant r\left(1+2+\cdots+\left[\frac{N}{r}\right]\right)+\left(N-r\left[\frac{N}{r}\right]\right)\left(\left[\frac{N}{r}\right]+1\right)=$$

$$= \left(N - \frac{r}{2}\left[\frac{N}{r}\right]\right)\left(\left[\frac{N}{r}\right]+1\right). \qquad (2)$$

С другой стороны, перегруппировкой слагаемых в (1), получаем

$$S = \sum_{i=0}^{t-1} (t-i)(a_\kappa - a_{i+1}) = \frac{t(t+1)}{2}(a_\kappa - a_1) - \sum_{i=1}^{t-1} (t-i)(a_\kappa - a_{\kappa-i} + a_{i+1} - a_1).$$

Отсюда и из (2), так как $a_\kappa - a_1 = l(A)$, следует

$$l(A) \geqslant \frac{1}{t(t+1)}\left(t(2\kappa - t - 1) - r\left[\frac{t(2\kappa-t-1)}{2r}\right]\left(\left[\frac{t(2\kappa-t-1)}{2r}\right]+1\right)\right) + \frac{2}{t(t+1)}\sum_{i=1}^{t-1}(t-i)(a_\kappa - a_{\kappa-i} + a_{i+1} - a_1). \qquad (3)$$

Так как $a_\kappa - a_{\kappa-i} + a_{i+1} - a_1 > 0$, то из (3) следует

$$l(A) > \frac{t(2\kappa-t-1)^2}{4r(t+1)}.$$

Полагая $t = O(\sqrt{\kappa})$, из последнего неравенства получаем следующую оценку.

Теорема. $L(\kappa, r) > \frac{1}{r}(\kappa^2 - O(\kappa^{3/2}))$.

Для получения численных результатов можно оценить величины $a_\kappa - a_{\kappa-i} + a_{i+1} - a_1$, например, используя тождество

$$a_\kappa - a_{\kappa-i} + a_{i+1} - a_1 = \sum_{j=0}^{i-1}(a_{\kappa-j} - a_{\kappa-j-1}) + \sum_{j=0}^{i-1}(a_{i+1-j} - a_{i+j}).$$

Среди $2i$ слагаемых в правой части каждое натуральное число встречается не более r раз, поэтому

$$a_\kappa - a_{\kappa-i} + a_{i+1} - a_1 \geqslant r\left(1+2+\cdots+\left[\frac{2i}{r}\right]\right) + \left(2i - r\left[\frac{2i}{r}\right]\right)\left(\left[\frac{2i}{r}\right]+1\right) = \left(2i - \frac{r}{2}\left[\frac{2i}{r}\right]\right)\left(\left[\frac{2i}{r}\right]+1\right).$$

Следовательно,

$$L(\kappa, r) \geqslant \frac{1}{t(t+1)}\left((2\kappa - t - 1)t - r\left[\frac{t(2\kappa-t-1)}{2r}\right]\left(\left[\frac{t(2\kappa-t-1)}{2r}\right]+1\right)\right) + \frac{2}{t(t+1)}\sum_{i=0}^{t-1}\left(2i - \frac{r}{2}\left[\frac{2i}{r}\right]\left(\left[\frac{2i}{r}\right]+1\right)\right)(t-i).$$

2. Приступим к описанию алгоритма построения $\Delta(\kappa, r)$-множеств. Начав с какого-либо известного $\Delta(\kappa_0, r)$-множества с $\kappa_0 < \kappa$, будем применять операцию расширения, увеличивая каждый раз мощность множества на единицу, пока не придем к $\Delta(\kappa, r)$-множеству с требуемым κ. Операция расширения состоит в следующем. Пусть $A = \{a_1, \ldots, a_\kappa\}$ является $\Delta(\kappa, r)$-множеством, причем $a_i < a_j$ при $i < j$. Обозначим через $r(A, d)$ количество таких i, что $a_{i+1} - a_i = d$. Рассмотрим множество $M(A)$ таких чисел d, что $d \leqslant l(A)+1$ и $r(A, d) < r$. Выберем наименьший элемент m множества $M(A)$ и рассмотрим множества

$$A^{(t)} = \{a_1, \ldots, a_t, a_t + m, a_{t+1} + m, \ldots, a_\kappa + m\}, \quad t = 1, \ldots, \kappa.$$

Относительно каждого из $A^{(t)}$ проверим, является ли оно $\Delta(\kappa+1, r)$-множеством. Если такое найдется, то оно является искомым результатом.

В противном случае выбираем в качестве m следующий по величине элемент множества $M(A)$ и повторяем описанную процедуру. Этот процесс всегда заканчивается результативно, так как, очевидно, $l(A)+1 \in M(A)$ и $\{a_1, a_2, ..., a_\kappa, a_\kappa+l(A)+1\}$ является $\Delta(\kappa+1, r)$-множеством.

Множество $\{1, 2, ..., r+1\}$, очевидно, является $\Delta(r+1, r)$-множеством при любом r. Отправляясь от него и применяя операцию расширения, можно построить $\Delta(\kappa, r)$-множество с любым κ.

Рассмотрим пример. Пусть $A=\{0, 1, 4, 6\}$. Нетрудно проверить, что A является $\Delta(4, 1)$-множеством. Множество $M(A)$ состоит из таких чисел d, что $1 \leqslant d \leqslant 7$ и $r(A, d)=0$, т. е. d не должно быть равно ни одной из разностей вида $a_{i+1}-a_i$. В данном случае исключаются значения 1, 2, 3. Следовательно, $M(A)=\{4, 5, 6, 7\}$. Выбираем наименьший элемент $m=4$ и образуем множества

$$A^{(1)}=\{0, 4, 5, 8, 10\},$$
$$A^{(2)}=\{0, 1, 5, 8, 10\},$$
$$A^{(3)}=\{0, 1, 4, 8, 10\},$$
$$A^{(4)}=\{0, 1, 4, 6, 10\}.$$

Ни одно из них не является $\Delta(5, 1)$-множеством, поэтому выбираем следующий по величине элемент $m=5$. Образуем множества

$$A^{(1)}=\{0, 5, 6, 9, 11\},$$
$$A^{(2)}=\{0, 1, 6, 9, 11\},$$
$$A^{(3)}=\{0, 1, 4, 9, 11\},$$
$$A^{(4)}=\{0, 1, 4, 6, 11\}$$

и убеждаемся, что $A^{(3)}$ является $\Delta(5,1)$-множеством.

Следует отметить эвристический характер этого алгоритма, он не гарантирует получения оптимального решения, более того, мы не можем даже указать приемлемых оценок длины получаемых последовательностей. Экспериментальные данные, однако, показывают, что во многих случаях этот метод дает хорошие результаты при сравнительно невысокой трудоемкости. В таблице приводятся $\Delta(\kappa, r)$-множества,

Таблица

r	κ	$\Delta(\kappa, r)$-множество	$L(\kappa, r)$
1	8	0, 1, 4, 9, 15, 22, 32, 34	32
2	5	0, 1, 3, 5, 6	6
2	6	0, 1, 3, 5, 8, 9	9
2	7	0, 1, 3, 7, 8, 11, 13	13
2	8	0, 1, 3, 7, 9, 14, 17, 18	17
2	9	0, 1, 3, 7, 9, 14, 19, 22, 23	22
2	10	0, 1, 3, 7, 9, 14, 19, 27, 30, 31	28
2	11	0, 1, 3, 7, 9, 16, 21, 26, 34, 37, 38	35
2	12	0, 1, 3, 7, 9, 16, 26, 31, 36, 44, 47, 48	42
2	13	0, 1, 3, 7, 9, 16, 27, 37, 42, 47, 55, 58, 59	50

Продолжение таблицы

r	κ	Δ (κ, r)-множество	$L(\kappa, r)$
2	14	0, 1, 3, 7, 9, 16, 27, 41, 51, 56, 61, 69, 72, 73	59
2	15	0, 1, 3, 7, 9, 16, 28, 39, 53, 63, 68, 73, 81, 84, 85	69
2	16	0, 1, 3, 7, 9, 16, 30, 42, 53, 67, 77, 82, 87, 95, 98, 99	79
2	17	0, 17, 18, 20, 24, 26, 33, 47, 59, 70, 84, 94, 99, 104, 112, 115, 116	90
2	18	0, 17, 18, 20, 24, 26, 33, 47, 59, 70, 84, 108, 118, 123, 128, 136, 139, 140	103
2	19	0, 17, 18, 20, 24, 26, 33, 47, 59, 70, 84, 106, 130, 140, 145, 150, 158, 161, 162	116
2	20	0, 17, 18, 20, 24, 26, 33, 47, 59, 70, 84, 106, 125, 149, 159, 164, 169, 177, 180, 181	129
2	21	0, 17, 18, 20, 24, 26, 33, 47, 59, 70, 84, 106, 125, 144, 168, 178, 183, 188, 196, 199, 200	144
2	22	0, 17, 18, 20, 24, 26, 33, 47, 59, 70, 84, 106, 135, 154, 173, 197, 207, 212, 217, 225, 228, 229	159
3	7	0, 1, 2, 4, 6, 9, 10	10
3	8	0, 1, 2, 4, 6, 9, 12, 13	13
3	9	0, 1, 3, 5, 9, 10, 13, 15, 16	16
3	10	0, 1, 2, 6, 11, 13, 15, 18, 21, 22	20
3	11	0, 1, 2, 6, 11, 13, 15, 18, 21, 24, 25	24
3	12	0, 1, 2, 6, 11, 18, 20, 22, 25, 28, 31, 32	29
3	13	0, 1, 3, 8, 10, 16, 20, 24, 25, 31, 34, 36, 37	35
3	14	0, 1, 3, 8, 10, 16, 26, 30, 34, 35, 41, 44, 46, 47	41
3	15	0, 1, 3, 8, 10, 16, 26, 30, 34, 35, 45, 51, 54, 56, 57	47
3	16	0, 1, 3, 8, 10, 16, 23, 33, 37, 41, 42, 52, 58, 61, 63, 64	54
3	17	0, 1, 3, 8, 10, 16, 23, 34, 44, 48, 52, 53, 63, 69, 72, 74, 75	62
3	18	0, 1, 3, 8, 10, 16, 23, 34, 44, 48, 52, 53, 63, 69, 80, 83, 85, 86	70
3	19	0, 1, 3, 8, 10, 16, 23, 36, 47, 57, 61, 65, 66, 76, 82, 93, 96, 98, 99	78
3	20	0, 1, 2, 6, 17, 30, 43, 52, 57, 65, 73, 80, 89, 91, 101, 103, 106, 109, 112, 113	88
3	21	0, 1, 2, 6, 17, 30, 37, 50, 59, 64, 72, 80, 87, 96, 98, 108, 110, 113, 116, 119, 120	98
3	22	0, 1, 2, 6, 17, 31, 44, 51, 64, 73, 78, 86, 94, 101, 110, 112, 122, 124, 127, 130, 133, 134	108
3	23	0, 1, 2, 6, 30, 41, 55, 68, 75, 88, 97, 102, 110, 118, 125, 134, 136, 146, 148, 151, 154, 157, 158	119
3	24	0, 18, 19, 21, 26, 28, 34, 41, 54, 66, 78, 90, 108, 119, 129, 133, 137, 138, 148, 154, 165, 168, 170, 171	130
3	25	18, 19, 21, 26, 28, 34, 41, 54, 68, 80, 92, 104, 122, 133, 143, 147, 151, 152, 162, 168, 179, 182, 184, 185	142
3	26	0, 18, 19, 21, 26, 28, 34, 41, 54, 78, 92, 104, 116, 128, 146, 157, 167, 171, 175, 176, 186, 192, 203, 206, 208, 209	155

Продолжение таблицы

r	κ	$\Delta(\kappa, r)$-множество	$L(\kappa, r)$
4	8	0, 1, 2, 3, 5, 7, 8, 10	10
4	9	0, 1, 2, 4, 6, 7, 9, 12, 13	13
4	10	0, 1, 3, 5, 7, 8, 12, 13, 15, 16	16
4	11	0, 1, 6, 8, 10, 12, 13, 17, 18, 20, 21	19
4	12	0, 1, 6, 8, 10, 12, 17, 18, 22, 23, 25, 26	23
4	13	0, 1, 6, 8, 10, 12, 17, 18, 23, 27, 28, 30, 31	27
4	14	0, 1, 6, 8, 10, 12, 17, 23, 24, 29, 33, 34, 36, 37	32
4	15	0, 1, 6, 8, 14, 16, 18, 23, 29, 30, 35, 39, 40, 42, 43	37
4	16	0, 1, 6, 8, 14, 22, 24, 26, 31, 37, 38, 43, 47, 48, 50, 51	42
4	17	0, 1, 6, 8, 14, 22, 24, 26, 35, 40, 46, 47, 52, 56, 57, 59, 60	48
4	18	0, 3, 4, 9, 11, 17, 25, 27, 29, 38, 43, 49, 50, 55, 59, 60, 62, 63	54
4	19	0, 3, 4, 9, 11, 17, 25, 27, 29, 38, 47, 52, 58, 59, 64, 68, 69, 71, 72	60
4	20	0, 3, 4, 9, 11, 19, 25, 33, 35, 37, 46, 55, 60, 66, 67, 72, 76, 77,79, 80	67
4	21	0, 3, 4, 9, 11, 19, 25, 33, 35, 37, 48, 57, 66, 71, 77, 78, 83, 87, 88, 90, 91	75
4	22	0, 3, 4, 9, 20, 22, 30, 36, 44, 46, 48, 59, 68, 77, 82, 88, 89, 94, 98, 99, 101, 102	82
4	23	0, 3, 4, 9, 20, 22, 30, 36, 44, 46, 48, 59, 68, 77, 91, 96, 102, 103, 108, 112, 113, 115, 116	91
4	24	0, 3, 4, 9, 20, 22, 30, 44, 50, 58, 60, 62, 73, 82, 91, 105, 110, 116, 117, 122, 126, 127, 129, 130	99
4	25	0, 3, 4, 9, 20, 22, 30, 44, 50, 58, 60, 62, 73, 82, 91, 105, 110, 116, 117, 122, 126, 137, 138, 140, 141	108
4	26	0, 3, 4, 9, 20, 22, 30, 44, 50, 60, 62, 73, 82, 91, 108, 122, 127, 133, 134, 139, 143, 154, 155, 157, 158	118
5	10	0, 1, 2, 3, 5, 7, 8, 10, 13, 14	14
5	11	0, 1, 2, 3, 6, 8, 10, 11, 13, 16, 17	16
5	12	0, 1, 2, 3, 7, 10, 12, 14, 15, 17, 20, 21	19
5	13	0, 1, 2, 3, 7, 10, 12, 14, 17, 18, 20, 23, 24	23
5	14	0, 1, 2, 3, 7, 11, 14, 16, 18, 21, 22, 24, 27, 28	26
5	15	0, 1, 2, 3, 8, 12, 16, 19, 21, 23, 26, 27, 29, 32, 33	30
5	16	0, 1, 2, 3, 8, 13, 17, 21, 24, 26, 28, 31, 32, 34, 37, 38	35
5	17	0, 1, 2, 3, 8, 13, 17, 21, 24, 29, 31, 33, 36, 37, 39, 42, 43	39
5	18	0, 1, 2, 3, 8, 13, 17, 21, 24, 29, 31, 33, 38, 41, 42, 44, 47, 48	44
5	19	0, 1, 2, 3, 8, 14, 19, 23, 27, 30, 35, 37, 39, 44, 47, 48, 50, 53, 54	49

r	κ	$\Delta(\kappa, r)$-множество	$L(\kappa, r)$
5	20	0, 1, 2, 3, 8, 16, 22, 27, 31, 35, 38, 43, 45, 47, 52, 55, 56, 58, 61, 62	55
5	21	0, 1, 2, 3, 8, 16, 22, 27, 31, 35, 38, 43, 45, 47, 56, 61, 64, 65, 67, 70, 71	61
5	22	0, 1, 2, 3, 8, 15, 23, 29, 34, 38, 42, 45, 50, 52, 54, 63, 68, 71, 72, 74, 77, 78	67
5	23	0, 1, 2, 3, 8, 15, 23, 29, 34, 38, 42, 45, 50, 57, 59, 61, 70, 75, 78, 79, 81, 84, 85	74
5	24	0, 1, 2, 3, 8, 15, 23, 29, 34, 38, 42, 50, 57, 59, 61, 70, 75, 86, 89, 90, 92, 95, 96	81
5	25	0, 1, 2, 3, 8, 15, 23, 29, 42, 47, 51, 55, 58, 63, 70, 72, 74, 83, 88, 99, 102, 103, 105, 108, 109	88
5	26	0, 1, 2, 3, 10, 15, 22, 30, 36, 49, 54, 58, 62, 65, 70, 77, 79, 81, 90, 95, 106, 109, 110, 112, 115, 116	96
5	27	0, 1, 2, 3, 10, 15, 22, 30, 36, 49, 62, 67, 71, 75, 78, 83, 90, 92, 94, 103, 108, 119, 122, 123, 125, 128, 129	103
6	12	0, 1, 2, 4, 6, 7, 10, 12, 13, 15, 16, 17	17
6	13	0, 1, 3, 5, 6, 9, 10, 11, 13, 16, 17, 18, 20	20
6	14	0, 1, 3, 5, 6, 9, 13, 14, 15, 17, 20, 21, 22, 24	23
6	15	0, 1, 3, 5, 6, 9, 13, 14, 15, 19, 21, 24, 25, 26, 28	26
6	16	0, 1, 3, 5, 6, 9, 13, 14, 15, 19, 21, 24, 27, 28, 29, 31	30
6	17	0, 1, 3, 5, 6, 9, 13, 18, 19, 20, 24, 26, 29, 32, 33, 34, 36	34
6	18	0, 1, 3, 5, 6, 9, 13, 18, 19, 20, 25, 29, 31, 34, 37, 38, 39, 41	38
6	19	0, 1, 3, 5, 10, 11, 14, 18, 23, 24, 25, 30, 34, 36, 39, 42, 43, 44, 46	42
6	20	0, 1, 3, 5, 10, 11, 14, 18, 24, 29, 30, 31, 36, 40, 42, 45, 48, 49, 50, 52	47
6	21	0, 1, 3, 5, 10, 11, 14, 18, 24, 29, 30, 31, 38, 43, 47, 49, 52, 55, 56, 57, 59	52
6	22	0, 1, 3, 5, 10, 11, 14, 18, 24, 29, 30, 31, 38, 44, 49, 53, 55, 58, 61, 62, 63, 65	57
6	23	0, 1, 3, 5, 10, 18, 19, 22, 26, 32, 37, 38, 39, 46, 52, 57, 61, 63, 66, 69, 70, 71, 73	63
6	24	0, 1, 3, 5, 10, 18, 19, 22, 26, 32, 38, 43, 44, 45, 52, 58, 63, 67, 69, 72, 75, 76, 77, 79	68
6	25	0, 1, 3, 5, 10, 18, 19, 22, 26, 32, 38, 43, 44, 45, 52, 58, 63, 67, 73, 75, 78, 81, 82, 83, 84	74
6	26	0, 1, 3, 5, 10, 18, 19, 22, 25, 29, 38, 43, 44, 45, 52, 61, 67, 72, 76, 82, 84, 87, 90, 91, 92, 94	81
6	27	0, 1, 3, 12, 14, 19, 27, 28, 31, 35, 41, 47, 52, 53, 54, 61, 70, 76, 81, 85, 91, 93, 96, 99, 100, 101, 103	87
7	13	0, 2, 3, 4, 5, 7, 9, 10, 13, 14, 15, 17, 18	18
7	14	0, 2, 3, 4, 5, 7, 9, 10, 13, 14, 15, 17, 20, 21	20
7	15	0, 2, 3, 4, 8, 9, 11, 13, 14, 17, 18, 19, 21, 24, 25	23
7	16	0, 2, 3, 4, 8, 9, 11, 13, 14, 17, 20, 21, 22, 24, 27, 28	26

r	κ	Δ (κ, r)-множество	$L(\kappa, r)$
7	17	0, 2, 3, 4, 9, 13, 14, 16, 18, 19, 22, 25, 26, 27, 29, 32, 33	30
7	18	0, 2, 3, 4, 9, 13, 14, 16, 18, 19, 22, 25, 29, 30, 31, 33, 36, 37	33
7	19	0, 2, 3, 4, 9, 13, 14, 16, 18, 19, 23, 26, 29, 33, 34, 35, 37, 40, 41	37
7	20	0, 2, 3, 4, 10, 15, 19, 20, 22, 24, 25, 29, 32, 35, 39, 40, 41, 43, 46, 47	41
7	21	0, 2, 3, 4, 10, 16, 21, 25, 26, 28, 30, 31, 35, 38, 41, 45, 46, 47, 49, 52, 53	45
7	22	0, 2, 3, 4, 10, 16, 21, 25, 26, 28, 30, 35, 36, 40, 43, 46, 50, 51, 52, 54, 57, 58	50
7	23	0, 2, 3, 4, 10, 16, 21, 25, 26, 28, 30, 35, 36, 40, 43, 49, 52, 53, 54, 56, 59, 60, 64	55
7	24	0, 2, 3, 4, 11, 17, 23, 28, 32, 33, 35, 37, 42, 43, 47, 50, 56, 59, 63, 64, 65, 67, 70, 71	60
7	25	0, 8, 10, 11, 12, 19, 25, 31, 36, 40, 41, 43, 45, 50, 51, 55, 58, 64, 67, 71, 72, 73, 75, 78, 79	65
7	26	0, 8, 10, 11, 12, 19, 25, 31, 36, 40, 41, 43, 45, 53, 58, 59, 63, 66, 72, 75, 79, 80, 81, 83, 86, 87	70
7	27	0, 2, 10, 12, 13, 14, 21, 27, 33, 38, 42, 43, 45, 47, 55, 60, 61, 65, 68, 74, 77, 81, 82, 83, 85, 88, 89	76
8	14	0, 1, 2, 4, 5, 7, 9, 10, 12, 13, 14, 16, 17, 18	18
8	15	0, 1, 2, 4, 7, 8, 10, 12, 13, 15, 16, 17, 19, 20, 21	21
8	16	0, 1, 2, 4, 7, 8, 10, 12, 13, 15, 18, 19, 20, 22, 23, 24	24
8	17	0, 1, 2, 4, 7, 8, 11, 13, 15, 16, 18, 21, 22, 23, 25, 26, 27	27
8	18	0, 1, 2, 4, 7, 8, 11, 13, 17, 19, 20, 22, 25, 26, 27, 29, 30, 31	30
8	19	0, 1, 2, 4, 7, 11, 12, 15, 17, 21, 23, 24, 26, 29, 30, 31, 33, 34, 35	33
8	20	0, 1, 2, 4, 7, 11, 12, 15, 17, 21, 23, 24, 26, 29, 30, 31, 34, 36, 37, 38	37
8	21	0, 1, 2, 4, 7, 11, 12, 15, 17, 21, 23, 24, 26, 30, 33, 34, 35, 38, 40, 41, 42	40
8	22	0, 1, 2, 4, 7, 12, 16, 17, 20, 22, 26, 28, 29, 31, 35, 38, 39, 40, 43, 45, 46, 47	44
8	23	0, 1, 2, 4, 7, 12, 16, 17, 20, 25, 27, 31, 33, 34, 36, 40, 43, 44, 45, 48, 50, 51, 52	49
8	24	0, 1, 2, 4, 7, 12, 16, 17, 20, 26, 31, 33, 37, 39, 40, 42, 46, 49, 50, 51, 54, 56, 57, 58	53
8	25	0, 1, 2, 4, 7, 12, 16, 17, 20, 26, 32, 37, 39, 43, 45, 46, 48, 52, 55, 56, 57, 60, 62, 63, 64	58
8	26	0, 1, 2, 4, 7, 12, 15, 17, 20, 26, 32, 37, 39, 43, 45, 46, 48, 54, 58, 61, 62, 63, 66, 68, 69, 70	62
8	27	0, 1, 2, 4, 7, 12, 16, 17, 20, 27, 33, 39, 44, 46, 50, 52, 53, 55, 61, 65, 68, 69, 70, 73, 75, 76, 77	67
9	16	0, 1, 3, 5, 6, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 22	22
9	17	0, 1, 3, 5, 6, 9, 11, 12, 13, 16, 18, 19, 20, 22, 23, 24, 25	24
9	18	0, 1, 4, 6, 8, 9, 12, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28	27
9	19	0, 1, 4, 6, 8, 9, 12, 14, 15, 16, 20, 23, 25, 26, 27, 29, 30, 31, 32	30

Продолжение таблицы

r	κ	$\Delta(\kappa, r)$-множество	$L(\kappa, r)$
9	20	0, 1, 5, 8, 10, 12, 13, 16, 18, 19, 20, 24, 27, 29, 30, 31, 33, 34, 35, 36	33
9	21	0, 1, 6, 10, 13, 15, 17, 18, 21, 23, 24, 25, 29, 32, 34, 35, 36, 38, 39, 40, 41	37
9	22	0, 1, 6, 10, 13, 18, 20, 22, 23, 26, 28, 29, 30, 34, 37, 39, 40, 41, 43, 44, 45, 46	40
9	23	0, 1, 6, 10, 13, 18, 20, 22, 27, 28, 31, 33, 34, 35, 39, 42, 44, 45, 46, 48, 49, 50, 51	44
9	24	0, 1, 6, 10, 13, 18, 20, 22, 27, 28, 31, 33, 34, 35, 39, 42, 47, 49, 50, 51, 53, 54, 55, 56	48
9	25	0, 1, 6, 10, 13, 18, 20, 22, 27, 28, 31, 33, 34, 35, 39, 42, 45, 50, 52, 53, 54, 56, 57, 58, 59	52

часть из которых была найдена полным перебором, но большинство построено с помощью описанного алгоритма на ЭВМ. Множества с $r=1$ неоднократно описаны в литературе, поэтому в таблице приводится только одно из них — с $\kappa=8$, так как оно имеет меньшее l, чем известные $\Delta(8, 1)$-множества. В последней графе приведено значение нижней границы для $L(\kappa, r)$, полученное методом, который был описан выше.

ЛИТЕРАТУРА

1. Свердлик М. Б. Оптимальные двоичные сигналы. М., Сов. радио, 1975.
2. Mandelbaum D. M. Some classes of multiple-burst error correcting codes using threshold decoding. IEEE Trans. Inform. Theory, 18, N 2, 285 (1972).
3. Холл М. Комбинаторика. М., Мир, 1970.
4. Алексеев В. Е. Новый метод построения самоортогональных корректирующих кодов. «Изв. высш. учеб. зав. — Радиофизика», 13, № 11, 1741 (1970).

Горьковский государственный университет

[12/XI 1977]

К ВОПРОСУ ОБ АЛГЕБРАИЧЕСКОЙ РАЗРЕШИМОСТИ ДИАДИЧЕСКИХ ИГР

Н. Н. Воробьев

Как известно, описание множества всех ситуаций равновесия произвольной биматричной игры может быть произведено рациональным путем, т. е. путем применения к элементам матриц выигрышей конечного числа арифметических действий [1, 2]. За пределами класса биматричных игр это свойство конечных бескоалиционных игр, вообще говоря, утрачивается. Уже в статье Дж. Нэша [3] был приведен пример игры трех лиц, для описания ситуаций равновесия которой приходилось вводить квадратичные иррациональности относительно значений функций выигрыша, а автор [4] указал на диадические игры n лиц (т. е. игры с двумя стратегиями у каждого из игроков), в которых ситуации равновесия описываются иррациональностями степени $n-1$.

Принципиальный результат в этом направлении был получен В. С. Бубялисом [5], показавшим, что для любого полинома f степени r с целыми коэффициентами существует бескоалиционная игра n лиц с $m+1$-стратегией у каждого игрока, причем $m^{n-1} \geqq r$ и с целыми зна-

чениями функций выигрыша, для которой число α является выигрышем игрока во вполне смешанной ситуации равновесия тогда и только тогда, когда α есть вещественный корень полинома f.

Это утверждение оставляет, однако, открытым вопрос об иррациональности решений игр с $m=1$, т. е. для диадических игр. В данной заметке приводится принципиальное решение этого вопроса.

Теорема. Пусть

$$f(t)=t^r-a_1 t^{r-1}+\cdots+(-1)^r a_r$$

— полином произвольной степени r с рациональными коэффициентами, все корни которого $\alpha_1, \ldots, \alpha_r$ вещественны и лежат в интервале (0, 1).

Тогда существует диадическая игра $2r$ лиц Г с рациональными значениями функции выигрыша, в которой во всякой вполне смешанной ситуации равновесия

$$x^*=(\xi_1^*, \ldots, \xi_r^*, \xi_{r+1}^*, \ldots, \xi_{2r}^*),$$

первые компоненты $\xi_1^*, \ldots, \xi_r^*$ составляют некоторую перестановку корней $\alpha_1, \ldots, \alpha_r$ полинома f, а остальные компоненты $\xi_{r+1}^*, \ldots, \xi_{2r}^*$ являются произвольными заранее заданными рациональными числами из интервала (0, 1).

Фактически нами будет построена игра, в которой значениями функций выигрыша (на ситуациях в чистых стратегиях) будут некоторые натуральные числа, коэффициенты полинома f, а также те числа, которые мы выбрали в качестве значений $\xi_{r+1}^*, \ldots, \xi_{2r}^*$.

Действительно, рассмотрим диадическую игру Г с множеством игроков $\{1, \ldots, 2r\}$, множеством $\{0, 1\}$ стратегий каждого из игроков, а функции выигрыша в которой определяются следующими соотношениями:

$$H_i(x\|0) = \begin{cases} 1, \text{ если игрок } r+i \text{ выбирает стратегию } 1 \\ 0 \text{ в противном случае} \end{cases}; \tag{1}$$

$$H_i(x\|1) = \xi_{r+i}^*, \quad \text{где } \xi_{r+i}^* \in (0, 1); \tag{2}$$

$H_{r+i}(x \parallel 0)$ для каждого $i=1, \ldots, r$ равно числу сочетаний по i из игроков среди тех из числа $1, \ldots, r$, которые в ситуации x выбирают свою стратегию 1 (3)

(так, например,

$$H_{r+i}(1_1, \ldots, 1_k, 0_{k+1}, \ldots, 0_r, x_{r+1}, \ldots, x_{r+i-1}, 0_{r+i}, x_{r+i+1}, \ldots, x_{2r}) = c_k^i,$$

каковы бы ни были обозначенные буквами x (с индексами) стратегии).

$$H_{r+i}(x \parallel 1) = a_i, \quad \text{где } a_i > 0 \quad (i=1, \ldots, r), \tag{4}$$

есть абсолютная величина соответствующего коэффициента полинома f.

Возьмем теперь некоторую ситуацию в смешанных стратегиях

$$x=(\xi_1, \ldots, \xi_r, \xi_{r+1}, \ldots, \xi_{2r}),$$

вычислим выигрыш каждого из игроков $i=1, \ldots, 2r$ в соответствующих ситуациях $H_i(x\|0)$ и $H_i(x\|1)$ и выпишем применительно к рассматриваемой игре равенства вида

$$H_i(x\|0) = H_i(x\|1), \tag{5}$$

соблюдение которых является необходимым и достаточным условием равновесности ситуации x во вполне смешанных стратегиях.

Для $i=1,\ldots,r$, ввиду (1), выигрыш $H_i(x\|0)$ равен вероятности выбора в ситуации x игроком $r+i$ своей стратегии 1, т. е.

$$H_i(x\|0)=\xi_{r+i}. \tag{6}$$

Вместе с тем, переходя в (2) к смешанным стратегиям всех отличных от i игроков, получаем

$$\xi H_i(x\|0)=\xi^*_{r+i}. \tag{7}$$

Равенства (6) и (7) позволяют записать (5) как

$$\xi_{r+i}=\xi^*_{r+i} \quad \text{для } i=1,\ldots,r. \tag{8}$$

Возьмем теперь игрока с номером $r+i$ и обратимся к формулировке (3). Игроки $k_1,\ldots,k_i$, составляющие произвольное фиксированное сочетание из игроков $1,\ldots,r$ по i, выбирают одновременно в условиях ситуации x свои 1-стратегии с вероятностью $\xi_{k_1}\cdots\xi_{k_i}$. Значит это произведение есть математическое ожидание «числа раз», с которым игроки $k_1,\ldots,k_i$ выбирают вместе свои 1-стратегии. Математическое же ожидание «числа раз», с которым первую стратегию выбирает какое-либо сочетание по i из r игроков, есть поэтому сумма всех таких произведений. Иными словами,

$$H_{r+i}(x\|0)=\sigma_i(\xi_1,\ldots,\xi_n), \tag{9}$$

где σ_i — основная симметрическая функция степени i от обозначенных под ее знаком переменных.

Ясно также, что переход в (4) к смешанным стратегиям всех игроков, отличных от $r+i$, приводит к

$$H_{r+i}(x\|0)=a_i. \tag{10}$$

Равенства (9) и (10) дают (5) в виде

$$\sigma_i(\xi_1,\ldots,\xi_r)=a_i \quad \text{для } i=1,\ldots,r,$$

т. е. вероятности $\xi_1,\ldots,\xi_r$ составляют некоторую перестановку корней полинома f. Вместе с (8) это показывает, что построенная игра Γ является искомой.

Подчеркнем в заключение, что множество вполне смешанных ситуаций равновесия в игре Γ является конечным, и потому каждая из этих ситуаций является изолированной точкой в пространстве всех ситуаций в смешанных стратегиях. Поэтому для ее описания нахождение корней полинома f оказывается неизбежным.

ЛИТЕРАТУРА

1. Воробьев Н. Н. Ситуации равновесия в биматричных играх. «Теория вероятности и ее применение», 3, № 3, 21 (1958).
2. Воробьев Н. Н. Бескоалиционные игры. «Проблемы кибернетики», 32, 52 (1977).
3. Нэш Дж. Бескоалиционные игры. — В сб.: «Матрич. игры», М., Физматгиз, 1961, с. 205.
4. Воробьев Н. Н. Современное состояние теории игр. УМН, 25, № 2, 81 (1970).
5. Бубялис В. С. К вопросу структуры ситуаций равновесия в конечных бескоалиционных играх. «Мат. методы в соц. науках», № 4, 37 (1974).

Институт социально-экономических проблем
АН СССР

[15/XI 1977]

ОБ ЭЛЕМЕНТАРНЫХ ТЕОРИЯХ НЕКОТОРЫХ ДИСТРИБУТИВНЫХ РЕШЕТОК С АДДИТИВНОЙ МЕРОЙ

Ю. В. Глебский, Е. И. Гордон

1. ФОРМУЛИРОВКА ОСНОВНЫХ РЕЗУЛЬТАТОВ

Известно [1], что элементарная теория дистрибутивных решеток с относительными дополнениями разрешима. В [2] установлена эффективная неотделимость множеств истинных и конечно-опровержимых предложений элементарной теории булевых алгебр с вероятностной мерой. Отсюда, разумеется, следует неразрешимость элементарной теории дистрибутивных решеток с относительными дополнениями с аддитивной мерой. В настоящей работе устанавливается разрешимость некоторых классов таких решеток. Эти классы включают в себя многие известные решетки, например решетку ограниченных измеримых подмножеств R^n с мерой Лебега.

Рассматриваются элементарные теории некоторых классов двух основных моделей вида

$$<D,\ \leqslant;\ R_+,\ +,\ \cdot,\ \mu>, \tag{1}$$

где $<D, \leqslant>$-дистрибутивная решетка; R — поле действительных чисел; $\mu : D \longrightarrow R$ — неотрицательная конечно-аддитивная мера на D, R_+ — множество неотрицательных действительных чисел.

Пусть дана некоторая модель вида (1). Пусть $I(D)$ — идеал, содержащий те и только те элементы, которые являются конечными объединениями атомов D. Определим классы K_0, K_1, K_2, K_3 моделей (1). Все решетки в моделях этих классов предполагаются дистрибутивными решетками с относительными дополнениями и с минимальным элементом O_D (считаем, что всегда $O_D \in I(D)$), удовлетворяющими следующим условиям:

$$\forall t \in R_+ \ \exists\, d \in D\,[\mu(d) = t]; \tag{2}$$

$$\forall\, d \in I(D)\,[\mu(d) = 0]. \tag{3}$$

Различаются классы K_0—K_3 друг от друга условиями

$$\forall d \in D\,[d = \sup\{d_1 \in I(D) \mid d_1 \leqslant d\}]; \tag{4}$$

$$\forall\, d \in D \setminus I(D)\ \forall\, t_1, t_2 \in R_+ [t_1 + t_2 = \mu(d) \longrightarrow$$
$$\longrightarrow\ \exists\, d_1, d_2 \in D \setminus I(D)\,[d_1 \cap d_2 = O_D \,\&\, d_1 \cup d_2 = d \,\&\, \mu(d_1) = t_1 \,\&\, \mu(d_2) = t_2]]; \tag{5}$$

$$\forall d \in D \setminus I(D)\,[\mu(d) > 0 \,\&\, \forall\, t_1, t_2 > 0 [t_1 + t_2 = \mu(d) \longrightarrow$$
$$\longrightarrow \exists\, d_1, d_2 [d_1 \cap d_2 = O_D \,\&\, d_1 \cup d_2 = d \,\&\, \mu(d_1) = t_1 \,\&\, \mu(d_2) = t_2]]; \tag{6}$$

$$I(D) = \{O_D\}. \tag{7}$$

Условие (4) выполняется только в классах K_0 и K_1 и означает, что решетки в моделях этих классов атомны. Классы K_0 и K_1 отличаются тем, что в моделях K_0 выполнено условие (5), а в моделях K_1 — условие (6). Отсюда следует, в частности, что классы K_0 и K_1 не пересекаются, так как условие (5) влечет существование элементов меры O, не принадлежащих $I(D)$, а условие (6) влечет отсутствие таких элементов.

В классах K_2 и K_3 выполнено условие (7), которое означает, что решетки в моделях этих классов безатомны. При этом отличаются K_2 и K_3 опять тем, что в K_2 выполнено условие (5), которое в данном случае

влечет наличие ненулевых элементов меры ноль, а в K_3 — условие (6), которое влечет отсутствие таких элементов.

Теорема 1. Элементарная теория класса K_i—$Th(K_i)$ $(i=0, 1, 2, 3)$ полна и разрешима.

В качестве примеров моделей класса K_0 можно указать решетку ограниченных множеств из класса $F_\sigma \cap G_\delta$, решетку ограниченных борелевских и решетку ограниченных измеримых подмножеств R^n с мерой Лебега. Таким образом, все эти модели оказываются, что вполне естественно, элементарно эквивалентными.

В качестве примера модели, принадлежащей K_1, возьмем модель

$$\Theta_0 = <D_0, \subseteq, R_+, +, \cdot, \mu>,$$

где D_0 есть семейство таких ограниченных подмножеств R, каждое из которых представимо в виде конечного объединения открытых интервалов и отдельных точек, μ — мера Лебега.

Примерами моделей из классов K_2 и K_3 служат фактор-решетки решеток класса K_0 по идеалу $I(D)$ и по идеалу элементов меры O соответственно.

Результаты о разрешимости, сформулированные в теореме 1, без труда переносятся на булевы алгебры с вероятностной мерой. Рассматриваются модели вида

$$<B, \leqslant; [0, 1], +, \cdot, \mu>,$$

где $<B, \leqslant>$ — булева алгебра, $\mu: B \longrightarrow [0, 1]$ — вероятностная мера на B, $I(B)$ — идеал, определяемый аналогично $I(D)$. Классы K_0', K_1', K_2', K_3' определяются аналогично классам K_0, K_1, K_2, K_3 с помощью условий (2)—(7) с заменой в них R_+ на $[0, 1]$. Имеет место

Теорема 1'.

Элементарная теория классов K_i', т. е. $Th(K_i')$ $(i=0, 1, 2, 3)$ полна и разрешима.

Замечание. Булевые алгебры из классов K_0' и K_1' есть бесконечные атомные булевы алгебры, тогда легко видеть, что все они имеют одинаковую характеристику из работы [1] и, следовательно, элементарно эквивалентны. То же самое относится и к классам K_2' и K_3', булевы алгебры которых безатомны.

Из результатов работы [2] следует неразрешимость элементарной теории конечных булевых алгебр с вероятностной мерой. Однако если предположить, что мера удовлетворяет следующему условию:

$$\forall b_1, b_2 \in B (b_1, b_2 \text{ — атомы } B \longrightarrow \mu(b_1) = \mu(b_2)), \tag{8}$$

соответствующему классической схеме определения вероятностей, то этот факт не сохраняется.

Теорема 2. Элементарная теория класса K_4 моделей вида

$$<B, \leqslant; R_+, +, \mu>, \tag{9}$$

где $<B, \leqslant>$ — конечная булева алгебра, μ: $B \longrightarrow [0, 1]$ — вероятностная мера на B, удовлетворяющих (8), разрешима.

Все предыдущие утверждения относятся к дистрибутивным решеткам с относительными дополнениями. Последнее условие существенно уже потому, что элементарная теория дистрибутивных решеток без этого условия неразрешима [3]. В [4] установлена разрешимость элементарных теорий решеток открытых, замкнутых, F_σ и G_δ подмножеств R. Однако расширение теорий этих и даже более простых решеток посредством добавления меры приводит уже к неразрешимым теориям. Рассмотрим модель

$$\Theta_1 = <D_1, \subseteq; R_+, +, \mu>,$$

где D_1 — семейство таких подмножеств R, каждое из которых есть конечное объединение замкнутых интервалов и отдельных точек, μ — мера Лебега.

Теорема 3. Элементарная теория $Th(\Theta_1)$ неразрешима.

Интересно сопоставить модели Θ_0 и Θ_1. Очевидно, $D_0 \supseteq D_1$, Θ_0 и Θ_1 есть дистрибутивные решетки подмножеств R с мерой Лебега, удовлетворяющие условиям (2)—(4), (6). Элементарные теории решеток $<D_0, \subseteq>$, $<D_1, \subseteq>$ разрешимы. Элементарные теории двухосновных моделей $<D_0 \subseteq; R, \leqslant, \in>$ и $<D_1 \subseteq; R_+, \leqslant, \in>$, где $\leqslant$ рассматривается на R, а $\in$ — на $R \times D_i$ $(i=0,1)$, также разрешимы. Это легко доказать на основании результатов работы [4], в которой доказана разрешимость элементарной теории модели $<D_2, \subseteq; R, \leqslant, \in>$, где D_2— семейство F_σ подмножеств R. Легко видеть, что предикаты $d \in D_i$ $(i=0, 1)$ являются формульными в этой теории. Можно показать также неразрешимость теорий моделей $<D_0, \subseteq; R, \leqslant, +, \in>$ и $<D_1, \subseteq; R, \leqslant, +, \in>$ (см. [5]). Таким образом, видим, что многие элементарные теории, связанные с решетками $<D_0, \subseteq>$ и $<D_1, \subseteq>$, разрешимы или неразрешимы одновременно. Однако $Th(\Theta_0)$ разрешима, а $Th(\Theta_1)$ неразрешима. Заметим также, что умножение в сигнатуре Θ_0 отсутствует. Сложение можно было бы также не включать в сигнатуры Θ_0 и Θ_1, так как предикат $t_1+t_2=t_3$ формульный в этих теориях:

$$t_1+t_2=t_3 \longleftrightarrow \exists d_1 d_2 d_3 (d_1 \cap d_2 = O_D \,\&\, d_1 \cup d_2 = d_3 \,\&\, \mu(d_1) = t_1 \,\&\, \mu(d_2) = t_2 \,\&\, \mu(d_3) = t_3).$$

Пусть D_3 — семейство ограниченных G_δ, D_4 — открытых, D_5 — замкнутых подмножеств R.

Теорема 4. Элементарные теории $Th(\Theta_i)$ где

$$\Theta_i = <D_i, \subseteq; R, +, \mu> \quad (i=4, 5)$$

неразрешимы.

Теорема 4 является следствием теоремы 3. Вопрос о разрешимости $Th(\Theta_2)$ и $Th(\Theta_3)$ остается открытым.

2. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Пусть L_1 — множество формул сигнатуры $\sigma_1 = <\leqslant; +, \cdot, \mu>$ с переменными двух сортов ($d_1, \ldots, d_n, \ldots$ — переменные из D; $t_1, \ldots, t_n$— переменные из R) и элементарными формулами $d_i \leqslant d_j$, $t_i + t_j = t_\kappa$, $t_i \cdot t_j = t_\kappa$, $\mu(d_i) = t_j$, причем кванторы допускаются по переменным обоих сортов. Тогда $Th(K_i)$ (элементарная теория K_i) есть множество предложений L_1, истинных во всех моделях класса K_i $(i=0, 1, 2, 3)$.

Прежде всего, сведем вопрос о разрешимости $Th(K_i)$ к вопросу о разрешимости элементарной теории некоторого класса $\tilde{K}_i$ одноосновных моделей. Каждой модели вида (1) $M \in K_i$ поставим в соответствие модель

$$<D, \leqslant, E, \Pi> = \tilde{M}, \tag{9а}$$

где $E(d_1, d_2) \longleftrightarrow \mu(d_1) = \mu(d_2)$; $\Pi(d_1, d_2, d_3) \longleftrightarrow \mu(d_1) \cdot \mu(d_2) = \mu(d_3)$. Совокупность всех моделей $\tilde{M}$ вида (9а), соответствующих моделям $M \in K_i$, образует класс $\tilde{K}_i$. Будем обозначать L_2 множество всех формул в сигнатуре $\sigma_2 = <\leqslant, E, \Pi>$. Легко видеть, что предикаты E и Π формульны относительно сигнатуры σ_1.

Лемма 1. По любой формуле $F(d_1, \ldots, d_m, t_1, \ldots, t_\kappa) \in L_1$ $(m \geqslant 0, \kappa \geqslant 0)$ можно построить формулу $\Phi(d_1, \ldots, d_m, d_1', \ldots, d_\kappa') \in L_2$ такую, что для любой модели $M \in K_i$ и соответствующей ей модели $\tilde{M} \in \tilde{K}_i$ $(i=0, 1, 2, 3)$ имеет место следующее условие:

$$\forall b_1, \ldots, b_m \in D \forall \tau_1, \ldots, \tau_\kappa \in R_+ \forall b_1', \ldots, b_\kappa' \left[\bigwedge_{i=1}^{\kappa} \mu(b_i') = \right.$$

$$= \tau_i' \longrightarrow M \models F(b_1, \ldots, b_m, \tau_1, \ldots, \tau_\kappa) \equiv \bar{M} \models \Phi(b_1, \ldots, b_m, b_1', \ldots, b_\kappa').$$

Доказательство. Построим формулы, удовлетворяющие условиям леммы для элементарных формул L_1. Тогда для произвольной формулы L_1 доказательство легко получается индукцией по числу логических связок и кванторов в F, причем при рассмотрении формулы $\exists t_i F$ используется условие (2). Достаточно рассмотреть, очевидно, формулы $\mu(d) = t$, $t_1 + t_2 = t_3$, $t_1 \cdot t_2 = t_3$, которым сопоставим формулы $E(d, d')$; $d_1' \cap d_2' = O_D \,\&\, E(d_1' \cup d_2', d_3)$; $\Pi(d_1', d_2', d_3')$ соответственно. Так как мера μ конечно-аддитивна, то легко видеть, что условие (10) для этих формул выполнено.

Следствие. Разрешимость $Th(\bar{K}_i)$ влечет разрешимость $Th(K_i)$.

В самом деле, из условия (10) и условия (2) следует, что формула F выполнима на некоторой модели $M \in K_i$ тогда и только тогда, когда соответствующая ей формула Φ выполнима на некоторой модели $\bar{M} \in \bar{K}_i$ $(i = 0, 1, 2, 3)$.

Перейдем к доказательству разрешимости $Th(K_0)$. Введем в рассмотрение алгебры

$$N_1 = \langle N_\infty;\ +,\ P \rangle,$$
$$N_2 = \langle R_+;\ +,\ \cdot \rangle,$$

где $N_\infty = \{0, 1, 2, \ldots\} \cup \{\Theta\}$, а $+$ есть обычное сложение на $N_\infty \setminus \{\Theta\}$, удовлетворяющее условию $\forall\, x(x + \theta = \theta)$, $p(x) \longleftrightarrow x = \theta$.

Лемма 2. $Th(N_1)$ и $Th(N_2)$ разрешимы. Доказательство разрешимости $Th(N_1)$ получается незначительной модификацией алгоритма элиминации кванторов для арифметики Пресбургера, описанного, например, в [6]. Разрешимость $Th(N_2)$ доказана Тарским [7].

Введем некоторые обозначения и определения. Пусть

$$\bar{x} = \langle x_1, \ldots, x_n \rangle \in N_\infty^n, \quad \bar{y} = \langle y_1, \ldots, y_n \rangle \in R_+^n.$$

Пару $\langle \bar{x}, \bar{y} \rangle$ будем называть согласованной, если $x_i \neq \theta \longrightarrow y_i = 0$ $(i = 1, \ldots, n)$. Множество всех согласованных пар из $N_\infty^n \times R_+^n$ будем обозначать Ω^n.

Зафиксируем произвольную модель $\bar{M} \in \bar{K}_0$. Пусть $\vec{b} = \langle b_1, \ldots, b_n \rangle \in D^n$, $\vec{\alpha} = \langle \alpha_1, \ldots, \alpha_n \rangle \in \{0, 1\}^n$. Положим $[\vec{b}, \vec{\alpha}] = b_1^{\alpha_1} \cap b_2^{\alpha_2} \cap \cdots \cap b_n^{\alpha_n}$, где

$$b_i^{\alpha_i} = \begin{cases} b_i, & \alpha_i = 1 \\ (b_1 \cup \cdots \cup b_n) \setminus b_i, & \alpha_i = 0. \end{cases} \tag{11}$$

Заметим, что $\forall \vec{b} \in D^n [\vec{b}, \vec{0}] = O_D$, где $\vec{0} = \langle 0, 0, \ldots, 0 \rangle$, поэтому в дальнейших рассмотрениях всегда будем предполагать $\vec{\alpha} \neq \vec{0}$. Пусть $b \in D$. Положим $\xi(b) = n$, если b содержит в точности n атомов $(n \geqslant 0)$ и $\xi(b) = \theta$, если число атомов в b бесконечно.

Пусть $\vec{\alpha} = \langle \alpha_1, \ldots, \alpha_n \rangle \in \{0, 1\}^n$, положим

$$\chi_n(\vec{\alpha}) = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \cdots + \alpha_n.$$

Когда $\vec{\alpha}$ принимает все значения, кроме $\vec{0}$, $\chi_n(\vec{\alpha})$ принимает все значения из множества $\{1, 2, \ldots, 2^n - 1\}$. Определим функции ξ_n: $D^n \longrightarrow N_\infty^{2^n - 1}$ и η_n: $D^n \longrightarrow R_+^{2^n - 1}$, положив

$$\xi_n(\vec{b}) = \bar{x} = \langle x_1, \ldots, x_{2^n - 1} \rangle; \quad \eta_n(\vec{b}) = \bar{y} = \langle y_1, \ldots, y_{2^n - 1} \rangle, \tag{12}$$

где $x_{\chi_n(\vec{\alpha})} = \xi([\vec{b}, \vec{\alpha}])$, $y_{\chi_n(\vec{\alpha})} = \mu([\vec{b}, \vec{\alpha}])$ для любого $\vec{\alpha} \in \{0, 1\}^n \setminus \{\vec{0}\}$.

Таким образом, вектор $\xi_n(\vec{b})$ определяет число атомов в каждой конституенте (11), а $\eta_n(\vec{b})$ — меру каждой конституенты (11). Из условия (3) следует, что $\forall \vec{b} \in D^n$ пара $<\xi_n(\vec{b}), \eta_n(\vec{b})>$ согласованна, т. е. $<\xi_n(\vec{b}), \eta_n(\vec{b})> \in \Omega^{2^n-1}$. Положим $\Xi(\vec{b}) = <\xi_n(\vec{b}), \eta_n(\vec{b})>$ для любого $\vec{b} \in D^n$.

Лемма 3. Для любой пары $<\bar{x}, \bar{y}> \in \Omega^{2^n-1}$ найдется такое $\vec{b} \in D^n$, что $\Xi(\vec{b}) = <\bar{x}, \bar{y}>$.

Доказательство. Пусть $<\bar{x}, \bar{y}> \in \Omega^{2^n-1}$ и $x_{R_i} = r_i$ для $i = 1, ..., s$, а все остальные компоненты $\bar{x}$ равны θ, тогда $y_{\kappa_i} = 0$ $(i = 1, ..., s)$. Выберем $\delta_1, ..., \delta_{2^n-1} \in D$ так, что $\delta_i \vee \delta_j = O_D$ при $i \neq j$, $\mu(\delta_j) = y_j$, причем если $j \neq \kappa_i$ $(i = 1, ..., s)$, то δ_i является объединением бесконечного множества атомов, а если при некотором $i \in \{1, ..., s\}$ $j = \kappa_i$, то δ_j является объединением в точности r_i атомов. В силу того, что в K_0 выполнены условия (2), (4), (5), это всегда можно сделать. Пусть $\mu_m \subseteq \{0, 1\}^n$ — множество тех и только тех наборов $\vec{\alpha}$, у которых m-я компонента равна единице. Тогда $\forall m \leqslant n$ положим

$$b_m = \bigvee_{\vec{\alpha} \in M_m} \delta_{\chi_n(\vec{\alpha})}.$$

Легко проверить, что если $\vec{b} = <b_1, ..., b_n>$, то $[\vec{b}, \vec{\alpha}] = \delta_{\chi_n(\vec{\alpha})}$, откуда немедленно следует утверждение леммы.

Пусть $F(d_1, ..., d_n) \in L_2$; $S(F)$ обозначим множество $\{<b_1, ..., b_n> \mid \bar{M} \models F(b_1, ..., b_n)\}$. Аналогично, если $\Phi(z_1, ..., z_\kappa)$, $\Psi(t_1, ..., t_\kappa)$ — формулы сигнатур $\sigma_2 = <+, P>$ и $\sigma_3 = <+, \cdot>$ соответственно, то

$$S(\Phi) = \{<x_1, ..., x_\kappa> \in N_\infty^\kappa \mid |N_1| = \Phi(x_1, ..., x_\kappa)\},$$

$$S(\Psi) = \{<y_1, ..., y_\kappa> \in R_+^\kappa \mid |N_2| = \Psi(y_1, ..., y_\kappa)\}.$$

Лемма 4. По любой формуле $F(d_1, ..., d_n) \in L_2$ можно построить такое число k и такое семейство из k пар формул

$$\{<\Phi_F^i(z_1, ..., z_{2^n-1}), \Psi_F^i(t_1, ..., t_{2^n-1})> \mid \Phi_F^i \in L_{\sigma_2}, \Psi_F \in L_{\sigma_3} \quad i = 1, ..., \kappa\},$$

что для любой модели $\bar{M} \in \bar{K}_0$ имеют место следующие соотношения:

$$\Xi(S(F)) = \left(\bigcup_{i=1}^{\kappa} S(\Phi_F^i) \times S(\Psi_F^i)\right) \cap \Omega^{2^n-1}, \tag{13}$$

$$\Xi^{-1}(\Xi(S(F))) = S(F). \tag{14}$$

Доказательство леммы будем проводить индукцией по числу логических связок и кванторов в формуле F.

1. Рассмотрим элементарные формулы L_2.

а) $F(d_1, d_2) \longleftrightarrow d_1 \leqslant d_2$. Здесь $k = 1$; в качестве Φ_F возьмем формулу $z_2 = 0$, в качестве Ψ_F — любую тождественно-истинную формулу L_{σ_3} трех переменных. Пусть $<b_1, b_2> \in D^2$ таковы, что $b_1 \leqslant b_2$, тогда $b_1 \cap ((b_1 \cup b_2) - b_2) = O_D$, т. е. $\xi(b_1 \cap ((b_1 \cup b_2) - b_2)) = 0$, т. е. $\Xi(<b_1, b_2>) \in (S(\Phi_F) \times S(\Psi_F)) \cap \Omega^3$. Пусть, наоборот, $<\bar{x}, \bar{y}> \in (S(\Phi_F) \times (\Psi_F)) \cap \Omega^3$, тогда по лемме 3 найдутся такие $b_1, b_2 \in D$, что $\Xi(<b_1, b_2>) = <\bar{x}, \bar{y}>$, а так как $\bar{x} \in S(\Phi_F)$, то $x_2 = 0$, т. е. $b_1 \cap ((b_1 \cup b_2) - b_2 = O_D$, т. е. $b_1 \leqslant b_2$, что и доказывает соотношения (13), (14).

б) $F(d_1, d_2) \longleftrightarrow E(d_1, d_2)$. Здесь $k=1$, в качестве Φ_F берем произвольную тождественно-истинную формулу L_{σ_2} трех переменных, в качестве Ψ_F формулу $t_1=t_2$. Проверка соотношений (13), (14) проводится аналогично а).

в) $F(d_1, d_2, d_3) \longleftrightarrow \Pi(d_1, d_2, d_3)$. Снова $k=1$; в качестве Φ_F опять берем произвольную тождественно-истинную формулу семи переменных, в качестве Ψ_F формулу

$$(t_4+t_5+t_6+t_7)\,(t_2+t_3+t_6+t_7) = (t_1+t_3+t_5+t_7).$$

Для доказательства соотношений (13) и (14) заметим, что если $\vec{b}=<b_1, b_2, b_3>$, то $y_{\chi_3}(\alpha)$ определяет меру конституенты $[\vec{b}, \vec{\alpha}]$. Рассмотрим, например, b_1. Имеем

$$b_1=[\vec{b}, <1,0,0>]\cup[\vec{b}, <1,0,1>]\cup[\vec{b}, <1,1,0>]\cup[\vec{b}, <1,1,1>],$$

причем элементы, стоящие справа, попарно не пересекаются. Следовательно,

$$\mu(b_1) = y_4+y_5+y_6+y_7.$$

Дальнейшая проверка проводится аналогично а).

2. Пусть для формулы F построено семейство пар формул $\{<\Phi_F^i, \Psi_F^i> \mid i=1, \ldots, \kappa\}$, удовлетворяющее (13), (14). Рассмотрим формулу $\neg F$. Ограничимся для наглядности случаем $k=2$. Общий случай рассматривается аналогично.

Имеем, в силу (14), $\vec{b}\in S(F) \longleftrightarrow \Xi(\vec{b})\in\Xi(S(F))$. Очевидно, $\vec{b}\in S(\neg F) \longleftrightarrow \vec{b}\in\overline{S(F)}$, тогда по предыдущему соотношению

$$\vec{b}\in S(\neg F) \longleftrightarrow \Xi(\vec{b})\in\Omega^{2^n-1} - \Xi(S(F)) =$$

$$= \Omega^{2^n-1} \cap (S(\Phi_F^1)\times S(\Psi_F^1)\cup S(\Phi_F^2)\times S(\Psi_F^2)) =$$

$$= [(S(\neg\Phi_F^1)\cap S(\neg\Phi_F^2))\times R_+^{2^n-1}\cup S(\neg\Phi_F^2)\times S(\neg\Psi_F^1)\cup$$

$$\cup S(\neg\Phi_F^1)\times S(\neg\Psi_F^2)\cup N_\infty^{2^n-1}\times (S(\neg\Psi_F^1)\cap S(\neg\Psi_F^2))]\cap\Omega^{2^n-1}.$$

Теперь видно, что в качестве семейства пар для формулы $\neg F$ можно взять следующее семейство: $\{<\neg\Phi_F^1 \,\&\, \neg\Phi_F^2;\ t_1=t_1>;$

$$<\neg\Phi_F^2;\ \neg\Psi_F^1>;\ <\neg\Phi_F^1;\ \neg\Psi_F^2>;\ <z_1=z_2;$$

$$\neg\Psi_F^1 \,\&\, \neg\Psi_F^2>\}.$$

3. Пусть для формулы $F(d_1, d_2, \ldots, d_n, d_{n+1})$ требуемое семейство пар формул $\{<\Phi_F^i, \Psi_F^i> \mid i=1, \ldots, \kappa\}$ уже построено. Рассмотрим формулу $\exists d_{n+1} F(d_1, d_2, \ldots, d_n, d_{n+1})$.

Введем следующие обозначения. Если $\vec{b}\in D^{n+1}$, то $\pi(\vec{b})\in D^n$ есть проекция b на первые n компонент. Если $\vec{\alpha}\in\{1,0\}^n$, то $\vec{\alpha\,\delta}$ есть вектор, первые n компонент которого совпадают с $\vec{\alpha}$, а последняя есть $\delta(\delta=0,1)$. Пусть $\bar{x}'\in N_\infty^{2^{n+1}-1}$, $\bar{y}'\in R_+^{2^{n+1}-1}$, $\bar{x}\in N^{2^n-1}$, $\bar{y}\in R_+^{2^n-1}$. Положим

$$\begin{gathered}\bar{x}=\pi(\bar{x}') \longleftrightarrow x_i = x'_{2i}+x'_{2i+1},\\ \bar{y}=\pi(\bar{y}') \longleftrightarrow y_i = y'_{2i}+y'_{2i+1},\\ <\bar{x},\bar{y}>=\pi(\bar{x}',\bar{y}') \longleftrightarrow \bar{x}=\pi(\bar{x}')\,\&\,\bar{y}=\pi(\bar{y}').\end{gathered} \tag{15}$$

Имеем $[\pi(\vec{b}), \vec{\alpha}] = [\vec{b}, \vec{\alpha\,0}]\cup[\vec{b}, \vec{\alpha\,1}]$, тогда очевидно $\mu([\pi(\vec{b}), \vec{\alpha}]) =$

$=\mu([\vec{b},\overrightarrow{\alpha 0}])+\mu([\vec{b},\overrightarrow{\alpha 1}])$; $\xi([\pi(\vec{b}),\vec{\alpha}])=\xi([\vec{b},\overrightarrow{\alpha 0}])+\xi([\vec{b},\overrightarrow{\alpha 1}])$. Таким образом, если $\Xi(\vec{b})=<\bar{x}',\bar{y}'>$, то $\Xi(\pi(\vec{b}))=\pi(\bar{x}',\bar{y}')$.

Обратно, пусть теперь $\vec{c}\in D^n$, $\Xi(\vec{c})=<\bar{x},\bar{y}>$, $<\bar{x},\bar{y}>=\pi(\bar{x}',\bar{y}')$ и $<\bar{x}',\bar{y}'>\in\Omega^{2^{n+1}-1}$. Тогда, в силу того, что в нашей модели $\bar{M}$ выполнены условия (2)—(5), для любого $\vec{\alpha}\in\{0,1\}^n$ можно найти такие $c^0(\vec{\alpha})$, $c'(\vec{\alpha})\in D$, а также такое $c_0\in D$, что

$$c^0(\vec{\alpha})\cup c'(\vec{\alpha})=[\vec{c},\vec{\alpha}];\quad c^0(\vec{\alpha})\cap c'(\vec{\alpha})=c^0(\vec{\alpha})\cap c_0=c'(\vec{\alpha})\cap c_0=O_D,$$

$$\xi(c^\delta(\vec{\alpha}))=x'_{\chi_{n+1}(\overrightarrow{\alpha\delta})};\quad \mu(c^\delta(\vec{\alpha}))=y'_{\chi_{n+1}(\overrightarrow{\alpha\delta})}\quad \delta=(0,1),$$

$$\xi(c_0)=x'_1,\quad \mu(c_0)=y'_1.$$

Пусть $\vec{c}=<c_1,\ldots,c_n>$. Возьмем $c_{n+1}=c_0\cup(\bigcup\limits_{\vec{x}\in\{0,1\}^n-\{0\}} c'(\vec{\alpha}))$ и рассмотрим вектор $\vec{b}=<c_1,\ldots,c_n,c_{n+1})$. Тогда легко видеть, что $\pi(\vec{b})=\vec{c}$ и $\Xi(\vec{b})=<\bar{x},\bar{y}>$.

Итак,

$$\forall\vec{b}\in D^{n+1}\,\Xi(\pi(\vec{b}))=\pi(\Xi(\vec{b})),\tag{16}$$

$$\forall\vec{c}\in D^n\,\&\,\forall<\bar{x}',\bar{y}'>\in\Omega^{2^{n+1}-1}\ (\pi(\bar{x}',\bar{y}')=\Xi(\vec{c})\longrightarrow$$

$$\longrightarrow\exists\vec{b}\in D^{n+1}(\Xi(\vec{b})=<\bar{x}',\bar{y}'>\&\,\pi(\vec{b})=\vec{c}).\tag{17}$$

Пусть $\Phi(z_1,\ldots,z_{2^{n+1}-1})$ — формула сигнатуры σ_2, $A\subseteq\{1,\ldots,2^{n+1}-1\}$. Через Φ^A обозначим формулу

$$\Phi\,\&(\&\limits_{i\in A} z_i=\theta)\&(\&\limits_{j\in\bar{A}} z_j\neq\theta).$$

Если $\Psi(t_1,\ldots,t_{2^{n+1}-1})\in L_{\sigma_3}$, то через Ψ^A обозначим формулу

$$\Psi\,\&(\&\limits_{j\in\bar{A}} y_j=0).$$

Имеем

$$<\bar{x},\bar{y}>\in(S(\Phi)\times S(\Psi))\cap\Omega^{2^{n+1}-1}\longleftrightarrow<\bar{x},\bar{y}>\in\bigcup_A S(\Phi^A)\times S(\Psi^A).\tag{18}$$

Пусть $\vec{c}\in D^n$, $\Xi(\vec{c})=<\bar{x},\bar{y}>$. Используя (16)—(18), легко получить, что

$$\vec{c}\in S(\exists d_{n+1}F)\longleftrightarrow\vec{b}\in S(F)\,(\vec{c}=\pi(\vec{b}))\longleftrightarrow$$

$$\longleftrightarrow\bar{x}',\bar{y}'(<\bar{x},\bar{y}>=\pi(\bar{x}',\bar{y}')\&<\bar{x}',\bar{y}'>\in\Xi(S(F))\longleftrightarrow$$

$$\longleftrightarrow\bar{x}',\bar{y}'(<\bar{x},\bar{y}>=\pi(\bar{x}',\bar{y}')\&<\bar{x}',\bar{y}'>\in\bigcup_{i=1}^{\kappa}(S(\Phi_F^i)\times$$

$$\times S(\Psi_F^i))\cap\Omega^{2^{n+1}-1})\longleftrightarrow<\bar{x},\bar{y}>\in\bigcup_{i=1}^{\kappa}(\bigcup_A S(\exists\bar{z}'(\bar{z}=\pi(\bar{z}')\&$$

$$\&\,\Phi_F^{iA}(z')))\times S(\exists\bar{t}'(\bar{t}=\pi(\bar{t}')\&\Psi_F^{iA}(\bar{t}')))).$$

Легко видеть, что любая пара из множества, стоящего справа в последней эквивалентности, согласована, так как из (15) непосредственно видно, что $<\bar{x},\bar{y}>\in\Omega^{2^{n+1}-1}\longrightarrow\pi(\bar{x},\bar{y})\in\Omega^{2^n-1}$. Кроме того, из (14) видно, что предикаты $\bar{x}=\pi(\bar{x}')$ и $\bar{y}=\pi(\bar{y}')$ формульны в сигнатурах σ_2 и σ_3 соответственно.

Используя лемму 3 и последнюю эквивалентность, немедленно получаем, что если формуле $\exists d_{n+1} F$ сопоставить семейство пар

$$\{<\exists \bar{z}'[\bar{z}=\pi(\bar{z}')\&\Phi_F^{iA}(z)];$$

$$\exists \bar{t}'[\bar{t}=\pi(\bar{t}')\&\Psi_F^{iA}(t)]\,|\,i=\overline{1,\kappa};\ A\subseteq\{1,\ldots,2^{n+1}-1\}\},$$

то соотношения (13) и (14) будут выполнены.

4. Пусть формуле $F(d_1, d_2, \ldots, d_n)$ уже сопоставлено семейство пар $\{<\Phi_F^i,\ \Psi_F^i>|i=\overline{1,\kappa}\}$, удовлетворяющее условиям леммы, и пусть

$$G(d_1, d_2, \ldots, d_n, d_{n+1}) \equiv F(d_1, \ldots, d_n),$$

тогда рассуждениями, сходными с теми, которые были использованы в пункте 3, можно показать, что если формуле G сопоставить семейство

$$\{<\Phi_F^{iA}(z_2+z_3, \ldots, z_{2^{n+1}-2}+z_{2^{n+1}-1}),$$

$$\Psi_F^{iA}(t_2+t_3, \ldots, t_{2^{n+1}-2}+t_{2^{n+1}-1})>|i=\overline{1,\kappa}\},$$

то соотношения (13) и (14) будут выполнены.

5. Пусть для формул F и G уже построены семейства $\{<\Phi_F^i,\ \Psi_F^i>\}$ и $\{<\Phi_G^i,\ \Psi_G^i>\}$, удовлетворяющие условиям леммы. В силу пункта 4, можно считать, что F и G имеют одинаковый список свободных переменных. Тогда если формуле $F\vee G$ сопоставить семейство $\{<\Phi_F^i,\ \Psi_F^i>\}\cup\{<\Phi_G^i,\ \Psi_G^i>\}$, то условия леммы будут очевидным образом выполнены. Лемма полностью доказана.

Из леммы 4 легко следует полнота и разрешимость $Th(\bar{K}_0)$. В самом деле, если $F(d_1, \ldots, d_n)$ выполнима на какой-нибудь модели $\bar{M}\in\bar{K}_0$, то по лемме 4 она выполнима и на любой другой модели из K_0, так как построенная последовательность формул $\{<\Phi_F^i,\ \Psi_F^i>\}$ не зависит от выбора модели $\bar{M}\in\bar{K}_0$, т. е. все эти модели оказываются элементарно эквивалентными.

Для установления этой выполнимости надо проверить, выполнимы ли одновременно какие-нибудь две формулы, образующие пару семейства

$$\{<\Phi_F^{iA},\ \Psi_F^{iA}>|A\subseteq\{1, 2, \ldots, 2^{n+1}-1\}\,i=1, \ldots, \kappa\}.$$

Это мы всегда можем сделать на основании леммы 2. Разрешимость $Th(K_0)$ следует из леммы 1.

Доказательство разрешимости $Th(K_1)$ совершенно аналогично, только в качестве множества согласованных пар надо взять множество

$$\Omega_1^{2^n-1} = \{<\bar{x}, \bar{y}>|x_i=0\equiv y_i\neq 0\}.$$

Это следует из того, что в моделях K_1 выполнено условие (6).

Поясним идею доказательства разрешимости $\mathrm{Th}(K_2)$. Все модели в $Th(K_2)$ безатомны (условие (7)), тогда каждому набору $\vec{b}=<b_1, \ldots, b_n>\in D^n$ можно сопоставить пару $<\xi'(\vec{b}),\ \eta'(\vec{b})>$, где $\xi'(\vec{b})\in\{0,1\}^{2^n-1}$, $\eta'(\vec{b})\in R_+^{2^n-1}$ и

$$\forall\vec{\alpha}\in\{0,1\}^n\quad \xi'(\vec{b})_{\chi_n(\vec{\alpha})}=\begin{cases} 0 & [\vec{b},\vec{\alpha}]=O_D,\\ 1 & [\vec{b},\vec{\alpha}]\neq O_D,\end{cases}$$

$$\eta'(\vec{b})_{\chi_n(\vec{\alpha})}=\mu([\vec{b},\vec{\alpha}]).$$

Тогда $\forall i\leqslant 2^n-1$, $\xi'(\vec{b})_i=0\longrightarrow\eta'(\vec{b})_i=0$. Дальнейшее доказательство

проходит совершенно аналогично доказательству разрешимости $Th(K_0)$, только вместо алгебры N_1 нужно взять совсем простую алгебру:

$$N_3 = \langle \{0, 1\};\ \vee \rangle \quad \text{(дизъюнкция)}.$$

Замечание. В лемме 4 попутно, как легко видеть, устанавливается, что любые два набора $\vec{b}_1 \in D^n$ и $\vec{b}_2 \in D^n$ в модели $M \in K_0$ такие, что $\Xi(\vec{b}_1) = \Xi(\vec{b}_2)$ элементарно эквивалентны. То же самое имеет место в случае модели $M \in K_2$ для $\Xi'(\vec{b}_1)$ и $\Xi'(\vec{b}_2)$ $(\Xi'(\vec{b}) = \langle \xi'(\vec{b}), \eta'(\vec{b}) \rangle)$. Доказательство разрешимости $Th(K_3)$ несколько проще предыдущих. Дело в том, что из условий (6) и (7) непосредственно видно, что если модель вида (1) $M \in K_3$, то

$$\forall b \in D [\mu(b) = 0 \equiv b = O_D].$$

Лемма 5. По любой формуле $F(d_1, d_2, ..., d_n) \in L_2$ может быть построена формула $\Phi_F(t_1, ..., t_{2^n}) \in L_{\sigma_3}$ такая, что для любой модели $\tilde{M} \in \tilde{K}_3$ имеет место

$$\eta_n(S(F)) = S(\Phi_F),$$

$$\eta_n^{-1}(S(\Phi_F)) = S(F).$$

Здесь $\eta_n(\vec{b})$ определяется формулами (12). Для пояснения леммы 5 заметим, что в случае класса K_3 $d_1 \leqslant d_2 \longleftrightarrow \mu(d_1 \cap ((d_1 \cup d_2) - d_2)) = 0$. Таким образом, каждой элементарной формуле L_2 сопоставлена формула L_{σ_3}, удовлетворяющая условиям леммы (см. пп. 1б, 1в в доказательстве леммы 4). Дальнейшее доказательство легко получается индукцией по числу логических связок и кванторов в F с использованием условий (2), (6). Из леммы 5 непосредственно следует разрешимость $Th(K_3)$.

3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2

Обозначим L_3 множество всех формул сигнатуры $\langle \leqslant;\ +;\ \mu \rangle$. Пусть дана модель вида (9) $M \in K_4$. Так как μ — вероятностная мера на B, то μ — аддитивная мера такая, что $\mu(1_B) = 1$. Рассмотрим модель $\tilde{M} = \langle B;\ \leqslant;\ R_+,\ +,\ \tilde{\mu} \rangle$, где μ — такая мера на B, что для любого атома $b \in B$ $\tilde{\mu}(b) = 1$.

$$\tilde{K}_4 = \{\tilde{M} \mid M \in K_4\}.$$

Лемма 6. $\forall M \in K_4 [Th(M) = Th(\tilde{M})]$ и, следовательно, $Th(K_4) = Th(\tilde{K}_4)$.

Доказательство. Пусть дана модель вида (9) $M \in K_4$ и n — число атомов в B. Тогда если $b \in B$ есть атом, то $\mu(b) = 1/n$. Пусть $F(d_1, d_2, ..., d_r, t_1, ..., t_\kappa) \in L_3$ (здесь, как и раньше, d_i — переменные, принимающие значения из B, t_i — переменные, принимающие значения из R_+). Тогда легко показать индукцией по числу логических связок и кванторов в формуле F, что

$$\forall b_1, ..., b_r \in B \forall \tau_1, ..., \tau_\kappa \in R_+ [M \models F(b_1, ..., b_r, \tau_1, ..., \tau_\kappa) \equiv \tilde{M} \models F(b_1, ..., b_r, n\tau_1, ..., n\tau_\kappa)].$$

Рассмотрим для примера элементарную формулу $\mu(d) = t$, тогда очевидно, что если $\mu(b) = \tau$, то $\tilde{\mu}(b) = n\tau$, и обратно. Из соотношения (19) немедленно вытекает утверждение леммы.

Перейдем теперь к доказательству разрешимости $Th(\tilde{K}_4)$. Введем в рассмотрение систему

$$N_4 = \langle R_+, +, \omega \rangle,$$

где $\forall \tau \in R_+ \omega(\tau) \longleftrightarrow \tau$ — целое число. Разрешимость $Th(N_4)$ установлена в [8].

Обозначим $\omega_\kappa(t)$ формулу сигнатуры $\sigma_4 = <+, \omega>$

$$\omega(t) \;\&\; t \leqslant \kappa. \tag{20}$$

Через N_4^κ обозначим систему $<R_+, +, \omega_\kappa>$ $(\kappa = 0, 1, 2 \ldots)$. Дальнейшее доказательство сходно с доказательством теоремы 1. Пусть $\vec{b} \in B^n$, $\vec{\alpha} \in \{0,1\}^n$. Тогда $[\vec{b}, \vec{\alpha}]$ определяется соотношением (11). Определим аналогично (12) отображение $\zeta_n : B^n \longrightarrow R_+^{2^n-1}$, положив $\zeta_n(\vec{b}) = \bar{x} = <x_1, \ldots, x_n>$, где $x_{\chi_n(\vec{\alpha})} = \tilde{\mu}([\vec{b}, \vec{\alpha}])$.

Отметим, что в данном случае $\forall b \in B$ $\tilde{\mu}(b)$ есть просто число атомов b, т. е. имеет место $\omega_\kappa(\tilde{\mu}(b))$, где κ — число атомов в B. Тогда легко видеть, что для любых $\tau_1, \ldots, \tau_r \in R_+$, удовлетворяющих условию

$$(\mathop{\&}_{i=1}^{r} \omega_\kappa(\tau_i)) \;\&\; \omega_\kappa(\sum_{i=1}^{r} \tau_i),$$

найдутся такие $b_1, \ldots, b_r \in B$, что имеет место

$$(\mathop{\&}_{i=1}^{n} \tilde{\mu}(b_i) = \tau_i \;\&\; (b_i = 0 \equiv \tau_i = 0) \;\&\; (\mathop{\&}_{i \neq j} b_i \cap b_j = O_B)).$$

Аналогично лемме 4 может быть доказана

Лемма 7. По любой формуле $F(d_1, \ldots, d_n, t_1, \ldots, t_r) \in L_3$ $(n \geqslant 0, r \geqslant 0)$ может быть построена формула сигнатуры $\sigma_4^\kappa = <+, \omega_\kappa>$ $\Phi_F(z_1, \ldots, z_{2^n-1}, t_1, \ldots, t_r)$, вид которой не зависит от конкретного значения κ, и такая, что для любой модели $\tilde{M} \in \tilde{K}_4$ выполнены следующие условия:

1) $\Phi_F(z_1, \ldots, z_{2^n-1}\ t_1, \ldots, t_r) \longrightarrow \mathop{\&}_{i=1}^{2^n-1} \omega_\kappa(z_i)$;

2) $\forall \vec{b} \in B^n \; \forall \vec{\tau} \in R_+^r \; [\tilde{M} \models F(\vec{b}, \vec{\tau}) \equiv N_4 \models \Phi_F(\zeta_n(\vec{b}), \vec{\tau})]$;

3) $\forall \vec{\theta} \in R_+^{2^n-1} \forall \vec{\tau} \in R_+^r \; \forall b \in B^n [\zeta_n(\vec{b}) = \vec{\theta} \longrightarrow \tilde{M} \models F(\vec{b}, \vec{\tau}) \equiv$

$$\equiv N_4^\kappa \models \Phi_F(\vec{\theta}, \vec{\tau})].$$

(Здесь κ — число атомов B).

Из леммы 7 легко следует разрешимость $Th(\tilde{K}_4)$. В самом деле пусть F — предложение L_3, построим по нему предложение Φ_F сигнатуры σ_4^κ, удовлетворяющее условиям леммы. Заменив в Φ_F предикатный символ ω_κ формулой (20), получим формулу $\Phi_F'(\kappa)$ сигнатуры σ_4 с одной свободной переменной κ. Теперь очевидно

$$F \in Th(\tilde{K}_4) \longleftrightarrow \forall \kappa(\omega(\kappa) \longrightarrow \Phi_F'(\kappa)) \in Th(N_4),$$

что и доказывает теорему 2.

Замечание. Все предыдущие рассуждения без труда переносятся на случай, когда μ — любая аддитивная, а не обязательно вероятностная мера, т. е. на случай, когда $\mu(1_B) \neq 1$.

4. ДОКАЗАТЕЛЬСТВО ТЕОРЕМ 3, 4

В основе доказательства теоремы 3 лежит следующий результат И. А. Лаврова [9]: множества истинных и конечно-опровержимых предложений элементарной теории двух линейных порядков эффективно неотделимы (на возможность использования здесь этого результата указал авторам Э. С. Васильев). Таким образом, элементарная теория класса конечных множеств с двумя линейными порядками неразреши-

ма. Покажем, что эта теория рекурсивно сводима к $\mathrm{Th}(\vartheta_1)$. Введем некоторые предикаты на ϑ_1, формульные относительно сигнатуры $\sigma_5 = <\subseteq, +, \mu>$.

1) $T(d) \longleftrightarrow d$ — точка,

$$T(d) \longleftrightarrow d_1(d_1 \subseteq d \,\&\, \neg d_1 = O_{D_1} \longrightarrow d_1 = d).$$

2) $\mathrm{Int}(d) \longleftrightarrow d$ — замкнутый интервал:

$$\mathrm{Int}(d) \longleftrightarrow \neg \exists\, d_1 d_2 [d_1 \neq O_{D_1} \,\&\, d_2 \neq O_{D_1} \,\&\, d_1 \cap d_2 = O_{D_1} \,\&\, d_1 \cup d_2 = d] \,\&\, \neg T(d).$$

Последняя эквивалентность следует из того, что все элементы D_1 есть замкнутые подмножества R и того, что замкнутое множество d — замкнутый интервал.

3) $M(d_1, d_2) \longleftrightarrow d_1$ есть максимальный интервал в d_2

$$M(d_1, d_2) \longleftrightarrow \mathrm{Int}(d_1) \,\&\, d_1 \subseteq d_2 \,\&\, \forall\, d(\mathrm{Int}(d) \,\&\, d_1 \subseteq d \subseteq d_2 \longrightarrow d_1 = d).$$

4) $P(d) \longleftrightarrow d$ не содержит изолированных точек

$$P(d) \longleftrightarrow \forall d_1 (T(d) \,\&\, d_1 \in d \longrightarrow \exists\, d_2 (\mathrm{Int}(d_2) \,\&\, d_1 \subseteq d_2 \subseteq d).$$

5) $\Pi(d_1, d_2) \longleftrightarrow d_1, d_2$ не содержат изолированных точек, и d_1 поинтервально включено в d_2.

$$\Pi(d_1, d_2) \longleftrightarrow P(d_1) \,\&\, P(d_2) \,\&\, \forall\, d_3 [(M(d_3, d_1) \longrightarrow \exists\, d_4 (M(d_4, d_2) \,\&\, d_3 \subseteq d_4)) \,\&\, (M(d_3, d_2) \longrightarrow \exists\, ! d_4 (M(d_4, d_1) \,\&\, d_4 \subseteq d_3))].$$

6) $L(d)$ — максимальные интервалы d линейно упорядочены по мере

$$L(d) \longleftrightarrow \forall\, d_1, d_2 (M(d_1, d) \,\&\, M(d_2, d) \,\&\, d_1 \neq d_2 \longrightarrow \mu(d_1) \neq \mu(d_2)).$$

7) $$S_1(d_1, d_2, d_3, d_4) \longleftrightarrow \Pi(d_3, d_4) \,\&\, M(d_1, d_4) \,\&\, M(d_2, d_4) \,\&\, L(d_3) \,\&\, L(d_4) \,\&\, \mu(d_1) \leqslant \mu(d_2),$$

8) $$S_2(d_1, d_2, d_3, d_4) \longleftrightarrow \Pi(d_3, d_4) \,\&\, L(d_3) \,\&\, L(d_4) \,\&\, M(d_1, d_4) \,\&\, M(d_2, d_4) \,\&\, \forall\, d_5 d_6 [M(d_5, d_3) \,\&\, M(d_6, d_3) \,\&\, d_5 \subseteq d_1 \,\&\, d_6 \subseteq d_2 \longrightarrow \mu(d_5) \leqslant \mu(d_6)].$$

Если имеется пара множеств d_1, $d_2 \in D$ такая, что $\Pi(d_1, d_2) \,\&\, L(d_1) \,\&\, L(d_2)$, то на семействе максимальных интервалов d_2 определены два линейных порядка. Если d_3, d_4 — максимальные интервалы d_2, $d_3 \leqslant_1 d_4 \longleftrightarrow \mu(d_3) \leqslant \mu(d_4)$, что определяется формулой $S_1(d_3, d_4, d_1, d_2)$ и $d_3 \leqslant_2 d_4 \longleftrightarrow \mu(d_3') \leqslant \mu(d_4')$, где d_3', d_4' — максимальные интервалы d_1, включенные в d_3 и d_4 соответственно, — это условие определяется формулой $S_2(d_3, d_4, d_1, d_2)$.

Дальнейшее доказательство теоремы 3 очевидно. Для доказательства неразрешимости $Th(\Theta_5)$ заметим, что $D_1 \subseteq D_5$ и предикат $d \in D_1$ является формульным относительно сигнатуры $Th(\Theta_5)$. Это легко доказывается с использованием того факта, что подмножество R связно тогда и только тогда, когда оно является интервалом. Теория $Th(\Theta_4)$ легко сводится к $Th(\Theta_5)$.

Авторы выражают благодарность Э. С. Васильеву за полезное обсуждение.

ЛИТЕРАТУРА

1. Ершов Ю. Л. Разрешимость элементарной теории дистрибутивных структур с относительными дополнениями и теории фильтров. «Алгебра и логика», 3, № 3, 17 (1964).

2. Васильев Э. С. Об элементарных теориях двухосновных моделей. Третья всесоюзная конференция по математической логике. (Тезисы докл.), Новосибирск, 1974, с. 27.

3. Grzegorczyk. A. Undecidability of some topological theories, Fund., Math., N 38, 137 (1951).

4. Rabin M. O. Decidability of secohd-order theories and automata on infinitite trees, Transactions of the American Mathematical Society, 141, N 7, p. 1 (1969).
(Рус. пер.: «Кибернет. сб.». Новая серия, вып. 8, 1971, с. 72).

5. Глебский Ю. В., Гордон Е. И. Асинхронные автоматы с задержками и логические языки. «Автоматика и телемеханика», № 12, 143 (1974).

6. Клини С. К. Введение в математику. М., ИЛ, 1957.

7. Tarski A. A decision method for elementary algebra and geometry, Second adition revised, Betreby and Los Angelos, 1951.
8. Гордон Е. И. Об элементарной теории действительных чисел со сложением порядком и предиктом, выделяющим целые числа. Третья всесоюзная конференция по математической логике (тезисы докладов), Новосибирск, 1974, с. 50.
9. Лавров И. А. Эффективная неотделимость множества тождественно истинных и множества конечно-опровержимых формул некоторых элементарных теорий. «Алгебра и логика», 2, № 2, 5 (1963).

Горьковский государственный университет

[23/X 1978]

ЛОКАЛЬНЫЙ АЛГОРИТМ ВЫДЕЛЕНИЯ БЛОКОВ В ГРАФЕ

В. А. Евстигнеев

В работе [1] был предложен алгоритм выделения блоков и разделяющих вершин в связном графе. Ниже будет показано, что этот алгоритм по своей природе есть локальный в смысле Ю. И. Журавлева [2, 3]. Будет предложена его модификация, представляющая собой локальный алгоритм с памятью 3.

Все определения, касающиеся локальных алгоритмов, могут быть найдены в [2, 3]. Кроме этого, будем использовать понятие последовательного локального алгоритма, введенного в [4].

Определение 1. Последовательным итеративным локальным алгоритмом называется такой алгоритм, в котором каждый шаг состоит в вычислении значений предиката (приписывании метки) одному какому-нибудь элементу графа: ребру, дуге, вершине — с учетом значений этого же предиката, вычисленных на предыдущих шагах. При этом ранее выставленные метки «Δ» не изменяются до тех пор, пока не будут вычислены значения предиката для всех элементов графа. После этого начинается вторая итерация.

В последовательных алгоритмах отсутствие метки рассматривается как наличие дополнительного значения предиката — пустого. Тем самым последовательный алгоритм практически использует четырехзначную логику вместо трехзначной у локального алгоритма Журавлева, который будем называть параллельным.

Нетрудно видеть, что в основе понятия последовательного итеративного локального алгоритма лежит идея вычисления значений предиката во время обхода графа или его части. В локальных алгоритмах с памятью $k>1$, т. е. с k предикатами $P_1, P_2, ..., P_k$, значения некоторых предикатов может вычисляться последовательным процессом, других— параллельным. В результате локальный алгоритм с памятью, большей единицы, может представлять собой комбинацию нескольких алгоритмов разного типа действия.

Определение 2. Окрестностью $\Xi_1(x_i)$ порядка один вершины x_i неориентированного графа G называется подграф, порожденный вершиной x_i и всеми смежными с ней вершинами.

Определение 2а. Окрестностью $\Xi_l(x_i)$ порядка l вершины x_i неориентированного графа называется подграф, порожденный всеми вершинами из $\Xi_{l-1}(x_i)$ и всеми смежными с ними вершинами.

Определения 2 и 2а соответствуют определению главных окрестностей в [2].

Пусть задан предикат $P_1(x)$ — «вершина x есть разделяющая вершина в графе». Напомним (см. [5]), что вершина x графа называется разделяющей, если при ее удалении вместе со всеми инцидентными ребрами нарушается связность графа. Нахождение всех разделяющих вершин решает полностью задачу выделения блоков [1, 5], этим и объясняется выбор предиката $P_1(x)$.

Пусть предикат $P_1(x)$ принимает значения из множества $\{\Delta, 0, 1\}$, причем $P_1(x)=1$, если вершина x — разделяющая, 0 — в противном случае и Δ, если ничего определенного о вершине сказать нельзя. Вычисление значений предиката $P_1(x)$ будет производиться следующим параллельным алгоритмом. Предварительно напомним определение блока [5].

Определение 3. Два ребра u_1 и u_2 называются сильно циклически связанными, если существует такая последовательность $C_1, \ldots, C_r$ простых циклов, что u_1 принадлежит C_1, u_2 принадлежит C_r и любая пара соседних циклов C_i и C_{i+1} имеет, по крайней мере, одно общее ребро.

Определение 4. Множество всех ребер, сильно циклически связанных с ребром u, образует подграф, называемый блоком, определяемым ребром u.

Другими словами, блок есть максимальный по включению подграф, не содержащий разделяющих вершин.

Алгоритм B_1

Шаг 1. Рассматриваем окрестности $\Xi_\kappa(x)$ вершин графа (независимо друг от друга) и полагаем:

$P_1(x)=1$, если

а) вершина x есть концевая вершина висячего ребра (данное ребро образует простейший блок);

б) в окрестности $\Xi_\kappa(x)$ целиком помещается висячий подграф, для которого x есть единственная общая с остальной частью графа вершина.

$P_1(x)=0$, если в удаление вершины x из ее окрестности $\Xi_\kappa(x)$ не нарушает связности этого подграфа.

$P_1(x)=\Delta$ в остальных случаях.

Общий шаг. Полагаем

$P_1(x)=1$, если в $\Xi_\kappa(x)$ целиком помещается блок, для которого x является разделяющей вершиной.

Нетрудно видеть, что алгоритм B_1 полностью задачу об отыскании разделяющих вершин не решает. Необходимо организовать сбор дополнительной информации о строении графа. Введем с этой целью два вспомогательный предиката:

$P_2(u)$ — «ребро u принадлежит каркасу графа»,

$P_3(u)$ — «ребро u отделимое».

Необходимость введения таких предикатов вытекает из описанного в [1] алгоритма. Напомним кратко его содержание, опустив не интересующие нас детали.

Предложенный в [1] алгоритм основан на определенном способе обхода графа. Под обходом Q понимается движение от вершины к вершине по ребрам графа, причем каждое ребро проходится не более одного раза в каждом направлении. Траектория движения при обходе Q обозначается той же буквой Q, начальная вершина (она может быть любой) — буквой x_0. Считается, что последовательным вершинам $x_0, x_1, \ldots, x_t, \ldots, x_m$ маршрута Q соответствуют последовательные моменты $0, 1, \ldots, t, \ldots, m$ обхода, а ребрам его — ходы обхода. Первый ход по ребру называется прямым, второй (в противоположном направлении) — обратным.

Правила обхода. а) Если вершина x впервые встретилась при обходе, то следующий ход должен быть прямым по любому ребру, инцидентному x и не фигурировавшему ранее в обходе, если такое существует; в противном случае следующими должны быть обратный ход по ребру u_κ (по которому мы попали в x), если $x \neq x_0$, и окончание обхода при $x=x_0$.

б) Если прямым ходом попадаем в вершину, уже фигурировавшую в обходе, то следующий ход должен быть обратным по тому же ребру (такое ребро графа и такой момент обхода будем называть ребром (моментом) прикосновения*.

в) Если обратным ходом снова попадаем в вершину x, то далее поступаем так же, как в случае а).

Рассмотрим часть $\overline{Q}$ обхода Q, получаемую при выбрасывании из Q всех ребер прикосновения. Легко видеть, что $\overline{Q}$ может рассматриваться как обход дерева $\overline{G}$, содержащего вершины графа G, т. е. его каркаса. Подробности в [1].

По структуре, задаваемой на графе G каркасом $\overline{G}$, однозначно определяется любая ветвь блоков G', а именно: множество вершин ветви блоков образует в каркасе $\overline{G}$ отделимую ветвь в следующем смысле.

Рассмотрим часть каркаса $\overline{G}$, отделяемую ребром u от корня дерева $\overline{G}$ — вершины x_0. Присоединим к ней само ребро $u=(z, y)$. Полученную часть $\overline{G}_u$ каркаса будем называть его ветвью, висящей на ребре u и на вершине z. Множество вершин ветви $\overline{G}_u$, кроме z, т. е. внутренних вершин, обозначим через V_u. Ветвь $\overline{G}_u$ будем называть отделимой, если из вершин множества V_u не исходит ребро (необходимо ребер прикосновения) в вершины из $V \setminus (V_u \cup \{z\})$. В [1] показано, что отделимая ветвь $\overline{G}_u$, $u=(z, y)$ задает одну и только одну ветвь блоков (висящую на вершине z) с множеством внутренних вершин $V_u \overline{\ni} x_0$.

Рассмотрим теперь задачу нахождения отделимых ветвей в процессе обхода. Очевидно, обход ветви $\overline{G}_u$ есть часть обхода Q, начинающаяся прямым ходом по ребру u и кончающаяся обратным ходом по нему. Часть обхода Q, заключенную в этом промежутке, назовем ветвью обхода и обозначим Q_u. Определение отделимости распространим на ветви обхода:

Q_u отделима $\longleftrightarrow$ $\overline{G}_u$ отделима.

Легко вывести, что ветвь обхода Q_u при $u=(z, y)$ представляет собой обход подграфа $G_u=G(V \cup \{z\})$ плюс прикосновение к вершинам пути L_z из x_0 в z (кроме z). Тем самым можно считать обоснованным следующий

Критерий отделимости: ветвь Q_u, где $u=(z, y)$, отделима в том и только в том случае, когда на протяжении Q_u не было прикосновений к вершинам текущего пути, расположенным на нем ближе к началу (вершине x_0), чем вершина z.

Покажем, как этот критерий отделимости используется в процессе обхода. Каждое ребро, отличное от ребра прикосновения, с момента его появления на текущем пути L (т. е. после прямого хода по нему) считается «подозрительным». Метка подозрительности снимается следующим образом. Пусть в момент t был совершен прямой ход по ребру прикосновения $(y, z): x_t=y$, $x_{t+1}=z$. Тогда, очевидно, все ребра, расположенные на текущем пути $L(t)$ дальше от начала, чем ребро, исходящее из z, не могут порождать отделимую ветвь обхода. Поэтому все такие ребра, имеющие в рассматриваемый момент метку подозрительности, освобождаются от нее. Очевидно, что отделимость ветви обхода Q_u эквивалентна тому, что к моменту обратного хода по ребру u оно еще считается подозрительным.

Покажем теперь, как нахождение отделимых ветвей обхода влечет за собой выделение блоков графа G. Пусть в момент обратного хода по ребру $u=(z, y)$ обнаружилось, что ветвь Q_u отделимая. Тогда множество внутренних вершин соответствующей ветви блоков есть V_u и может быть найдено в этот момент как множество вершин, встретившихся в обходе не ранее, чем вершина y. Для того чтобы в момент на-

* В [1] — бетрефальное ребро.

хождения ветви блоков выделить множество вершин ее корневого блока (это достаточно для выделения всех блоков графа), достаточно при нахождении каждой ветви блоков множество ее внутренних вершин исключать из дальнейшего рассмотрения. Тогда к моменту завершения обхода любой ветви блоков G' все ее подветви, висящие на корневом блоке $\tilde{B}$, будут обойдены, а их внутренние вершины исключены. Останутся вершины из $\tilde{B}$, что и требовалось показать.

Перейдем теперь к описанию локального алгоритма и его обоснованию.

Пусть предикат $P_2(u)$ принимает значения из множества $\{\varnothing, \Delta, 0, 1\}$ и эти значения вычисляются следующим последовательным итеративным процессом. Отдельное изложение процесса вычисления значений предиката $P_2(u)$ преследует цель сделать более понятным изложение полного алгоритма, а также потому, что этот алгоритм имеет и самостоятельное значение — он локальным образом строит каркас графа.

Будем считать, что $P_2(u)=1$, если u принадлежит каркасу, $P_2(u)=0$, если ребро u есть ребро прикосновения, и $P_2(u)=\Delta$ в остальных случаях.

Алгоритм B_2

Шаг 1. Для некоторого произвольного ребра u полагаем $P_2(u)=\Delta$.

Шаг 2. Пусть ребро $v=(x, y)$ инцидентно ребру u с $P_2(u)=\Delta$. Если вершина y не инцидентна ни одному ребру с вычисленным значением предиката P_2, полагаем $P_2(v)=\Delta$ и переходим к шагу 4. В противном случае полагаем $P_2(v)=0$ и переходим к шагу 3.

Шаг 3. Пусть ребро u — последнее помеченное меткой ребро, после которого ребру v была приписана метка 0. Если из конца ребра u выходит ребро, для которого значение предиката P_2 не вычислено, то переходим к шагу 4. В противном случае полагаем $P_2(w)=1$ и переходим к шагу 5.

Шаг 4. Повторяем шаг 2, беря в качестве ребра u последнее помеченное меткой Δ ребро.

Шаг 5. Повторяем шаг 3, беря в качестве ребра u ребро, помеченное меткой Δ и инцидентное ребру с меткой 1. Если такого ребра нет, переходим к шагу 1, беря в качестве ребра u любое ребро без метки, в противном случае — стоп.

Нетрудно видеть, что после окончания работы алгоритма B_2 в графе не остается ребер с меткой Δ.

Перейдем теперь к описанию искомого алгоритма отыскания разделяющих вершин.

Общий алгоритм

Шаг 1. Вычисляем значения предиката $P_1(x)$ алгоритмом B_1, значения всех остальных предикатов не вычислены.

Комментарий: после завершения шага 1 вершины имеют метки 1, 0, Δ, ребра имеют пустые метки $(\varnothing, \varnothing)$.

Шаг 2. Выбираем произвольно некоторое ребро u, придаем ему ориентацию (если u висячее, то ориентируем его от висячей вершины) и полагаем $P_2(u)=P_3(u)=\Delta$.

Комментарий: Полагаем возможным нарисовать стрелку на ребре. Другой способ состоит в использовании трех меток для обозначения ориентации, например, используя метки 0, 1, 2 и расставляя их так, как это показано на рис. 1 [6, 7].

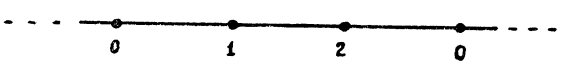


Рис. 1

Шаг 3. Пусть ребро $u=(x,y)$ — последнее помеченное меткой (Δ,Δ) ребро, тогда либо из конца ребра u (ребро u ориентировано) выходит не помеченное меткой (Δ,Δ) ребро $v=(y,z)$, либо такого ребра нет. В первом случае ориентируем ребро v от y к z и полагаем для него $P_2(v)=P_3(v)=\Delta$. Повторяем этот процесс пока возможно, т. е. пока из помеченного ребра не будет исходить ни одного непомеченного ребра. Затем переходим к шагу 4.

Комментарий: Отыскиваем ребро, инцидентное вершине, в которую заходит ориентированное ребро с меткой (Δ,Δ). Такое ребро может быть не одно, но все они инцидентны одной и той же вершине. Из них выбирается одно произвольным образом.

Шаг 4. Пусть из конца ориентированного ребра u с меткой (Δ,Δ) не выходит ни одно непомеченное ребро. Возможны следующие случаи:

а) ребро $u=(x,y)$ висячее; полагаем $P_2(u)=P_3(u)=1$, ориентируем его к висячей вершине; вершина x уже имеет метку «1», т. е. $P_1(x)=1$ (метка поставлена на шаге 1), переходим к шагу 8;

б) в вершину y заходит ориентированное ребро $v^{\Delta,\Delta}$ с меткой (Δ,Δ), а из y исходит ориентированное ребро $w^{\Delta,\Delta}$ с меткой (Δ,Δ) (рис. 2), переход к шагу 5;

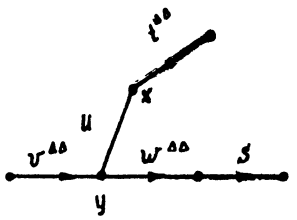


Рис. 2

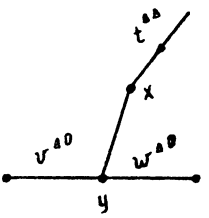


Рис. 3

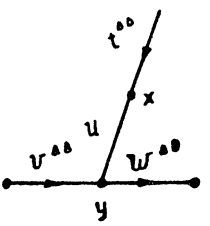


Рис. 4

в) в вершину y заходит ориентированное ребро $v^{\Delta,0}$ с меткой $(\Delta,0)$, а из y исходит ориентированное ребро $w^{\Delta,0}$ с меткой $(\Delta,0)$ (рис. 3), переход к шагу 6;

г) в вершину y заходит ориентированное ребро $v^{\Delta,\Delta}$ с меткой (Δ,Δ), а из y исходит ориентированное ребро $w^{\Delta,0}$ с меткой $(\Delta,0)$ (рис. 4), переход к шагу 7.

Комментарий: случай б) реализуется при замыкании контура (см. рис. 5, *а*), случаи в) и г) реализуются при повторном замыкании контура, т. е. при обходе контура, непосредственно связанного с только что замкнутым (см. рис. 5, *б* и 5, *в*).

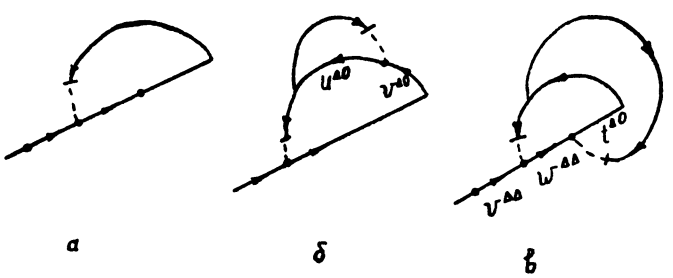


Рис. 5

Шаг 5. Ребро $u^{\Delta,\Delta}$ есть ребро прикосновения. Выделим в графе помеченное ребро $s^{\Delta,\alpha}$, имеющее окрестность, включающую часть, пока-

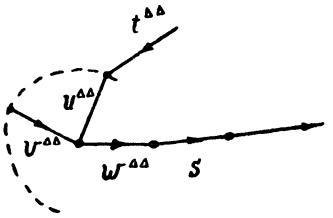


Рис. 6

занную на рис. 6. Если это ребро имеет метку (Δ, Δ), то полагаем для него $P_3(u)=0$, в противном случае оставляем все без изменения. Полагаем далее для ребра $u^{\Delta,\Delta}$ (его окрестность ясна из рис. 6) $P_2(u)=P_3(u)=0$ и затем для ребра $t^{\Delta,\Delta}$ — $P_3(u)=0$. Для каждого ребра с меткой (Δ, Δ), заходящего в ребро с меткой $(\Delta, 0)$ (кроме $w^{\Delta,\Delta}$), и для каждого ребра с меткой (Δ, Δ), исходящего из ребра с меткой $(\Delta, 0)$, полагаем $P_3(u)=0$; после завершения переход к шагу 8.

Шаг 6. Ребро $u^{\Delta,\Delta}$ есть ребро прикосновения. Полагаем для него $P_2(u)=P_3(u)=0$, а для ребра $t^{\Delta,\Delta}$, заходящего в ребро $u^{\Delta,0}$, — $P_3(u)=0$. Для каждого ребра с меткой (Δ, Δ), заходящего в начало ребра с меткой $(\Delta, 0)$, полагаем $P_3(u)=0$. Продолжаем, пока возможно. Переход к шагу 8.

Шаг 7. Поступаем так же, как и в шаге 6.

Комментарий: из рисунка 6 вытекает, что порядок окрестности должен быть, по крайней мере, равен двум. Когда говорит о рассмотрении того или иного ребра, то нужно понимать это так: находим ребро, имеющее окрестность такого-то вида и т. д. Для удобства изложения отказываемся от такого описания.

Шаг 8. Пусть $u^{\Delta,0}=(x, y)$ — последнее ребро с $P_2(u)=\Delta$, т. е. это то ребро, из конца которого — вершины y не исходит ни одно ребро с $P_2(u)=\Delta$. Возможны два случая:

а) из вершины y исходит непомеченное ребро — в этом случае переходим к шагу 3;

б) из вершины y непомеченных ребер не исходит. В этом случае полагаем $P_2(u)=1$ и переходим к рассмотрению ребра v с $P_2(v)=\Delta$, заходящего в вершину x, если $P_3(u)=0$, либо полагаем $P_2(u)=1$, $P_3(u)=1$ и $P_1(x)=1$ и переходим к рассмотрению ребра v с $P_2(v)=\Delta$, заходящего в вершину x, если для ребра u было $P_3(u)=\Delta$.

Алгоритм заканчивается, если такого ребра v нет. В этом случае полагаем $P_2(u)=1$, $P_3(u)=0$ и $P_1(x)=0$ для всех вершин с $P_1(x)=\Delta$.

Пример. Пусть граф имеет вид, показанный на рис. 7.

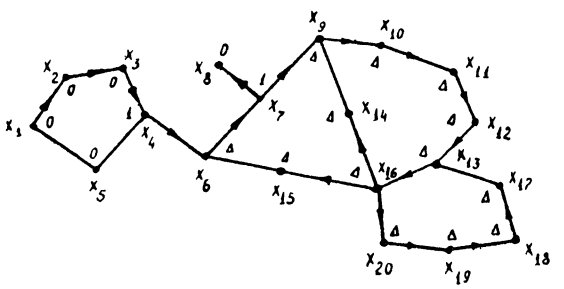
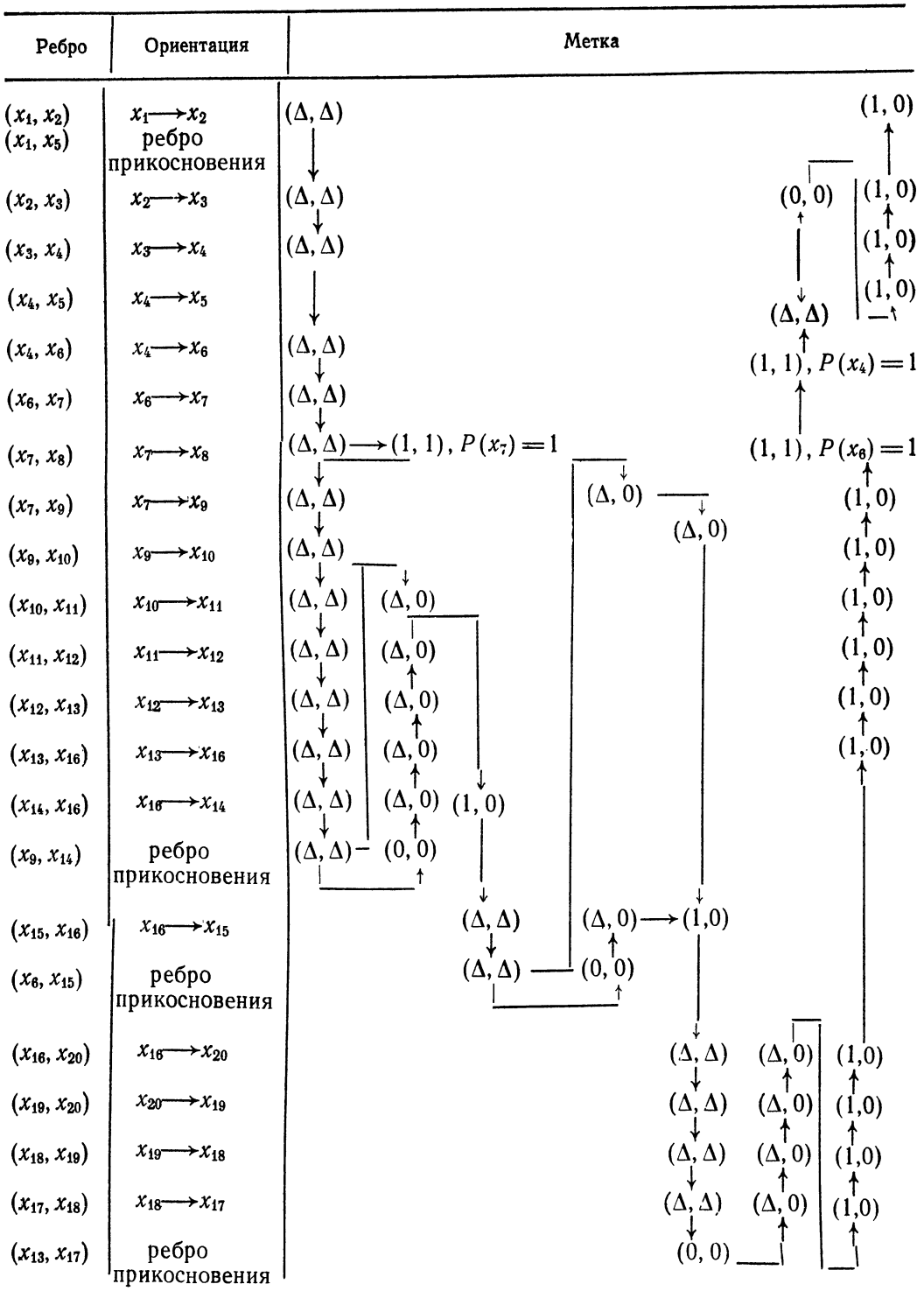


Рис. 7

Результаты работы алгоритма над окрестностями порядка два показаны в таблице, результаты вычисления предиката $P_1(x)$ на шаге 1 показаны на рис. 7. Отсюда вытекает, что разделяющими вершинами являются x_7, x_4 (они были найдены на шаге 1) и x_6.



Легко видеть, что алгоритм заканчивается за конечное число шагов (это следует из монотонности функций, изменяющих значения предикатов) и после завершения его работы ни один предикат не имеет значения, равного Δ. Обоснование самого алгоритма см. в [1].

ЛИТЕРАТУРА

1. Диниц Е. А., Зайцев М. А., Карзанов А. В. Экономный алгоритм выделения блоков в графе. ЖВМиМФ, **14**, № 5, 1309 (1974).
2. Журавлев Ю. И. Локальные алгоритмы вычисления информации. «Кибернетика», № 1, 12 (1965).
3. Журавлев Ю. И. Алгоритм локальный. — В кн.: Математическая энциклопедия, т. 1. М., «Сов. энцикл.», 1977, с. 207.
4. Евстигнеев В. А. О решении двух задач теории графов с помощью локальных алгоритмов. IV Всесоюз. конф. по проблемам теорет. кибернетики. (Тезисы докл.). Новосибирск, 1977, с. 135.
5. Оре О. Теория графов. М., Наука, 1968.
6. Тюренков В. А. Алгоритм нахождения кратчайшего пути. В сб.: «Вычислит. системы». Новосибирск, 1963, вып. 6, с. 41.
7. Зыков А. А. Теория конечных графов, т. 1. Новосибирск, Наука, СО АН СССР, 1969.

Новосибирский государственный университет

[13/XII 1977]

О СЛОЖНОСТИ ОПРЕДЕЛЕНИЯ КАЧЕСТВА ПОЗИЦИИ В НЕКОТОРЫХ КЛАССАХ ИГР НАД СЛОВАМИ

Л. П. Жильцова, Д. И. Коган

Предметом изучения настоящей работы являются специальные классы словарных игр. Каждая отдельная игра из этих классов, будучи конечной позиционной игрой с полной информацией, имеет решения в чистых стратегиях. Но проблема определения качества (т. е. выигрышности при оптимальном поведении) позиции для того или иного игрока, хотя и является алгоритмически разрешимой, может свестись к практически непреодолимым трудностям перебора чрезвычайно большого числа вариантов. В силу этого, важной является задача изучения вычислительной сложности алгоритмов определения качества позиций для отдельных классов игр и выделения классов, для которых решающие алгоритмы относительно просты.

Работа состоит из двух разделов. В первом разделе даются формальные определения и примеры классов игр над словами. Вводится понятие конечно-автоматно определимого класса игр; класс игр конечно-автоматно определим, если вопрос о выигрышности произвольной позиции для первого (второго) игрока решается посредством «прогона» этой позиции через некоторый определяемый классом игр конечный автомат. Устанавливается, что проблема определения по классу игр, является ли он конечно-автоматно определимым, алгоритмически неразрешима.

Во втором разделе вводится понятие класса монотонных игр; доказывается, что каждый класс монотонных игр одного лица конечно-автоматно определим. Показывается, что в монотонных классах игр двух лиц вопрос о выигрышности произвольной позиции для одного или другого игрока имеет тьюрингову сложность l^2 (l — длина позиции).

1. Пусть $A=\{a_1, a_2, ..., a_n\}$ — алфавит, а A^* — множество всех слов (конечных последовательностей букв) в A; для $\alpha\in A^*$ через $l(\alpha)$ обозначим длину слова α, т. е. количество букв в нем. Продукциями (правилами преобразования слов) в алфавите A назовем пары $P=(\gamma, \delta)$, $\gamma\in A^*$, $\delta\in A^*$. Если слово α имеет вид $\tilde{\alpha}\,\gamma\,\tilde{\tilde{\alpha}}$, то к нему можно применить продукцию P, и результатом такого применения будет слово

$\alpha^P = \tilde{\alpha}\,\delta\,\tilde{\tilde{\alpha}}$. Продукцию $P=(\gamma, \delta)$ назовем продукцией, сохраняющей длину, если $l(\gamma)=l(\delta)$.

Каждый класс словарных игр двух лиц задается совокупностью

$$K_{\text{И}} = \langle A, P_1, P_2, R_1, R_2 \rangle,$$

где $A=\{a_1, a_2, ..., a_n\}$ — алфавит, $P_i=\{(\gamma_1^i, \delta_1^i), (\gamma_2^i, \delta_2^i), ..., (\gamma_\kappa^i, \delta_\kappa^i)\}$ — множества сохраняющих длину продукций алфавита A, $i=1, 2$; R_1 и R_2 — непересекающиеся регулярные (т. е. конечно-автоматно определимые) [1] множества слов из A^*. Конкретная игра класса $K_{\text{И}}$ задается своей начальной позицией π^0, $\pi^0 \in A^*$. В нечетные моменты дискретного времени ходит игрок I_1, в четные — игрок I_2. Ход игрока $I_i (i=1, 2)$ состоит в замене в текущем слове-позиции одного из подслов γ_j^i ($\gamma \in \{1, 2, ..., \kappa\}$) на подслово δ_j^i и в получении таким образом новой позиции рассматриваемой игры. Игрок, не имеющий возможности сделать очередной ход, считается проигравшим. Кроме того, финальными являются позиции из $R_1 \cup R_2$; игрок I_i выигрывает, если игра заканчивается в позиции из R_i. Игре, продолжающейся бесконечно долго, приписывается ничейный исход.

Для примера рассмотрим некоторый вариант игры полиомино [2] на шахматной доске размера $8 \times n$ и поясним возможность его задания классом словарных игр. В рассматриваемом варианте полиомино в распоряжении каждого игрока имеются составленные из шахматных клеток плоские связные фигуры, каждая фигура состоит не более чем из пяти клеток. Считаем, что игроки имеют неограниченное число фигур каждого типа. Ход игрока состоит в покрытии незанятого фрагмента доски некоторой фигурой. Выигравшим считается игрок, сделавший последний возможный ход.

Очевидно, что каждое из вертикальных (т. е. высоты восемь) полей доски может быть не более чем в 2^8 различных состояниях, где состояние отождествляется с перечнем клеток, на которые уложены фигуры. Введем алфавит $A_{\text{п}}=\{a_0, a_1, ..., a_{255}\}$, отождествляя каждое a_i с возможным состоянием вертикального поля. Тогда позиции на доске кодируются n-буквенными словами из $A_{\text{п}}^*$.

Множества продукций P_1 и P_2 в конструируемом классе словарных игр $K^{\text{п}}_{\text{И}}$ совпадают. Каждое такое множество состоит из всех продукций вида $(a_{i_1} a_{i_2} ... a_{i_5}, a_{j_1} a_{j_2} ... a_{j_5})$, где слово $a_{i_1} a_{i_2} ... a_{i_5}$ описывает некоторую конфигурацию α на некотором фрагменте доски, размер фрагмента 8×5, а слово $a_{j_1} a_{j_2} ... a_{j_5}$ соответствует конфигурации β на том же фрагменте, причем конфигурация β отличается от α тем, что в ней задана еще одна уложенная фигура. Множества R_1 и R_2 считаем пустыми, каждая игра класса $K^{\text{п}}_{\text{И}}$ заканчивается лишь при невозможности совершения очередного хода.

Так определяется класс $K^{\text{п}}_{\text{И}}$. Легко видеть, что каждая игра класса $K^{\text{п}}_{\text{И}}$ имитирует некоторую игру полиомино, начинающуюся с некоторой, вообще говоря, непустой позиции на доске. И, наоборот, каждая игра полиомино имитируется некоторой игрой класса $K^{\text{п}}_{\text{И}}$.

Отметим, что в рамках словарных игр двух лиц можно записать классы, конкретизациями которых будут дискретные задачи преследования в прямоугольной области, шашки, шахматы и т. д. При задании классов словарных игр, в указанном смысле соответствующих шашкам и шахматам множества R_1 и R_2, очевидно, не будут пустыми. Входящие в них слова описывают матовые позиции черных и белых соответственно. В классе словарных игр, адекватном дискретным задачам преследования, непусто множество R_1, его слова описывают позиции, в которых убегающий игрок пойман преследователем.

Если класс $K_{\text{И}}$ таков, что

$$P_2=\{(a_1, a_1),\ (a_2,\ a_2), ..., (a_n, a_n)\},$$

а $R_2=\varnothing$, то игры из $K_{\text{И}}$ оказываются фактически играми одного лица, такие классы будем обозначать $K^1_{\text{И}}$

$$K^1_{\text{И}}=<A, P_1, R_1>.$$

В качестве примера приведем задачу о шахматном коне [3]. Имеется доска размера $8\times n$, отмечены клетки, в которых конь по одному разу уже побывал, известна клетка, где он сейчас находится. Ситуация выигрышна, если можно так организовать процесс дальнейшего движения коня, что он будет посещать только клетки, в которых еще ни разу не был и посетит таким образом все ранее не отмеченные клетки. Опишем задачу в рамках следующего класса $K^{\kappa}_{\text{И}}$. Введем алфавит $A=\{a_1, a_2, ..., a_z\}$, каждая буква a_i соответствует некоторому состоянию вертикального поля. Состояние задается перечнем клеток, в которых конь не бывал (в остальных клетках он был по разу), и возможным указанием клетки поля, где он сейчас находится. Очевидно, что достаточно считать алфавит $9\cdot 2^8$-буквенным. Позиции на доске кодируются n-буквенными словами из A^*. Множество продукций P_1 в конструируемом классе словарных игр состоит из всех продукций вида $(a_{i_1}a_{i_2}a_{i_3},\ a_{j_1}a_{j_2}a_{j_3})$, где слово $a_{i_1}a_{i_2}a_{i_3}$ описывает некоторую конфигурацию α на некотором фрагменте доски, размер фрагмента 8×3. Слово $a_{j_1}a_{j_2}a_{j_3}$ соответствует конфигурации β на том же фрагменте, причем конфигурация β отличается от α тем, что в ней отмечен еще один совершенный в пределах рассматриваемого фрагмента ход коня (совершенный ход должен быть допустимым, т. е. должен ставить коня в клетку, в которой он еще не был). Множество R_1 класса $K^{\kappa}_{\text{И}}$ есть $(a_1 \cup a_2 \cup \ldots \cup a_9)$,* где a_i $(i=1, 2, ..., 8)$ соответствует вертикальному полю, в i-ой клетке которого находится конь при условии, что в остальных клетках этого поля он уже был по разу, а a_9 кодирует вертикальное поле, в котором нет коня при условии, что во всех клетках поля он уже был по разу. Описание класса $K^{\kappa}_{\text{И}}$ закончено.

О широте класса задач управляемого преобразования слов, записываемых посредством словарных игр одного лица, говорит следующее. В [4] исследуются алгоритмы, определяемые посредством конечных автоматов с выходом и выделенным финальным состоянием. Пусть задан такой автомат $\bar{A}$. Пропускаем через него ленту с записанным на ней словом, полученную ленту вновь пропускаем через автомат и т. д. до тех пор, пока автомат не перейдет в выделенное финальное состояние. Если при этом брать только конечные автоматы, не изменяющие длины ленты, и считать, что автомат представляет множество тех слов, для которых он останавливается, то класс таким способом представимых множеств шире класса регулярных, но у́же класса примитивно-рекурсивных множеств. Для недетерминированного автомата с выходом и выделенным финальным состоянием $\bar{A}$ множество представляемых им слов обозначим $C(\bar{A})$. Класс всех таким образом представимых множеств будем называть классом C-множеств. Примерами C-множеств являются контекстно-свободные и контекстные языки [5].

Лемма 1. По любому автомату $\bar{A}$ эффективно строится класс игр одного лица $K^1_{\text{И}}$ такой, что множество позиций, начиная с которых это лицо выигрывает, совпадает с множеством $C(\bar{A})$. По любому классу игр $C(\bar{A})$ эффективно строится автомат $\bar{A}$ такой, что множество $C(\bar{A})$

совпадает с совокупностью позиций, начиная из которых активный (т. е. первый) игрок может обеспечить себе выигрыш.

Простое доказательство этой леммы, основанное на построении игры, имитирующей функционирование автомата $\bar{A}$, и, наоборот, автомата, варианты работы которого имитируют возможные течения игры, опускается.

Пусть $K_И$ — некоторый класс словарных игр. Обозначим через $П^i(K_И)$ множество позиций, начиная из которых i-й игрок может обеспечить себе победу ($i=1, 2$). Так как каждая из входящих в $K_И$ игр, будучи конечной позиционной игрой с полной информацией, имеет решения в эффективным образом конструируемых чистых стратегиях, множества слов $П^1(K_И)$ и $П^2(K_И)$ рекурсивны [6]. Таким образом, для каждого класса $K_И$ в алфавите A может быть построена однолентоточная машина Тьюринга [6] $T(K_И)$, определяющая по произвольному слову-позиции α, принадлежит ли α множеству $П^1(K_И)$. Если для $K_И$ существует машина Тьюринга $T(K_И)$, распознающая принадлежность слова α множеству $П^1(K_И)$ за количество тактов работы, не превышающее $f(l(\alpha))$, то функцией $f(l)$ будем оценивать сложность множества $П^1(K_И)$ и самого класса $K_И$. Будем говорить, что $K_И$ имеет тьюрингову сложность $f(l)$. Наиболее простыми представляются классы игр, для которых сложность множества $П^1$ оценивается функцией $f(l)$, равной l, т. е. классы игр, для которых $П^1(K_И)$ суть регулярные множества. Такие классы игр назовем конечно-автоматно определимыми [1].

Теорема 1. Проблема определения по классу игр

$$K_И = <A, P_1, P_2, R_1, R_2>,$$

является ли множество $П^1(K_И)$ регулярным, алгоритмически неразрешима.

Эта теорема — следствие леммы 1, факта принадлежности контекстно-свободных языков классу C-множеств и неразрешимости проблемы определения по контекстно-свободному языку, является ли он регулярным (см. [5]).

2. Будем говорить, что игры класса $K_И$ монотонны, если продукции из $P_1 \cup P_2$ имеют вид

$$a_{i_1}a_{i_2} \cdots a_{i_t} \longrightarrow a_{i_1+\varepsilon_1}a_{i_2+\varepsilon_2} \cdots a_{i_t+\varepsilon_t},$$

вектор $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_t)$ ненулевой, его компоненты суть неотрицательные целые числа, значение и размерность вектора в различных продукциях различны.

Примером монотонной игры двух лиц может служить описанная выше игра в полиомино. Достаточно заметить, что при отождествлении букв алфавита с возможными ситуациями в вертикальном столбце шахматной доски индекс i буквы a_i можно рассматривать как двоичное число, $i=i_1 i_2 ... i_8$, где $i_к=0$, если $к$-я клетка столбца доски свободна, и $i_к=1$, если она занята некоторой фигурой полиомино. Легко проверить, что после применения любой продукции к любому фрагменту размером 8×5 индекс i буквы a_i, соответствующей вертикальному столбцу, может только увеличиться.

Заметим, что в ходе монотонной игры любая позиция может встретиться только один раз. Отсюда ясно, что игры классов $K_И$, отдельные конкретизации которых соответствуют шахматам и шашкам, не являются монотонными.

Теорема 2. Если класс игр $K^1_И$ монотонен, то множество $П^1(K^1_И)$ регулярно.

Пусть класс $K^1_И$ задается тройкой $<A, P, R>$, где $A=\{a_1, a_2, ...,$

$a_n\}$ — алфавит, $P=\{P_1, P_2, ..., P_m\}$ — совокупность сохраняющих длину продукций, R — регулярное множество слов в A. И пусть s_0 — начальное состояние конечного автомата K_R, выделяющего R; пусть S^* — выделенное подмножество состояний K_R. Будем считать, что левые (а следовательно, и правые) части всех продукций из P имеют одинаковую длину l^*. Обозначим через S^0 подмножество S такое, что для любого $s_i \in S^0$ существует слово в A, переводящее автомат K_R из s_i в одно из состояний множества S^*.

Пусть $\pi = a_{i_1} a_{i_2} \cdots a_{i_N}$ — произвольное слово в алфавите A. Введем в рассмотрение следующую последовательность $\Phi_1, \Phi_2, ..., \Phi_M$ фрагментов слова π:

$$\Phi_1 = a_{i_1} a_{i_2} \cdots a_{i_L}, \quad L = 3l^*,$$

фрагменты $\Phi_2, \Phi_3, ..., \Phi_M$ — также подслова слова π, начальная (длины l^*) часть каждого последующего фрагмента совпадает с окончанием предыдущего фрагмента. Длина каждого фрагмента, кроме последнего, равна L, длина последнего фрагмента меньше или равна L.

Последовательность продукций $P^j = P^j_1, P^j_2, ..., P^j_r$ назовем допустимой для фрагмента $\Phi_j = f_{j_1} f_{j_2} ... f_{j_\kappa}$, $j = 2, 3, ..., M-1$, если существует последовательность слов $\sigma_0 = \Phi_j, \sigma_1, \sigma_2, ..., \sigma_{2r}$ такая, что:

1) соответствующие буквы слов σ_{2m} и σ_{2m+1}, за исключением крайне левых и крайне правых отрезков длины l^* этих слов, совпадают;

2) если соответствующие буквы $f^{2m}_{j_\alpha}$ и $f^{2m+1}_{j_\alpha}$ слов σ_{2m} и σ_{2m+1} не совпадают (и, таким образом, принадлежат крайним отрезкам), то буква $f^{2m+1}_{j_\alpha}$ в алфавите A имеет бо́льший номер, чем буква $f^{2m}_{j_\alpha}$);

3) σ_{2m} есть результат применения продукции P^j_m к слову σ_{2m-1}.

4) существует пара состояний s_1 и s_2 ($s_1 \in S^0$, $s_2 \in S^0$) автомата K_R такая, что слово σ_{2r} переводит автомат K_R из состояния s_1 в состояние s_2.

Определение допустимости последовательности продукций для фрагментов Φ_1 и Φ_M аналогично, но в условии 1 для $\Phi_1(\Phi_M)$ не должны фигурировать крайние левые (правые) отрезки слов σ_{2m} и σ_{2m+1}, а в условии 4 для $\Phi_1(\Phi_M)$ в качестве s_1 должно быть взято начальное состояние автомата K_M (в качестве s_2 должно быть взято состояние из множества S^*).

Через D_j обозначим множество всех допустимых последовательностей продукций для фрагмента Φ_j ($j = 1, 2, ..., M$). Отметим, что из монотонности K^1 и следует, что все D_j суть конечные множества.

Под сцепкой $\Phi_{j-1,j}$ фрагментов Φ_{j-1} и Φ_j будем понимать то минимальное подслово слова π, фрагментами которого являются слова Φ_{j-1} и Φ_j. Будем считать, что понятие допустимой последовательности естественным образом (т. е. с сохранением условий 1—4) обобщено на сцепки фрагментов.

Последовательность продукций P_j из D_j назовем совместимой с Φ_{j-1}, если существует последовательность P_{j-1} из D_j такая, что можно построить последовательность $P_{j-1,j}$, содержащую P_{j-1} и P_j в качестве подпоследовательностей и являющуюся допустимой для слова $\Phi_{j-1,j}$. В таком случае P_j и P_{j-1} также будем называть совместимыми ($j = 2, 3, ..., M$).

Очевидно, для того чтобы в игре с начальной позицией существовала выигрывающая стратегия оперирующего игрока, необходимо и достаточно, чтобы в D_M существовала последовательность P_M, для которой существуют последовательно P_{M-1}, P_{M-2}, ..., P_1 такие, что все последовательности P_{j-1} и P_j ($j = 2, 3, ..., M$) совместимы.

Составим теперь список троек $\Gamma=\{\Delta_i, V_i, W_i\}$, где $\Delta_i\in\{0,1,2\}$, $V_i\in A^*$, $W_i\in A^*$, $l(V_\kappa)\leqslant L$, $l(W_\kappa)\leqslant L$; $(0, V_i, W_i)\in\Gamma$ тогда и только тогда, когда V_i и W_i соответственно первый и второй совместимые фрагменты некоторого слова-позиции; $(1, V_i, W_i)\in\Gamma$ тогда и только тогда, когда V_i и W_i — два совместимых промежуточных фрагмента позиции; $(2, V_i, W_i)\in\Gamma$ тогда и только тогда, когда W_i — последний, а V_i — предпоследний совместимые фрагменты. Список F конечен. Поэтому нетрудно построить конечный автомат B, проверяющий принадлежность любой пары фрагментов списку Γ.

Из существования автомата B следует верность теоремы 2.

Следствие. Множество позиций, из которых можно правильно завершить обход доски размера $8\times n$ в сформулированной в разделе 1 задаче о шахматном коне, является регулярным.

Приведенное утверждение непосредственно вытекает из факта монотонности соответствующего класса словарных игр $K^\kappa_{\text{И}}$ и теоремы 2.

Примером класса монотонных игр двух лиц с нерегулярными множествами выигрышных для первого и второго игрока позиций является $K^0_{\text{И}}=\langle A, P_1, P_2, R_1, R_2\rangle$, где $A=\{a, b, u, v\}$, $P_1=\{(a, u)\}$, $P_2=\{(b, v)\}$, $R_1=\{a, u, v\}^*$, $R_2=\{b, u, v\}^*$. Легко видеть, что позиция π выигрышна для первого игрока, если число вхождений буквы a в слове π больше, чем число вхождений в это слово буквы b; в противном случае позиция π выигрышна для второго игрока. Но конечного автомата, сравнивающего числа вхождений во входное слово различных букв, существовать не может [7].

Теорема 3. Если класс $K^2_{\text{И}}$ является классом монотонных игр двух лиц, то существует машина Тьюринга, распознающая принадлежность произвольной позиции α множеству $\Pi^1(K^2_{\text{И}})$ за $l^2(\alpha)$ тактов работы.

Пусть $K^2_{\text{И}}=\langle A, P_1, P_2, R_1, R_2\rangle$. Для множества R_1 определим последовательность множеств Q_1^1, Q_2^1, Q_1^2, Q_2^2, ... В Q_1^1 входят слова алфавита A, каждое из которых посредством применения одной продукции из P_1 переводится в слово из R_1; в Q_2^1 входят слова из A^*, которые посредством однократного применения любой продукции из P_2 переводятся лишь в слова множества $R_1\cup Q_1^1$; в множество Q_1^κ входят слова из A^*, каждое из которых посредством применения некоторой продукции из P_1 переводится в слово из $Q_2^{\kappa-1}$; в множество Q_2^κ входят слова, которые посредством однократного применения любой из продукций множества P_2 переводятся в слова из $R_1\cup(\bigcup_{i=1}^{\kappa} Q_1^i)$. Если в игре ход принадлежит первому игроку, то, как легко видеть, $\Pi^1(K_{\text{И}})=\bigcup_{i=1}^{\infty} Q_1^i$. Так как нами рассматривается класс монотонных игр, то каждая конкретная игра длится не более чем nl шагов, где n — число букв в A, а l — длина позиции игры. Поэтому, если мы ограничиваемся рассмотрением игр над словами длины l, то можно считать, что $\Pi^1(K_{\Sigma})=\bigcup_{i=1}^{nl} Q_1^i$. Как легко видеть, каждое из множеств Q_1^i, Q_2^i регулярно; каждый из выделяющих эти множества автоматов эффективно строится за конечное не зависящее от l время.

Принадлежность тестируемого слова множеству $\Pi^1(K^2_{\text{И}})$ определяется посредством «прогона» слова через автоматы, выделяющие множества Q_1^1, Q_1^2, ..., Q_1^{nl}, т. е. посредством cl^2 тьюринговых опера-

ций. Здесь c — константа, определяемая спецификой машины Тьюринга; согласно известным теоремам об ускорении, можно считать c равным единице.

ЛИТЕРАТУРА

1. Глушков В. М. Синтез цифровых автоматов. М., Физматгиз, 1962.
2. Гарднер М. Математические головоломки и развлечения. М., «Мир», 1971.
3. Гарднер М. Математические новеллы. М., «Мир», 1974.
4. Глебский Ю. В. и др. Алгоритмы, осуществляемые повторяющимися применениями конечных автоматов. — В сб.: «Проблемы кибернетики», М., Физматгиз, 1965, вып. 13, с. 241.
5. Гинзбург С. Математическая теория контекстно-свободных языков. М., «Мир», 1970.
6. Мальцев А. И. Алгоритмы и рекурсивные функции. М., Физматгиз, 1965.
7. Рабин М., Скотт Д. Конечные автоматы и задачи их разрешения. «Кибернет. сб.», М., ИЛ, 1962, вып. 4, с. 58.

Горьковский государственный универсиет

[22/III 1978]

ОЦЕНКИ ПАРАМЕТРОВ Д. Н. Ф. НЕ ВСЮДУ ОПРЕДЕЛЕННЫХ (ЧАСТИЧНЫХ) ФУНКЦИЙ АЛГЕБРЫ ЛОГИКИ

Л. М. Караханян, А. А. Сапоженко

Исследованию соотношений между различными дизъюнктивными нормальными формами (д. н. ф.) всюду определенных булевых функций посвящен целый ряд работ [1—6], в которых для получения оценок разработаны довольно тонкие конструкции. Тем не менее для многих параметров не удалось получить окончательных оценок.

Данная работа посвящена исследованию метрических соотношений между различными типами д. н. ф. не всюду определенных (частичных) булевых функций. Для некоторых параметров удается, получить окончательные или близкие к окончательным оценки. При этом неполная определенность позволяет существенно упростить конструирование примеров функций, обладающих экстремальными свойствами. В статье рассмотрены также соотношения между максимальными значениями параметров всюду определенных и частичных функций.

1. ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Здесь даны обозначения и определены некоторые понятия, связанные с частичными функциями и их д. н. ф. Используемые, но не определяемые в этой статье понятия можно найти в [7—9]. Множество всех частичных булевых функций, зависящих от n переменных, будет обозначаться через P^n, а множество всюду определенных — через $\bar{P}^n$. Множество всех двоичных наборов длины n называется единичным n-мерным кубом и обозначается через B^n. Весом набора $(\alpha_1, \ldots, \alpha_n)$ называется сумма его координат. Через B_κ^n обозначается множество наборов веса κ из B^n. Через $N_f(N_{\bar{f}}, N_{\tilde{f}})$ обозначается множество тех вершин $\tilde{\alpha}$ из B^n, для которых $f(\tilde{\alpha})=1$ (соответственно $f(\tilde{\alpha})=0$, $f(\tilde{\alpha})$ не определено). Импликантом частичной функции называется элементарная конъюнкция K, такая что существует набор $\tilde{\alpha}$ из N_f, обращающий конъюнкцию K в единицу, и такая, что для всякого $\tilde{\beta}\in N_{\bar{f}}$ справед-

ливо K $(\tilde{\beta})=0$. Простым импликантом функции f называется импликант K такой, что любая конъюнкция, полученная из K отбрасыванием некоторой буквы, не является импликантом функции f. Дизъюнкция всех простых импликантов функции f называется сокращенной д. н. ф. и обозначается через $D_c(f)$. Грань единичного куба, соответствующая импликанту (простому импликанту) функции f, называется ее интервалом (максимальным интервалом) и обозначается через N_K. Число переменных, входящих в импликант K, называется рангом K и обозначается через $r(K)$. Через $l(D)$ обозначается длина д. н. ф. D, т. е. число ее элементарных конъюнкций (слагаемых), а через $L(D)$ — сложность д. н. ф. D (число букв в ней). Д. н. ф. D, составленная из импликантов $D_c(f)$ и реализующая f, но не реализующая f при отбрасывании любого из слагаемых называется тупиковой д. н. ф. (т. д. н. ф.) функции f. Тупиковая д. н. ф. функции f, имеющая наименьшую сложность (длину) среди всех т. д. н. ф. функции f, называется минимальной (кратчайшей). Через $\Gamma(f)$, $M(f)$ и $K_{\text{кр.}}(f)$ обозначается множество тупиковых, минимальных и кратчайших д. н. ф. функции f соответственно. Пусть $l^c(f)=l(D_c(f))$ — длина сокращенной д. н. ф., $l^\kappa(f)$ — длина кратчайшей д. н. ф., $l^T(f)$ — наибольшая из длин тупиковых д. н. ф., $L^M(f)$ — сложность минимальной д. н. ф. функции f, тогда через

$$l^c_Q(n)=\max_{f\in Q} l^c(f), \qquad l^T_Q(n)=\max_{f\in Q} l^T(f),$$

$$l^\kappa_Q(n)=\max_{f\in Q} l^\kappa(f), \qquad l^M_Q(n)=\max_{f\in Q} L^M(f)$$

обозначаются соответственно максимальное значение длин сокращенных, тупиковых, кратчайших и максимальное значение сложности минимальных д. н. ф. на множестве $Q\subseteq P^n$.

2. СООТНОШЕНИЕ МЕЖДУ ПАРАМЕТРАМИ Д. Н .Ф. ВСЮДУ ОПРЕДЕЛЕННЫХ И ЧАСТИЧНЫХ ФУНКЦИЙ

Пусть $\chi(f)$ — некоторый числовой параметр, определенный на множестве P^n. Будем обозначать $\max\limits_{f\in\tilde{P}^n}\chi(f)$ через $\chi^{\sim}_P(n)$, а $\max\limits_{f\in P^n}\chi(f)$ через $\chi_P(n)$.

Замечание 1. Поскольку $\tilde{P}^n\subset P^n$, то, очевидно,

$$\chi^{\sim}_P(n)\leqslant\chi_P(n). \tag{1}$$

Ниже будет показано, что для многих основных параметров, характеризующий сложность д. н. ф., неравенство (1) обращается в равенство. С другой стороны, результаты разделов 3, 4 дают примеры параметров, для которых в (1) имеет место строгое неравенство.

Пусть $f\in P^n$, а D — некоторая д.н.ф., реализующая функцию f. Через F_D будет обозначаться всюду определенная функция, реализуемая д.н.ф. D.

Лемма 1. Пусть $f\in P^n$, а D — ее сокращенная д.н.ф. Тогда всякий простой импликант функции f является простым импликантом для всюду определенной функции $\varphi=F_D$.

Доказательство. Отметим, что $N_f\subseteq N_\varphi$, $N_{\bar{f}}\subseteq N_{\bar{\varphi}}$. Пусть K — простой импликант функции f. Из определения функции φ вытекает, что $N_\varphi\cap N_K\neq\varnothing$, $N_{\bar{\varphi}}\cap N_K=\varnothing$, т. е. K — импликант функции φ. Покажем, что из K нельзя удалить ни одной буквы. Пусть K' — конъюнкция, полученная из K удалением некоторой буквы. Имеем $N_{K'}\cap N_{\bar{f}}\neq\varnothing$, поскольку K — простой импликант функции f. Но $N_{\bar{f}}\subseteq N_{\bar{\varphi}}$. Следователь-

но, K' не является импликантом функции φ. Лемма доказана.

Из леммы следует, что $l^c(f) \leqslant l^c(F_{D_c(f)})$. Приведенный ниже пример показывает, что это неравенство может быть строгим для некоторых функций f.

Пример 1. Функция $f(x_1, x_2, x_3) \in P^3$ такова, что $N_f = \{(010), (101)\}$, $N_f^{\sim} = \{(011), (111)\}$ (рис. 1, *а*).

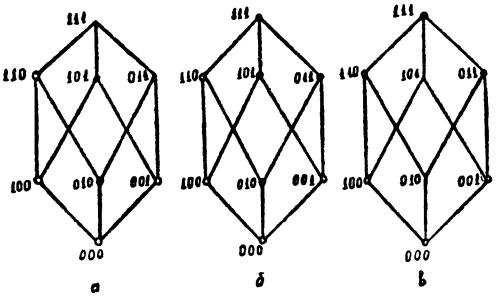


Рис. 1

Тогда $D = D_c(f) = \bar{x}_1 x_2 \vee x_1 x_3$. В то же время сокращенная д.н.ф. функции F_D имеет вид $\bar{x}_1 x_2 \vee x_1 x_3 \vee x_2 x_3$ (рис. 1, *б*).

Лемма 2. Пусть D — тупиковая д. н. ф. функции f. Тогда D является тупиковой д.н.ф. функции F_D.

Доказательство. Из предыдущей леммы вытекает, что каждое слагаемое д.н.ф. D является простым импликантом функции F_D. Следовательно, ни из одного слагаемого нельзя отбросить букву. Покажем, что нельзя отбросить слагаемые.

После отбрасывания произвольного слагаемого из D получается д.н.ф. D', не реализующая f. Эта новая д.н.ф. D' не может реализовать и функцию F_D, поскольку $N_{D'} \subseteq N_f \subseteq N_{F_D}$. Следовательно, из D нельзя отбросить ни одного слагаемого. Лемма доказана.

Лемма 3. Если D — минимальная (кратчайшая) д.н.ф. функции f из P^r, то D является также минимальной (кратчайшей) д.н.ф. функции F_D.

Доказательство. Предположим противное. Пусть, например, D_1 — минимальная д.н.ф. функции F_D, причем $L(D_1) < L(D)$. Рассмотрим д.н.ф. D_2 составленную из всех конъюнкций K, входящих в D_1, и таких, что $N_K \cap N_f \neq \varnothing$. Ясно, что $N_f \subseteq N_{D_2}$. Но это означает, что D_2 реализует f и имеет меньшую сложность, чем D. Полученное противоречие доказывает лемму.

Возникает вопрос, верно ли обратное к лемме 3 утверждение. а именно: верно ли следующее

Утверждение. Пусть D — минимальная (кратчайшая) д.н.ф. всюду определенной функции φ. Пусть f — произвольная частичная функция, для которой D является т.д.н.ф. Тогда D — минимальная (кратчайшая) д.н.ф. функции f.

Утверждение, вообще говоря, неверно, как показывает следующий

Пример 2. Пусть φ — всюду определенная функция, реализуемая д.н.ф. $D = \bar{x}_1 x_2 \vee x_1 x_3$ (рис. 1, *б*). Д.н.ф. D является минимальной и кратчайшей для функции φ. Пусть f — частичная функция такая, что $N_f = \{(011), (111)\}$, $N_f^{\sim} = \{(010), (101)\}$ (рис. 1, *в*). Д.н.ф. D есть т.д.н.ф. функции f, а кратчайшей и минимальной является д.н.ф. $D_1 = x_2 x_3$.

Теорема 1. Пусть $\chi(f)$ — произвольный из параметров $l^c(f)$, $l^T(f)$, $l^k(f)$, $L^M(f)$. Тогда

$$\chi_P(n) = \chi_P^{\sim}(n).$$

Доказательство. Из лемм 1—3 вытекает, что для произвольного параметра χ из перечисленных в условии теоремы и произвольной функций $f \in P^n$ существует функция $\varphi \in P^n$ такая, что $\chi(f) \leqslant \chi(\varphi)$. Отсюда и из замечания 1 вытекает утверждение теоремы.

3. РАЗБРОС ДЛИН И СЛОЖНОСТЕЙ Т. Д. Н. Ф.

В работах [1] рассматривались соотношения между длинами и сложностями т.д.н.ф., реализующих одну и ту же всюду определенную функцию алгебры логики.

Пусть $f \in P^n$. Величина $У(f) = \max\limits_{D_1, D_2 \in \Gamma(f)} \dfrac{l(D_1)}{l(D_2)}$ называется разбросом длин, а величина $R(f) = \max\limits_{D_1, D_2 \in \Gamma(f)} \dfrac{L(D_1)}{L(D_2)}$ — разбросом сложностей т.д.н.ф. функции f. Пусть $Q \subseteq P^n$. Положим $У_Q(n) = \max\limits_{f \in Q} У(f)$, $R_Q(n) = \max\limits_{f \in Q} R(f)$. В [1] Ю. Л. Васильев показал, что

$$2^{n-3\sqrt{n}} \leqslant У_P^{\sim}(n) \leqslant 2^{n-\log n},$$

$$2^{n-3\sqrt{n}} \leqslant R_P^{\sim}(n) \leqslant 2^n.$$

Оказывается, что для множества не всюду определенных функций можно получить асимптотические оценки.

Теорема 2.

$$У_P(n) \sim 2^{n-1}, \quad R_P(n) \sim n \cdot 2^{n-1}.$$

Доказательство. Оценка сверху для $У_P(n)$. Пусть функция f из P^n такова, что $У(f) = У_P(n)$, и пусть D_1, D_2 — т.д.н.ф. функции f такие, что $У_P(n) = У(f) = l(D_1)/l(D_2)$.

Возможны два случая:

1) $l(D_2) = 1$. Тогда существует грань g куба B^n, содержащая все вершины из N_f. Ранг этой грани больше нуля, так как в противном случае функция имеет единственную т.д.н.ф. и, следовательно, $У(f) = 1$. Пусть грань g имеет ранг $r \geqslant 1$, тогда

$$У_P(n) = У(f) = l(D_1) \leqslant |N_f| \leqslant 2^{n-r} \leqslant 2^{n-1}.$$

2) $l(D_2) \geqslant 2$. Тогда $У_P(n) = У(f) \leqslant |N_f|/l(D_2) \leqslant 2^{n-1}$. Отсюда и вытекает, что $У_P(n) \leqslant 2^{n-1}$.

Оценка сверху для $R_P(n)$. Пусть функция f из P^n такова, что $R(f) = R_P(n)$, и пусть D_1, D_2 — т.д.н.ф. функции f такие, что $R(f) = L(D_1)/L(D_2)$. Заметим, что $N_{\bar{f}} \neq \varnothing$ и, следовательно, любой импликант функции f имеет ранг больше нуля. Тогда

$$R_P(n) = R(f) = \frac{L(D_1)}{L(D_2)} \leqslant \frac{l(D_1) \cdot \max\limits_{K_1 \in D_1} r(K_1)}{l(D_2) \cdot \min\limits_{K_2 \in D_2} r(K_2)} \leqslant У_P(n) \cdot n \leqslant n \cdot 2^{n-1},$$

где $r(K)$ — ранг конъюнкции K. Итак,

$$R_P(n) \leqslant n \cdot 2^{n-1}.$$

Нижние оценки. Рассмотрим произвольную всюду определенную функцию $f(x_1, \ldots, x_{n-1})$. Определим частичную функцию $\varphi_f(x_1, \ldots, x_{n-1}, x_n)$ следующим образом:

$$\varphi_f(\alpha_1, ..., \alpha_{n-1}, 0) = 0, \text{ если } f(\alpha_1, ..., \alpha_{n-1}) = 0,$$

$$\varphi_f(\alpha_1, ..., \alpha_{n-1}, 1) = 1, \text{ если } f(\alpha_1, ..., \alpha_{n-1}) = 1.$$

На остальных наборах $(\alpha_1, ..., \alpha_n)$ функция φ_f не определена.

Отметим следующие свойства функции:

1) Д.н.ф. x_n реализует φ_f и является минимальной и кратчайшей.

2) Всякая т.д.н.ф. функции f является т.д.н.ф. функции φ_f. В работе В. В. Глаголева [2] построена для любого (достаточно большого) n функция $f(x_1, ..., x_{n-1})$, у которой существует т.д.н.ф. D такая, что $l(D) \sim 2^{n-1}$, $L(D) \sim n \cdot 2^{n-1}$. Отсюда вытекает, что для соответствующей функции φ_f справедливо

$$У(\varphi_f) \geqslant 2^{n-1}(1-\delta_n'), \quad R(\varphi_f) \geqslant n \cdot 2^{n-1}(1-\delta_n''),$$

где δ_n', $\delta_n'' \longrightarrow 0$ при $n \longrightarrow \infty$. Теорема доказана.

4. СРАВНЕНИЕ СЛОЖНОСТИ КРАТЧАЙШИХ И МИНИМАЛЬНЫХ Д. Н. Ф.

В работе Лин Син-ляна [3] рассматривалось соотношение между сложностями различных кратчайших д. н. ф. одной и той же всюду определенной булевой функции. Рассматривался также вопрос об отношении сложностей кратчайших и минимальных д. н. ф. Пусть

$$U(f) = \max_{K_1, K_2 \in K(f)} \frac{L(K_1)}{L(K_2)},$$

где максимум берется по всем парам к. д. н. ф. функции f. Пусть

$$V(f) = \min_{K \in K(f)} \frac{L(K)}{L(f_m)}, \quad \text{где} \quad f_m \in M(f).$$

В работе [3] показано, что

$$\max_{f \in \tilde{P}^n} V(f) \sim \max_{f \in \tilde{P}^n} U(f) \sim \frac{n}{2}.$$

Пусть $U_P(n) = \max\limits_{f \in P^n} U(f)$, $V_P(n) = \max\limits_{f \in P^n} V(f)$.

Теорема 3.

$$U_P(n) = n-1, \quad V_P(n) \sim n.$$

Доказательство. Оценка сверху. Оценим сверху отношение $L(K)/L(T)$, где K — кратчайшая, а T — тупиковая д. н. ф. функции f из P^n. Заметим, что если в с. д. н. ф. $D_c(f)$ функции f входит конъюнкция ранга n, то она входит в ядро. Пусть s — число конъюнкций ранга n, а K' и T' есть д. н. ф., получающаяся соответственно из K и T отбрасыванием этих конъюнкций. Тогда

$$\frac{L(K)}{L(T)} = \frac{n \cdot s + L(K')}{n \cdot s + L(T')} \leqslant \frac{n \cdot s + (n-1)[l(K) - s]}{n \cdot s + [l(T) - s]} \leqslant$$

$$\leqslant \frac{n \cdot s + (n-1)[l(T) - s]}{n \cdot s + [l(T) - s]} \leqslant n-1.$$

Отсюда вытекает, что для всякой функции $f \in P^n$ справедливы неравенства $U(f) \leqslant n-1$, $V(f) \leqslant n-1$.

Оценка снизу для $U_P(n)$. Рассмотрим функцию $f \in P^n$, определенную следующим образом (рис. 2):

$$f(\alpha_1, ..., \alpha_n) = \begin{cases} 1, \text{ если } \alpha_1 = \cdots = \alpha_n = 1, \\ 0, \text{ если } \alpha_n = 0, \ \sum\limits_{i=1}^{n-1} \alpha_i = n-2, \\ \text{не определена в остальных случаях.} \end{cases}$$

Очевидно, что для функции f д. н. ф. $K_1 = x_1 x_2 \cdots x_{n-1}$ и $K_2 = x_n$ являются кратчайшими. При этом $L(K_1)/L\ (K_2) = n-1$. Отсюда $U_P(n) \geqslant n-1$.

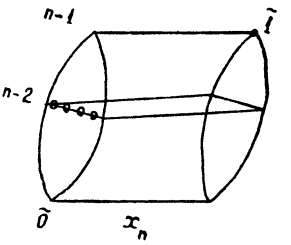


Рис. 2

Оценка снизу для $V_P(n)$. Построим функцию $f \in P^n$, которая дает нижнюю оценку. Пусть S_1 — множество всех двоичных наборов $(\alpha_1, \cdots, \alpha_n)$ таких, что $\sum_{i=1}^{\kappa} \alpha_i = 0$, $\sum_{i=\kappa+1}^{n} = 2$. Обозначим через $\tilde{0}$ набор длины n, состоящий из одних нулей. Положим $S = S_1 \cup \{\tilde{0}\}$.

Обозначим через $\tilde{\beta}_{i,j}$ набор $(\beta_1, \ldots, \beta_n)$ такой, что $\beta_i = \beta_j = 1$, а все остальные координаты равны нулю. Положим $E_i = \bigcup_{j=\kappa+1}^{2\kappa-1} \{\tilde{\beta}_{i,j}\}$, $E = \bigcup_{i=1}^{\kappa} E_i$.

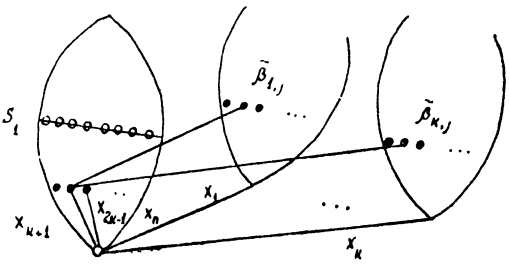


Рис. 3

Определим теперь функцию f из P^n следующим образом (рис. 3):

$$f(\tilde{\alpha}) = \begin{cases} 1, \text{ если } \tilde{\alpha} \in E; \\ 0, \text{ если } \tilde{\alpha} \in S; \\ \text{не определено, если } \alpha \overline{\in} S \cup E. \end{cases}$$

Отметим следующие свойства функции f.

1) Сокращенная д.н.ф. функции f имеет вид $D_c(f) = x_1 \vee \ldots \vee x_\kappa \vee a_1 \vee \ldots \vee a_{\kappa-1}$, где $a_j = \bar{x}_{\kappa+1} \ldots \bar{x}_{\kappa+j-1}\, x_{\kappa+j}\, \bar{x}_{\kappa+j+1} \ldots \bar{x}_n$, $j = 1, \ldots, n$. Нетрудно убедиться, что конъюнкции из $D_c(f)$ являются простыми импликантами. Убедимся, что других простых импликантов у функции f нет. Пусть K — произвольный простой импликант, а $I = N_K$ — соответствующий максимальный интервал. Рассмотрим тот набор $\tilde{\alpha}$ из интервала I, который имеет наименьший вес. Вес набора $\tilde{\alpha}$ не превосходит двух, так как I содержит хотя бы один набор из E, а вес такого набора равен двум. Покажем, что вес набора $\tilde{\alpha}$ не может быть равен двум. Отметим, что поскольку $\tilde{\alpha}$ набор наименьшего веса в I, то всякий набор из интервала I, может быть получен из $\tilde{\alpha}$ заменой некоторых нулей на единицу. Отсюда следует, что если вес $\tilde{\alpha}$ равен двум, то $\tilde{\alpha}$ совпадает с некоторым набором $\tilde{\beta}_{i,j}$ из E. Но всякий интервал, в котором $\tilde{\beta}_{i,j}$ является набором наименьшего веса, содержится в интервале N_{x_i}. Это противоречит максимальности интервала I. Таким образом, вес $\tilde{\alpha}$ равен одному. Ясно, что единичная координата набора $\tilde{\alpha}$ имеет номер, меньший $2k$, поскольку в противном случае ни один набор из E не мог бы содержаться в I. Если единичная координата набора $\tilde{\alpha}$ имеет номер $t\ (t \leqslant k)$ то, очевидно, $I = N_{x_t}$. Если же $k < t < 2k$, то $I = N_{a_t}$.

2) Существует ровно две тупиковые д.н.ф. функции f: $D_1 = x_1 \vee \ldots \vee x_k$ и $D_2 = a_1 \vee \ldots \vee a_{k-1}$. Нетрудно проверить, что D_1 и D_2 являются т.д.н.ф. Тот факт, что не существует других т.д.н.ф. функции f, вытекает из следующего замечания. Пусть некоторая д.н.ф. D реализует f и состоит из конъюнкций д.н.ф. $D_c(f)$. Пусть в D отсутствует одна из конъюнкций x_i (или a_j), тогда в D входят все конъюнкции a_j (соответственно x_i). Пусть отсутствует конъюнкция x_i. Рассмотрим наборы из E_i. Ни один из них не покрывается интервалом вида N_{x_t}, $1 \leqslant t \leqslant k$, $t \neq i$. Вместе с тем набор $\tilde{\beta}_{i,j}$ покрывается интервалом N_{a_j} и только им.

3) Д. н. ф. D_2 является кратчайшей, а D_1 — минимальной (при $n > 2k$), притом $L(D_1) = k$, $L(D_2) = (k-1)(n-k)$. Таким образом, $V(f) = n\left(1 - \frac{1}{k}\right)\left(1 - \frac{1}{n}\right)$. Полагая $k = \sqrt{n}$, получаем отсюда, что $V_P(n) \gtrsim n$. Теорема доказана.

5. ОБ ОТНОСИТЕЛЬНОЙ СЛОЖНОСТИ СОКРАЩЕННОЙ Д. Н. Ф.

Пусть $D_{UT}(f)$ ($D_{UM}(f)$, $D_{UK}(f)$) — д.н.ф., состоящая из всех конъюнкций, входящих хотя бы в одну из тупиковых (соответственно минимальных, кратчайших) д.н.ф. функции $f \in P^n$.

В работе [4] показано, что с.д.н.ф. функции f из P^n может иметь существенно больше слагаемых (в $3^{n(1-\theta(1))}$ раз), чем д.н.ф. $D_{UT}(f)$ или $D_{UM}(f)$. В другой работе [5] исследовалось отношение длины $D_c(f)$ к длине $D_c(\bar{f})$, где $\bar{f}$ — отрицание функции f. В [5] показано, что для функций из $\tilde{P}^n$ это отношение также может достигать величины $3^{n(1-\delta_n)}$, где $\delta_n \longrightarrow 0$ при $n \longrightarrow \infty$.

В этом разделе исследуются эти же соотношения для частичных функций P^n. При этом под отрицанием частичной функции f понимается функция φ такая, что $N_\varphi = N_{\bar{f}}$, $N_{\bar{\varphi}} = N_f$, $N_{\tilde{\varphi}} = N_{\tilde{f}}$. Здесь исследуется также отношение длины с.д.н.ф. функции f из P^n к длине д.н.ф. $D_{UK}(f)$. Полученные здесь оценки имеют тот же порядок роста, что и оценки соответствующих параметров для всюду определенных функций. Примечательно то, что нижние оценки получаются для всех параметров сразу с помощью весьма простой конструкции. Пусть

$$A_P(n) = \max_{f \in P^n} \frac{l(D_c(f))}{l(D_{UP}(f))}; \quad B_P(n) = \max_{f \in P^n} \frac{l(D_c(f))}{l(D_{UM}(f))};$$

$$C_P(n) = \max_{f \in P^n} \frac{l(D_c(f))}{l(D_{UK}(f))}; \quad D_P(n) = \max_{f \in P^n} \frac{l(D_c(f))}{l(D_c(\bar{f}))}.$$

Теорема 4. Если $\chi(n)$ — произвольный из параметров $A_P(n)$, $B_P(n)$, $C_P(n)$, $D_P(n)$, то

$$1 + l^c_{\tilde{P}}(n-1) \leqslant \chi(n) \leqslant l^c_{\tilde{P}}(n).$$

Доказательство. Оценка сверху. Очевидно, что $\chi(n) \leqslant l^c_P(n)$. В силу теоремы 1, $l^c_P(n) = l^c_{\tilde{P}}(n)$. Отсюда и вытекает верхняя оценка.

Нижняя оценка. Пусть $f(x_1, \ldots, x_{n-1})$ — всюду определенная функция такая, что $l(D_c(f)) = l^c_P(n-1)$. Заметим, что f не является константой. Рассмотрим частичную функцию ψ из P^n следующего вида:

$$N_\psi = \{(\alpha_1, \ldots, \alpha_{n-1}, 1) / (\alpha_1, \ldots, \alpha_{n-1}) \in B^{n-1}\},$$

$$N_{\bar{\psi}} = \{(\alpha_1, \ldots, \alpha_{n-1}, 0) / (\alpha_1, \ldots, \alpha_{n-1}) \in B^{n-1}\}.$$

Очевидны следующие свойства функции:

1) $D_c(\psi)=D_c(\bar{f})$.

2) Единственной тупиковой, а следовательно, единственной минимальной и кратчайшей является д.н.ф. x_n.

3) Сокращенной д.н.ф. отрицания функции ψ является д.н.ф. $\bar{x}_n$.

Из свойств 1—3 вытекает, что для любого из параметров $\chi(n)$ из условия теоремы справедливо неравенство $\chi(n)\geqslant 1+l^c_{\tilde{P}}(n-1)$. Теорема доказана.

Следствие. Пусть $\chi(n)$ — произвольный параметр из перечисленных в условии теоремы 4. Тогда

$$\chi(n)=3^{n\left(1+0\left(\frac{\log n}{n}\right)\right)}.$$

Доказательство. Утверждение вытекает из оценок параметров, полученных в работе А. П. Викулина [6]. Там показано, что

$$C_1\cdot\frac{3^n}{n}\leqslant l^c_{\tilde{P}}(n)\leqslant C_2\cdot\frac{3^n}{\sqrt{n}},$$

где C_1, C_2 — константы.

6. СООТНОШЕНИЯ МЕЖДУ ТУПИКОВЫМИ, МИНИМАЛЬНЫМИ И КРАТЧАЙШИМИ Д. Н. Ф.

Оценки для максимального числа тупиковых д.н.ф. у функций из $\tilde{P}^n$ изучались в [8], [9]. Здесь приводятся примеры частичных функций, дающих высокие нижние оценки для числа тупиковых д.н.ф. и отношения числа тупиковых д.н.ф. к числу минимальных (кратчайших) д.н.ф.

Пример 3. Функция f определена следующим образом:

$$N_f=B^n_{k-1}\cup B^n_{k+1},\quad N_{\bar{f}}=B^n_k\cup B^n_{k-l-2}\cup B^n_{k+l+2},$$

где $k=\left[\frac{n}{2}\right]$, $l=\left[\frac{n}{4}\right]$.

Всякое тупиковое покрытие множества N_f состоит из проходящих через вершины множества N_f и не пересекающихся с множеством $N_{\bar{f}}$ граней размерности l. При этом для каждой вершины из N_f в тупиковое покрытие входит ровно одна грань. Легко проверить, что число максимальных интервалов, содержащих вершину $\tilde{\alpha}\in B^n_{k-1}$, $(\tilde{\alpha}\in B^n_{k+1})$, равно C^l_{k-1} (соответственно C^l_{n-k-1}). Таким образом, число тупиковых покрытий равно

$$(C^l_{k-1})^{C^{k-1}_n}\cdot(C^l_{n-k-1})^{C^{k+1}_n}.$$

При $k=\left[\frac{n}{2}\right]$ и $l=\left[\frac{n}{4}\right]$ и достаточно больших n эта величина равна $2^{(1+0(1))\cdot\sqrt{\frac{n}{2\pi}}\,2^n}$. Очевидно, что всякая т.д.н.ф. является кратчайшей и минимальной.

Приведем теперь пример частичной функции, имеющей большое число т.д.н.ф. и единственную минимальную (кратчайшую) д.н.ф.

Пример 4. Функция φ из P^n определена следующим образом (рис. 4):

$$N_\varphi = \{(\alpha_1, ..., \alpha_n)/\alpha_n = 1, \sum_{i=1}^{n-1} \alpha_i \in \{k-1,\ k+1\}\},$$

$$N_\varphi^- = \{(\alpha_1, ..., \alpha_n)/\alpha_n = 0, \sum_{i=1}^{n-1} \alpha_i \in \{k,\ k-l-2,\ k+l+2\}\},$$

где $k = \left[\frac{n-1}{2}\right]$, $l = \left[\frac{n-1}{4}\right]$.

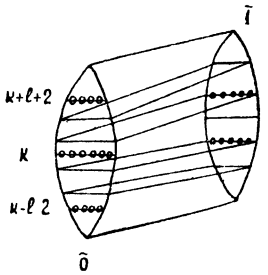


Рис. 4.

Нетрудно видеть, что единственной минимальной и кратчайшей д.н.ф. является д.н.ф. x_n. Кроме нее, тупиковыми д.н.ф. являются все тупиковые д.н.ф. функции $f(x_1, ..., x_{n-1})$, построенной в предыдущем примере. Таким образом, если $\tau(\psi)$, $\mu(\varphi)$, $\varkappa(\varphi)$ соответственно есть число тупиковых, минимальных, кратчайших д.н.ф. функции φ, то

$$\tau(\varphi) = \frac{\tau(\varphi)}{\mu(\varphi)} = \frac{\tau(\varphi)}{\varkappa(\varphi)} > \tau(f) \geqslant 2^{(1+0(1))\sqrt{\frac{n}{2\pi}}\cdot 2^{n-1}}$$

Отметим, что функция φ из P^n относится к классу так называемых «плотных» функций (см. [8]):

а) ее протяженность равна 2;

б) разброс длин тупиковых д.н.ф. равен $c' \cdot \frac{2^n}{\sqrt{n}}$, а разброс сложностей — $c'' \cdot \sqrt{n} \cdot 2^n$;

в) число тупиковых д.н.ф. $\tau(\varphi) > 2^{c\cdot\sqrt{n}\cdot 2^n}$;

г) среди тупиковых д.н.ф. имеется всего лишь одна минимальная (кратчайшая) д. н. ф.

ЛИТЕРАТУРА

1. Васильев Ю. Л. О сравнении сложности тупиковых и минимальных дизъюнктивных нормальных форм. Сб. «Проблемы кибернетики». М., Физматгиз, 1963, вып. 10, с. 5.

2. Глаголев В. В. О длине тупиковой дизъюнктивной нормальной формы. «Мат. заметки», 2, № 6, 665 (1967).

3. Лин Син-лян. О сравнении сложностей минимальных и кратчайших дизъюнктивных нормальных форм для функций алгебры логики. Сб. «Проблемы кибернетики». М., Наука, 1967, вып. 18, с. 11.

4. Левин А. А. Об относительной сложности сокращенной д. н. ф. Сб. «Дискрет. анализ». Новосибирск, ИМ СО АН СССР, 1969, вып. 15, с. 25.

5. Левин А. А. Об отношении сложности д. н. ф. функции к сложности д. н. ф. ее отрицания. Сб. «Дискрет. анализ». Новосибирск, ИМ СО АН СССР, 1970, вып. 16, с. 77.

6. Викулин А. П. Оценка числа конъюнкций в сокращенной д. н. ф. Сб. «Проблемы кибернетики». М., «Наука», 1974, вып. 29, с. 151.

7. Журавлев Ю. Л. Алгоритмы построения минимальных дизъюнктивных нормальных форм для функций алгебры логики. Сб. «Дискрет. математика и мат. вопр. кибернетики», т. 1. М., Наука, 1974, с. 67.

8. Васильев Ю. Л., Глаголев В. В. Метрические свойства дизъюнктивных нормальных форм. Сб. «Дискрет. математика и мат. вопр. кибернетики», т. 1. М., Наука, 1974, с. 99.

9. Сапоженко. Дизъюнктивные нормальные формы (метрическая теория). М., Изд-во МГУ, 1975.

Московский государственный университет

[4/X 1977]

О НЕКОТОРЫХ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫХ УПАКОВКАХ

Н. Н. Кузюрин

1. ОПРЕДЕЛЕНИЯ И ОБОЗНАЧЕНИЯ

Предлагается один общий метод построения максимальных упаковок и оценки их мощности, связанный с подсчетом числа решений систем сравнений определенного вида. Задача об упаковке рассматривается в следующей постановке. Пусть $q \geqslant 2$ — целое, $A = \{a_0, ..., a_{q-1}\}$ — частично-упорядоченное множество с выделенным элементом a_0, называемым нулевым, и частичным порядком $a_j \geqslant a_0$, $a_j \geqslant a_j$, $j = 0, 1, ..., q-1$. Пусть заданы натуральные числа l, k, n такие, что $1 \leqslant l \leqslant k \leqslant n$. Обозначим через A^n множество всех векторов $\vec{v} = (v_1, ..., v_n)$ таких, что $v_i \in A$, $i = 1, 2, ..., n$. Весом вектора $\vec{v}$ (обозначение $\|\vec{v}\|$) назовем число его ненулевых координат. Пусть $A_k^n = \{\vec{v} \in A^n : \|\vec{v}\| = k\}$. Будем говорить, что вектор $\vec{u} = (u_1, ..., u_n)$ покрывается вектором $\vec{v} = (v_1, ..., v_n)$ (обозначение $\vec{u} \leqslant \vec{v}$), если $u_i \leqslant v_i$, $i = 1, 2, ..., n$.

Упаковкой векторов веса l векторами веса k называется подмножество векторов $P_q(n, k, l) \subseteq A_k^n$, для которого выполняется условие: любой вектор веса l покрывается не более чем одним вектором из $P_q(n, k, l)$. Число векторов в максимальной по мощности упаковке обозначается через $m_q(n, k, l)$. Покрытием множества A_l^n векторами из A_k^n называется подмножество $Q_q(n, k, l) \subseteq A_k^n$ такое, что для любого $\vec{v} \in A_l^n$ найдется $\vec{u} \in Q_q(n, k, l)$, покрывающий $\vec{v}$ ($\vec{u} \geqslant \vec{v}$). Задача об упаковке заключается в нахождении или оценке функции $m_q(n; k, l)$. Эта задача рассматривалась многими авторами ([1—5]). Известно точное значение $m_2(n, 3, 2)$ [1] и для некоторых классов n значение $m_2(n, 4, 2)$ ([2], [4]).

В работе [3] доказано, что

$$\lim_{n\to\infty} \frac{m_2(n, k, 2) \cdot C_k^2}{C_n^2} = 1 \quad \text{и} \quad \lim_{n\to\infty} \frac{m_2(n, p+1, 3) \cdot C_{p+1}^3}{C_n^3} = 1,$$

где p — степень простого числа. При $q = 3$ задача допускает следующую геометрическую интерпретацию. В качестве $A = \{a_0, a_1, a_2\}$ выбирается $A = \{-, 0, 1\}$, причем a_0 соответствует символу $\{-\}$. Тогда множеству A^n соответствует множество всех граней единичного n-мерного куба, причем вектору веса k соответствует грань размерности $n-k$. Задача нахождения функции $m_3(n, n-k, n-l)$ эквивалентна нахождению максимального числа граней размерности k единичного n-мерного куба, никакие две из которых не содержатся в грани размерности l.

Из мощностных соображений нетрудно получить следующую оценку, хорошо известную при $q = 2$ ([1], [3]):

$$m_q(n, k, l) \leqslant \frac{C_n^l}{C_k^l} (q-1)^l. \tag{1}$$

Более точной является оценка, доказанная для $q=2$ в [1]:

$$m_q(n,k,l) \leqslant \left[\frac{n}{k}(q-1)\left[\frac{n-1}{k-1}(q-1)\left[\cdots\left[\frac{(n-l+1)}{(k-l+1)}(q-1)\right]\cdots\right]\right]\right]. \quad (2)$$

При $q=2$, $k=3$, $l=2$ в (2) достигается равенство тогда и только тогда, когда $n\not\equiv 5 \pmod 6$ ([1]). Нижнюю оценку для максимальных упаковок можно получить известным методом исчерпывания, подсчитывая все векторы веса k, которые покрывают хотя бы один вектор веса l, покрываемый фиксированным вектором из A_k^n:

$$m_q(n,k,l) \geqslant \frac{C_n^k \cdot (q-1)^k}{\sum\limits_{i=0}^{k-l}\sum\limits_{j=0}^{i} C_k^i \cdot C_i^j \cdot C_{n-k}^{i-j} \cdot (q-2)^j \cdot (q-1)^{i-j}}, \quad (3)$$

где $0^0=1$. Однако при растущих n и k оценка (3) отличается от (1) порядком. В [6] доказана асимптотическая оптимальность оценки (1) при $q=2$, $l=k-1$, $\frac{k}{n}\longrightarrow 0$ и $n\longrightarrow\infty$. Аналогичный результат имеет место и для $q>2$ ([7]). Далее получим две нижние оценки $m_q(n,k,l)$, которые близки к (1).

Примем следующие обозначения. Пусть $N=\{1,2,\ldots,n\}$ и $A'=A\setminus\{a_0\}$ — множество ненулевых элементов A. Через $B_1\times B_2$ будем обозначать декартово произведение множеств B_1 и B_2. Пусть заданы система подмножеств $\{N_i\}_{i=1}^k$, где $N_i\subseteq N$, $i=1,\ldots,k$, и вектор $(z_1,\ldots,z_k)$, где $z_i=(y_i,t_i)$, $y_i\in N_i$, $t_i\in A'$, причем $y_i\neq y_j$ $(i\neq j)$. Этому вектору поставим в соответствие вектор $\vec{v}\in A_k^n$ такой, что $y_1,\ldots,y_k$ — номера его ненулевых компонент, а $t_1,\ldots,t_k$ — значения этих компонент. Вектор $(z_1,\ldots,z_k)$, соответствующих вектору $\vec{v}\in A_k$, будем обозначать через $T_q(\vec{v})$. Пусть $r=r(m)$ обозначает наибольшее простое число, не большее m. Из теории чисел [8] известна оценка: для любого $\varepsilon>0$ найдется m_0 такое, что при $m\geqslant m_0$ $|r(m)-m|\leqslant m^\alpha$, где $\alpha=3/5+\varepsilon$. Наконец, для простых p через Z_p будем обозначать поле вычетов по модулю p.

2. НЕКОТОРЫЕ КОНСТРУКЦИИ И ОЦЕНКИ ДЛЯ УПАКОВОК

Предлагаемый способ построения упаковок с фиксированным весом векторов заключается в задании специального соответствия между некоторым множеством k-мерных векторов $\{(x_1,\ldots,x_k)\}$ и векторами из A_k^n и выборе в качестве множества k-мерных векторов всех решений некоторой системы сравнений:

$$\begin{cases} F_1(x_1,\ldots,x_k)\equiv c_1 \\ \ldots\ldots\ldots \\ F_{k-l}(x,\ldots,x_k)\equiv c_{k-l} \end{cases} \pmod p, \quad (4)$$

где функции $F_1,\ldots,F_{k-l}$ подбираются так, чтобы множество векторов из A_k^n, соответствующие решениям системы (4), было упаковкой множества A_l^n. Правило соответствия определяется некоторой фиксированной системой подмножеств $\{N_i\}_{i=1}^k$, $N_i\subseteq N$, $i=1,2,\ldots,k$. А именно, пусть $N_i'=\{1,2,\ldots,r_i\}$, где $r_i\leqslant|N_i|\cdot(q-1)$, и заданы взаимно одно-

значные отображения N_i' в $N_i \times A'$ φ_i: $N_i' \longrightarrow N_i \times A'$, $i=1,\ldots,k$, удовлетворяющие условию согласования:

если $\varphi_i(x_0) \in (N_i \cap N_j) \times A'$, то $\varphi_j(x_0) = \varphi_i(x_0)$, $i,j=1,2,\ldots,k$.

Положим $X^k = \{(x_1,\ldots,x_k),\ x_i \in N_i',\ i=1,2,\ldots,k\}$. Тогда любому подмножеству $Y \subseteq X^k$ соответствует множество $P(Y)$ векторов из A_k^n, задаваемое равенством $P(Y) = \{\vec{v} \in A_k^n$: существует $(y_1,\ldots,y_k) \in Y$ такой, что $(\varphi_1(y_1),\ldots,\varphi_k(y_k)) = T_q(\vec{v})\}$. Функции $F_i(x_1,\ldots,x_k)$, $i=1,\ldots,k-l$ выбираются такими, чтобы они удовлетворяли двум условиям:

1) правило перестановки: если $\varphi_i(x_i) = (y_i, t_i)$, $\varphi_j(x_j) = (y_j, t_j)$ и $y_j,\ y_i \in N_i \cap N_j$, то при любых $z_1,\ldots,z_{i-1},\ z_{i+1},\ldots,z_{j-1},\ z_{j+1},\ldots,z_k,\ z_\mu \in N_\mu'$, $\mu=1,\ldots,k$ выполняется равенство

$$F_t(z_1,\ldots,z_{i-1},\ x_i,\ z_{i+1},\ldots,z_{j-1},\ x_j,\ z_{j+1},\ldots,z_k) =$$

$$= F_t(z_1,\ldots,z_{i-1},\ x_j,\ z_{i+1},\ldots,z_{j-1},\ x_i,\ z_{j+1},\ldots,z_k),\ t=1,\ldots,k-l.$$

2) l — однозначная p-разрешимость: при фиксировании любых l переменных в системе (4), оставшиеся определяются однозначно с точностью до перестановок (условие 1) при любых $c_1,\ldots,c_{k-l}$, причем $x_i \in N_i'$. Множество функций $\{F_1,\ldots,F_{k-l}\}$, удовлетворяющее условию 2, будем называть l — однозначным над $\{N_i'\}_{i=1}^k$.

Если $Y = \{(x_1,\ldots,x_k)\}$ — множество решений системы (4), причем для тех x_i, x_j, для которых $\varphi_i(x_i) = (y_i, t_i)$, $\varphi_j(x_j) = (y_j, t_j)$ и $y_i,\ y_j \in N_i \cap N_j$ выполнено условие $y_i \neq y_j$, $(i \neq j)$, то соответствующее множеству Y множество $P(Y) \subseteq A_k^n$ является упаковкой A_l^n в силу свойств 1 и 2.

Рассмотрим вариант этого метода, когда система подмножеств $\{N_i\}_{i=1}^k$ удовлетворяет условию $N_i \cap N_j = \varnothing$ $(i \neq j)$. Нетрудно видеть, что в этом случае отсутствует первое ограничение на функции $F_1,\ldots,F_{k-l}$ — правило перестановки. Выберем эти функции линейными.

Теорема 1: Пусть q — целое, $q \geqslant 2$ и последовательности натуральных чисел $k=k(n)$ и $l=l(n)$ удовлетворяют условиям:

1) $k(n) \longrightarrow \infty$ и $k^2 + (q-1)^\alpha \cdot (n-k)^\alpha \cdot k^{1-\alpha} - (q-1)(n-k) < 0$ при $n \longrightarrow \infty$ и некотором $\alpha > 3/5$;

2) $l / \sqrt{k} \longrightarrow 0$ при $n \longrightarrow \infty$;

3) $l / \left(\frac{n}{k}\right)^{1-\alpha} \longrightarrow 0$ при $n \longrightarrow \infty$.

Тогда $\lim\limits_{n\to\infty} \dfrac{m_q(n,k,l) \cdot k^l}{n^l \cdot (q-1)^l} = 1$.

Доказательство. Разобьем множество N на k непересекающихся подмножеств N_i таких, что $||N_i| - |N_j|| \leqslant 1$, $i,j=1,2,\ldots,k$. Положим $m = \left[\frac{n}{k}\right] \cdot (q-1)$ и выберем подмножества $\bar{N}_i \subseteq N_i \times A'$ так, чтобы $|\bar{N}_i| = r(m)$, где $r(m)$ — наибольшее простое число не большее m.

Пусть φ_i — взаимно однозначное отображение $N_i' = \{1,2,\ldots,r\}$ на $\bar{N}_i$

$$\varphi_i : N_i' \longrightarrow \bar{N}_i,\ i=1,2,\ldots,k.$$

Из условий теоремы следует, что найдется число n_0, такое, что при $n \geqslant n_0$ выполнено неравенство $r > k$.

Пусть $n \geqslant n_0$; рассмотрим систему сравнений:

$$\begin{cases} \sum\limits_{i=1}^{k} x_i \equiv c_1 \\ \sum\limits_{i=1}^{k} i \cdot x_i \equiv c_2 \pmod r, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \sum\limits_{i=1}^{k} i^{k-l-1} \cdot x_i \equiv c_{k-l} \end{cases} \tag{5}$$

где $c_1, \ldots, c_{k-l}$ фиксированы из $\{0, 1, \ldots, r-1\}$ $x_i \in \{1, 2, \ldots, r\}$ $i = 1, 2, \ldots, k$.

Сопоставим каждому решению $(x_1^0, \ldots, x_k^0)$ системы (5) q-ный вектор $\vec{v} \in A_k^n$ по правилу $T_q(\vec{v}) = (\varphi_1(x_1^0), \ldots, \varphi_k(x_k^0))$. Получим некоторое подмножество $K_q \subseteq A_k^n$, которое является упаковкой векторов веса l, поскольку в двух различных решениях системы (5) не могут совпадать значения l соответствующих переменных (главный определитель системы — определитель Вандермонда). При достаточно больших n справедливы оценки

$$|K_q| = |\bar{N}_i|^l = r^l \geqslant \left(\left(\frac{n}{k} - 1\right)(q-1) - \left(\frac{n}{k} - 1\right)^{\alpha} \cdot (q-1)^{\alpha}\right)^l \gtrsim$$

$$\gtrsim \left(\frac{n}{k}\right)^l \cdot (q-1)^l \cdot \left(1 - \frac{l}{\left(\frac{n}{k}(q-1)\right)^{1-\alpha}}\right) \gtrsim \left(\frac{n}{k}(q-1)\right)^l.$$

Получим $\dfrac{m_q(n, k, l) \cdot C_k^l}{C_n^l \cdot (q-1)^l} \gtrsim \dfrac{(k)_l}{k^l} \geqslant 1 - \dfrac{C_l^2}{k} \geqslant 1 - \varepsilon_n$,

где $\varepsilon_n \longrightarrow 0$ при $n \longrightarrow \infty$. Сравнивая с (1), убеждаемся в справедливости теоремы.

Из вышесказанного вытекает справедливость следующего ослабленного варианта гипотезы Эрдеша—Ханани [4].

Следствие. При $q \geqslant 2$, $l \geqslant 2$ имеет место равенство

$$\lim_{k \to \infty} \lim_{n \to \infty} \frac{m_q(n, k, l) \cdot C_k^l}{C_n^l \cdot (q-1)^l} = 1.$$

Рассмотрим теперь другой вариант описанного метода, при котором система подмножеств $\{N_i\}_{i=1}^k$ выбирается из условия $N_i = N$, $i = 1, \ldots, k$, $N_i' = \{1, 2, \ldots, n(q-1)\}$. Пусть φ — взаимно однозначное отображение $\varphi : \{1, 2, \ldots, n(q-1)\} \longrightarrow N \times A'$. В этом случае правилу перестановки удовлетворяют только симметрические функции от переменных $x_1, \ldots, x_k$, а второе соответствует однозначной разрешимости системы симметрических функций

$$\begin{cases} F_1(x_1, \ldots, x_k) \equiv c_1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ F_{k-l}(x_1, \ldots, x_k) \equiv c_{k-l} \end{cases} \pmod p, \tag{6}$$

где $p \geqslant m = n(q-1)$, p — простое число, $x_i \in \{1, 2, \ldots, m\}$, $i = 1, 2, \ldots, k$.

Упаковку, соответствующую множеству решений системы (6), обозначим через $T_S^p(c_1, \ldots, c_{k-l})$, где $S = \{F_1, \ldots, F_{k-l}\}$. Оказывается, что в

таком виде можно представить любую упаковку, в том числе и максимальную.

Теорема 2. Пусть $1 \leqslant l < k < n$, p_1 и p_2 — простые числа, удовлетворяющие условию $p_2 > p_1 \geqslant m$. Для любой упаковки $P_q(n, k, l)$ существуют l-однозначное над $N_i' = \{1, 2, ..., m\}$ множество $S^* = \{F_1^*, ..., F_{k-l}^*\}$ симметрических функций аргументов $x_1, ..., x_k$ и $c_1^0, ..., c_{k-l}^0$ из Z_p такие, что

$$P_q(n, k, l) = T_{S^*}^{p_2}(c_1^0, ..., c_{k-l}^0).$$

Доказательство. Достаточно, чтобы функции $F_1^*, ..., F_{k-l}^*$ удовлетворяли условию:

$$F_i^*(x_1, ..., x_k) = \begin{cases} p_1, \text{ если существует } \vec{v} \in p_q(n, k, l) \text{ такой, что } T_q(\vec{v}) = \\ \quad = (\varphi(x_1), ..., \varphi(x_k)), \\ \sigma_i(x_1, ..., x_k) \pmod{p_1} \text{ в противном случае,} \end{cases}$$

где $\sigma_1, ..., \sigma_{k-l}$ — первые $k-l$ элементарных симметрических функций от $x_1, ..., x_k$.

Нетрудно проверить, что $F_1^*, ..., F_{k-l}^*$ — симметрические функции и система $S^* = \{F_1^*, ..., F_{k-l}^*\}$ l-однозначна над множеством $\{1, 2, ..., m\}$. Ясно также, что $P_q(n, k, l) = T_{S^*}^{p_2}(p_1, ..., p_1)$, т. е. $P_q(n, k, l)$ задается решениями системы

$$\begin{cases} F_1^*(x_1, ..., x_k) \equiv p_1 \\ \quad \cdots \cdots \cdots \\ F_{k-l}^*(x_1, ..., x_k) \equiv p_1 \end{cases} \pmod{p_2},$$

где $x_i \in \{1, 2, ..., m\}$, $i = 1, ..., k$.

Так как при заданном l — однозначном множестве функций $S = \{F_1, ..., F_{k-l}\}$ число систем вида (6) равно p^{k-l}, а число всевозможных векторов $(x_1, ..., x_k)$, $x_i \in \{1, 2, ..., m\}$, с условием $y_i \neq y_j$, $(i \neq j)$, где $\varphi(x_i) = (y_i, t_i)$, $i = 1, 2, ..., k$, равно $(n)_k \cdot (q-1)^k$, то справедлива

Теорема 3. Пусть $S = \{F_1, ..., F_{k-l}\}$ — l-однозначное над $\{1, 2, ..., m\}$ множество симметрических функций аргументов $x_1, ..., x_k$ над полем Z_p. Тогда

$$m_q(n, k, l) \geqslant \max_{c_1, ..., c_{k-l} \in Z_p} |T_S^p(c_1, ..., c_{k-l})| \geqslant \frac{(n)_k \cdot (q-1)^k}{p^{k-l} \cdot k!}. \qquad (7)$$

Например, при $k < p$ множество $S_0 = \{\sigma_1, ..., \sigma_{k-l}\}$ первых $k-l$ элементарных симметрических функций от переменных $x_1, ..., x_k$ является l-однозначным над Z_p. При фиксировании $x_1, ..., x_l$ получаем из (6) систему вида

$$\begin{cases} \sigma_1(x_{l+1}, ..., x_k) \equiv c'_1 \\ \quad \cdots \cdots \cdots \\ \sigma_{k-l}(x_{l+1}, ..., x_k) \equiv c'_{k-l} \end{cases} \pmod{p},$$

которая, как известно, имеет в поле Z_p не более $(k-l)!$ решений, так как если $(y_1, ..., y_{k-l})$ — решение системы, то $y_1, ..., y_{k-l}$ — корни уравнения $x^{k-l} - c_1' x^{k-l-1} + \cdots + (-1)^{k-l} \cdot c'_{k-l} \equiv 0 \pmod{p}$.

Если $k-l$ не зависит от n, то из оценки (7) получается порядок роста величины $m_q(n, k, l)$ при $n \longrightarrow \infty$, $k \leqslant c \cdot n$, где $c < 1$ — константа.

Действительно, имеем

$$\frac{(n)_l}{(k)_l}(q-1)^l \geqslant m_q(n,k,l) \geqslant \frac{(n)_k \cdot (q-1)^k}{(n(q-1)+0(n(q-1)))^{k-l} \cdot k!} \gtrsim$$

$$\gtrsim \frac{(n)_l}{(k)_l}(q-1)^l \cdot (1-c)^{k-l} \cdot \frac{1}{(k-l)!}.$$

В частности, если $l=k-1$ и $k=o(n)$ при $n \to \infty$, то при $q \geqslant 2$, $m_q(n,k,k-1) \sim \frac{c_n^{k-1}}{k}(q-1)^{k-1}$. Оценки типа (7) могут быть получены из рассмотрения других систем функций, например $S_i=\{\sigma_1, ..., \sigma_i, \sigma_{i+l+1}, ..., \sigma_k\}$, где $k-l>i \geqslant 1$.

Нетрудно проверить, что при фиксировании l переменных в системе

$$\begin{cases} \sigma_i(x_1, ..., x_k) \equiv c_1 \\ \dots\dots\dots\dots \\ \sigma_i(x_1, ..., x_k) \equiv c_i \\ \sigma_{i+l+1}(x_1, ..., x_k) \equiv c_{i+1} \\ \dots\dots\dots\dots \\ \sigma_k(x_1, ..., x_k) \equiv c_{k-l}. \end{cases} \pmod p.$$

получим однозначно разрешимую систему (с точностью до перестановки переменных), если $c_{k-l} \not\equiv 0 \pmod p$.

Известно, что любую функцию от k переменных над полем Z_p можно представить в виде полинома [9], а симметрический полином, в свою очередь, в виде

$$F_t(x_1, ..., x_k) = f_t(s_1, ..., s_k),$$

где $k<p$, $t=1, ..., k-l$ и $s_i = \sum_{j=1}^{k} x_j^i$ $(i=1, 2, ..., k)$ — степенные симметрические функции и f_t — некоторый полином от k переменных. Простейшим является случай, когда f_t — полином первой степени, т. е. $f_t = \sum_{j=1}^{k} c_{tj} \cdot s_j(x_1, ..., x_k)$. Система (6) в этом случае задается матрицей коэффициентов (c_{tj}), $t=1, ..., k-l$; $j=1, ..., k$. Будем называть такие системы линейными, понимая под этим линейность относительно $\{s_1, ..., s_k\}$. Рассмотренная выше система

$$\begin{cases} \sigma_1(x_1, ..., x_k) \equiv c_1 \\ \dots\dots\dots\dots \\ \sigma_{k-l}(x_1, ..., x_k) \equiv c_{k-l} \end{cases} \pmod p$$

эквивалентна системе

$$\begin{cases} s_1(x_1, ..., x_k) \equiv c_1' \\ \dots\dots\dots\dots \\ s_{k-l}(x_1, ..., x_k) \equiv c_{k-l}' \end{cases} \pmod p, \qquad (8)$$

которая, очевидно, является линейной. Таким образом, оценка (7) может быть получена уже в классе линейных систем из рассмотрения системы (8). В частности, при $l=k-1$ асимптотически оптимальные упаковки существуют в классе линейных систем. Естественно исследовать поэтому насколько хороши упаковки, существующие в классе линейных систем.

Система сравнений (8) изучалась в теории чисел ([10—14]). В работе [11] доказано, что число решений (8) можно представить в виде $p^l + \Theta \cdot ((k-l)\sqrt{p})^k$, где $|\Theta| \leqslant 1$. Отсюда вытекает, при некото-

рых ограничениях (см. [11]), асимптотика для числа решений (8). Опираясь на эти результаты, покажем, что при некоторых ограничениях оценка (7) не может быть асимптотически улучшена в классе линейных систем.

Рассмотрим более общий случай, когда

$$F_j(x_1, ..., x_k) = \sum_{i=1}^{k} f_j(x_i), \quad j=1, ..., k-l. \tag{9}$$

Очевидно, что всякая функция $f(s_1, ..., s_k)$, где f — полином первой степени, представима в виде (9), причем $\deg f_j(x) \leqslant k$, где $\deg f_j$ — степень полинома f_j, $j=1, ..., k-l$. Положим $R = \max\limits_{j=1, ..., k-l} \deg f_j(x)$. Оценим число решений (6) с левыми частями вида (9). Пусть $f_i(x) = \sum\limits_{j=0}^{p-1} c_{ij} x^j$ — представление в виде полинома для $f_i(x)$, $i=1, ..., k-l$ (все операции в Z_p). Рассмотрим p-мерное векторное пространство H^p над полем Z_p. Через $L\{\vec{b}_1, ..., \vec{b}_t\}$, где $\vec{b}_i \in H^p$, $i=1, ..., t$, будем обозначать линейную оболочку векторов $\vec{b}_1, ..., \vec{b}_t$. Положим $\vec{c}_i = (c_{i,0}, ..., c_{i,p-1})$, $\vec{b}_i = (c_{i,0}, ..., c_{i,p-1}, c_i)$, где c_i — правая часть i-го сравнения в (6). Пусть размерность подпространства $L = \{\vec{c}_1, ..., \vec{c}_{k-l}\}$ равна r, $1 \leqslant r \leqslant k-l$, и $\vec{c}_1, ..., \vec{c}_r$ — его базис (для простоты записи мы выбрали первые r векторов). Систему (6) можно переписать в виде

$$\begin{cases} \sum\limits_{j=0}^{p-1} c_{1,j} \cdot \left(\sum\limits_{i=1}^{k} x_i^j \right) \equiv c_1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad , \quad , \\ \sum\limits_{j=0}^{p-1} c_{k-l,j} \cdot \left(\sum\limits_{i=1}^{k} x_i^j \right) \equiv c_{k-l} \end{cases} \pmod p,$$

где $x_i \in \{1, 2, ..., m\}$, $i=1, ..., k$.

Пусть T — число решений этой системы. Если найдется $j_0 \in \{1, 2, ..., k-l\}$ такой, что $\vec{b}_{j_0} \in L\{\vec{b}_1, ..., \vec{b}_r\}$, то эта система несовместна, и поэтому $T=0$. В противном случае множество решений этой системы совпадает с множеством решений системы

$$\begin{cases} \sum\limits_{i=1}^{k} f_1(x_i) \equiv c_1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \sum\limits_{i=1}^{k} f_r(x_i) \equiv c_r \end{cases} \pmod p, \tag{10}$$

где $x_i \in \{1, 2, ..., m\}$, $i=1, ..., k$.

Теорема 4. Пусть векторы $\vec{c}_1, ..., \vec{c}_r$ линейно независимы над Z_p, где $\vec{c}_i$ — вектор коэффициентов в представлении функции $f_i(x)$ в виде полинома в Z_p, $i=1, ..., r$. Тогда для числа решений системы (10) имеет место равенство

$$T = \frac{m^k}{p^r} + \Theta(R\sqrt{p} + p - m)^k, \quad \text{где} \quad |\Theta| \leqslant 1.$$

Доказательство. Используя равенство

$$\sum_{x=0}^{p-1} \exp\left(\frac{2\pi i}{p} a x \right) = \begin{cases} p \text{ при } a \equiv 0 \pmod p \\ 0 \text{ при } a \not\equiv 0 \pmod p \end{cases}, \quad a \in Z_p,$$

число решений (10) можно представить в виде

$$T=\frac{1}{p^r}\sum_{x_1,\dots,x_k\in\{0,\dots,m-1\}}\prod_{s=1}^{r}\sum_{x=0}^{p-1}\exp\left[\frac{2\pi i}{p}x\left(\sum_{i=1}^{k}f_s(x_i)-c_s\right)\right]=$$

$$=p^{-r}\sum_{t_1,\dots,t_r\in\{0,\dots,p-1\}}\exp\left(-\frac{2\pi i}{p}\sum_{s=1}^{r}t_s c_s\right)\sum_{x_1,\dots,x_k\in\{0,\dots,m-1\}}\exp\left[\frac{2\pi i}{p}\times\right.$$

$$\left.\times\sum_{\nu=1}^{r}t_\nu\sum_{i=1}^{k}f_\nu(x_i)\right]=p^{-r}\sum_{t_1,\dots,t_r\in 0,\dots,p-1}\exp\left(-\frac{2\pi i}{p}\sum_{s=1}^{r}t_s c_s\right)\times$$

$$\times\left(\sum_{x=0}^{m-1}\exp\left(\frac{2\pi i}{p}\sum_{g=0}^{R}\sum_{\nu=1}^{r}t_\nu c_{\nu,g}x^g\right)\right)^k.$$

Выделяя из этой суммы член, соответствующий $t_1=\dots=t_r=0$, и применяя к остальным оценку А. Вейля (см. [11], [12])

$$\left|\sum_{x=0}^{p-1}\exp\left[\frac{2\pi i}{p}(a_1x+\dots+a_{s+1}x^{s+1})\right]\right|\leqslant s\sqrt{p},\qquad(11)$$

если существует $a_i\not\equiv 0(\mathrm{mod}\,p)$, $a_j\in Z_p$, $j=1,\dots,s$,

то получим $T=\dfrac{m^k}{p^r}+\Theta(R\sqrt{p}+p-m)^k$.

Применение оценки (11) корректно, поскольку, в силу линейной независимости $\vec{c}_1,\dots,\vec{c}_r$, найдется номер g такой, что

$$\sum_{\nu=1}^{r}t_\nu c_{\nu,g}\not\equiv 0\ (\mathrm{mod}\,p).$$

Замечание. Доказательство проведено методом работы [11] с дополнительным использованием линейной независимости $\vec{c}_1,\dots,\vec{c}_r$ и оценки

$$\left|\sum_{x=0}^{m-1}\exp\left[\frac{2\pi i}{p}(a_1x+\dots+a_{s+1}x^{s+1})\right]\right|\leqslant$$

$$\leqslant\left|\sum_{x=0}^{p-1}\exp\left[\frac{2\pi i}{p}(a_1x+\dots+a_{s+1}x^{s+1})\right]\right|+$$

$$+\left|\sum_{x=m}^{p-1}\exp\left[\frac{2\pi i}{p}(a_1x+\dots+a_{s+1}x^{s+1})\right]\right|\leqslant s\sqrt{p}+p-m.$$

Нетрудно убедиться, что если $n\longrightarrow\infty$, q фиксировано и выполнены условия

$$R\lesssim p^\varepsilon,\qquad(12)$$

где $0<\varepsilon<1/2$ и существует $0<\delta<1$ такое, что $\dfrac{p-m}{p^\delta}\longrightarrow 0$,

$$k\geqslant(2r+1)\Big/\left(\frac{2\log m}{\log p}-1-\frac{2\log\left(R+\dfrac{p-m}{\sqrt{p}}\right)}{\log p}\right)\gtrsim 2cr,$$

где

$$c\geqslant\max\{(1-2\varepsilon)^{-1},\ (2-2\delta)^{-1}\},$$

то из теоремы 4 получаем

$$T\sim n^{k-r}(q-1)^r\quad\text{при}\quad n\longrightarrow\infty.\qquad(14)$$

Если выполнены условия (12), (13), то предыдущее равенство показывает, что в классе линейных систем нельзя улучшить оценку (7),

так как $$n^l(q-1)^l \sim \frac{(n)_k(q-1)^k}{p^{k-l}}$$

Из теоремы 4 можно сделать некоторые выводы и о покрытиях. Из мощностных соображений следует, что не существует покрытий $Q_q(n, k, l)$ мощности меньшей, чем $\frac{C_n^l}{C_k^l}(q-1)^l$. Сравнивая эту оценку с (14), убеждаемся, что в классе могут существовать упаковки множества A_l^n, являющиеся одновременно покрытиями A_{l-1}^n.

Теорема 5: Если $2(n-k+2)(q-1)-p-2(q-1)^2>0$, то в классе линейных систем существует упаковка множества A_{k-1}^n, являющаяся одновременно покрытием A_{k-2}^n.

Доказательство. Рассмотрим сравнение

$$\sum_{i=1}^{k} x_i \equiv c \pmod p,$$

где $x_i=y_i+(t_i-1)n$, $0\leqslant y_i\leqslant n-1$, $1\leqslant t_i\leqslant q-1$, $i=1, \ldots, k$.

При любых фиксированных $x_1, \ldots, x_{k-2}$ таких, что $y_i\neq y_j$ $(i\neq j)$, получаем из (15) сравнение вида $x_{k-1}+x_k\equiv c'(\mathrm{mod}\, p)$, которое имеет не менее $2(n-k+2)(q-1)-p-2(q-1)^2$ решений, удовлетворяющих условию $y_{k-1}\neq y_k$, y_{k-1}, $y_k\in\overline{\{y_1, \ldots, y_{k-2}\}}$, поскольку сравнение $2x+(t_{k-1}+t_k)\cdot n\equiv c'(\mathrm{mod}\, p)$ имеет не более $2(q-1)^2$ решений. Наличие этих свойств и означает, что упаковка множества A_{k-1}^n, соответствующая множеству решений (15), является одновременно покрытием A_{k-2}^n.

В заключение автор благодарит А. А. Сапоженко за внимание к работе.

ЛИТЕРАТУРА

1. Schönheim J. On maximal systems of k-tuples. Studia Sci. Math. Hungar. 1, N 3—4, 363 (1966).

2. Brower A. E. Optimal packings of K^1_4 s into K_n-the case $n\equiv 5$ (mod 6), Math Centre report, ZW 82/76, Amsterdam, sept. 1976.

3. Erdös P., Hanani H. On a limit theorem in combinatorial analysis. Publ. Math. Debrecen, N 10, 10, (1963).

4. Эрдеш П., Спенсер Дж. Вероятностные методы в комбинаторике. М., Мир, 1976.

5. Ph. Delsarte. Fowe fundamental parameters of a code and their combinatorial significance, Inform. and Control, 23, N 5, 407 (1973).

6. Кузюрин Н. Н. О минимальных покрытиях и максимальных упаковках $(\kappa-1)$-подмножеств κ-подмножествами. «Мат. заметки», 21, № 4, 565 (1977).

7. Кузюрин Н. Н. Об асимптотической сложности покрытий и упаковок в единичном, n-мерном кубе. IV Всесоюз. конф. по проблемам теорет. кибернетики. (Тезисы докл.). Новосибирск, 1977, с. 173.

8. Монтгомери. Мультипликативная теория чисел. М., Мир, 1974.

9. Яблонский С. В. Введение в теорию функций κ-значной логики. — В кн.: «Дискрет. математика и мат. вопр. кибернетики», т. 1. М., Наука, 1974, с. 9.

10. Марджанишвили К. К. О некоторых нелинейных системах уравнений в целых числах. Мат. сб., № 33 (75), 639 (1953)

11. Линник Ю. В. Некоторые замечания об оценках тригонометрических сумм. «Успехи мат. наук», 14, № 3, 153 (1959).

12. Карацуба А. А. Об одной системе сравнений. «Мат. заметки», 19, № 3, 389 (1976).

13. Марджанишвили К. К. Об одном особом ряде. Труды МИ АН СССР, М., 1976, 142, с 174.

14. Varshamov R. R. A class of codes for asymmetric channels and problem from the additive theory of numbers, IEEE Trans. Inform. Theory, 19, N 1, 92, (1973).

Научный совет по комплексной проблеме «Кибернетика» АН СССР

[20/XII 1979]

Заказ 9258

ОДНО МНОГОЗНАЧНОЕ РАЗЛОЖЕНИЕ ЛАГРАНЖА, ВЫРАЖЕННОЕ ЧЕРЕЗ КОЭФФИЦИЕНТЫ ИСХОДНЫХ РЯДОВ

А. В. Куприков

Настоящая работа является продолжением [1]. Пусть даны голоморфная функция в окрестности начала координат

$$f(z)=f(z_1, ..., z_n)$$

и отображение

$$w_j=(z_j+\varphi_j(z))^{\kappa_j}\cdot\psi_j(z), \quad j=1, ..., n, \tag{1}$$

где φ_j и ψ_j — функции, голоморфные в окрестности нуля, удовлетворяющие условиям

$$\varphi_j(0)=0, \quad \frac{\partial\varphi_j}{\partial z_i}\Big|_0=0, \quad \psi_j(0)\neq 0, \quad i, j=1, ..., n, \tag{2}$$

$\kappa_j\geqslant 1$ — целые.

В [1] показано, что отображение (1) в некоторой окрестности нуля V имеет многозначное обратное отображение с порядком ветвления $\kappa_1\cdot ...\cdot\kappa_n$, причем плоскостями ветвления являются координатные плоскости. Эта задача является обобщением задачи об обращении системы степенных рядов, рассмотренной в [2, 3]. Обобщения на случай системы неявных функций рассмотрены в работах [4, 5].

В настоящей работе решается следующая задача. Пусть функции f, φ_j и ψ_j, $j=1, ..., n$, заданы в окрестности нуля своими рядами Тейлора

$$\begin{aligned} f(z)&=\sum_{\mu\geqslant 0} a_\mu z^\mu,\\ \psi_j(z)&=\sum_{\mu\geqslant 0} b_{j\mu} z^\mu,\\ \varphi_j(z)&=\sum_{\mu\geqslant 0} c_{j\mu} z^\mu,\\ j&=1, ..., n, \end{aligned} \tag{3}$$

и выполнены условия (2). Найти разложение функции $f(z(w))$ в ряд, коэффициенты которой выражены через коэффициенты рядов (3). Здесь $z(w)$ — отображение, обратное к (1). Из [1]

$$z_j=z_j(w)=\sum_{\alpha\geqslant 0} g_\alpha^j\, w^{\frac{\alpha}{\kappa}},$$

где

$$g_\alpha^j=\sum_{2|\alpha|\leqslant|\beta|\leqslant|\alpha|}\frac{(-1)^{|\beta-\alpha|}}{\alpha!(\beta-\alpha)!}\frac{\partial^{|\beta|}}{\partial\zeta^\beta}\left[\frac{\zeta_j\varphi^{\beta-\alpha}}{\psi^{\frac{(\alpha+1)}{\kappa}}}\cdot\frac{\partial(h)}{\partial(\zeta)}\right]\Bigg|_{\zeta=0},$$

$$h(\zeta)=((z_1+\varphi_1)\cdot\psi_1^{\frac{1}{\kappa_1}}, ..., (z_n+\varphi_n)\cdot\psi^{\frac{1}{\kappa_n}}),$$

здесь и далее предполагается, что неопределенность $0^0=1$.

В одномерном случае при $\varphi(z)\equiv 0$ поставленная задача решается в [6] с помощью обобщенных полиномов Белла.

При заданных ограничениях справедлива

Теорема. В некоторой окрестности $0\in c^n$ функция $f(z(w))$ представима в виде

$$f(z(w))=\sum_{\gamma\geqslant 0} g_\gamma\, w^{\frac{\gamma}{\kappa}},$$

где

$$g_\nu = \Sigma' \frac{(-1)^{|\beta-\gamma+\alpha|}\beta!}{\kappa\gamma!} \frac{\left(\frac{\gamma+\kappa}{\kappa}\right)_\alpha}{b_0^{\frac{\gamma+\kappa}{\kappa}+\alpha}} a_\xi \prod_{\chi,\lambda} \frac{c_\chi^{\nu_\chi} b_\lambda^{\alpha_\lambda}}{\gamma_\chi!\,\alpha_\lambda!} \Delta. \qquad (4)$$

Δ — определитель с общим членом

$$A_{ij} = \kappa_i(\mu_j^{(i)}+1)c_{i\mu^{(i)}+I_j} b_{i\nu^{(i)}} + (\nu_j^{(i)} +$$

$$+1)c_{i\mu^{(i)}} b_{i\nu^{(i)}+I_j} + d_{\mu^{(i)}}(\nu_j^{(i)} + p_{ij}) b_{i\nu^{(i)}+I_j-I_i}, \qquad (5)$$

здесь $p_{ij}=1$ для $i\neq j$, $p_{ii}=\kappa_i$, $I_j=(0,\ldots,\overset{j}{1},\ldots,0)$, $d_{\mu^{(i)}}=0$ для $\mu^{(i)}\neq 0$, $d_0=0$.

Суммирование Σ' ведется по наборам

$$\beta\geqslant 0,\ \xi\geqslant 0,\ \sum_\chi |\chi\gamma_\chi| + \sum_\lambda |\lambda\alpha_\lambda| + |\mu+\nu| + \xi = \beta,$$

$$\sum_{\chi^{(i)}} \gamma_{\chi^{(i)}} = \gamma_i, \qquad \sum_{\lambda^{(i)}} \alpha_{\lambda^{(i)}} = \alpha_i,$$

где $\sum_{\chi^{(i)}} = \sum_{\beta\geqslant\chi^{(i)}\geqslant 0}$, $\sum_{\lambda^{(i)}} = \sum_{\beta\geqslant\lambda^{(i)}\geqslant 0}$.

Доказательство. В [1] формула (4) в интегральной форме имеет вид

$$f(r(\eta)) = \sum_{\beta\geqslant 0} \frac{1}{(2\pi i)^n} \int_\Gamma f \frac{\left(\frac{\eta}{\psi^{\frac{1}{\kappa}}} - \varphi\right)^\beta}{\psi^{\frac{1}{\kappa}}\zeta^{\beta+I}} \frac{\partial(h)}{\partial(\zeta)} a\zeta,$$

$$\Gamma = \{\zeta\in C^n : |\zeta_1| = \cdots = |\zeta_n| = \varepsilon\},\quad \eta_j = h_j(\zeta),\quad j=1,\ldots,n.$$

Производя дифференцирование в якобиане и вынося множитель $1/(\kappa\cdot\psi^{\frac{\kappa-1}{\kappa}})$, получаем $\frac{\partial(h)}{\partial(\zeta)} = \frac{1}{\kappa\psi^{\frac{\kappa-1}{\kappa}}}\Delta_h$.

Общий член Δ_h есть

$$B_{ij} = \sum_{\substack{\mu\geqslant 0\\ \nu\geqslant 0}} (\kappa_j(\mu_j+1)c_{i\mu+I_j}\cdot b_{i\nu} + (\nu_j+1)c_{i\mu} b_{i\nu+I_j} +$$

$$+ d_\mu(\nu_j+p_{ij}) b_{i\nu+I_j-I_i})\zeta^{\mu+\nu}.$$

Вынося знаки суммирования и переменные по столбцам из определителя, имеем

$$\Delta_h = \sum_{\substack{\mu^{(i)}\geqslant 0\\ \nu^{(i)}\geqslant 0\\ i=1,\ldots,n}} \zeta^{\sum_1^n(\mu^{(i)}+\nu^{(i)})} \Delta,$$

с общим членом определителя Δ из (5). Отсюда следует, что

$$f(z(\eta))=\sum_{\nu\geqslant 0}\Bigg(\sum_{\substack{\mu^{(i)},\,\nu^{(i)}\geqslant 0\\ i=1,\,\dots,\,n}}\frac{(-1)^{(\beta-\nu)}}{\kappa}\binom{\beta}{\nu}\frac{1}{(2\pi i)^n}\int\limits_{\Gamma} f\cdot\varphi^{\beta-\nu}\cdot\psi^{-\frac{\nu+\varkappa}{\varkappa}}\times$$

$$\times\zeta^{\Sigma(\mu^{(i)}+\nu^{(i)})-\beta-I}\cdot\Delta\,d\zeta\Bigg)\eta^{\nu}=\sum_{\nu\geqslant 0}g_{\nu}\eta^{\nu}. \tag{6}$$

Из интегрального представления в (6) видно, что те члены рядов $\varphi_j^{\beta_j-\nu_j}$ и $\psi^{\frac{\varkappa_j+\nu_j}{\varkappa_j}}$, у которых хотя бы одна степень переменного ζ_i больше соответствующей степени β_i, после почленного интегрирования, будут равны нулю. Применяя полиномиальную формулу для возведения в соответствующую степень отрезков рядов φ_j и ψ_j, имеем

$$g_{\nu}=\sum_{\substack{\beta\geqslant 0\\ \mu^{(i)},\,\nu^{(i)}\geqslant 0}}\frac{(-1)^{|\beta-\nu|}}{\kappa}\binom{\beta}{\nu}\Delta\,\frac{1}{(2\pi i)^n}\int\limits_{\Gamma}\Big(\sum_{\xi\geqslant 0}a_{\xi}\zeta^{\xi}\Big)\times$$

$$\times\prod_{j=1}^{n}\Bigg(\sum_{\sum_{\chi^{(j)}}\nu_{\chi^{(j)}}=\beta_j-\nu_j}(\beta_j-\nu_j)!\prod_{\chi^{(j)}}\frac{c_{j\chi^{(j)}}^{\nu_{\chi^{(j)}}}}{\nu_{\chi^{(j)}}!}\zeta^{\sum_{\chi^{(j)}}\chi^{(j)}\nu_{\chi^{(j)}}}\Bigg)\times$$

$$\times\prod_{j=1}^{n}\Bigg(\sum_{\substack{\sum_{\lambda^{(j)}}\alpha_{\lambda^{(j)}}=\alpha_j\\ \alpha_j\geqslant 0}}\frac{(-1)^{\alpha_j}\binom{\nu_j+\varkappa_j}{\varkappa_j}_{\alpha_j}}{b_0^{\frac{\nu_j+\varkappa_j}{\varkappa_j}+\alpha_j}}\prod_{\lambda^{(j)}}\frac{b_{j\lambda^{(j)}}^{\alpha_{\lambda^{(j)}}}}{\alpha_{\lambda^{(j)}}!}\xi^{\sum_{\lambda^{(j)}}\lambda^{(j)}\alpha_{\lambda^{(j)}}}\Bigg)\times$$

$$\times\zeta^{\Sigma(\mu^{(i)}+\nu^{(i)})-\beta-I}\,d\zeta.$$

Перемножая ряды, стоящие под знаком интеграла, изменяя порядок суммирования и интегрирования, интегрируя почленно и используя стандартные обозначения для мультииндексов, получаем

$$g_{\nu}=\Sigma'\frac{(-1)^{|\beta-\nu+\alpha|}}{\kappa}\,\frac{\beta!}{\nu!}\,\frac{\binom{\nu+\kappa}{\kappa}_{\alpha}}{b_0^{\frac{\nu+\varkappa}{\varkappa}+\alpha}}\,a_{\xi}\prod_{\chi,\lambda}\frac{c_{\lambda}^{\nu_{\chi}}\cdot b_{\lambda}^{\alpha_{\lambda}}}{\nu_{\lambda}!\,\alpha_{\lambda}!}\,\Delta.$$

Суммирование ведется по наборам, удовлетворяющим следующим условиям

$$\beta\geqslant 0,\ \xi\geqslant 0,\ \sum_{j=1}^{n}\Big(\sum_{\chi^{(j)}}\chi^{(j)}\nu_{\chi^{(j)}}+\sum_{\lambda^{(j)}}\lambda^{(j)}\alpha_{\lambda^{(j)}}+\mu^{(j)}+\nu^{(j)}\Big)+\xi=\beta,$$

$$\sum_{\chi^{(j)}}\nu_{\chi^{(j)}}=\nu_j,\qquad\sum_{\lambda^{(j)}}\alpha_{\lambda^{(j)}}=\alpha_j.$$

Учитывая, что $\eta=w^{\frac{1}{\varkappa}}$, получаем утверждение теоремы.

Следствие 1. Если в системе (1) $\varphi_j(\zeta)\equiv 0$, $j=1,\ldots,n$, то $\beta=\gamma$ и

$$g_\gamma=\sum_{\sum_\lambda|\lambda\alpha_\lambda|+|\nu|+\xi=\gamma}\frac{(-1)^{|\alpha|}}{\kappa}\cdot\frac{\left(\frac{\gamma+\kappa}{\kappa}\right)_\alpha}{b_0^{\frac{\gamma+\kappa}{\kappa}+\alpha}}a_\xi\prod_\lambda\frac{b_\lambda^{\alpha_\lambda}}{\alpha_\lambda!}\Delta, \tag{7}$$

где общий член определителя $A_{ij}=(\nu_j+p_{ij})b_{i\nu^{(i)}+I_j-I_i}$.

Формула (7) получается непосредственно из (4).

Следствие 2. Если в системе (1) $\psi_j(\zeta)\equiv 1$, $j=1,\ldots,n$, то

$$g_\gamma=\sum_{\substack{\beta\geqslant 0\\ \sum_\chi|\chi\nu_\chi|+|\mu|+\xi=\beta}}\frac{(-1)^{|\beta-\nu|}}{\kappa}\frac{\beta!}{\gamma!}a_\xi\prod_\chi\frac{c_\chi^{\nu_\chi}}{\gamma_\chi!}\Delta,$$

$$A_{ij}=\kappa_i(\mu_j^{(i)}+1)c_{i\mu^{(i)}+I_j}.$$

Замечание. В частности, при $n=1$ формула (7) принимает вид

$$g_\gamma=\sum_{\sum_{\lambda=1}^{\gamma}\lambda\alpha_\lambda+\nu+\xi=\gamma}\frac{(-1)^{\sum_1^\nu\alpha_\lambda}\left(\frac{\gamma+\kappa}{\kappa}\right)_{\sum_1^\nu\alpha_\lambda}}{\kappa\cdot b_0^{\frac{\gamma+\kappa}{\kappa}+\sum\alpha_\lambda}}a_\xi\prod_{\lambda=1}^{\nu}\frac{b_\lambda^{\alpha_\lambda}}{\alpha_\lambda}(\nu+\kappa)b_\nu, \tag{8}$$

и вычисление коэффициентов g_γ в этом случае нам представляется достаточно простым. Тем более, что суммирование в (8) ведется по наборам, удовлетворяющим фиксированному уравнению, решения которого могут быть заранее сведены в таблицу хотя бы для начальных значений γ.

Выражаю признательность Г. П. Егорычеву и А. П. Южакову за полученные замечания и внимание к работе.

ЛИТЕРАТУРА

1. Куприков А. В. Ряд Лагранжа для одного многозначного обратного отображения. Сб. «Комбинаторн. и асимптот. анализ», 1975, Красноярск, Изд-во ГУ, вып. 1, с 163.

2. Cayley A. Note sur une formule pour la reversion des series J. reine and angew. Math, 52 (1856), p. 276.

3. Sack R. A. Interpretation of lagrange's expansion and its generalization to several variables as integration formulas J. Soc. Indust. Appl. Math., **13**, 1 (1965), p. 47

4. Болотов В. А., Южаков А. П. Обобщение формул обращения степенных рядов на системы неявных функций. «Математ. заметки», **23**, 1, 47 (1978).

5. Южаков А. П. Элементы теории многомерных вычетов. Красноярск, Изд-во ГУ, 1975, с. 182.

6. Селиванов Б. И. Комбинаторный подход к формуле обращения Бурмана—Лагранжа. Сб. «Комбинаторн. и асимптот. анализ», 1977, Красноярск, Изд-во ГУ, вып. 2, с. 153.

Красноярский государственный университет

[15/XI 1977]

ПРОБЛЕМА СЛЕДСТВИЯ В НЕКОТОРЫХ ПОДАЛГЕБРАХ АЛГЕБР ДЕЙСТВИТЕЛЬНЫХ ФУНКЦИЙ

М. Ю. Мошков

Проблема следствия и тесно связанная с ней проблема совместности возникают при изучении процессов получения и переработки информации, в частности, при выявлении избыточности информации и при распознавании противоречивости ее. Проблема совместности в форме вопроса о совместности системы уравнений и проблема следствия в форме вопроса о том, является ли неравенство следствием системы неравенств, возникли давно и неоднократно занимали значительное место в развитии алгебры и ее приложений. Отметим лишь несколько известных результатов: «основная теорема алгебры», теорема Кронекера—Капелли о совместности систем линейных уравнений, отрицательное решение десятой проблемы Гильберта, теорема Минковского—Фаркаша о линейных неравенствах-следствиях совместной системы линейных неравенств.

В настоящей работе для ряда алгебраических систем изучается разрешимость формализованной проблемы следствия. Имеются некоторые особенности подхода, связанные с тем, что проблема следствия изучается применительно к исследованию алгоритмов обработки информации: изучаются в основном элементарные функции и предикаты, наиболее часто используемые в качестве базисных операций алгоритмов; исследуются подмножества множества действительных чисел, состоящие из чисел, имеющих конечное описание, например, множество рациональных, множество натуральных чисел.

Статья состоит из трех разделов.

В первом приведены основные понятия и доказано несколько лемм о разрешимости проблемы следствия.

Второй разбит на две части.

Первая посвящена алгебраическим системам с разрешимой проблемой следствия.

Вторая посвящена алгебраическим системам с неразрешимой проблемой следствия.

В разделе 3 рассматривается вопрос о перечислимости неравенств-следствий с помощью так называемых естественных правил вывода. Этот вопрос полностью решен для алгебр линейных функций.

1. ОСНОВНЫЕ ПОНЯТИЯ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Сигнатурой называется последовательность

$$\sigma = <f_1^{(m_1)}, \ldots, f_s^{(m_s)}; P_1^{(n_1)}, \ldots, P_l^{(n_l)}>,$$

где $f_i^{(m_i)}$ — символ m_i-местной функции, $P_i^{(n_i)}$ — символ n_i-местного предиката. Алгебраической системой (а. системой) сигнатуры σ называется последовательность вида $W = <M; f_1^{(m_1)}, \ldots, f_s^{(m_s)}; P_1^{(n_1)}, \ldots, P_l^{(n_l)}>$, где M непустое множество, называемое основным множеством системы W, $f_i^{(m_i)}$ — m_i-местная функция, определенная на множестве M, $P_i^{(n_i)}$ — n_i-местный предикат, определенный на множестве M. Алгебраическая система W называется алгеброй, если $l=0$, т. е. отсутствуют предикаты. Всюду в этой статье формулой сигнатуры σ будем называть формулу узкого исчисления предикатов с равенством, все

внелогические константы которой содержатся в σ. Предикат $P(x_1, ..., x_n)$, определенный на M, назовем формульным на алгебре W сигнатуры σ, если существует формула $Q(x_1, ..., x_n)$ сигнатуры σ со свободными переменными $x_1, ..., x_n$ такая, что для W выражение $Q(x_1, ..., x_n)$ истинно для тех и только тех значений $x_1, ..., x_n$ из M, для которых $P(x_1, ..., x_n) = И^*$.

Простейшими формулами сигнатуры σ или простейшими формулами а. системы W сигнатуры σ будем называть формулы вида $P(\alpha_1, ..., \alpha_m)$, где $\alpha_1, ..., \alpha_m$-термы сигнатуры σ, P — предикатный символ сигнатуры σ.

Дадим формальные определения массовых проблем, рассматриваемых в настоящей работе. Пусть W — а. система сигнатуры σ.

Проблема следствия для а. системы W: по произвольному выражению вида

$$(\forall x_1 \cdots x_n)(A_1 \& \cdots \& A_\kappa \longrightarrow A_{\kappa+1}), \tag{1}$$

где $A_1, ..., A_\kappa, A_{\kappa+1}$ — простейшие формулы а. системы W от $x_1, ..., x_n$ или их отрицания, определить, истинно ли оно для W.

Проблема совместности для а. системы W: по произвольному выражению вида

$$(\forall x_1 \cdots x_n)(A_1 \& \cdots \& A_\kappa \longrightarrow \neg A_1) \tag{2}$$

определить, истинно ли оно для W.

Докажем лемму, позволяющую при изучении разрешимости рассматриваемых проблем ограничиться исследованием проблемы следствия.

Лемма 1. Для любой а. системы W проблема следствия разрешима тогда и только тогда, когда для нее разрешима проблема совместности.

Доказательство. Необходимость. Множество выражений вида (2) а. системы W является подмножеством выражений вида (1) а. системы W. Поэтому если для а. системы W проблема следствия разрешима, то для нее разрешима и проблема совместности. Достаточность. Выражение (1) истинно тогда и только тогда, когда истинно выражение вида (2):

$$(\forall x_1 \cdots x_n)(A_1 \& \cdots \& A_\kappa \& \neg A_{\kappa+1} \longrightarrow \neg A_1).$$

Поэтому если для а. системы W разрешима проблема совместности, то для нее разрешима и проблема следствия. Лемма доказана.

Нам потребуется уточнение понятия разрешимости проблемы следствия. Обозначим $K(W)$ множество выражений вида (1) а. системы W. Истинные для W выражения вида (1) называются квазитождествами а. системы W. Обозначим $K^+(W)$ множество квазитождеств а. системы W. Рассмотрим некоторую геделевскую нумерацию Nom формул сигнатуры σ, например нумерацию, используемую в [1]. При такой нумерации каждой формуле h сигнатуры σ приписан номер $Nom(h)$, вычислимый по данной формуле. По заданному натуральному числу можно определить, является ли оно номером некоторой формулы сигнатуры σ, и если является, то однозначно восстановить эту формулу.

Будем говорить, что проблема следствия соответственно разрешима или рекурсивно-перечислима для а. системы W, если множество $Nom(K^+(W))$ номеров формул из $K^+(W)$ рекурсивно или рекурсивно-перечислимо. Заметим, что множество $Nom(K(W))$ рекурсивно.

Введем некоторые обозначения: R — множество действительных чисел, Q — множество рациональных чисел, N — множество натуральных чисел.

---

* В дальнейшем будем рассматривать только либо формульные на алгебре предикаты, либо элементарные предикаты из множества $\{x=y, x \geqslant y, x>y\}$. Таким образом, основным объектом нашего исследования являются алгебры. Этими соображениями и объясняется название статьи.

Докажем еще несколько лемм. Элементарной теорией алгебры W сигнатуры σ называется множество истинных для W формул сигнатуры σ. Обозначим это множество $H^+(W)$. Будем говорить, что элементарная теория алгебры W разрешима, если множество $Nom(H^+(W))$ номеров формул из $H^+(W)$ рекурсивно.

Лемма 2. Если элементарная теория алгебры $W=<M; f_1^{(m_1)}, ..., f_s^{(m_s)}>$ разрешима и $\{P_1^{(n_1)}, ..., P_l^{(n_l)}\}$ — некоторое конечное множество формульных на W предикатов, то для а. системы $<M; f_1^{(m_1)}, ..., f_s^{(m_s)}; P_1^{(n_1)}, ..., P_l^{(n_l)}>$ разрешима проблема следствия.

Доказательство. Справедливость утверждения леммы непосредственно вытекает из определения предикатов, формульных на W, и разрешимости элементарной теории алгебры W. Лемма доказана.

Вычислимыми а. системами или v-системами будем называть алгебраические системы вида $<N; f_1^{(m_1)}, ..., f_s^{(m_s)}; P_1^{(n_1)}, ..., P_l^{(n_l)}>$, где $f_i^{(m_i)}$ — m_i—местная общерекурсивная функция, $P_i^{(n_i)}$ — n_i—местный рекурсивный предикат.

Лемма 3. Если W — v-система, $L\subseteq K(W)$ и множество $Nom(L)$ рекурсивно, то множество $Nom(L\cap K^+(W)))$ рекурсивно тогда и только тогда, когда оно рекурсивно — перечислимо.

Доказательство. Необходимость. Обозначим $L^+=L\cap K^+(W)$. Если множество $Nom(L^+)$ рекурсивно, то оно, очевидно, рекурсивно-перечислимо. Достаточность. Пусть множество $Nom(L^+)$ рекурсивно-перечислимо. Докажем рекурсивную перечислимость множества $N\setminus Nom(L^+)$. Опишем частичную функцию $\beta(n)$, множество значений которой совпадает с $N\setminus Nom(L^+)$. Пусть (n_1, n_2) — пара натуральных чисел, канторовским номером которой является n. $\beta(n)=n_1$ тогда и только тогда, когда $n_1=Nom(h)$ для некоторого $h\in L$ и $\psi(t_1, ..., t_m)=Л$, где $\psi(x_1, ..., x_m)$ — обозначение послекванторной части выражения h, а $(t_1, ..., t_m)$ — m-ка натуральных чисел, канторовским номером которой является n_2. В остальных случаях значение $\beta(n)$ не определено.

Считая тезис Черча справедливым, учитывая рекурсивность множества $Nom(L)$, свойства нумерации Nom и канторовской нумерации n-ок натуральных чисел, нетрудно доказать, что функция $\beta(n)$—частично-рекурсивная функция. Таким образом, множество $Nom(L^+)$ и его дополнение оба рекурсивно-перечислимы. Поэтому множество $Nom(L^+)$ рекурсивно. Лемма доказана.

Следствие. Для v-системы W проблема следствия разрешима тогда и только тогда, когда она рекурсивно-перечислима.

Замечание. Результат леммы 3 нетрудно перенести на а. систему W, для которой существует нумерация α основного множества а. системы W, такая, что для любой функции $f(x_1, ..., x_n)$ а. системы W найдется общерекурсивная функция $\bar{f}(x_1, ..., x_n)$, для любого предиката $P(x_1, ..., x_n)$ а. системы W найдется рекурсивный предикат $\bar{P}(x_1, ..., x_n)$ так, что для любого набора натуральных чисел $(m_1, ..., m_n)$ $f(\alpha m_1, ..., \alpha m_n)=\alpha f(m_1, ..., m_n)$ и $P(\alpha m_1, ..., \alpha m_n)=\bar{P}(m_1, ..., m_n)$. Подобные а. системы будем называть вычислимыми нумерованными а. системами.

2. ИССЛЕДОВАНИЕ КОНКРЕТНЫХ АЛГЕБРАИЧЕСКИХ СИСТЕМ

В этом разделе изучается разрешимость проблемы следствия для ряда алгебраических систем.

Алгебраические системы с разрешимой проблемой следствия. Все исследуемые а. системы разобьем на три группы, в зависимости от того, является ли основным множеством а. системы множество R, Q или N.

Теорема 1. Для а. системы

$$<R;\ x+y,\ x\cdot y,\ 0,\ 1;\ U>, \tag{3}$$

где U — некоторое конечное множество формульных на алгебре $<R;\ x+y,\ x\cdot y,\ 0,\ 1>$ предикатов, проблема следствия разрешима.

Доказательство. Элементарная теория алгебры $<R;\ x+y,\ x\cdot y,\ 0,\ 1>$ разрешима [2]. Используя лемму 2, получаем, что проблема следствия для системы (3) разрешима. Теорема доказана.

Пусть $<Q;\ F_s;\ x\geqslant 0,\ x>0>$ — вычислимая нумерованная а. система, обладающая следующим свойством: для любой функции $\varphi\in F_s$ $\operatorname{sign}(\varphi(x_1,\ldots,x_n))=\operatorname{sign}(\varphi(\operatorname{sign}(x_1),\ldots,\operatorname{sign}(x_n))$ и для любого $r\in Q$ можно вычислить номер r.

Теорема 2. Для а. систем

$$<Q;\ x+y,\ 0,\ 1;\ x>y,\ x\geqslant y> \tag{4}$$

и

$$<Q;\ F_s;\ x\geqslant 0,\ x>0> \tag{5}$$

проблема следствия разрешима.

Доказательство. Докажем первую часть утверждения теоремы. Пусть $L_{1,1}$, $L_{1,2}$, ..., $L_{\kappa,1}$, $L_{\kappa,2}$, L_1, L_2 — термы сигнатуры $<x+y,\ 0,\ 1>$ от $x_1,\ldots,x_n$. Эти же обозначения сохраним и для функций, соответствующих перечисленным термам. Проблема установления истинности выражений вида

$$(\forall x_1\cdots x_n)\,((L_{1,1}\geqslant L_{1,2})\,\&\cdots\&\,(L_{\kappa,1}\geqslant L_{\kappa,2})\longrightarrow\neg(L_{1,1}\geqslant L_{1,2})), \tag{6}$$

разрешима ([3] теорема 1.5). Пусть (6) ложно, т. е. рассматриваемая система неравенств совместна. Тогда, как следует из теоремы Минковского—Фаркаша ([3], лемма 2.4), выражение

$$(\forall x_1\cdots x_n)\,((L_{1,1}\geqslant L_{1,2})\,\&\cdots\&\,(L_{\kappa,1}\geqslant L_{\kappa,2})\longrightarrow(L_1\geqslant L_2)), \tag{7}$$

истинно тогда и только тогда, когда существуют неотрицательные рациональные числа $p_1,\ldots,p_\kappa$, для которых имеет место тождественное относительно $(x_1,\ldots,x_n)\in Q^n$ соотношение

$$\sum_{i=1}^{\kappa} p_i(L_{i,1}-L_{i,2})=L_1-L_2. \tag{8}$$

Нетрудно показать, что проблема установления тождественной истинности выражений вида (8) разрешима. Поэтому формула (8) дает способ перечисления всех квазитождеств вида (7) а. системы (4), для которых соответствующее выражение вида (6) ложно. Множество номеров выражений вида (7), для которых соответствующее выражение вида (6) ложно, при нумерации *Nom* формул а. системы (4), очевидно, является рекурсивным; а. система (4) — вычислимая нумерованная система. Учитывая замечание к лемме 3, получаем, что проблема установления истинности выражений вида (7), для которых соответствующее выражение вида (6) ложно, разрешима. Если (6) истинно, то и (7) истинно. Объединяя эти факты, получаем, что проблема установления истинности выражений вида (7) разрешима. Покажем теперь, что для а. системы (4) разрешима проблема совместности. Рассмотрим произвольное выражение вида

$$(\forall x_1\cdots x_n)\,((L_{1,1}>L_{1,2})\,\&\cdots\&\,(L_{m,1}>L_{m,2})\,\&\,(L_{m+1,1}\geqslant L_{m+1,2})\,\&\cdots$$
$$\cdots\&\,(L_{\kappa,1}\geqslant L_{\kappa,2})\longrightarrow\neg(L_{1,1}>L_{1,2}), \tag{9}$$

где $m\leqslant\kappa$.

Рассмотрим квазитождество (6), полученное из (9) заменой всюду знака $>$ на $\geqslant$. Если (6) истинно, то и (9) истинно. Пусть (6) ложно. Устанавливаем, истинны или ложны квазитождества вида (7):

$$(\forall x_1 \cdots x_n)\,((L_{1,1} \geqslant L_{1,2}) \& \cdots \& (L_{\kappa,1} \geqslant L_{\kappa,2}) \longrightarrow (L_{j,2} \geqslant L_{j,1})) \qquad (10)$$

для $j=1, \ldots, n$. Пусть все эти квазитождества ложны. Это означает, что для каждого $j \in \{1, \ldots, n\}$ существует набор из n рациональных чисел $\tilde{r}_j = (r_{j,1}, \ldots, r_{j,n})$ такой, что $h_6(\tilde{r}_j) = Л$ и $L_{j,1}(\tilde{r}_j) > L_{j,2}(\tilde{r}_j)$, где $h_6(x_1, \ldots, x_n)$ — обозначение послекванторной части выражения (6). Рассмотрим набор $\tilde{r} = \frac{1}{m} \sum_{j=1}^{m} \tilde{r}_j$. Очевидно, на этом наборе $h_9(\tilde{r}) = Л$, где $h_9(x_1, \ldots, x_n)$ — обозначение послекванторной части выражения (9), т. е. (9) ложно. Пусть для некоторого $j_0 \in \{1, \ldots, n\}$ выражение (10) истинно. В этом случае истинно и выражение (9), так как для всех решений равенства $(L_{1,1} \geqslant L_{1,2}) \& \cdots \& (L_{\kappa,1} \geqslant L_{\kappa,2}) = И$ справедливо равенство $L_{j_0,1} = L_{j_0,2}$. Тем самым разрешимость проблемы совместности и, следовательно (используем результат леммы 1), разрешимость проблемы следствия для а. системы (4) доказана.

Докажем, что для а. системы (5) разрешима проблема следствия. Рассмотрим произвольное выражение вида

$$(\forall x_1 \ldots x_n)\,(A_1 \& \cdots \& A_\kappa \longrightarrow A_0), \qquad (11)$$

где $A_0, A_1, \ldots, A_\kappa$ — простейшие формулы а. системы (5) или их отрицания. Пусть $A(x_1, \ldots, x_n)$ — некоторая простейшая формула а. системы (5). Нетрудно показать, что $A(x_1, \ldots, x_n) = И$ тогда и только тогда, когда $A(\mathrm{sign}(x_1), \ldots, \mathrm{sign}(x_n)) = И$. Используя этот факт, нетрудно показать, что (11) истинно тогда и только тогда, когда высказывание $A_1 \& \cdots \& A_\kappa \longrightarrow A_0$ тождественно истинно на множестве $\{-1, 0, +1\}^n$, что можно проверить, так как (5) — вычислимая нумерованная система, и по числам -1, 0, $+1$ можно определить их номера в нумерации а. системы (5). Теорема доказана.

Теорема 3. Для а. систем

$$<N;\ x+y,\ 0,\ 1;\ U>, \qquad (12)$$

где U — некоторое конечное множество формульных на алгебре $<N; x+y, 0, 1>$ предикатов, и

$$<N;\ x+y,\ x \cdot y,\ 1 \dot{-} x,\ x \dot{-} 1,\ x^y,\ \max(x, y),\ \min(x, y);\ x=0> \qquad (13)$$

проблема следствия разрешима.

Доказательство. Элементарная теория алгебры $<N; x+y, 0, 1>$ разрешима [4]. Используя результат леммы 2, получаем, что проблема следствия для а. системы (12) разрешима. Первая часть теоремы доказана, докажем вторую часть.

Известно [5], что для а. системы (13) разрешима проблема установления истинности выражений вида

$$(\forall x_1 \cdots x_n)\,(f(x_1, \ldots, x_n) = 0),$$

где $f(x_1, \ldots, x_n)$ — терм сигнатуры $\sigma = <x+y,\ x \cdot y,\ 1 \dot{-} x,\ x \dot{-} 1,\ \max(x, y),\ \min(x, y),\ x^y>$ от $x_1, \ldots, x_n$. Покажем, что решение проблемы следствия для а. системы (13) сводится к установлению истинности подобных выражений. Любая формула сигнатуры σ вида $\neg\,(f=0)$, где f — терм сигнатуры σ, эквивалентна простейшей формуле сигнатуры σ $1 \dot{-} f = 0$. Поэтому произвольное выражение вида (1) сигнатуры σ можно представить в виде $(\forall x_1 \cdots x_n)\,((\varphi_1 = 0) \& \cdots \& (\varphi_\kappa = 0) \longrightarrow (\varphi_0 = 0))$, где

$\varphi_0, \ldots, \varphi_\kappa$ — термы сигнатуры σ от $x_1, \ldots, x_n$. Нетрудно проверить, что это выражение истинно тогда и только тогда, когда истинно выражение $(\forall x_1 \cdots x_n)(\varphi_0 \cdot \prod_{i=1}^{\kappa} (1 \dot{-} \varphi_i) = 0)$. Теорема доказана.

Мы исследуем лишь вопрос о существовании алгоритмов решения проблемы следствия, не интересуясь их сложностью. Приведем все же один пример, характеризующий эту сложность. Проблема: «по данным натуральным α, β, γ выяснить, имеет ли натуральное решение уравнение $\alpha x_1^2 + \beta x_2 - \gamma = 0$» есть NP-полная проблема [6].

Алгебраические системы с неразрешимой проблемой следствия. Используя тот факт, что существует общерекурсивная функция $f_0(x)$, множество значений которой нерекурсивно [7], нетрудно привести пример а. системы с неразрешимой проблемой следствия. Покажем, что для системы

$$<N; f_0(x), x+1, 1; x=y> \tag{14}$$

проблема следствия неразрешима. Обозначим n терм $1+(1+(\cdots+(1)\cdots)$, в котором символ «1» встречается n раз. Допустим, что проблема следствия для системы (14) разрешима. Тогда для любого $n \in N$ можно установить, истинно ли выражение $(\forall x)((f_0(x)=n) \longrightarrow \neg (f_0(x)=n))$, что противоречит нерекурсивности множества значений $f_0(x)$. Утверждение доказано.

Теорема 4. Для а. системы

$$<N; x+y, x \cdot y, 0, 1; x=y> \tag{15}$$

проблема следствия неразрешима.

Доказательство. Из предположения о разрешимости проблемы следствия для а. системы (15) следует существование алгоритма, устанавливающего по произвольному диофантову уравнению, имеет ли оно решение в целых числах, что неверно [8]. Полученное противоречие доказывает теорему.

Замечание. Некоторый интерес представляет следующее утверждение для алгебры

$$<N; x+y, x \cdot y, x \dot{-} y, 1> \tag{16}$$

проблема установления истинности выражений вида

$$(\forall x_1 \cdots x_n)(f(x_1, \ldots, x_n) = 0), \tag{17}$$

где $f(x_1, \ldots, x_n)$ — термы сигнатуры $\sigma = <x+y, x \cdot y, x \dot{-} y, 1>$ от $x_1, \ldots, x_n$, неразрешима. Действительно, используя тот факт, что выражение $x=y$ эквивалентно конъюнкции $(x \dot{-} y = 0) \& (y \dot{-} x = 0)$, выражение $(x=y)$ эквивалентно выражению $(x \dot{-} y) + (y \dot{-} x) = 0$, и выражение $x \neq 0$ эквивалентно выражению $1 \dot{-} x = 0$, можно любое выражение вида (1) а. системы

$$<N; x+y, x \cdot y, x \dot{-} y, 1; x=y> \tag{18}$$

привести к виду

$$(\forall x_1 \cdots x_n)((f_1=0) \& \cdots \& (f_\kappa=0) \longrightarrow (f_{\kappa+1}=0)), \tag{19}$$

где $f_1, \ldots, f_\kappa, f_{\kappa+1}$ — термы сигнатуры σ от $x_1, \ldots, x_n$. Допустим, что проблема установления истинности выражений вида (17) разрешима. Тогда, почти пословно повторяя доказательство второй части теоремы 3, получаем, что проблема установления истинности выражений вида (19) разрешима, и, следовательно, разрешима проблема следствия для а. системы (18) и тем более для а. системы (15). Полученное противоречие доказывает утверждение.

3. ЕСТЕСТВЕННЫЕ ПРАВИЛА ВЫВОДА НЕРАВЕНСТВ-СЛЕДСТВИЙ

В этом разделе изучается вопрос о перечислимости линейных неравенств — следствий системы линейных неравенств с помощью естественных правил вывода. Наш подход здесь будет скорее алгебраическим, чем алгоритмическим: будем рассматривать произвольные а. системы вида

$$W=\langle R; F_W; x\geqslant 0,\ x\leqslant 0\}, \tag{20}$$

где $F_W\subseteq S=\{\sum\limits_{j=1}^{n} a_j x_{i_j} \mid n\in N,\ a_j\in R,\ j=\overline{1,n}\}$, в том числе и W с несчетными F_W. Чтобы не вводить новых терминов, подобные объекты также называем а. системами. Пусть W — некоторая а. система вида (20). Обозначим $F(W)$ замыкание относительно суперпозиции множества функций F_W на множестве переменных $\{x_1, x_2, ..., x_n, ...\}$ и $G(W)=\{f\geqslant 0,\ f\leqslant 0 \mid f\in F(W)\}$. Пусть $\sigma\in\{-1, +1\}$. Запись $\sigma x\geqslant 0$ означает $x\geqslant 0$, если $\sigma=1$, и $x\leqslant 0$, если $\sigma=-1$. Обозначим P_W множество всевозможных выражений вида

$$\&_{i=1}^{\kappa}(\sigma_i x_i\geqslant 0)\longrightarrow \sigma_0\sum_{i=1}^{\kappa} a_i x_i\geqslant 0, \tag{21}$$

где $\sum\limits_{i=1}^{\kappa} a_i x_i\in F(W)$, $\sigma_i\in\{-1, +1\}$ для $i=\overline{0,\kappa}$ и $\sigma_i=\sigma_0\operatorname{sign}(a_i)$ для $i=\overline{1,\kappa}$.

Назовем P_W множеством естественных правил вывода а. системы W. Конъюнкцию $\&_{i=1}^{\kappa}(\sigma_i x_i\geqslant 0)$ назовем левой частью, а неравенство $\sigma_0\sum\limits_{i=1}^{\kappa} a_i x_i\geqslant 0$ — правой частью выражения (21). Определим действие P_W на некоторое $B\subseteq G(W)$ и опишем полученное множество выражений $P_W(B)$. Подставив в выражение (21), вместо переменных $x_1, ..., x_\kappa$, произвольные функции $f_1, ..., f_\kappa$ из $F(W)$, получим

$$\&_{i=1}^{\kappa}(\sigma_i f_i\geqslant 0)\longrightarrow \sigma_0\sum_{i=1}^{\kappa} a_i f_i\geqslant 0. \tag{22}$$

Обозначим Ω множество всех выражений вида (22), которые указанным способом можно получить из выражений множества P_W. Ищем в Ω такие выражения, у которых все неравенства левой части $\sigma_i f_i\geqslant 0$ содержатся во множестве B. Правые части всех этих выражений и составляют множество $P_W(B)$. Нетрудно показать, что для любого множества $B\subseteq G(W)$

$$P_W(P_W(B))=P_W(B). \tag{23}$$

Множество P_W назовем $\exists$-полным, если для любого истинного для W выражения вида $(\forall x_1 ... x_n)(\&_{i=1}^{\kappa}(\sigma_i f_i\geqslant 0)\longrightarrow(\sigma_{\kappa+1} f_{\kappa+1}\geqslant 0)$ (где $f_i\in F(W)$, f_i зависит от $x_1, ..., x_n$, $\sigma_i\in\{-1, +1\}$, $i=\overline{1,\kappa+1}$, найдется неравенство $(\varphi\geqslant 0)\in P_W(\sigma_1 f_1\geqslant 0, ..., \sigma_\kappa f_\kappa\geqslant 0)$ такое, что равенство $\sigma_{\kappa+1} f_{\kappa+1}=\sigma\varphi$ тождественно истинно на R.

Получим критерий $\exists$— полноты P_W для а.системы W вида (20). Определим T-частичную функцию, заданную на конечных упорядоченных подмножествах множества S, со значениями во множестве S. Пусть $\kappa\in N$, $\{f_1, ..., f_{\kappa+1}\}\subset F$. $T(f_1, ..., f_{\kappa+1})=\sum\limits_{i=1}^{\kappa} a_i x_i$, если $f_1, ..., f_\kappa$ — линейно независимая система функций и $f_{\kappa+1}=\sum\limits_{i=1}^{\kappa} a_i f_i$, и $T(f_1, ..., f_{\kappa+1})$ не определена в противном случае.

Лемма 4. Множество $P_W\exists$ -полно для а. системы W вида (20) тогда и только тогда, когда множество $F(W)$ замкнуто относительно применения операции T.

Доказательство. Необходимость. Рассмотрим а. систему W вида (20), для которой $P_W\exists$-полно. Докажем, что множество $F(W)$ замкнуто относительно применения операции T. Пусть $\{f_1, ..., f_{\kappa+1}\}\subset F(W)$, система $f_1, ..., f_\kappa$ линейно независима, $f_{\kappa+1}=\sum\limits_{i=1}^{\kappa} a_i f_i$ и f_i зависит от $x_1, ..., x_n$, $i=\overline{1, \kappa+1}$. Покажем, что $\sum\limits_{i=1}^{\kappa} a_i x_i\in F(W)$. Очевидно, выражение

$$(\forall x_1, ..., x_n)\left(\mathop{\&}_{i=1}^{\kappa} (\operatorname{sign}(a_i) f_i(x_1, ..., x_n)\geqslant 0)\longrightarrow f_{\kappa+1}(x_1, ..., x_n)\geqslant 0\right)$$

истинно для а. системы W. Множество P_W должно содержать правило $\mathop{\&}\limits_{i=1}^{\kappa} (\operatorname{sign}(a_i) x_i\geqslant 0)\longrightarrow(\sum\limits_{i=1}^{\kappa} b_i x_i\geqslant 0)$ такое, что для W истинно выражение

$$(\forall x_1, ..., x_n)\left(\sum_{i=1}^{\kappa} b_i f_i(x_1, ..., x_n)=f_{\kappa+1}(x_1, ..., x_n)\right).$$

Из линейной независимости множества $\{f_1, ..., f_\kappa\}$ следует единственность разложения $f_{\kappa+1}$ по $f_1, ..., f_\kappa$. Поэтому $b_i=a_i$ для $i=\overline{1, \kappa}$ и $\sum\limits_{i=1}^{\kappa} a_i x_i\in F(W)$. Достаточность. Пусть множество $F(W)$ замкнуто относительно применения операции T. Покажем, что множество правил вывода $P_W\exists$ -полно для W. Рассмотрим произвольное истинное для W выражение вида

$$(\forall x_1, ..., x_n)\left(\mathop{\&}_{i=1}^{\kappa} (\sigma_i f_i\geqslant 0)\longrightarrow(\sigma_{\kappa+1} f_{\kappa+1}\geqslant 0)\right), \qquad (24)$$

где $f_i\in F(W)$, f_i зависит от $x_1, ..., x_n$, $i=\overline{1, \kappa+1}$. Известно ([3], лемма 2.3), что если (24) истинно, то найдется линейно независимое множество функций $\{f_{i_1}, ..., f_{i_l}\}\subseteq\{f_1, ..., f_\kappa\}$ такое, что истинно выражение

$$(\forall x_1 \cdots x_n)\left(\mathop{\&}_{j=1}^{l} (\sigma_{i_j} f_{i_j}(x_1, ..., x_n)\geqslant 0)\longrightarrow(\sigma_{\kappa+1} f_{\kappa+1}(x_1, ..., x_n)\geqslant 0)\right).$$

Из теоремы Минковского—Фаркаша ([3], лемма 2.4) следует, что $\sigma_{\kappa+1} f_{\kappa+1}=\sum\limits_{j=1}^{l} p_{i_j}\sigma_{i_j} f_{i_j}$, где p_{i_j} — неотрицательное действительное число, $j=\overline{1, l}$. Из замкнутости $F(W)$ относительно применения операции T следует, что $\sum\limits_{j=1}^{l} p_{i_j}\sigma_{i_j} x_j\in F(W)$. Поэтому P_W содержит правило

$$(\forall x_1 \cdots x_n)\left(\mathop{\&}_{j=1}^{l} (\sigma_{i_j} x_j\geqslant 0)\longrightarrow(\sum_{j=1}^{l} p_{i_j}\sigma_{i_j} x_j\geqslant 0)\right).$$

Очевидно, применение этого правила к множеству $\{\sigma_1 f_1\geqslant 0, ..., ..., \sigma_\kappa f_\kappa\geqslant 0\}$ дает $\sigma_{\kappa+1} f_{\kappa+1}\geqslant 0$, что и требовалось доказать. Лемма доказана.

Таким образом, нам нужно описать систему множеств линейных функций, замкнутых относительно применения операции T и относительно суперпозиции.

Введем некоторые обозначения. Пусть W — а. система вида (20). Пусть $f=\sum\limits_{i=1}^{n} a_i x_{j_i} \in F(W)$. Обозначим $\pi(f)=\sum\limits_{i:a_i\neq 0} 1$, $\pi(W)=$ $=\max\limits_{f\in F(W)} \pi(f)$. Очевидно, $\pi(W)\in\{0, 1, \infty\}$. Обозначим $v(f)=\sum\limits_{i=1}^{n} a_i$, $v(W)=\{v(f)\,|\,f\in F(W)\}$ и $A(f)=\{a_1, ..., a_n\}$, $A(W)=\bigcup\limits_{f\in F(W)} A(f)$. Очевидно, $v(W)\subseteq A(W)$. Переменные из множества $\{x_1, x_2, ..., x_n, ...\}$ обозначим через x, y, z, t.

Теорема 5. Множество естественных правил вывода P_W $\exists$-полно для а. системы W вида (20) тогда и только тогда, когда W удовлетворяет одному из следующих четырех условий:

1) $F(W)=\{0\cdot x_i\,|\,i\in N\}$;

2) $F(W)=\{ax_i\,|\,i\in N,\ a\in G\}$, где $G=G_1$ или $G=G_1\cup\{0\}$, а G_1 — произвольная мультипликативная группа действительных чисел;

3) $F(W)=\{\sum\limits_{i=1}^{n} a_i x_{j_i}\,|\,n\in N, j_i\in N, a_i\in R_1\}$, где R_1 — произвольное подполе поля R;

4) $F(W)=\left\{\dfrac{\sum\limits_{i=1}^{n} a_i x_{j_i}}{\sum\limits_{i=1}^{n} a_i}\ \middle|\ n\in N,\ j_i\in N,\ a_i\in R_1,\ \sum\limits_{i=1}^{n} a_i\neq 0\right\}$, где R_1 — произвольное подполе поля R.

Доказательство теоремы состоит из четырех частей: для W с $\pi(W)=0$, для W с $\pi(W)=1$, для W с $\pi(W)=\infty$ и $v(W)\neq\{1\}$, для W с $\pi(W)=\infty$ и $v(W)=\{1\}$. Очевидно, рассматриваемые случаи охватывают все множество а. систем вида (20).

Случай 1. Пусть $\pi(W)=0$. Тогда $F(W)=\{0\,x_i\,|\,i\in N\}$. Очевидно, $F(W)$ замкнуто относительно суперпозиции и применения операции T. Итак, для W с $\pi(W)=0$ теорема верна. В дальнейшем для каждого рассматриваемого случая будем фиксировать некоторую а. систему W вида (20) и вместо обозначений $F(W)$, $\pi(W)$, $v(W)$, $A(W)$ будем использовать обозначения F, π, v, A соответственно.

Случай 2. Необходимость. Пусть P_W $\exists$-полно для W с $\pi(W)=1$. Покажем, что W удовлетворяет условию 2) теоремы 5. Если $ax\in F$, то и $a^2x\in F$, так как F замкнуто относительно суперпозиции. Пусть $a\neq 0$. Тогда $T(a^2x, ax)=\dfrac{1}{a}x\in F$. Из условия $\pi(W)=1$ получаем, что в F найдется функция ax с $a\neq 0$, поэтому $a\cdot\dfrac{1}{a}x=x\in F$. Если $ax, by\in F$, то $abx\in F$. Для рассматриваемой а. системы W $A=v$. Доказано, что $1\in A$; если $a\in A$ и $a\neq 0$, то $\dfrac{1}{a}\in A$; если $a, b\in A$, то $a\cdot b\in A$. Таким образом, $v=A=G_1$ или $v=A=G_1\cup\{0\}$, где G_1 — некоторая мультипликативная группа действительных чисел. Достаточность. Пусть W удовлетворяет условию 2) теоремы 5. Нетрудно проверить, что F замкнуто относительно суперпозиции и относительно применения операции T. Таким образом, для а. систем W с $\pi(W)=1$ теорема верна.

Случай 3. Пусть $\pi(W)=\infty$ и $v(W)\neq\{1\}$. Необходимость. Пусть P_W $\exists$-полно для W. Докажем, что в этом случае W удовлетворяет условию 3) теоремы 5. Покажем, что v — поле. Нетрудно доказать, что $v\neq\{0\}$ и $v\neq\{0, 1\}$. Повторяя рассуждения, проделанные для случая

2), получаем, что $1\in v$; если $a, b\in v$, то $ab\in v$; если $a\in v$ и $a\neq 0$, то $\frac{1}{a}\in v$. Покажем, что $0\in v$. Из условия $\pi=\infty$ следует, что найдется функция $ax+by\in F$ с $a\neq 0$ и $b\neq 0$. Тогда $T(ax+by, y, x)=\frac{1}{a}x-$ $-\frac{b}{a}y\in F$. Возьмем $\kappa\in v$ такое, что $\kappa\neq 0$ и $\kappa\neq 1$. Тогда из замкнутости F относительно суперпозиции следует, что $\frac{\kappa}{a}x-\frac{\kappa b}{a}y\in F$ и $a\left(\frac{\kappa}{a}x-\right.$ $\left.-\frac{\kappa b}{a}y\right)+by=\kappa x+b(1-\kappa)y\in F$. Далее, $T(\kappa x+b(1-\kappa)y, x, y)=$ $=\frac{1}{b(1-\kappa)}-\frac{\kappa}{b(1-\kappa)}y\in F$. Подставляя в эту функцию κx вместо x, получаем, что

$$\frac{\kappa}{b(1-\kappa)}x-\frac{\kappa}{b(1-\kappa)}y\in F. \tag{25}$$

Отождествляя x и y, получаем, что $0x\in F$ и, следовательно, $0\in v$. Далее, используя доказанные выше свойства v и включение (25), нетрудно показать, что $-1\in v$ и $x+y\in F$. Таким образом, если $a, b\in v$, то и $a+b\in v$. Из сказанного выше следует, что v — поле. Покажем, что $A\subseteq v$ и, следовательно, $A=v$. Пусть $a\in A$, тогда найдется функция $\sum\limits_{i=1}^{n}a_i x_i+ax_{n+1}\in F$. Подставляя в эту функцию $0x$ вместо x_i для $i=\overline{1, n}$, получаем, что $ax_{n+1}\in F$ и $a\in v$. Итак, A — подполе поля действительных чисел. Используя равенство $v=A$ и то, что $x+y\in F$, нетрудно показать, что W удовлетворяет условию 3) теоремы 5 с $R_1=A$. Достаточность. Пусть W удовлетворяет условию 3) теоремы 5. Покажем, что P_W $\exists$-полно для W. Очевидно, F замкнуто относительно суперпозиции. Покажем, что F замкнуто относительно применения операции T. Пусть $\{f_1, \ldots, f_{\kappa+1}\}\subset F$, система $\{f_1, \ldots, f_\kappa\}$ линейно независима и $f_{\kappa+1}=\sum\limits_{i=1}^{\kappa}a_i f_i$. Хорошо известно, что для $i=\overline{1, \kappa}$ a_i представимо в виде частного от деления некоторого определителя, составленного из элементов множества $\bigcup\limits_{i=1}^{\kappa}A(f_i)$, на определитель такого же вида (правило Крамера). Из свойств определителя следует, что если все его коэффициенты принадлежат полю R_1, то и его значение принадлежит полю R_1, поэтому $\sum\limits_{i=1}^{\kappa}a_i x_i\in F$. Таким образом, для W с $\pi(W)=\infty$ и $v(W)\neq$ $\neq\{1\}$ теорема верна.

Случай 4. Пусть $\pi(W)=\infty$ и $v(W)=\{1\}$. Необходимость. Пусть P_W $\exists$-полно для W. Докажем, что W удовлетворяет условию 4) теоремы 5. Покажем, что A — поле. Очевидно, $0\in A$ и $1\in A$. Пусть $a\in A$, нетрудно заметить, что $ax+(1-a)y\in F$, т. е. $(1-a)\in A$. Пусть $a\in A$ и $a\neq 0$. Покажем, что $\frac{1}{a}\in A$. Действительно, $T(ax+(1-a)y, y, x)=$ $=\frac{1}{a}x+\frac{a-1}{a}y\in F$, следовательно, $\frac{1}{a}\in A$. Пусть $a, b\in A$, покажем,

что $ab \in A$. Подставим $bx+(1-b)y$ вместо x в выражение $ax+(1-a)y$. Получаем, что $abx+(1-ab)y \in F$, т. е. $ab \in A$. Покажем, что $x+y-z \in F$. Возьмем некоторое $\kappa \in A$ такое, что $\kappa \neq 0$ и $\kappa \neq 1$. Существование такого κ следует из свойств $\pi = \infty$ и $v = \{1\}$. Очевидно, что $\kappa x+(1-\kappa)z \in F$ и $\frac{1}{\kappa}x+\left(1-\frac{1}{\kappa}\right)y \in F$. Подставляя второе выражение в первое вместо x, получаем

$$x+(\kappa-1)y+(1-\kappa)z \in F. \tag{26}$$

Таким образом, $(\kappa-1) \in A$, следовательно, $\frac{1}{\kappa-1} \in A$ и

$$\frac{1}{\kappa-1}y+\left(1-\frac{1}{\kappa-1}\right)z \in F. \tag{27}$$

Подставляя (27) в (26) вместо y, получаем, что

$$x+y-z \in F \tag{28}$$

и, следовательно, $-1 \in A$. Далее, пусть $a, b \in A$. Подставляя в (28) $ax+(1-a)y$ вместо x и $bx+(1-b)y$ вместо y, получаем, что $(a+b)x+(2-a-b)y-z \in F$, т. е. $a+b \in A$. Из сказанного выше следует, что A — поле. Покажем, что W удовлетворяет условию 4) теоремы 5. Покажем, что любая функция вида $\frac{\sum\limits_{i=1}^{n} a_i x_i}{\sum\limits_{i=1}^{n} a_i}$, где $a_i \in A$ и $\sum\limits_{i=1}^{n} a_i \neq 0$, содержится в F. Очевидно, $f_i(x_i, z) = \frac{a_i x_i}{\sum\limits_{i=1}^{n} a_i}+\left(1-\frac{a_i}{\sum\limits_{i=1}^{n} a_i}\right)z \in F$ для $i=\overline{1, n}$. Определим $\psi_1 = f_1$ и $\psi_{i+1} = \psi_i + f_{i+1} - z$ для $i=\overline{1, n-1}$. Используя принадлежность $x+y-z$ множеству F и замкнутость f относительно суперпозиции, нетрудно показать, что $\psi_i \in F$ для $i=\overline{1, n}$ и $\psi_n = f(x_1, \ldots, x_n)$. Кроме того, любая функция из F представима для некоторого $n \in N$ в виде $\frac{\sum\limits_{i=1}^{n} a_i x_{j_i}}{\sum\limits_{i=1}^{n} a_i}$, где $a_i \in A$ и $\sum\limits_{i=1}^{n} a_i \neq 0$. Необходимость доказана.

Достаточность. Пусть W удовлетворяет условию 4) теоремы 5. Очевидно, F замкнуто относительно суперпозиции. Покажем, что F замкнуто относительно применения операции T. Пусть $\{f_1, \ldots, f_\kappa, f_{\kappa+1}\} \subset F$, система $\{f_1, \ldots, f_\kappa\}$ линейно независима и $f_{\kappa+1} = \sum\limits_{i=1}^{\kappa} a_i f_i$. Повторяя рассуждения случая 3), получаем, что $a_i \in R_1$. Далее, приравнивая к единице все переменные, от которых существенно зависят $f_1, \ldots, f_{\kappa+1}$, получаем равенство $\sum\limits_{i=1}^{\kappa} a_i = 1$, что и требовалось доказать. Таким образом, для W с $v(W) = \{1\}$ и $\pi(W) = \infty$ теорема верна. Теорема доказана.

ЛИТЕРАТУРА

1. Ершов Ю. Л., Лавров И. А., Тайманов А. Д., Тайцлин М. А. Элементарные теории. УМН, **20**, № 4, 37 (1965).

2. Tarski A. Arithmetical classes and types of mathematical systems, Mathe-

matical aspecty of arithmetical classes and types, arithmetical classes and types of Boolean algebras, Arithmetical classes and types of algebraically closed and real closed fields, Bull. Amer. Math. Soc. 55, 63 (1949).
3. Черников С. Н. Линейные неравенства. М., Наука, 1968.
4. Presburger M., Über die Vollständigkeit eines gevissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als, einrige Operation hervrtritt, Comptes rendus du I Congres des Mathematiciens des Pays Slaves, Warszawa, 1929, 395, p. 92.
5. Rousseau G., A decidable class of number theoretic equations. J. of the London Math Soc., v. 41, N 164, 737 (1966).
6. Manders Kenneth, Adleman Leonard, NP — complete decision problems for quadratic polinomials, «Conf. Rec. 8th Annu. ACM Sump. Theory Comput., Hershey, Pa. Calif., 1976». New York. N. Y., 1976, p. 23.
7. Мальцев А. И. Алгоритмы и рекурсивные функции. М., Наука, 1964.
8. Матиясевич Ю. В. Диофантовость перечислимых множеств. ДАН СССР, 191, № 2, 279 (1970).

Горьковский государственный университет

[19/XII 1977]

НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ РЕАЛИЗАЦИИ ХАРАКТЕРИСТИЧЕСКИХ ФУНКЦИЙ ГРУППОВЫХ КОДОВ П-СХЕМАМИ

А. К. Пулатов

Настоящая работа посвящена установлению оценок сложности реализации характеристических функций групповых кодов (групповые функции) параллельно-последовательными контактными схемами (П-схемами). Работа в основном имеет дело с нижними оценками, и основные результаты состоят в нелинейности этих оценок. Изучение класса групповых функций с позиций оценок сложности позволило также получить результаты как в понимании природы самих этих функций, так и в выяснении роли нулевых цепей в построении минимальных П-схем, реализующих булевые функции.

Следует отметить, что настоящая статья содержит развернутое изложение результатов автора, которые ранее были опубликованы либо разрозненно, либо в виде тезисов.

Перед тем как перейти к изложению результатов, отметим, что все необходимые понятия, связанные с n-мерным единичным кубом и контактными схемами, можно найти, например, в работах [1, 2].

Число контактов в П-схеме S обозначим через $L_{\text{П}}(S)$. Сложностью реализации булевой функции f П-схемами, как обычно, назовем число $L_{\text{П}}(f) = \min L_{\text{П}}(S)$, где минимум берется по всем П-схемам S, реализующим f.

Работа состоит из трех разделов.

Раздел 1 носит, в основном, подготовительный характер и посвящен собственно групповым кодам. Здесь изучается строение группового кода как подмножества вершин n-мерного единичного куба E^n. Исходным результатом является лемма 1, характеризующая проекцию группового кода на грань куба. Далее доказано, что вершины произвольного группового кода G_n равномерно (по количеству вершин) распределены по граням размерности $n-d'+1$ куба E^n, где d' — минимальное расстояние кода, двойственного коду G_n (теорема 1). Вместе с тем некоторые грани размерности $n-d'$ уже не содержат кодовых вершин. Кроме того, лемма 1 приводит к интеративному построению кодов, являющемуся обобщением построения Ю. Л. Васильева [3] на случай больших расстояний. Этим способом найден класс РМ-кодов — класс

групповых и негрупповых кодов, содержащий хорошо известные коды Рида—Маллера. Перечисленные результаты существенно используются во втором разделе получения нижних оценок сложности реализации групповых функций, а также могут представлять интерес в теории корректирующих кодов.

Раздел 2 посвящен нахождению нижних оценок сложности реализации групповых функций П-схемами.

Пусть $G_{n,\kappa}$ — произвольный $[n,\kappa]$-код (групповой (линейный) код длины n, размерности κ), $d'=d(G^{\perp}_{n,\kappa})$, т. е. d' — минимальное расстояние кода $G^{\perp}_{n,\kappa}$ двойственного коду $G_{n,\kappa}$. Пусть $g_{G_{n,\kappa}}(x_1,\ldots,x_n)$ — характеристическая функция кода $G_{n,\kappa}$. Доказано, что*

$$L_{\text{П}}\left(g_{G_{n,\kappa}}(x_1,\ldots,x_n)\right)\geq\frac{d'\log d'}{\log\log d'}. \tag{1}$$

Отсюда, например, при $d'\asymp\frac{n}{\sqrt{\log n}}$ (известно, что такое условие выполняется для весьма широкого класса групповых кодов, см., например, теорему 4, 9 из [4]) следуют нелинейные нижние оценки сложности реализации соответствующих функций. Оценка (1) получена с применением результата работы [5] для групповых функций. При этом существенно используется приведенное в теореме 1 свойство групповых кодов.

Другая нижняя оценка сложности для групповых функций получена В. М. Храпченко. Используя метод работы [6], он показал, что при $d=d(G_{n,\kappa})\geqslant 2$

$$L_{\text{П}}\left(g_{G_{n,\kappa}}(x_1,\ldots,x_n)\right)\geq\frac{n^{3/2}}{\sqrt{n-\kappa}}. \tag{2}$$

Этот результат дает нелинейные нижние оценки сложности реализации групповых функций в случае, когда $\kappa=n-0(n)$. Оценки (1) и (2) не исключают, а дополняют друг друга. Отметим, что, например, при $d'\asymp(n-\kappa)\asymp n$ оценка (1) сильнее (2).

Для характеристических функций кодов Рида—Маллера в работе получены более сильные нижние оценки (чем оценки (1) и (2)) следующего вида. Пусть $P_{m,r}$ — код Рида—Маллера длины $n=2^m$ и порядка r. Доказано, что

$$L_{\text{П}}\left(g_{P_{m,r}}(x_1,\ldots,x_n)\right)\geqslant 2^{2(r+1)}\geqslant (d')^2, \tag{3}$$

где $d'=d(P^{\perp}_{m,r})$. При $r=m-\text{const}$ из (3) следуют квадратичные нижние оценки сложности соответствующих функций. Оценка (3) получена путем сведения характеристических функций кодов Рида—Маллера к линейной функции. Это сведение опирается на итеративное построение РМ-кодов.

Для сравнения с полученными нижними оценками можно привести следующую верхнюю оценку сложности реализации групповых функций П-схемами. Пусть $G_{n,\kappa}$ — произвольный $[n,\kappa]$-код. Тогда

$$L_{\text{П}}\left(g_{G_{n,\kappa}}(x_1,\ldots,x_n)\right)<\frac{9}{8}n^2(n-\kappa). \tag{4}$$

Оценка (4) достаточно просто следует из задания группового кода через его проверочную матрицу, и поэтому ее приведем без доказательства. В качестве примера применения полученных оценок можно при-

* В работе знак log означает логарифм по основанию 2.

вести оценки сложности для характеристической функции кода Хэмминга χ_n:

$$n^2 \lesssim L_{\Pi}(g_{\chi_n}(x_1, ..., x_n)) \lesssim n^2 \log n.$$

Целью раздела 3 является изучение вопроса о влиянии нулевых цепей на сложность реализации булевых функций П-схемами. Пусть $L^*_{\Pi}(f)$ — сложность реализации функции f П-схемами, содержащими лишь ненулевые цепи, и $\mu_{\Pi}(n) = \max L^*_{\Pi}(f)/L_{\Pi}(f)$, где максимум берется по всем функциям f от n аргументов.

Пусть $g(x_1, ..., x_n)$ — характеристическая функция произвольного (n, d)-кода (n — длина, d — минимальное расстояние кода) мощности M и $d \geqslant 2$. Установлено, что

$$L^*_{\Pi}(g(x_1, ..., x_n)) \geqslant d \cdot M^{d/n}.$$

Отсюда, в частности, следует, что в случае П-схем без нулевых цепей сложность реализации характеристической функции группового кода с $\kappa \asymp n$ и $d \asymp n$ (существование такого кода обеспечивается границей Варшамова—Гильберта) имеет экспоненциальный относительно числа аргументов рост. С другой стороны, из верхней оценки (4) следует, что произвольная групповая функция в классе П-схем реализуется со сложностью не больше, чем n^3. Таким образом, показано, что

$$\mu_{\Pi}(n) \geqslant 2^{cn},$$

где $c < 1$ — некоторая константа. Это показывает, что в реализации булевых функций П-схемами нулевые цепи играют весьма существенную роль.

1. О ПОСТРОЕНИИ ГРУППОВЫХ КОДОВ В E^n

1.1. Геометрические свойства групповых кодов. Рассмотрим произвольную содержащую нулевую вершину грань n-мерного единичного куба E^n. Каждая такая грань однозначно определяется своей вершиной $\tau = (\tau_1, ..., \tau_n)$ максимального веса и поэтому обозначается через $\Gamma(\tau)$. Размерность грани $\Gamma(\tau)$ равна $\|\tau\|$, где $\|\tau\| = \sum_{i=1}^{n} \tau_i$ — вес вектора τ. Пусть $i_1, i_2, ..., i_{\|\tau\|}$ — номера компонент вектора $\tau = (\tau_1, \tau_2, ..., \tau_n)$ со значением, равным единице (тем самым грань $\Gamma(\tau)$ включает $i_1, i_2, ..., i_{\|\tau\|}$ — направления куба).

Для произвольного вектора $\sigma = (\sigma_1, \sigma_2, ..., \sigma_n) \in E^n$ вектор $(\sigma_{i_1}, \sigma_{i_2}, ..., \sigma_{i_{\|\tau\|}})$ будем называть проекцией σ на грань $\Gamma(\tau)$. Проекции всех вершин куба E^n на грань $\Gamma(\tau)$ образуют $\|\tau\|$-мерный куб $E^{\|\tau\|}$. Проекции всех вершин подмножества $A \subseteq E^n$ на грань $\Gamma(\tau)$ образуют подмножество в упомянутом $\|\tau\|$-мерном кубе, которое обозначим через ${}^{\tau}A$. Заметим, что понятие проекции подмножества вершин n-мерного куба на грань куба определяет понятие проекции булевой функции на грань куба. А именно, если $f(x_1, ..., x_n)$ — характеристическая функция подмножества $A \subseteq E^n$, то характеристическая функция $\varphi(x_{i_1}, x_{i_2}, ..., x_{i_{\|\tau\|}})$ подмножества ${}^{\tau}A \subseteq E^{\|\tau\|}$ называется проекцией функции $f(x_1, ..., x_n)$.

Определение. Пусть A — произвольное подмножество в E^n. Вектор $\alpha \in A$ называется нижним вектором для A, если среди ненулевых векторов из A нет вектора, предшествующего вектору α (вектор $\sigma' = (\sigma_1', \sigma_2', ..., \sigma_n')$ предшествует вектору $\sigma'' = (\sigma_1'', \sigma_2'', ..., \sigma_n'')$, если $\sigma_i' \leqslant \sigma_i''$, $i = 1, 2, ..., n$).

Пусть G_n — произвольный групповой код в E^n и $G_n^\perp$ — двойственный код. Пусть L_n — множество всех векторов четного веса в E^n.

Очевидно, что проекция группового кода является групповым кодом.

Лемма 1. ${}^\tau G_n = L_{\|\tau\|}$ тогда и только тогда, когда τ является нижним вектором для $G_n^\perp$.

Утверждение леммы эквивалентно следующему. Проекция характеристической функции группового кода на грань $\Gamma(\tau)$ куба E^n является линейной функцией от $\|\tau\|$ переменных тогда и только тогда, когда τ есть нижний вектор двойственного кода.

Доказательство. 1) Пусть τ — произвольный нижний вектор из $G_n^\perp$ (таковым является, например, любой ненулевой кодовый вектор минимального веса). Покажем, что ${}^\tau G_n = L_{\|\tau\|}$. Для простоты будем считать, что $\tau = (\underbrace{1 \ldots 10 \ldots 0}_{t})$, где $t = \|\tau\|$. Пусть α — произвольный вектор из E^n. Его проекция представляет собой вектор, составленный из первых t компонент вектора α (здесь и далее, где не указано направление проектирования, будем подразумевать, что проекция берется на грань $\Gamma(\tau)$). Вектор α не будет принадлежать групповому коду G_n, **если*** $\sum\limits_{j=1}^{t} \oplus \alpha_j = 1$ (так как скалярное произведение $(\alpha, \tau) = \sum\limits_{j=1}^{t} \oplus \alpha_j \neq 0$).

Это равносильно тому, что ${}^\tau G_n$ входят только векторы четного веса из E^n, т. е.

$$ {}^\tau G_n \subseteq L_t. \tag{5}$$

Теперь допустим, что ${}^\tau G_n \neq L_t$. Так как ${}^\tau G_n$ является групповым кодом в E^t, то, в силу (5), размерность ${}^\tau G_n$ не больше, чем $t-2$ ($t-1$ есть размерность L_t). Тогда двойственный код $({}^\tau G_n)^\perp$ имеет размерность не меньшую, чем 2, и, следовательно, содержит ненулевой вектор веса $l (l < t)$. Не ограничивая общности, можно считать, что таковым является вектор $\nu = (\underbrace{1 \ldots 10 \ldots 0}_{l}) \in E^t$. Как и выше, все векторы $\mu = (\mu_1, \mu_2, \ldots, \mu_t) \in E^t$, для которых $\sum\limits_{i=1}^{l} \oplus \mu_i = 1$, дают $(\mu, \nu) \neq 0$, т. е. эти векторы не входят в ${}^\tau G_n$. Таким образом, из $(\sigma_1, \sigma_2, \ldots, \sigma_n) \in G_n$ следует $\sum\limits_{i=1}^{l} \oplus \sigma_i = 0$. Переходя от вектора ν к вектору $a = (\underbrace{1 \ldots 10 \ldots 0}_{l})$, $a \in E^n$, получим вектор, который, с одной стороны, ортогонален коду G_n, т. е. входит в $G_n^\perp$ ($\sum\limits_{i=1}^{l} \oplus \sigma_i = 0$ можно записать как $(\sigma, a) = 0$), а с другой стороны, предшествует вектору τ, являющемуся для $G_n^\perp$ нижним вектором, т. е. получим противоречие. Следовательно, ${}^\tau G_n = L_t$.

2) Пусть ${}^\tau G_n = L_{\|\tau\|}$. Покажем, что τ является нижним вектором для $G_n^\perp$. Пусть $t = \|\tau\|$. Очевидно, что $\tau \in G_n^\perp$. Допустим, что τ не является нижним вектором. Тогда в $G_n^\perp$ найдется вектор τ', предшествующий τ и являющийся нижним. Пусть $\|\tau'\| = t'$, так что $t' < t$. Не ограничивая общности, можно считать, что

$$\tau = (\underbrace{11 \ldots 10 \ldots 0}_{t}), \quad \tau' = (\underbrace{11 \ldots 10 \ldots 0}_{t'}).$$

Введем еще вектор $\tau'' = (\underbrace{11 \ldots 10 \ldots 0}_{t'})$, $\tau'' \in E^t$. Из определений этих

* По обозначению $\sum\limits_{i=1}^{\kappa} \oplus \sigma_i = \sigma_1 \oplus \ldots \oplus \sigma_\kappa$, где $\oplus$ — сложение по mod 2.

векторов следует, что

$$^{\tau'}G_n = L_{t'} \quad \text{и} \quad ^{\tau''}(^{\tau}G_n) = {}^{\tau'}G_n.$$

С учетом исходного предположения получим, что $^{\tau}L_t = L_{t'}$. С другой стороны, для любого вектора $\hat{\beta}$ из E^t, $\beta \neq (11\ldots1)$ имеет место $^{\beta}L_t = E^{\|\beta\|}$. Полученное противоречие доказывает, что τ является нижним вектором в $G_n^{\perp}$. Лемма доказана.

Теперь вернемся к изучению свойств групповых кодов. Напомним, что в E^n существуют $(n-d')$-мерные грани $\Gamma^{n-d'}$, такие, что $G_n \cap \Gamma^{n-d'} = \varnothing$. Доказывается, что число $n-d$ является максимальной размерностью грани куба, которая лежит в дополнении кода. Это вытекает из следующей теоремы.

Теорема 1. Для каждого фиксированного m, $n-d'+1 \leqslant m \leqslant n$ и для каждой m-мерной грани Γ^m в E^n число $|\Gamma^m \cap G_n|$ постоянно и равно $\frac{|G_n|}{2^{n-m}}$. (Для множества A через $|A|$ обозначена его мощность).

Доказательство. Допустим, что существует грань Γ^s, $s \geqslant n-d'+1$ и $\Gamma^s \cap G_n = \varnothing$. Пусть $j_1, j_2, \ldots, j_{n-s}$ — разряды, на которых постоянны компоненты векторов из Γ^s. Рассмотрим вектор $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) : \sigma_i = 1$ тогда и только тогда, когда $i \in \{j_1, j_2, \ldots, j_{n-s}\}$, так что $\|\sigma\| \leqslant d'-1$. Далее рассмотрим проекцию кода G_n на грань $\Gamma(\sigma)$ (грань $\Gamma(\sigma)$ ортогональна к исходной грани Γ^s). Рассуждения, аналогичные рассуждениям из первой части доказательства леммы 1, приводят к тому, что в $G_n^{\perp}$ существует вектор веса не больше, чем $d'-1$ (этим вектором является σ или некоторый вектор, предшествующий вектору σ). Это противоречит определению числа d'. Следовательно, при $m \geqslant n-d'+1$ для произвольной грани Γ^m следует, что $\Gamma^m \cap G_n \neq \varnothing$. С другой стороны, очевидно, что для любого κ, $1 \leqslant \kappa \leqslant n$ все параллельные κ-мерные грани куба, имеющие непустое пересечение с G_n, содержат по одинаковому числу векторов из G_n. Число параллельных κ-мерных граней произвольного направления равно $2^{n-\kappa}$. Следовательно, при $m \geqslant n-d'+1$ для произвольной грани Γ^m имеем

$$|\Gamma^m \cap G_n| = \frac{|G_n|}{2^{n-m}}.$$

1.2. Описание РМ-кодов. Одним из важных классов $[n, \kappa]$-кодов являются коды Рида — Маллера. Для любых натуральных m и $r < m$ существует код из этого класса (код Рида—Маллера порядка r), для которого

$$\left.\begin{aligned} n &= 2^m, \\ \kappa &= \sum_{i=0}^{r} C_m^i, \\ d &= 2^{m-r}. \end{aligned}\right\} \tag{6}$$

Разные способы задания кодов Рида — Маллера описаны, например, в работе [4]. Целью настоящего раздела является итеративное построение класса групповых и негрупповых кодов, содержащих коды и имеющих те же параметры (длина кода, мощность, кодовое расстояние), что и коды Рида — Маллера. Далее эти коды будем называть РМ-кодами. Построению их предшествует построение класса кодов, для которых

$$\left.\begin{aligned} n &= 2^m - 1, \\ \text{мощность кода} &= 2^{\sum_{i=0}^{r} C_m^i}, \\ d &= 2^{m-r} - 1. \end{aligned}\right\} \tag{7}$$

Затем осуществляется переход к РМ-кодам. Коды с параметрами (7) назовем укороченными РМ-кодами. Отметим, что укороченный РМ-код порядка $r=m-2$ совпадает с плотно упакованным (п. у.) $(n, 3)$-кодом, а групповой такой код совпадает с кодом Хэмминга. Отметим также, что построение укороченных РМ-кодов является обобщением построения п. у. $(n, 3)$-кодов (см. [3]).

Исходные построения. Пусть n и d обозначают длину и минимальное расстояние кода, причем, число $\frac{d-1}{2}$ — нечетное. Рассмотрим произвольные (n, d)-код и $\left(n, \frac{d-1}{2}\right)$-код, содержащие нулевой набор и имеющие мощности $M_{n,d}$ и $M_{n\,\frac{d-1}{2}}$, обозначаемые через $C_{n,d}$ и $C_{n,\frac{d-1}{2}}$ соответственно. Из этих двух кодов построим следующий $(2n+1, d)$-код.

Пусть $\lambda(\tau)$ — произвольная функция, принимающая значения нуль и единица на вершинах $\tau=(\tau_1, ..., \tau_n)$ из $C_{n,d}$, причем $\lambda(0, ..., 0)=0$. Для набора $\alpha=(\alpha_1, ..., \alpha_n)$ положим $|\alpha|=\alpha_1 \oplus ... \oplus \alpha_n$. Паре наборов $\tau=(\tau_1, ..., \tau_n)$ и $\mu=(\mu_1, ..., \mu_n)$, $\tau \in C_{n,d}$, $\mu \in C_{n\,\frac{d-1}{2}}$ сопоставим набор

$$\mu_1, ..., \mu_n, \ |\mu| \oplus \lambda(\tau), \ \mu_1 \oplus \tau_1, ..., \mu_n \oplus \tau_n,$$

который обозначим через $\mu * \tau$. Обозначим через $C_{n,\frac{d-1}{2}} * C_{n,d}$ множество всех наборов вида $\mu * \tau$, где $\mu \in C_{n,\frac{d-1}{2}}$, $\tau \in C_{n,d}$.

Теорема 2. Для любой функции $\lambda(\tau)$ множество $C_{n,\frac{d-1}{2}} * C_{n,d}$ является $(2n+1, d)$-кодом мощности $M_{n,\frac{d-1}{2}} \times M_{n,d}$, содержащим нулевой набор.

Доказательство. Множество $C_{n,\frac{d-1}{2}} * C_{n,d}$ состоит из наборов длины $2n+1$. Очевидно, что нулевой набор $(0, 0, ..., 0)$ длины $2n+1$ входит в $C_{n,\frac{d-1}{2}} * C_{n,d}$ и мощность этого множества есть $M_{n,\frac{d-1}{2}} \times M_{n,d}$. Покажем, что расстояние ρ между любыми наборами из нашего множества не меньше d. Пусть

$$\mu * \tau = (\mu_1, ..., \mu_n, |\mu| \oplus \lambda(\tau), \mu_1 \oplus \tau_1 ..., \mu_n \oplus \tau_n) \text{ и}$$

$$u * v = (u_1, ..., u_n, |u| \oplus \lambda(v), u_1 \oplus v_1 ..., u_n \oplus v_n)$$

есть произвольные несовпадающие наборы из $C_{n,\frac{d-1}{2}} * C_{n,d}$, $\mu, u \in C_{n,\frac{d-1}{2}}$, $\tau, v \in C_{n,d}$.

1) Если $\tau \neq v$, то $\rho(\tau, v) \geqslant d$. Тогда при $\rho(\mu, u)=0, \frac{d-1}{2}, \frac{d-1}{2}+1, ..., d$ имеем (в силу неравенства треугольника и соотношения $d-\frac{d-1}{2}=\frac{d+1}{2}$) соответственно

$$\rho[(\mu_1 \oplus \tau_1, ..., \mu_n \oplus \tau_n), (u_1 \oplus v_1, ..., u_n \oplus v_n)] \geqslant d, \frac{d+1}{2}, \frac{d-1}{2}, ..., 0.$$

Следовательно, $\rho(\mu * \tau, \ u * v) \geqslant d$.

2) Если $\tau=\nu$, то $\lambda(\tau)=\lambda(\nu)$, а $\mu\neq u$. Возможны два случая:

а) $|\mu|\neq|u|$. Тогда $\rho(\mu, u)\geqslant\frac{d-1}{2}$. Следовательно, $\rho[(\mu_1\oplus\tau_1, \ldots, \mu_n\oplus\tau_n), (u_1\oplus\nu_1, \ldots, u_n\oplus\nu_n)]\geqslant\frac{d-1}{2}$, $|\mu|\oplus\lambda(\tau)\neq|u|\oplus\lambda(u)$. Поэтому $\rho(\mu*\tau, u*\nu)\geqslant\frac{d-1}{2}+\frac{d-1}{2}+1=d$,

б) $|\mu|=|u|$. Поскольку $\mu\neq u$ и $\rho(\mu, u)$ — четные (напомним, что по условию $\frac{d-1}{2}$ — нечетное число), то $\rho(\mu, u)\geqslant\frac{d+1}{2}$. Также $\rho[(\mu_1\oplus\tau_1, \ldots, \mu_n\oplus\tau_n), (u_1\oplus\nu_1, \ldots, u_n\oplus\nu_n)]\geqslant\frac{d+1}{2}$, откуда $\rho(u*\tau, u*\nu)\geqslant d+1$.

Теорема доказана.

Пусть $C_{n,d}$ и $C_{n,\frac{d-1}{2}}$ — групповые коды. Тогда в зависимости от функции $\lambda(\tau)$, участвовавшей в построении кода $C_{n,\frac{d-1}{2}}*C_{n,d}$, последний будет групповым или негрупповым:

если положить $\lambda(\tau)\equiv 0$ для всех $\tau\in C_{n,d}$, то получим групповой код;

если зафиксировать два каких-либо ненулевых набора τ', τ'' из $C_{n,d}$ и положить $\lambda(\tau'\oplus\tau'')\neq\lambda(\tau')\oplus\lambda(\tau'')$, то код будет негрупповым.

Построение укороченных РМ-кодов. Пользуясь теоремой 2, индуктивно построим класс укороченных РМ-кодов. Укороченный РМ-код длины $n=2^m-1$ и порядка r обозначим через $K_{m,r}$ (напомним, что минимальное расстояние этого кода $d=2^{m-r}-1$). Исходными являются коды $K_{m,m-1}$ и $K_{m,0}$, которые просто задаются:

$$K_{m,m-1}=E^n \quad \text{и} \quad K_{m,0}=\{(0, 0, \ldots, 0), (1, 1, \ldots, 1)\}.$$

Пусть уже построены коды $K_{m,r-1}$ и $K_{m,r}$. Тогда код $K_{m+1,r}$ задается соотношением

$$K_{m+1,r}=K_{m,r}*K_{m,r-1}.$$

Действительно, по теореме 2, код $K_{m,r}*K_{m,r-1}$ имеет длину $2^{m+1}-1$, кодовое расстояние $2^{m-(r-1)}=2^{m+1-r}$, мощность

$$2^{1+C_m^1+\cdots+C_m^r}\times 2^{1+C_m^1+\cdots+C_m^{r-1}}=2^{1+C_{m+1}^1+\cdots+C_{m+1}^r}$$

(так как $C_m^i+C_m^{i-1}=C_{m+1}^i$) и, следовательно, является укороченным РМ-кодом длины $2^{m+1}-1$ и порядка r. По построению коды $K_{m,r}$ могут оказаться как групповыми, так и негрупповыми (при $2\leqslant r\leqslant m-2$).

Построение РМ-кодов. Обозначим через $K_{m,r}^*$ код, получаемый из кода $K_{m,r}$ добавлением одной компоненты — проверки на четность кодовых векторов, т. е.

$$K_{m,r}^*=\{(\alpha, |\alpha|) : \alpha\in K_{m,r}\}.$$

Код $K_{m,r}^*$ имеет длину 2^m, и нетрудно проверить, что его кодовое расстояние на единицу больше кодового расстояния кода $K_{m,r}$ (напомним, что кодовое расстояние кода $K_{m,r}$ выражается нечетным числом). Следовательно, $K_{m,r}^*$ является РМ-кодом длины 2^m и порядка r. Тем самым получили класс РМ-кодов, содержащий как групповые, так и негрупповые коды.

Рассмотрим групповые РМ-коды. В нашем способе задания РМ-ко-

дов такие коды, как было отмечено, получаются при $\lambda(\tau)\equiv 0$. Пусть $n=2^m$ и

$$\tau=(\underbrace{11\ldots10}_{n/2}\ldots0)\in E^n,\quad \tau'=(\underbrace{11\ldots10}_{2^{r+1}}\ldots0)\in E^n.$$

Из построения РМ-кодов для проекций группового кода $K^*_{m,r}$ на грани $\Gamma(\tau)$ и $\Gamma(\tau')$ куба соответственно следуют

$$^{\tau}K^*_{m,r}=K^*_{m-1,r}\quad\text{и}\quad {}^{\tau'}K^*_{m,r}=K^*_{r+1,r}=L_{2^{r+1}}. \tag{8}$$

Таким образом, коды $K^*_{m,r}$ описаны через свои проекции. При этом исходными в построении являются «простые» коды $L_{2^{r+1}}$. Из (8) и леммы 1 следует, что вектор τ' является нижним для кода, двойственного к $K^*_{m,r}$. Отсюда получаем следующее

Предложение 1. Минимальное расстояние $d^{*\prime}_{m,r}$ кода $(K^*_{m,r})^{\perp}$ удовлетворяет неравенству $d^{*\prime}_{m,r}\leqslant 2^{r+1}$.

2. НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ ГРУППОВЫХ ФУНКЦИЙ П-СХЕМАМИ

2.1. Случай произвольных групповых кодов. Отметим следующие простые свойства групповых функций.

Предложение 2. Групповая функция $g_{G_{n,\varkappa}}(x_1,\ldots,x_n)$ существенно зависит от всех своих переменных тогда и только тогда, когда $d=d(G_{n,\varkappa})\geqslant 2$.

Доказательство. Достаточность предложения очевидна.

Необходимость. Допустим, что $d=1$, тогда в $G_{n,\varkappa}$ входят наборы $\sigma'=(\sigma_1,\ldots,\sigma_{i-1},\sigma_i,\sigma_{i+1},\ldots,\sigma_n)$ и $\sigma''=(\sigma_1,\ldots,\sigma_{i-1},\bar{\sigma}_i,\sigma_{i+1},\ldots,\sigma_n)$. Так как $G_{n,\varkappa}$ — группа, то набор $\sigma=\sigma'\oplus\sigma''=(0,\ldots,0,1,0,\ldots,0)\in G_{n,\varkappa}$. Поэтому для любого $\beta=(\beta_1,\ldots,\beta_{i-1},\beta_i,\beta_{i+1},\ldots,\beta_n)\in G_{n,\varkappa}$ следует, что $(\beta_1,\ldots,\beta_{i-1},\bar{\beta}_i,\beta_{i+1},\ldots,\beta_n)=\beta\oplus\sigma\in G_{n,\varkappa}$. Следовательно, для функции $g_{G_{n,\varkappa}}(x_1,\ldots,x_n)$ переменная x_i является фиктивной.

Предложение 3. Пусть* $f(x_1,\ldots,x_n)$ — произвольная групповая функция и g — функция, получаемая из f после удаления фиктивных переменных. Пусть $d_1'=d(N_f^{\perp})$ и $d_2'=d(N_g^{\perp})$. Тогда $d_1'=d_2'$.

Доказательство. Если функция f фиктивно зависит от i-го переменного, то из предложения 2 следует, что вектор $\sigma=(0\ldots010\ldots0)$, у которой i-я компонента равна единице, принадлежит к N_f. Поэтому для произвольного $\beta=(\beta_1,\beta_2,\ldots,\beta_n)\in N_f^{\perp}$ получим $\beta_i=0$ (иначе скалярное произведение $(\alpha,\beta)\neq 0$). Тем самым выбрасывание i-й компоненты вектора β не уменьшает его вес.

Определение [5]. Функция $f(x_1,\ldots,x_n)$ от n аргументов называется дифференцируемой порядка $m(m<n)$, если любая подфункция, получаемая из f подстановкой каких-либо констант на место каких-либо m аргументов, существенно зависит от $n-m$ аргументов.

Лемма 2. Пусть $g_{G_{n,\varkappa}}(x_1,\ldots,x_n)$ — характеристическая функция произвольного группового кода $G_{n,\varkappa}$ и $d'=d(G^{\perp}_{n,\varkappa})$. Тогда, если $g_{G_{n,\varkappa}}(x_1,\ldots,x_n)$ существенно зависит от всех аргументов, то она дифференцируема порядка $d'-1$.

* Для функции $f=f(x_1,\ldots,x_n)$ через N_f обозначается множество всех наборов $(\sigma_1,\ldots,\sigma_n)\in E^n$, таких, что $f(\sigma_1,\ldots,\sigma_n)=1$.

Доказательство. Пусть $\Gamma^{n-d'+1}$ — произвольная грань размерности $n-d'+1$ куба E^n. Из теоремы 1 имеем

$$\Gamma^{n-d'+1} \cap G_{n,\varkappa} = \varnothing.$$

Поэтому подфункция функции $g_{G_{n,\varkappa}}(x_1, \ldots, x_n)$, определенная на грани $\Gamma^{n-d'+1}$, не является тождественно нулевой. Тогда из предложения 2 и из предположения о существенности всех переменных для $g_{G_{n,\varkappa}}(x_1, \ldots, x_n)$ следует, что эта подфункция существенно зависит от всех своих $n-d'+1$ аргументов.

Лемма доказана.

Нижнюю оценку сложности реализации П-схемами групповой функции $g_{G_{n,\varkappa}}(x_1, \ldots, x_n)$ дает следующая

Теорема 3.

$$L_{\Pi}(g_{G_{n,\varkappa}}(x_1, \ldots, x_n)) \geq \frac{d' \log d'}{\log \log d'}.$$

Доказательство. В силу предложения 3, можем считать, что функция $g_{G_{n,\varkappa}}(x_1, \ldots, x_n)$ существенно зависит от всех своих аргументов. В работе [5] доказано, что если функция $f(x_1, \ldots, x_n)$ дифференцируема порядка m, то при $m \geqslant 8$

$$L_{\Pi}(f(x_1, \ldots, x_n)) \geqslant \frac{m}{2} \cdot \frac{\log m}{\log \log m}.$$

Тогда утверждение теоремы следует из леммы 2 и упомянутого результата.

Теорема доказана.

2.2. Случай РМ-кодов. Пусть $n = 2^m$, $m = 2, 3, \ldots$ и $g_{K^*_{m,r}}(x_1, \ldots, x_n)$ — характеристическая функция РМ-кода $K^*_{m,r}$, построенного в разделе 1. Напомним, что коды $K^*_{m,r}$ могут быть как групповыми, так и негрупповыми.

Теорема 4. $L_{\Pi}(g_{K^*}(x_1, \ldots, x_n)) \geqslant 2^{2(r+1)}$.

Следствие. Если $K^*_{m,r}$ — групповой код, то

$$L_{\Pi}(g_{K^*}(x_1, \ldots, x_n)) \geqslant (d^{*'}_{m,r})^2,$$

где $d^{*'}_{m,r} = d((K^*_{m,r})^{\perp})$. Следствие получается из неравенства $d^{*'}_{m,r} \leqslant 2^{r+1}$ (предложение 1).

Доказательство теоремы. По построению

$$K^*_{r+1,r} = \{(a, |a|) : a \in E^{2^{r+1}-1}\}.$$

Следовательно, $g_{K^*_{r+1,r}}(x_1, \ldots, x_{2^{r+1}}) = x_1 \oplus \ldots \oplus x_{2^{r+1}}$. В силу [7], получим

$$L_{\Pi}(g_{K^*_{r+1,r}}(x_1, \ldots, x_{2^{r+1}})) \geqslant 2^{2(r+1)}.$$

Остается доказать, что

$$L_{\Pi}(g_{K^*_{m,r}}(x_1, \ldots, x_n)) \geqslant L_{\Pi}(g_{K^*_{r+1,r}}(x_1, \ldots, x_{2^{r+1}})).$$

Проверим, что

$$L_{\text{П}}(g_{K^*_{m,r}}) \geqslant L_{\text{П}}(g_{K^*_{m-1,r}}) \geqslant \cdots \geqslant L_{\text{П}}(g_{K^*_{r+1,r}}).$$

Учитывая рекуррентное построение кода $K^*_{m,r}$, достаточно доказать только первое неравенство. Доказательство его основано на выделении в рассматриваемых кодах частей, играющих роль как бы диагоналей.

Рассмотрим произвольную П-схему S, реализующую функцию $g_{K^*_{m,r}}(x_1, \ldots, x_n)$. Над схемой S производим следующее преобразование. Пусть $i = 1, 2, \ldots, n/2$; $\sigma = 0, 1$. Переберем все ребра схемы. Ребра, которым приписана буква x_i^σ, оставим без изменения. Если ребру приписана буква $x_{n/2+i}^\sigma$, то эту букву заменяем на букву x_i^σ. Полученную схему обозначим через S'. Проверим, что схема S' реализует функцию $g_{K^*_{m-1,r}}(x_1, \ldots, x_{n/2})$. Каждая ненулевая цепь (нулевая цепь—цепь, имеющая тождественно нулевую проводимость) схемы S содержит контакты от всех n аргументов, ибо, в противном случае, код $K^*_{m,r}$ содержал бы некоторую пару соседних наборов куба E^n. Каждой ненулевой цепи из S отвечает такой набор из $K_{m,r}$, что на этом наборе замкнуты все контакты этой цепи и, наоборот, каждому набору из $K^*_{m,r}$ соответствует, в указанном смысле, одна или несколько цепей схемы S. По определению

$$K^*_{m,r} = \{(a, |a|) : a \in K_{m,r}\}.$$

В свою очередь,

$$K_{m,r} = \{(\mu, |\mu| \oplus \lambda(\tau),\ \mu \oplus \tau) : \mu \in K_{m-1,r},\ \tau \in K_{m-1,r-1}\}.$$

Следовательно,

$$K^*_{m,r} = \{(\mu, |\mu| \oplus \lambda(\tau), \mu \oplus \tau, |\mu \oplus \tau| \oplus \lambda(\tau)) : \mu \in K_{m-1,r}, \tau \in K_{m-1,r-1}\}.$$

Множество наборов кода $K^*_{m,r}$ (следовательно, и множество всех ненулевых цепей схемы S) разделим на два непересекающиеся подмножества. Пусть A_1 — подмножество всех наборов, которые порождаются при $\tau = (0, 0, \ldots, 0) \in K_{m-1,r-1}$, и пусть $A_2 = K^*_{m,r} \setminus A_1$. Учитывая, что $\lambda(0, 0, \ldots, 0) = 0$, имеем

$$A_1 = \{(\mu, |\mu|, \mu, |\mu|) : \mu \in K_{m-1,r}\}$$

(множество A_1 как раз и играет роль упомянутой диагонали).

Теперь переберем все цепи схемы S и рассмотрим, в какие цепи преобразуются они в схеме S'.

1) Очевидно, что нулевая цепь схемы S преобразуется в схеме S' также в нулевую цепь.

2) Рассмотрим произвольный набор из A_1. Он имеет вид $(\mu, |\mu|, \mu, |\mu|)$, где $\mu \in K_{m-1,r}$. Любая цепь схемы S, отвечающая этому набору, содержит контакты вида

$$\overset{\mu_1}{x_1},\ \ldots,\ \overset{\mu_{n/2-1}}{x_{n/2-1}},\ \overset{|\mu|}{x_{n/2}},\ \overset{\mu_1}{x_{n/2+1}},\ \ldots,\ \overset{\mu_{n/2-1}}{x_{n-1}},\ \overset{|\mu|}{x_n}$$

и никаких других конатктов не содержит. Тогда соответствующая цепь в S' состоит из контактов вида

$$\overset{\mu_1}{x_1},\ \ldots,\ \overset{\mu_{n/2-1}}{x_{n/2-1}},\ \overset{|\mu|}{x_{n/2}},$$

и она отвечает набору $(\mu_1, ..., \mu_{n/2-1}, |\mu|)$. По определению этот набор является элементом кода $K^*_{m-1,r}$. Следовательно, функция, реализуемая схемой S', принимает значение единицы на всех наборах из $K^*_{m-1,r}$.

3) Далее рассмотрим произвольный набор σ из A_2. Любая цепь схемы S, отвечающая этому набору, переходит в схеме S' в нулевую цепь. Действительно, пусть i-я компонента набора $\tau \in K_{m-1,r-1}$, участвующего в определении набора σ, равна единице $(1 \leqslant i \leqslant n/2-1)$. Это означает, что в наборе σ i-й компонентой является μ_i, а $(n/2+i)$-й компонентой является $\mu_i \oplus 1$. В любой цепи схемы S, отвечающей такому набору, контакты от аргументов x_i и $x_{n/2+i}$ имеют соответственно вид $x_i^{\mu_i}$ и $x_{n/2+i}^{\mu_i \oplus 1}$. Поэтому соответствующая цепь схемы S' содержит контакты вида $x_i^{\mu_i}$ и $x_i^{\mu_i \oplus 1}$, т. е. она является нулевой цепью.

Пункты 1—3 вместе означают, что схема S' реализует функцию $g_{K^*_{m-1,r}}(x_1, ..., x_{n/2})$.

Теорема доказана.

Случай укороченных РМ-кодов аналогичен рассмотренному.

Пусть $n = 2^m - 1$, $m = 2, 3, ...$ и $g_{K_{m,r}}(x_1, ..., x_n)$ — характеристическая функция укороченного РМ-кода $K_{m,r}$. Значение $r = m-1$ не представляет интереса: по построению $K_{m,m-1} = E^n$, и потому $g_{K_{m,m-1}}(x_1, ..., x_n) \equiv 1$.

Для остальных r имеет место

Теорема 4а. Если $r \leqslant m-2$, то

$$L_{\text{П}}(g_{K_{m,r}}(x_1, ..., x_n)) \geqslant 2^{2(r+1)}.$$

Доказательство повторяет доказательство теоремы 4. Из этой теоремы и предложения 1а вытекает, что если $K_{m,r}$ — групповой код, то

$$L_{\text{П}}(g_{K_{m,r}}(x_1, ..., x_n)) \geqslant (d_{m,r}')^2,$$

где $d'_{m,r} = d(K^{\perp}_{m,r})$.

Отметим, что для характеристической функции $g_{\chi_n}(x_1, ..., x_n)$ кода Хэмминга χ_n (укороченного РМ-кода длины $n = 2^m - 1$ и порядка $r = m-2$) из теоремы 4а следует, что

$$L_{\text{П}}(g_{\chi_n}(x_1, ..., x_n)) \geqslant \left(\frac{n+1}{2}\right)^2.$$

3. О ВЛИЯНИИ НУЛЕВЫХ ЦЕПЕЙ НА СЛОЖНОСТЬ П-СХЕМ

Исходным в получении нижних оценок сложности реализации булевых функций П-схемами без нулевых цепей является следующая*

Лемма 3. Пусть $f(x_1, ..., x_n)$ — произвольная булевская функция такая, что из $\alpha, \beta \in N_f$, $\alpha \neq \beta$, следует, что $\rho(\alpha, \beta) \geqslant 2$. Пусть S — минимальная П-схема, содержащая лишь ненулевые цепи и реализующая функцию $f(x_1, ..., x_n)$. Тогда каждая цепь схемы S содержит ровно по одному контакту от каждой переменной.

---

* Напомним, что под цепью понимается простая (без самопересечений) цепь, соединяющая полюсы контактной схемы.

Доказательство. Из условий леммы сразу следует, что каждая цепь схемы S содержит контакты от каждой переменной функции $f(x_1, ..., x_n)$ (в противном случае S содержит либо нулевую цепь, либо цепь, которая реализует наборы, находящиеся на расстоянии единицы). Покажем, что никакая цепь схемы S не содержит несколько контактов одного и того же вида. Будем пользоваться индуктивным определением П-схемы. Фиксируем произвольную цепь A схемы S. Пусть эта цепь содержит контакт вида z, где z — одно из букв $x_1, x_2, ..., x_n$, $\bar{x}_1, \bar{x}_2, ..., \bar{x}_n$. Схема S в общем случае разлагается на параллельные подсхемы.

Подсхему, содержащую рассматриваемую цепь, обозначим через S_1 (возможно, что $S_1 = S$). В свою очередь, схема S_1 разлагается на последовательно соединеннные подсхемы $S_{11}, S_{12}, ..., S_{1\varkappa_1}$. Покажем, что только одна из этих подсхем содержит контакт вида z (одна из этих подсхем содержит контакт вида z, так как рассматриваемая цепь A содержит такой контакт). Допустим, что подсхемы $S_{1i_1}, S_{1i_2}, ..., S_{1i_{l_1}}$, $l_1 \geqslant 2$, содержат контакты вида z ($\{i_1, i_2, ..., i_{l_1}\} \subseteq \{1, 2, ..., \varkappa_1\}$). Тогда, очевидно, никакая из подсхем $S_{11}, S_{12}, ..., S_{1\varkappa_1}$ не содержит контакт вида z (в противном случае непременно появится нулевая цепь). Вместе с тем, как было показано выше, каждая цепь схемы S содержит контакты от каждой переменной функции $f(x_1, ..., x_n)$. Следовательно, произвольная цепь схемы S_1 содержит контакт вида z. Это возможно только тогда, когда хотя бы в одной из подсхем $S_{1i_1}, S_{1i_2}, ..., S_{1i_{l_1}}$ существует сечение, состоящее сплошь из контактов вида z.

Рассмотрим одну из подсхем, в которой существует указанное сечение. Тогда контакты вида z в подсхемах $S_{1i_1}, S_{1i_2}, ..., S_{1i_{l_1}}$, кроме выделенной подсхемы, можем замкнуть, и от этого не изменится функция проводимости схемы S. Тем самым получим П-схему, содержащую меньшее число контактов, чем П-схема S, что противоречит минимальности S. Таким образом, только одна из подсхем $S_{11}, S_{12}, ..., S_{1\varkappa_1}$ содержит контакт вида z. Не ограничивая общности, можем считать, что подсхема S_{11} обладает этим свойством. При этом доказано, что произвольная цепь схемы S, проходящая через подсхему S_{11}, не содержит контакт вида z вне подсхемы S_{11}. В частности, цепь A содержит контакты вида z только в подсхеме S_{11}. Далее, схему S_{11} разложим на параллельные подсхемы и рассмотрим подсхему, по которой проходит цепь A. Эту подсхему обозначим через S_2. Отметим, что произвольная цепь схемы S, проходящая через подсхему S_2, не содержит контактов вида z вне подсхемы S_2. В свою очередь, схема S_2 разлагается на последовательно соединенные подсхемы $S_{21}, S_{22}, ..., S_{2\varkappa_2}$. Покажем, что только одна из этих подсхем содержит контакт вида z (одна из этих подсхем содержит контакт вида z, так как цепь A содержит такой контакт).

Допустим, что подсхемы $S_{2i_1}, S_{2i_2}, ..., S_{2i_{l_2}}$, $l_2 \geqslant 2$, содержат контакт вида z ($\{i_1, i_2, ..., i_{l_2}\} \subseteq \{1, 2, ..., \varkappa_2\}$). Тогда никакая из подсхем $S_{21}, S_{22}, ..., S_{2\varkappa_2}$ не содержит контакт вида $\bar{z}$. Так как произвольная цепь схемы S, проходящая через подсхему S_2, не содержит контакт вида z вне подсхемы S_2, то каждая цепь подсхемы S_2 содержит контакт вида z. Это возможно только тогда, когда хотя бы в одной из подсхем $S_{2i_1}, S_{2i_2}, ..., S_{2i_{l_2}}$ существует сечение, состоящее сплошь из контактов вида z. Отсюда снова придем к противоречию с минимальностью схемы

S. Таким образом, только одна из подсхем $S_{21}, S_{22}, ..., S_{2\kappa_2}$ содержит контакт вида z. Допустим, таковой является подсхема S_{21}. При этом произвольная цепь схемы S, проходящая через подсхему S_{21}, не содержит контакт вида z вне подсхемы S_{21}. В частности, цепь A содержит контакты вида z только в подсхеме S_{21}. Продолжая процесс расчленения схемы S, убедимся, что цепь A содержит только один контакт вида z. Лемма доказана.

В доказательстве нижеследующей теоремы наряду с П-схемой S будем рассматривать соответствующую ей П-сеть и граф, сохранив за ними то же обозначение S. Множество контактов схемы S, которое соответствует циклу графа S, назовем циклом схемы. При этом под длиной цикла будем подразумевать в графе число ребер, в схеме — число контактов.

Теорема 5. Пусть $g(x_1, ..., x_n)$ — характеристическая функция произвольного (n, d)-кода мощности M, $d \geqslant 2$. Тогда

$$L^*_{\text{п}}(g(x_1, ..., x_n)) \geqslant d \cdot M^{d/n}.$$

Доказательство. Пусть S — минимальная П-схема, содержащая лишь ненулевые цепи и реализующая функцию $g(x_1, ..., x_n)$. Покажем, что схема S не содержит циклов длины, меньшей чем $2d$. Допустим, в схеме S существует цикл B длины, меньшей чем $2d$. П-схему S разложим на две ее подсхемы (которые соединены либо параллельно, либо последовательно) так, чтобы цикл B целиком содержался в одной из них. Подсхему, содержащую цикл B, также разложим на две подсхемы и рассмотрим ту, которая целиком содержит цикл B. Продолжая этот процесс, определим подсхему S_B схемы S, которая целиком содержит рассматриваемый цикл, и никакая ее подсхема уже целиком не содержит этот цикл. Очевидно, что полюсы подсхемы S_B принадлежат циклу B. Из леммы 3 следует, что длина (число контактов) произвольной цепи схемы S равна n и каждая цепь содержит контакт от каждой переменной. Отсюда, в свою очередь, следует, что длины всех цепей подсхемы S_B равны. Пусть эта длина равна κ так, что каждая цепь подсхемы S_B содержит по одному контакту от одних и тех же κ переменных функции $g(x_1, ..., x_n)$. Таким образом, длина цикла B равна 2κ. По предположению $2\kappa < 2d$, т. е. $\kappa < d$. Отметим, что две цепи схемы S, реализующие различные наборы (n, d)-кода, различаются видом контактов, по крайней мере, от d переменных. В силу того, что схема S не содержит нулевых цепей и $\kappa < d$, то цепи схемы S, проходящие через подсхему S_B и совпадающие вне S_B, реализуют один и тот же кодовый набор. Поэтому все цепи подсхемы S_B содержат контакты одного и того же вида. Тогда в схеме S подсхему S_B можно заменить одной из ее цепей так, что получаемая схема также реализует функцию $g(x_1, ..., x_n)$ и содержит меньшее число контактов, чем схема S. Это противоречит с условием минимальности схемы S. Таким образом, схема S не содержит циклов длины меньше чем $2d$.

Будем говорить, что множество циклов П-схемы (или соответствующей П-сети) образует цепочку циклов, если в схеме найдутся две цепи, которые вместе содержат все контакты всех циклов этого множества. Число циклов в цепочке циклов назовем длиной цепочки. Нетрудно убедиться в том, что если два цикла П-схемы принадлежат некоторой цепочке циклов, то они не имеют общих контактов.

Теперь оценим снизу число контактов схемы S. Цепи схемы S имеют длину n, а длина произвольного цикла этой схемы не меньше чем $2d$. Отсюда следует, что максимальная длина цепочки циклов в схеме S не больше чем n/d. Далее рассмотрим П-сеть, соответствующей П-схеме S. Для того чтобы оценить снизу число ребер П-сети S, предвари-

тельно от П-сети S перейдем к другой, связанной с ней, П-сети S' следующим образом. Рассмотрим ребра сети S. Очевидно, что через каждое ребро сети S проходит хотя бы одна цепь. Если все цепи сети S, проходящие через обе вершины рассматриваемого ребра, непременно проходят и через это ребро, то такое ребро исключается из сети путем склеивания его вершин в одну вершину. При этом, если одна из вершин ребра являлась полюсом сети S, то новая вершина становится полюсом. Продолжая указанный процесс удаления ребер сети S, получим сеть, в которой для каждого ребра существуют цепи, проходящие через обе вершины ребра, как содержащие это ребро, так и не содержащие его. Полученная сеть, которая, очевидно, является П-сетью, как раз является упомянутой сетью S'.

Очевидно, что между цепями (циклами) П-сети S и П-сети S' существует взаимно однозначное соответствие, сохраняющее цепочки циклов. Таким образом, число цепей и максимальная длина цепочки циклов сети S' совпадают соответственно с числом цепей и максимальной длиной цепочки циклов сети S. Вместе с тем нетрудно убедиться в том, что в П-сети S' длина максимальной цепи совпадает с длиной ее максимальной цепочки циклов. Как было показано, сеть S не содержит цепочек циклов длины больше чем n/d. Тем самым максимальная длина цепи сети S' сверху оценивается величиной n/d. Сеть S (или то же самое сеть S') содержит не менее M различных цепей (функция $g(x_1, ..., x_n)$ принимает значение единицы на M наборах значений переменных).

Теперь можно оценить число ребер П-сети S'. Пусть S' содержит R ребер. Каждая цепь сети S' задается последовательностью не более n/d ребер. Очевидно, что число таких последовательностей не превосходит $R^{n/d}$. А поскольку сеть S' содержит, по крайней мере, M различных цепей, то число ребер R сети S' удовлетворяет неравенству $R^{n/d} \geqslant M$. Отсюда $R \geqslant M^{d/n}$. В свою очередь, из определения П-сети S' (учитывая, что минимальный цикл П-сети S имеет длину не меньше чем $2d$) следует, что сеть S содержит, по крайней мере, в d раз больше ребер, чем сеть S'. Таким образом, в силу минимальности схемы S, получим

$$L^*_{\text{П}}(g(x_1, ..., x_n)) \geqslant d \cdot M^{d/n}.$$

Теорема доказана.

Приведем два конкретных примера применения доказанной теоремы.

1) Пусть $g_n(x_1, ..., x_n)$ — характеристическая функция $[n, \kappa]$-кода с $\kappa \geqslant c_1 n$ и $d \geqslant c_2 n$ (где c_1, c_2 — некоторые константы). Существование такого кода обеспечивается границей Варшамова—Гильберта (см., например, [4]). Тогда

$$L^*_{\text{П}}(g_n) \geqslant 2^{cn}, \quad \text{где } c = c_1 \cdot c_2.$$

Отметим, что эта оценка не является эффективной в том смысле, что групповая функция g_n не указывается в явном виде.

2) Пусть $g_n(x_1, ..., x_n)$ — характеристическая функция кода Рида—Маллера длины $n = 2^m$ и порядка $r = m/2$. В этом случае $d = \sqrt{n}$ и $M = 2^{n/2}$. Поэтому

$$L^*_{\text{П}}(g_n) \geqslant \sqrt{n} \cdot 2^{1/2\sqrt{n}}.$$

Теперь перейдем к оценке величины $\mu_{\text{П}}(n)$. Нетрудно убедиться, что $\mu_{\text{П}}(n) < 2^n$.

Имеет место следующая

Теорема 6. $\mu_{\text{П}}(n) \geqslant 2^{cn}$, где $c < 1$ — некоторая константа.

Доказательство. Пусть $g_n(x_1, ..., x_n)$ — групповая функция, которая была рассмотрена в примере 1. Для этой функции справедливо неравенство

$$L^*_{\Pi}(g_n) \geqslant 2^{c'n},$$

где $c' < 1$ — некоторая константа.

Вместе с этим из верхней оценки (4) следует, что произвольная групповая функция реализуется в классе П-схем со сложностью не больше чем n^3. Поэтому $L_{\Pi}(g_n) < n^3$.

Таким образом,

$$\mu_{\Pi}(n) \geqslant \frac{L^*_{\Pi}(g_n)}{L_{\Pi}(g_n)} \geqslant 2^{cn}.$$

Теорема доказана.

ЛИТЕРАТУРА

1. Яблонский С. В. Функциональные постронаия в к-значной логике. — Труды МИ АН СССР, 1958, вып. 51, с. 5.

2. Лупанов О. Б. О синтезе некоторых классов управляющих систем. — В сб.: «Проблемы кибернетики». М., Физматгиз, 1963, вып. 10, с. 63.

3. Васильев Ю. Л. О негрупповых плотно упакованных кодах. — В сб.: «Проблемы кибернетики». М., Физматгиз, 1962, вып. 8, с. 337.

4. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. М., Мир, 1976.

5. Малышев В. А. Класс «почти всех» функций с нелинейной сложностью при реализации П-схемами. — В сб.: «Проблемы кибернетики». М., Наука, 1967, вып. 19, с. 299.

6. Субботовская Б. А. О реализации линейных функций формулами в базисе &, V. — ДАН СССР, **136**, № 3, 553 (1961).

7. Храпченко В. М. Об одном методе получения нижних оценок сложности П-схем. Мат. заметки, **10**, № 1, 83 (1971).

8. Пулатов А. К. О геометрических свойствах и схемной реализации подгрупп в E^n. — В сб.: «Дискрет. анализ». Новосибирск, 1973, вып. 23, с. 32.

9. Пулатов А. К. Нижняя оценка сложности схемной реализации для одного класса кодов. — В сб.: «Дискрет. анализ». Новосибирск, 1974, вып. 25, с. 56.

10. Пулатов А. К. Влияние нулевых цепей на сложность П-схем.Тезисы докл. IV Всесоюз. конф. по преблемам теорет. кибернетики. Новосибирск, 1977, с. 175.

Институт математики СО АН СССР

[16/XI 1977]

О КОЛИЧЕСТВЕННЫХ ХАРАКТЕРИСТИКАХ ЛОГИЧЕСКИХ ФОРМУЛ

В. А. Таланов

В настоящее время в математике накопилось большое число работ, в которых при рассмотрении какого-либо свойства объектов из некоторой бесконечной совокупности оказывается, что почти все объекты обладают этим свойством. Например, почти все графы связны или почти все ориентированные графы имеют гамильтонов контур. Подобные эффекты наблюдаются и при изучении алгоритмов. Так, в задачах дискретной оптимизации случается, что какой-либо простой алгоритм получения допустимого решения почти всегда приводит к оптимальному решению или алгоритм поиска объекта с данным свойством почти всегда его находит. Естественно возникает вопрос осмысления такой ситуации.

При математической постановке задачи приходится формулировать средства для описания изучаемых свойств. Универсальным средством

описания является язык математической логики. При таком выборе средств описания центральным становится вопрос об отношении числа моделей данной логической формулы на множестве из n предметов к числу всех интерпретаций ее нелогических символов в этом множестве. Заметим сразу, что существенный прогресс в этой области касается пока только языков первого порядка. Интересные результаты исследования асимптотического поведения доли выполнимости формул узкого исчисления предикатов были получены Ю. В. Глебским и докладывались им на IV Международном математическом конгрессе в августе 1966 года. Эти результаты дали толчок новым исследованиям [1]—[4], проведенным Ю. В. Глебским и его учениками. Интерес к данной тематике проявляется и за рубежом. Укажем, например, работу [5], основные результаты которой непосредственно следуют из более ранних работ Ю. В. Глебского и М. И. Лиогонького. Цель настоящей статьи— дать краткий обзор имеющихся результатов.

1. Рассмотрим язык L предикатов первого порядка с равенством, множество σ нелогических символов которого состоит из конечного множества σ_p предикатных символов и счетного множества индивидных констант $a_1, a_2, \ldots$. Константу a_i интерпретируем как натуральное число i $(i=1,2,\ldots)$.

Множество всех нелогических символов формулы A в языке L будем обозначать через $\sigma(A)$, а множество ее предикатных символов через $\sigma_p(A)$.

Объемом выполнимости предложения A с индивидными константами $a_{j_1}, a_{j_2}, \ldots, a_{j_s}$ в области из n предметов $(n \geqslant s)$ называется величина $v_n(A)$, равная числу всех интерпретаций сигнатуры $\sigma_p(A)$, обращающих A в истину и заданных на произвольном множестве $U_n \subseteq \{1, 2, \ldots\}$, состоящем из n элементов и содержащем $j_1, j_2, \ldots, j_s$.

Долей выполнимости предложения A называется величина $\delta_n(A) = v_n(A)/v_n(A \vee > A)$.

Если $\sigma_p(A) = \{P_1, P_2, \ldots, P_s\}$, где P_i—κ_i-местный предикат, то, очевидно, $v_n(A \vee > A) = 2^{n^{\kappa_1} + n^{\kappa_2} + \cdots + n^{\kappa_s}}$.

Для произвольной формулы A с индивидными переменными $x_1, x_2, \ldots, x_r$ нормальной долей выполнимости называется величина $\gamma_n(A) = \delta_n\left(A_{x_1, x_2, \ldots, x_r}^{b_1, b_2, \ldots, b_r}\right)$, где $b_1, b_2, \ldots, b_r$ — различные константы, отличные от всех констант формулы A, а $A_{x_1, x_2, \ldots, x_r}^{b_1, b_2, \ldots, b_r}$ — результат подстановки констант $b_1, b_2, \ldots, b_r$ в формулу A вместо $x_1, x_2, \ldots, x_r$ соответственно.

Очевидно, что для любой замкнутой формулы A $\delta_n(A) = \gamma_n(A)$. Отметим некоторые очевидные свойства величины $\delta_n(A)$.

Пусть A — формула с индивидными переменными $x_1, \ldots, x_r$ и B — формула с индивидными переменными $y_1, \ldots, y_t$; $b_1, b_2, \ldots, b_r$; $c_1, c_2, \ldots, c_t$— произвольные константы

1.1. Если $\models A \longrightarrow B$, то $\delta_n\left(A_{x_1 x_2 \cdots x_r}^{b_1 b_2 \cdots b_r}\right) \leqslant \delta_n\left(B_{y_1 y_2 \cdots y_t}^{b_1 b_2 \cdots b_t}\right)$.

1.2. Если $\models A \equiv B$, то $\delta_n\left(A_{x_1 x_2 \cdots x_r}^{b_1 b_2 \cdots b_r}\right) = \delta_n\left(B_{y_1 y_2 \cdots y_t}^{b_1 b_2 \cdots b_t}\right)$.

1.3. $\delta_n\left(> A_{x_1 x_2 \cdots x_r}^{b_1 b_2 \cdots b_r}\right) = 1 - \delta_n\left(A_{x_1 x_2 \cdots x_r}^{b_1 b_2 \cdots b_r}\right)$.

1.4. Если $\models \neg (A \,\&\, B)$, то $\delta_n\left(A_{x_1 x_2 \cdots x_r}^{b_1 b_2 \cdots b_r} \vee B_{y_1 y_2 \cdots y_t}^{c_1 c_2 \cdots c_t}\right) =$

$$=\delta_n\left(A^{b_1 b_2 \cdots b_r}_{x_1 x_2 \cdots x_r}\right)+\delta_n\left(B^{c_1 c_2 \cdots c_t}_{y_1 y_2 \cdots y_t}\right).$$

1.5. $\delta_n\left(A^{b_1 b_2 \cdots b_r}_{x_1 x_2 \cdots x_r}\right) \leqslant \delta_n\left(A^{b_1 b_2 \cdots b_r}_{x_1 x_2 \cdots x_r} \vee B^{c_1 c_2 \cdots c_t}_{y_1 y_2 \cdots y_t}\right) \leqslant$

$$\leqslant \delta_n\left(A^{b_1 b_2 \cdots b_r}_{x_1 x_2 \cdots x_r}\right)+\delta_n\left(B^{c_1 c_2 \cdots c_t}_{y_1 y_2 \cdots y_t}\right).$$

1.6. Если A и B не содержит общих предикатных символов, т. е. $\sigma(A) \cap \sigma(B)=\varnothing$, то $\delta_n\left(A^{b_1 b_2 \cdots b_r}_{x_1 x_2 \cdots x_r} \& B^{c_1 c_2 \cdots c_t}_{y_1 y_2 \cdots y_t}\right) =$

$$=\delta_n\left(A^{b_1 b_2 \cdots b_r}_{x_1 x_2 \cdots x_r}\right) \cdot \delta_n\left(B^{c_1 c_2 \cdots c_t}_{y_1 y_2 \cdots y_t}\right).$$

1.7. Если A имеет вид $p(x_1, x_2, \ldots, x_\kappa)$, где p — κ-местный предикатный символ, то $\delta_n\left(A^{b_1 b_2 \cdots b_\kappa}_{x_1 x_2 \cdots x_\kappa}\right)=\frac{1}{2}$.

2. Ниже сделаем набросок доказательства того, что для любого предложения A в языке L существует $\lim\limits_{n \to \infty} \delta_n(A)$, и если A не содержит индивидных констант и нульместных предикатов, то этот предел равен нулю или единице.

Введем два определяемых символа $\forall^{\cdot}$ и $\exists^{\cdot}$ — исключающие кванторы общности и существования соответственно. Выражения $\forall^{\cdot} xA$ и $\exists^{\cdot} xA$ будем считать сокращениями формул $\forall x(\mathop{\&}\limits_{i=1}^{\kappa}(x \neq y_i) \rightarrow A)$ и $\exists x(\mathop{\&}\limits_{i=1}^{\kappa}(x \neq y_i) \& A)$ соответственно, где A — формула и $x, y_1, y_2, \ldots, y_\kappa$ — список всех ее свободных переменных.

Выражения, являющиеся сокращениями формул языка L и не содержащие обычных кванторов, будем называть Г-формулами.

Поскольку

$$\models \forall xA \equiv \forall^{\cdot} xA \,\&\, \mathop{\&}\limits_{i=1}^{\kappa} A_x^{y_i} \quad \text{и} \quad \models \exists xA \equiv \exists^{\cdot} xA \vee \mathop{\vee}\limits_{i=1}^{\kappa} A_x^{y_i}, \qquad (1)$$

то для любой формулы языка L существует эквивалентная ей Г-формула.

Пусть $\{\alpha_n\}$ — последовательность действительных чисел. Будем говорить, что α_n стремится к a с геометрической скоростью и писать $\alpha \longrightarrow\!\!\!\!\rightarrow a$, если существует θ $(0 \leqslant \theta < 1)$ и натуральное N, что $\forall n > N$ $|\alpha_n - a| < \theta^n$.

В дальнейшем будет использовано следующее свойство таких последовательностей.

2.1. Если $\alpha_n \longrightarrow\!\!\!\!\rightarrow 0$, то $n \cdot \alpha_n \longrightarrow\!\!\!\!\rightarrow 0$.

Отметим также, что для любых формул A и B с исключающими кванторами справедливы утверждения:

2.2. Если $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 0$ и $\gamma_n(B) \longrightarrow\!\!\!\!\rightarrow 0$, то $\gamma_n(A \vee B) \longrightarrow\!\!\!\!\rightarrow 0$.

2.3. Если $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 1$ и $\gamma_n(B) \longrightarrow\!\!\!\!\rightarrow 1$, то $\gamma_n(A \,\&\, B) \longrightarrow\!\!\!\!\rightarrow 1$.

2.4. Если $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 1$ или $\gamma_n(B) \longrightarrow\!\!\!\!\rightarrow 1$, то $\gamma_n(A \vee B) \longrightarrow\!\!\!\!\rightarrow 1$.

2.5. Если $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 0$ или $\gamma_n(B) \longrightarrow\!\!\!\!\rightarrow 0$, то $\gamma_n(A \,\&\, B) \longrightarrow\!\!\!\!\rightarrow 0$.

2.6. Если $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 0$, то $\gamma_n(\neg A) \longrightarrow\!\!\!\!\rightarrow 1$.

2.7. $\gamma_n(\exists^{\cdot} xA) \leqslant n \cdot \gamma_n(A)$.

2.8. Если $\gamma_n(\forall^{\cdot} xA) \longrightarrow\!\!\!\!\rightarrow 0$ и $\gamma_n(B) \longrightarrow\!\!\!\!\rightarrow 0$, то $\gamma_n(\forall^{\cdot} x(A \vee B)) \longrightarrow\!\!\!\!\rightarrow 0$.

2.9. Если $\gamma_n(\exists^{\cdot} xA) \longrightarrow\!\!\!\!\rightarrow 1$ и $\gamma_n(B) \longrightarrow\!\!\!\!\rightarrow 1$, то $\gamma_n(\exists^{\cdot} x(B \,\&\, C)) \longrightarrow\!\!\!\!\rightarrow 1$.

Теорема 1. Для всякой Г-формулы A без свободных атомарных частей и 0-местных предикатов $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 0$ или $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 1$.

Доказательство можно провести индукцией по числу исключающих кванторов в формуле A.

При $m=1$ A имеет вид $\forall^{\cdot} xB$ или $\exists^{\cdot} xB$, где B — бескванторная формула и в каждую атомарную часть ее входит x. Непосредственным подсчетом можно показать, что

$$\gamma_n(\forall^{\cdot} xB) = \begin{cases} 1, & \text{если } |= B \\ 0 & \text{в противном случае} \end{cases} \quad \text{и} \quad \gamma_n(\exists^{\cdot} xB) = \begin{cases} 0, & \text{если } |= \neg B, \\ 1 & \text{в противном случае.} \end{cases}$$

Пусть для Г-формул с числом кванторов $\leqslant m$ утверждение теоремы справедливо и рассмотрим Г-формулу A с числом кванторов $m+1$. Если A имеет вид $B \vee C$, $B \& C$ или $\neg B$, то утверждение теоремы следует из 2.2—2.6. Поэтому достаточно рассмотреть формулы вида $\forall^{\cdot} xB$ и $\exists^{\cdot} xB$. Остановимся на формуле $\exists^{\cdot} xB$. Используя технику пронесения кванторов, формулу B можно привести к виду $\bigvee\limits_{i=1}^{s} C_i D_i$, где C_i — бескванторные формулы, все атомарные части которых зависят от x, а формулы D_i не содержат свободных атомарных частей и в каждую из них входит не более m исключающих кванторов. По предположению индукции утверждение теоремы справедливо для всех D_i. Рассмотрим два случая.

а) Для всех $i \in \{1, 2, ..., s\}$ $|= C_i$ или $\gamma_n(D_i) \longrightarrow\!\!\!\!\rightarrow 0$.

б) Существует $i_0 \in \{1, 2, ..., s\}$, что $|= C_{i_0}$ и $\gamma_n(D_{i_0}) \longrightarrow\!\!\!\!\rightarrow 1$.

В первом случае, используя последовательно 2.7, 1.5 и 2.1, имеем

$$\gamma_n(A) = \gamma_n(\exists^{\cdot} xB) \leqslant n \cdot \gamma_n\Big(\bigvee_{i=1}^{s} C_i D_i\Big) \leqslant n \sum_{i=1}^{s} \gamma_n(C_i D_i) \longrightarrow\!\!\!\!\rightarrow 0.$$

Во втором случае, используя 1.5 и 2.9, получаем

$$\gamma_n(A) = \gamma_n(\exists^{\cdot} xB) \geqslant \gamma_n(\exists^{\cdot} x C_{i_0} D_{i_0}) \longrightarrow\!\!\!\!\rightarrow 1.$$

Доказательство для формул вида $\forall^{\cdot} xB$ получается переходом к отрицанию. Теорема доказана.

Теорема 2. (0 «0 или 1»). Для всякого предложения A в языке L, не содержащего констант и нульместных предикатных символов, $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 0$ или $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow 1$.

Доказательство. Построим сначала предваренную нормальную форму для A, а затем, используя (1), заменяем все кванторы, начиная с внутреннего, исключающими. После таких преобразований придем к Г-формуле, эквивалентной A и удовлетворяющей теореме 1.

Теорема 3. Для всякого предложения A в языке L существуют неотрицательные целые числа l и s такие, что $\gamma_n(A) \longrightarrow\!\!\!\!\rightarrow \frac{l}{2^s}$.

Доказательство. Как и в доказательстве теоремы 2, строим эквивалентную формуле A Г-формулу B, однако теперь в B могут входить свободные атомарные части. Вынося их за знаки кванторов, можно получить формулу D, эквивалентную формуле A, имеющую вид

$$\bigvee_{i=1}^{d} q_1^{\sigma_1^i} q_2^{\sigma_2^i} \cdots q_t^{\sigma_t^i} B_i,$$

где $q_1, q_2, ..., q_t$ — атомарные формулы, $\sigma_j^i = 0$ или 1, а B_i — формулы, удовлетворяющие условиям теоремы 1. Непосредственный подсчет по-

казывает, что $\gamma_n(A)=\gamma_n(\bigvee_{i=1}^{d} q_1^{\sigma_1^i} q_2^{\sigma_2^i} \cdots q_t^{\sigma_t^i} B_i) = \sum_{i=1}^{d} \frac{1}{2^t}\gamma_n(B) =$

$= \frac{1}{2^t}\sum_{i=1}^{d}\gamma_n(B_i) = \frac{l}{2^s}$, где $l=\sum_{i=1}^{d}\gamma_n(B_i)$, $s=t$.

Если через T обозначить множество всех предложений A в языке L, для которых $\gamma_n(A)\longrightarrow 1$, то из теоремы 2 следует

Теорема 4. T — полная, разрешимая теория в сигнатуре σ_p.

3. В работе [2] и позднее в [5] рассмотрен вопрос об аксиоматическом задании теории T. Чтобы описать систему аксиом, отличную от всей теории, введем некоторые определения [6].

Пусть $X=\{x_1, x_2, ..., x_m\}$ — конечное множество, состоящее из m различных индивидных переменных. Полным открытым описанием $M(x_1, x_2, ..., x_m)$ назовем формулу $\&_{\Phi\in A}\Phi$, где A — множество формул вида $p(z_1, z_2, ..., z_m)$ или $\neg p(z_1, z_2, ..., z_m)$ $(p\in\sigma_p, z_i\in X)$, причем для каждого $p\in\sigma_p$ и каждого набора $<z_1, z_2, ..., z_m>\in X^m$ в A входит либо $p(z_1, z_2, ..., z_m)$, либо $\neg p(z_1, z_2, ..., z_m)$. Полное открытое описание $N(x_1, x_2, ..., x_m, y)$, где y — новая переменная, называется расширением полного открытого описания $M(x_1, x_2, ..., x_m)$, если каждый сомножитель из M содержится в N.

Как следует из работ [2] и [5], множество формул вида

$$\forall^{\cdot} x_1\, \forall^{\cdot} x_2 \cdots \forall^{\cdot} x_m (M(x_1, x_2, ..., x_m)\longrightarrow \exists^{\cdot} y N(x_1, x_2, ..., x_m, y))$$

является системой аксиом для теории T.

Изучая вероятностные меры на исчислении предикатов, Гайфман [6] строит меру $\mu(A)$ следующим образом:

1) Если A — атомарное предложение, то $\mu(A)=q$ $(0<q<1)$.

2) Если $A=\&_{i=1}^{s} A_i \,\&\, \&_{i=s+1}^{t}\neg A_i$, где A_i — атомарные предложения, то $\mu(A)=q^s(1-q)^{t-s}$.

3) $\mu(a_i=a_j)=0$, если a_i и a_j — различные константы.

4) Если A имеет вид $\exists x B$, то $\mu(A)=\sup\{\mu(\bigvee_{i=1}^{n} B_x^{a_i}) \mid i\in U_n\}$, где supremum берется по всевозможным n-подмножествам $U_n\subseteq\{1, 2, ...\}$.

В [6] показано, что строящаяся таким образом функция μ индуцирует единственную меру на исчислении предикатов, и что для любого предложения A $\mu(A)=0$ или 1. Из результатов работ [6] и следует, что множество предложений A, для которых $\mu(A)=1$, совпадает с T.

4. Рассмотрим вопросы, связанные с асимптотическим поведением доли выполнимости предложения по неизоморфным моделям.

Пусть A — предложение языка L, не содержащее констант и 0-местных предикатов. Через $\nu_n(A)$ обозначим отношение числа попарно неизоморфных интерпретаций сигнатуры $\sigma(A)$, обращающих A в истину, в универсе из n предметов к числу всех попарно неизоморфных интерпретаций сигнатуры $\sigma(A)$.

Карнап [7] доказал, что если $\sigma(A)$ состоит только из одноместных предикатов, то $\lim_{n\to\infty}\nu_n(A)$ существует и равен нулю или единице. В [2] и [5] доказана

Теорема 5. Для любого предложения A в языке L, не содержащего констант и нульместных предикатов $\lim_{n\to\infty}\nu_n(A)$, существует и равен $\lim_{n\to\infty}\gamma_n(A)$.

В случае, когда $\sigma(A)$ состоит только из одноместных предикатов, теорема 5 является следствием результата о том, что число s-наборов

$<x_1, x_2, ..., x_s>$ целых x_i, таких, что $x_1+x_2+\cdots+x_s=a$ и $0\leqslant x_i\leqslant a$ есть биномиальный коэффициент C_{a+s-1}^{s-1}.

В случае, когда $\sigma(A)$ содержит, по крайней мере, один более чем одноместный предикат, доказательство теоремы 5 основывается на следующем.

Пусть S — конечное множество предикатных символов, среди которых есть, по крайней мере, один неодноместный, $a_n(S)$ — число всех n-интерпретаций сигнатуры S, $b_n(S)$ — число попарно неизоморфных n интерпретаций, тогда $n!b_n(S)/a_n(S)\longrightarrow 1$ при $n\longrightarrow\infty$. Этот результат доказан в [8] в случае, когда S состоит из одного двухместного предиката в [9], в случае, когда S состоит из r-местных предикатов при фиксированном $r\geqslant 2$, и, наконец, в [2] утверждение доказано в общем случае.

5. Рассмотрим теперь некоторые результаты [4] об условной доле выполнимости логических формул.

Пусть A — предложение в сигнатуре σ и B — предложение в сигнатуре σ_p.

Долей выполнимости предложения B при условии выполнимости предложения A в области из n предметов называется величина $\delta_n(B/A)=v_n(B\,\&\,A)/v_n(A)$, где объемы выполнимости вычисляются относительно сигнатуры $\sigma(A\,\&\,B)$. Если для некоторого n $v_n(A)=0$, по определению считаем $\delta_n(B/A)=\dfrac{1}{2}$.

Пусть C_A — спектр предложения A, т. е. множество тех n, для которых $v_n(A)\neq 0$, и L' — множество предложений сигнатуры σ, для которых спектр бесконечен.

Если $\lim\limits_{n\to\infty}\gamma_n(A)=1$, то, очевидно, $\lim\limits_{n\to\infty}\delta_n(B/A)$ существует и равен $\lim\limits_{n\to\infty}\delta_n(B)$, поэтому рассматриваем предложения из L, для которых $\lim\limits_{n\to\infty}\delta_n(A)=0$.

Теорема 6. Если в σ_p входит хотя бы один более чем одноместный предикат, то не существует алгоритма, определяющего для произвольных предложений $A\in L'$ и $B\in L$, существует ли $\lim\limits_{n\to\infty}\delta_{n\in C_A}(B/A)$. Следующий пример [5] покажет, что предел последовательности $\delta_n(B/A)$ может не существовать. Пусть $A=\forall x\exists!\, y(x\neq y\,\&\,p(x,y)\,\&\,p(y,x))$, $B=\exists z(\forall x\neq z)(\exists!\, y\neq z)(x\neq y\,\&\,p(x,y)\,\&\,p(y,x))$. Тогда

$$\delta_n(A/A\vee B)=\begin{cases}0, & \text{если } n \text{ нечетно,}\\ 1 & \text{в противном случае.}\end{cases}$$

Пусть T_A — множество предложений B в сигнатуре σ, для которых $\lim\limits_{n\to\infty}\delta_n(B/A)=1$. В [4] доказано, что T_A является теорией. Чтобы T_A была полной, достаточно, чтобы для любого предложения B вида $\forall^* xC$, где C без кванторов и атомарных предложений, $\delta_n(B/A)\longrightarrow\to 1$ или $\delta_n(\neg B/A)\longrightarrow\to 1$. Если при этом совокупность предложений B указанного вида, для которых $\delta_n(B/A)\longrightarrow\to 1$ рекурсивна, то T_A — полная, разрешимая теория. В работах [4] и [5] имеется ряд примеров формул A, для которых T_A является полной разрешимой теорией. В частности, если предложение A не тождественно ложно, не содержит более чем одноместных предикатов и предиката равенства и имеет вид $\forall x\,C_0\,\&\exists x\,C_1\,\&\cdots\&\exists x\,C_s$, то T_A — полная, разрешимая теория.

В заключение приведем теорему, которая полностью решает вопрос о поведении $\delta_n(B/A)$ в случае, когда A сингулярно.

Теорема 7. [4]. Пусть A — сингулярное предложение без равенства. Тогда 1) для любого предложения B в языке L существует $\lim\limits_{n\to\infty}\delta_n(B/A)$, 2) совокупность возможных значений предела величины $\delta_n(B/A)$ для различных предложений B, не содержащих индивидных констант, конечна, 3) $\lim\limits_{n\to\infty}\delta_n(B/A)$ эффективно вычислим.

Пример. Пусть $A=\forall x\forall y(p(x)\longrightarrow p(y))$, где p — одноместный предикатный символ, тогда

$$\delta_n(B/A)=\begin{cases}0, & \text{если } B\,\&\forall x\,p(x) \text{ и } B\,\&\forall x\neg p(x) \text{ не имеет модели мощности } n.\\ 1, & \text{если } B\,\&\forall x\,p(x) \text{ и } B\,\&\forall x\neg p(x) \text{ имеют модель мощности } n.\\ \frac{1}{2} & \text{в противном случае.}\end{cases}$$

ЛИТЕРАТУРА

1. Глебский Ю. В., Коган Д. И., Лиогонький М. И., Таланов В. А. Объем и доля выполнимости формул узкого исчисления предикатов. «Кибернетика», № 2, 17 (1969).

2. Лиогонький М. И. К вопросу о количественных характеристиках логических формул. «Кибернетика», № 3, 16 (1969).

3. Лиогонький М. И. Об одном свойстве аксиомы эквивалентности в исчислении предикатов первого порядка. Учен. зап. ГГУ. Сер. мат., мех., 1969, вып. 105, с. 17.

4. Лиогонький М. И. Об условной доле выполнимости логических формул. Мат. зам. АН СССР, **6**, № 6, 651 (дек. 1969).

5. Faqin R. Probabieities on finite models. The Journal of Symbolic Logic, v. 41, N 1, March 1976, p. 50.

6. Gaifman H., Concerning Measures in Ferst Order Calculi, Israel Jornal of Mathematics, v. 2, 1964, p. 1.

7. Carnap R. Logical foundations of probability University of Chicago Press, Chicago, 1950.

8. Harary F. Hote on Carnaps relational asymptotic relative frequencies. The Journal, ot Symbolic Loguc, v. 23, 1958, p. 257.

9. Oberschelp W., Struktur zahlen in endlichen Relationssystemen, Contributions to Mathematical Logic (Proceedings of Logic Colloquium), Hannover, 1966, p. 199.

Горьковский государственный университет

[12/VII 1977]

ОБ ОДНОМ ОБОБЩЕНИИ ЗАДАЧИ О НАЗНАЧЕНИЯХ

В. А. Таланов, В. Н. Шевченко

1. Пусть $N=\{1,\ldots,n\}$ — множество работ, каждая из которых должна быть выполнена в точности одним исполнителем из множества $M=\{1,\ldots,m\}$; $I_j\subseteq M$ — множество исполнителей, которые могут делать j-ю работу ($j\in N$); числом C_{ij} измеряется польза от назначения i-го исполнителя на j-ю работу ($i\in M$, $j\in N$). Под задачей о назначениях понимают задачу нахождения таких $i_j\in I_j$, различных для различных j при которых максимизируется $f=\sum\limits_{j\in N} c_{i_j j}$.

Рассмотрим теперь ситуацию, в которой условие $j\neq l\longrightarrow i_j\neq i_l$ перестает быть обязательным, и можно, если это сулит существенное увеличение значения f, пойти κ раз на его нарушение, т. е. допустить κ

совместительств. Уточним, что если $\Gamma_\nu=\{j/i_j=\nu\}$ — множество работ, на которые назначен ν-й исполнитель (в частности может быть, что $\Gamma_\nu=\varnothing$), а y_ν — мощность Γ_ν, то число совместительств считаем равным $\sum\limits_{\nu\in M}\max\{0,(y_\nu-1)\}$. Задачу нахождения таких $i_j\in I_j(j\in N)$, при которых максимизируется $f=\sum\limits_{j\in N}c_{i_jj}$ и выполняется условие

$$\sum_{\nu\in M}\max\{0,(y_\nu-1)\}\leqslant\kappa,$$

назовем обобщенной задачей о назначениях (ОЗН). Очевидно, что при $\kappa=0$ получится задача из предыдущего абзаца.

2. Для каждого $j\in N$ положим $d_{ij}=1$ при $i\in I_j$ и $d_{ij}=0$ при $i\overline{\in}I_j$. Введем целочисленные переменные x_{ij} ($x_{ij}=1$, если i-го исполнителя назначают на j-ю работу, и $x_{ij}=0$ в противном случае) и $z_i=\max\{0,(y_i-1)\}$. Тогда ОЗН нетрудно записать в виде следующей задачи целочисленного линейного программирования:

$$\begin{gathered}
\sum_{i\in M,\ j\in N}c_{ij}x_{ij}\longrightarrow\max,\\
\sum_{i\in M}x_{ij}=1\quad(j\in N),\\
\sum_{j\in N}x_{ij}-y_i=0\quad(i\in M),\\
0\leqslant x_{ij}\leqslant d_{ij}\quad(i\in M,\ j\in N),\qquad(1)\\
y_i-1\leqslant z_i\quad(i\in M),\\
\sum_{i\in M}z_i\leqslant\kappa,\\
z_i\geqslant 0;\\
x_{ij},y_i,z_i\quad(i\in M,j\in N)\ —\ \text{целые}.
\end{gathered}$$

Очевидно, что переменные y_i могут быть исключены и ограничения (1) эквивалентны следующим:

$$\begin{gathered}
\sum_{i\in M}x_{ij}=1\quad(j\in N),\\
-z_i+\sum_{j\in N}x_{ij}\leqslant 1\quad(i\in M),\\
\sum_{i\in M}z_i\leqslant\kappa,\qquad(2)\\
0\leqslant x_{ij}\leqslant d_{ij}\quad(i\in M,\ j\in N),\\
z_i\geqslant 0\quad(i\in M),\\
x_{ij},\ z_i\quad(i\in M,\ j\in N)\ —\ \text{целые}.
\end{gathered}$$

Теорема. Пусть M_κ — множество векторов, удовлетворяющих системе ограничений (2). Если $M_\kappa\neq\varnothing$ и числа κ и d_{ij} ($i\in M$, $j\in N$) целые, то любая крайняя точка множества M_κ целочислена.

Для доказательства перепишем ограничения (3) в следующем виде:

$$\begin{gathered}
\sum_{i\in M}x_{ij}=1\quad(j\in N),\\
\sum_{j\in N}x_{ij}+u_i=z_i+w_i\quad(i\in M),\\
\sum_{i\in M}z_i\leqslant\kappa,\qquad(3)\\
0\leqslant x_{ij}\leqslant d_{ij}\quad(i\in M,\ j\in N),\\
z_i\geqslant 0,\quad u_i\geqslant 0,\quad w_i=1\quad(i\in M).
\end{gathered}$$

Переменные системы (3) проинтерпретируем как величины потока на дугах сети с узлами $A, B, C_1, C_2, ..., C_m, E_1, E_2, ..., E_n, F$. Эта сеть описывается следующей таблицей:

Дуга	Нижняя пропускная способность	Верхняя пропускная способность	Интерпретация величины потока
AB	0	κ	$\sum_{i \in M} z_i$
AC_i	1	1	w_i $(i \in M)$
BC_i	0	∞	z_i $(i \in M)$
C_iF	0	∞	w_i $(i \in M)$
C_iE_j	0	d_{ij}	x_{ij} $(i \in M, j \in N)$
E_jF	1	1	$\sum_{i \in M} x_{ij} (j \in N)$

Теперь доказываемое утверждение можно вывести из теоремы о целочисленности потока [1].

В заключение заметим, что потоковая интерпретация решает и вопрос о необходимых и достаточных условиях совместности системы (1).

ЛИТЕРАТУРА

1. Форд Л. П., Фалкерсон Д. Р. Потоки в сетях. М., Мир, 1966.

Горьковский государственный университет

[11/XI 1977]

ПРЕДСТАВЛЕНИЕ И РАСПОЗНАВАНИЕ ТРИАНГУЛИРОВАННЫХ ГРАФОВ

В. В. Усанов

В настоящей работе рассматриваются только конечные неориентированные графы без петель и кратных ребер; все не определяемые нами понятия могут быть найдены в [1].

Сложность алгоритмической обработки информации, представленной в виде графов, во многом зависит от способа задания графов. Так, для задания n-вершинного графа матрицей смежности требуется $\sim n^2$ двоичных символов. Другой универсальный способ задания графов — представление их системой множеств произвольной природы (граф пересечений системы множеств есть граф, вершинами которого служат сами множества, и вершины смежны тогда и только тогда, когда соответствующие множества имеют непустое пересечение). Известно, что любой граф L является графом пересечений $L(\Omega)$ некоторой системы множеств $\Omega = \{M_1, M_2, ..., M_n\}$ $(\bigcup_{i=1}^{n} M_i = M)$. В этом случае, если $|M| = \kappa$, то для задания графа пересечений требуется $\sim \kappa \cdot n$ двоичных символов (так как множество M_i задается κ-мерным вектором $(\alpha_1, \alpha_2, ..., \alpha_\kappa)^T$, где $\alpha_i = 1$, если i-й элемент принадлежит M_i и нулю в

противном случае). Ясно, что при $\kappa < n$ представление графа системой множеств может быть экономнее, нежели матрицей смежности.

Возникает вопрос о построении такой системы множеств Ω, для которой число κ наименьшее. В худшем случае, как показано в [2], для графа L лишь в множествах M с $\kappa \geqslant \left[\frac{n^2(L)}{4}\right]$ существуют системы подмножеств, графы пересечений которых изоморфны L. Однако для некоторых классов графов и специфических систем множеств удается эту оценку улучшить. В данной работе рассматривается один из таких классов — триангулированные графы (в дальнейшем T-графы)*.

T-графы — весьма обширный класс (например, графы интервалов [1] образуют его собственный подкласс), тем не менее для него в [3] получены эффективные алгоритмы решения задач о максимальном независимом множестве и о раскраске. T-графы изучались в [4] в связи с решением систем линейных уравнений с симметричной положительно определенной матрицей, большинство элементов которой — нули, и в [5] в связи с исследованиями в области генетики.

Основной результат настоящей работы показывает, что любой T-граф может быть представлен такой системой множеств, для которой $\kappa \leqslant n$.

Работа состоит из четырех разделов. В первых трех доказывается основной результат, в четвертом описывается алгоритм распознавания T-графов и оценивается его сложность.

Автор выражает глубокую благодарность В. Е. Алексееву, под руководством которого была выполнена эта работа, и А. А. Маркову за большую помощь при написании статьи.

1. ПРЕДВАРИТЕЛЬНЫЕ УТВЕРЖДЕНИЯ

Определение 1. Подмножество вершин дерева, порождающее связный подграф, назовем фрагментом. Дерево с выделенной на нем системой фрагментов назовем деревом фрагментов.

Определение 2. Граф $L=(X, U)$ называется графом фрагментов, если существует дерево D и такая система Ω фрагментов на нем, что граф пересечений $L(\Omega)$ изоморфен L.

Определение 3 ([4]). Разделяющее множество графа $L=(X, U)$ есть подмножество $S \subset X$ такое, что подграф $L(X|S)$ состоит из двух компонент связности. Минимальное разделяющее множество есть разделяющее множество, никакое подмножество которого не является разделяющим множеством.

Определение 4 ([5]). Вершина графа, окружение которой есть полный подграф, называется симплициальной.

Лемма 1 ([4]). Минимальное разделяющее множество в T-графе порождает полный подграф.

Доказательство. Пусть S — минимальное разделяющее и C_1, C_2 — компоненты $L(X|S)$. Так как S минимально, то каждая $s \in S$ смежна с некоторой вершиной в C_1 и с некоторой вершиной в C_2. Пусть $x, y \in S$ и пусть μ_i — кратчайшие цепи вида

$$[x\, c_{i1}\, c_{i2} \ldots c_{ip_i}\, y], \quad i=1,2,$$
$$c_{1j} \in C_1,$$
$$c_{2j} \in C_2.$$

* Граф L триангулирован, если для любого цикла $\mu=[x_1 x_2 \ldots x_l\, x_1]$ длины $l>3$ существует ребро L, соединяющее две несмежные вершины μ. Такие ребра называют хордами цикла.

Цикл, содержащий x и y, образованный μ_1 и μ_2, имеет длину $l \geqslant 4$, и единственно возможная хорда в нем — ребро $\{x, y\}$. Ввиду произвольности выбора $x, y \in S$, утверждение леммы доказано.

Лемма 2. Пусть L_n — полный n-вершинный граф и на дереве D ему соответствует система фрагментов $\Omega = \{M_1, M_2, ..., M_n\}$. Тогда

$$\bigcap_{i=1}^{n} M_i \neq \varnothing \text{ *}.$$

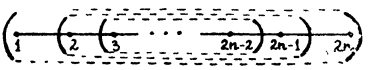


Рис. 1

Доказательство проведем индукцией по n. При $n=2$ утверждение совпадает с определением графа фрагментов. Пусть оно верно для $n-1$, т. е. при некотором изоморфизме на дереве D вершинам L_{n-1} соответствует система фрагментов $\Omega = \{M_1, M_2, ..., M_{n-1}\}$, имеющих множество общих вершин $\Sigma = \{\xi_1, \xi_2, ..., \xi_\kappa\}$. Добавим n-ю вершину в граф фрагментов и рассмотрим соответствующий ей на дереве D фрагмент M_n. Обозначим $N_i = M_n \cap M_i$ $(i = \overline{1, n-1})$. Так как по условию леммы L_n—полный, то $N_i \neq \varnothing$ $(i = \overline{1, n-1})$. Если все $N_i (i = \overline{1, n-1})$ совпадают, то лемма доказана. Пусть существуют $N_\kappa \neq N_l$ и $x \in N_\kappa$, $y \in N_l$ $(x \neq y)$. Очевидно, общая вершина n фрагментов должна принадлежать Σ. Предположим противное, т. е. пусть $\xi_j \overline{\in} M_n$ $(\forall j = \overline{1, \kappa})$. Тогда, пользуясь связностью M_κ и M_l, соединим некоторую вершину $\xi_j \in \Sigma$ с x цепью S_κ через M_κ и с y цепью S_l через M_l. С другой стороны, $x, y \in M_n$, и, значит, существует цепь S_n в M_n, соединяющая их. Но в дереве любые две вершины можно соединить лишь одной цепью, мы же построим две ($x S_\kappa \xi_j S_l y$ и $x S_n y$) несовпадающие цепи ($\xi_j \overline{\in} M_n$ по предположению), следовательно D не может быть деревом. Полученное противоречие говорит о том, что наше предположение неверно и существует $\xi_v \in M_n$, а значит, и $\xi_v \in \bigcap_{i=1}^{n} M_i$, что и требовалось доказать.

Лемма 3. Либо T-граф полный, либо в нем существует по крайней мере две несмежные симплициальные вершины. Доказательство проведем индукцией по числу вершин T-графа. Для $n=2$ утверждение очевидно. Пусть оно верно для всех T-графов с числом вершин $\leqslant n$. Покажем, что оно верно и для $(n+1)$-вершинного T-графа L (рис. 2).

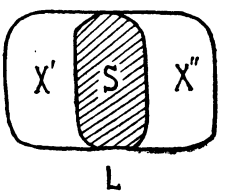


Рис. 2

Если L — полный граф, то лемма доказана. Пусть L не является полным графом. По лемме 1 минимальное разделяющее множество S в L порождает полный подграф $L(S)$.

* Заметим, что для полного графа всегда существует хотя бы одно дерево фрагментов, соответствующее ему, в частности, такое, как на рис. 1.

Рассмотрим подграф $L_1=L(X'\cup S)$. У него вершин $\leqslant n$, поэтому, по предположению, либо он является полным, либо в нем существуют две несмежные симплициальные вершины. В первом случае всякая вершина из X' симплициальная, во втором — хотя бы одна симплициальная вершина принадлежит X', так как в S все вершины попарно смежны.

Проводя аналогичные рассуждения для $L_2=L(X''\cup S)$, получим, что хотя бы одна вершина из X'' симплициальная.

Если заметить теперь, что никакие вершины $i\in X'$ и $j\in X''$ несмежны и окружение всякой вершины в $L(X')$ ($b\,L(X'')$) является ее окружением и в L, то ясно, что в L существует по крайней мере две симплициальные вершины: одна в X', другая в X''. Лемма доказана.

2. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Теорема 1. Класс графов фрагментов совпадает с классом T-графов.

Необходимость. Покажем, что любой граф фрагментов является T-графом.

Пусть $L=(X, U)$ — граф фрагментов на дереве D, $\mu=[x_1x_2\ldots x_lx_1]$ — какой-либо его цикл длины $l\geqslant 4$.

По условию теоремы существует такая система Ω из $n=n(L)$ фрагментов на дереве D, что $L(\Omega)$ изоморфен L. Пусть при некотором изоморфизме вершине x_i цикла μ отвечает фрагмент M_i (будем считать, что $M_{i+l}=M_i$ $(i=\overline{1,l})$).

Обозначим $N_{ij}=M_i\cap M_j$ $(\forall i,j>0)$. Тогда по определению графа $L(\Omega)$ имеем

$$N_{i\,i+1}\neq\varnothing \quad (\forall i>0).$$

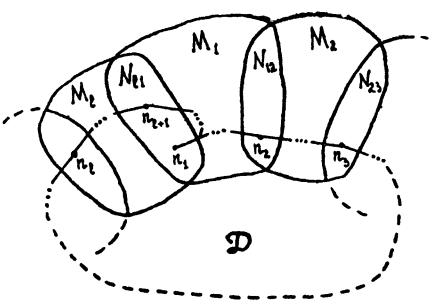


Рис. 3

Допустим теперь вопреки утверждению теоремы, что цикл μ не имеет хорд, т. е., что

$$N_{i\,i+\kappa}=\varnothing \quad (\forall i>0,\ 1<\kappa<l).$$

Тогда, так как $N_{12}\neq\varnothing$, $N_{l1}\neq\varnothing$, а M_1 — связный подграф, то существует цепь $n_1S_1n_2$, где S_1 — некоторая цепь в M_1, вершина $n_1\in N_{l1}$, а вершина $n_2\in N_{12}$, причем $n_2\in\overline{N_{l1}}$, так как по предположению, $N_{2l}=\varnothing$. Ввиду того, что M_2 — связный подграф и $N_{23}\neq\varnothing$, то мы сможем продолжить цепь из n_2 через M_2 в $n_3\in N_{23}$ ($n_3\in\overline{N_{12}}$, так как $N_{13}=\varnothing$). Продолжая таким образом построение цепи через все M_i $(i=1,l)$, на последнем шаге через M_l придем в некоторую вершину $n_{l+1}\in N_{l1}$ (в общем случае $n_{l+1}\neq n_1$), а так как M_1 — связный подграф, то всегда существует цепь, соединяющая n_{l+1} и n_1. Таким образом, цепь замкнулась либо в n_1, либо в одной из вершин цепи S_1.

Полученное противоречие с тем, что D — дерево, и доказывает необходимость теоремы.

Достаточность. Докажем, что любому T-графу соответствует дерево фрагментов. Доказательство проведем индукцией по числу вершин T-графа.

T-графы с числом вершин $n=1, 2, 3$ с точностью до изоморфизма являются графами фрагментов для таких деревьев фрагментов (рис. 4):

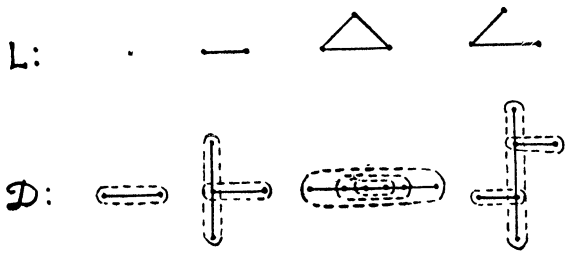


Рис. 4

Пусть теорема верна для всех T-графов с числом вершин, не превосходящем n. Покажем, что она верна для $(n+1)$-вершинного T-графа L.

Если L — полный граф, то утверждение доказано (см. замечание к лемме 2), в противном случае выделим в L минимальное разделяющее множество S, которое разделит его на две компоненты связанности: $L(X')$ и $L(X'')$. По лемме 1 S порождает полный подграф $L(S)$.

Рассмотрим подграфы $L_1=L(X' \cup S)$ и $L_2=L(X'' \cup S)$ (рис 5). Это T-графы с числом вершин, меньшим n, а для них по предположению индукции, существуют деревья D_1 и D_2 с системами фрагментов Ω_1 и Ω_2 соответственно.

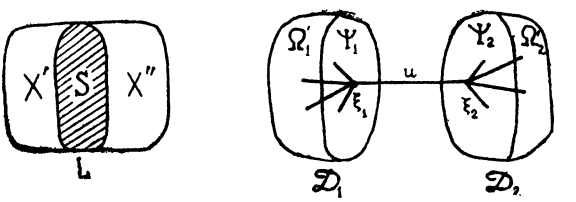


Рис. 5

Пусть $\Omega_1=\psi_1 \cup \Omega_1'$, $\Omega_2=\psi_2 \cup \Omega_2'$, где $\psi=\{M_1, M_2, ..., M_\kappa\}$ — подсистема фрагментов, соответствующая $L(S)$ в подграфе L_1 (i-й вершине S соответствует M_i), а подсистема фрагментов $\psi_2=\{M_1', ..., M_\kappa'\}$ соответствует $L(S)$ в подграфе L_2 (i-й вершине S соответствует M_i').

По лемме 2 существует вершина $\xi_1 \in \bigcap_{i=1}^{\kappa} M_i$, и аналогично существует вершина $\xi_2 \in \bigcap_{i=1}^{\kappa} M_i'$. Соединим ξ_1 и ξ_2 ребром u и рассмотрим дерево D, состоящее из D_1 и D_2, «склеенных» этим ребром. Это дерево фрагментов будет соответствовать L. Действительно, L состоит из $L(X')$, $L(S)$ и $L(X'')$; по построению каждой вершине из X' соответствует некоторый фрагмент из Ω_1', каждой вершине из X'' — фрагмент из Ω_2', а i-й вершине из S соответствует фрагмент $M_i \cup M_i'$. Теорема доказана.

3. ОЦЕНКА ЧИСЛА ВЕРШИН ДЕРЕВА ФРАГМЕНТОВ

Доказательство теоремы 1 дает не только конструктивный способ построения дерева фрагментов, но и позволяет оценить число его вершин.

Для каждого графа L и некоторого множества M введем функцию $f(L)=\min|M|$, где минимум берется по всем представлениям L системами подмножеств M (предполагается, что существует хотя бы одно такое представление). Если L — граф фрагментов, то $f(L)$ есть наименьшее число вершин дерева фрагментов, необходимое для представления L. Тогда оказывается справедливой.

Теорема 2. Для каждого n-вершинного T-графа L $f(L)\leqslant n$.

Доказательство. Пусть L представляется системой фрагментов $\Omega=\{M_1, M_2, ..., M_n\}$ на дереве D. Обозначим $M^{(\kappa)}=\bigcup\limits_{i=1}^{\kappa} M_i$ и заметим, что полный граф L_m можно наиболее экономно представить системой $\psi=\{N_1, N_2, ..., N_m\}$, где $N_1=N_2=\cdots=N_m=\{i\}$, i — некоторая вершина дерева. Из вышеописанного способа построения D имеем неравенство

$$|M^{(n)}|\leqslant 1+|M^{(n-1)}|,$$

откуда $f(L)\leqslant n$, что и требовалось доказать.

Оценка достигается на графах, показанных на рис. 6, которые представляются деревьями, изоморфными им же.

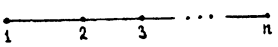


Рис. 6

Таким образом, полученая оценка на порядок ниже, чем в общем случае представления графа системой множеств. Более того, такая оценка дает возможность утверждать, что задание T-графов системой фрагментов не хуже (а для многих T-графов даже лучше), чем матрицей смежности.

4. АЛГОРИТМ РАСПОЗНАВАНИЯ Т-ГРАФОВ

Как видно из предыдущих параграфов, для T-графов получен достаточно удобный способ представления. Тем важнее иметь какой-либо алгоритм, распознающий, является ли данный граф T-графом. Один из таких алгоритмов приводится ниже.

Для построения алгоритма используем лемму 3, выражающую одно из характеристических свойств T-графов (назовем его τ-свойством). Заметим, что любой подграф T-графа L, порожденный множеством вершин X, есть T-граф, так как любой цикл в $L(X)$ есть тот же цикл в L и хорда этого цикла в L должна быть ребром и в $L(X)$. Следовательно, все свойства T-графа остаются у любого его подграфа. Смысл алгоритма заключается в проверке наличия τ-свойства у данного графа и существенной части его подграфов.

Алгоритм находит все симплициальные вершины в исходном графе. Если количество таких вершин не менее двух (т. е. граф обладает τ-свойством), то они исключаются из множества вершин. Далее таким же образом осуществляется проверка на τ-свойство подграфа, порожденного оставшимися вершинами. Процесс заканчивается, когда множество вершин исчерпает себя; в этом случае делается вывод о том, что исходный граф триангулирован. Если же на какой-то итерации проверяемый подграф не обладает τ-свойством, то исходный граф не триангулирован.

Опишем алгоритм более формально.

1) Для графа $L(X)$ найти все симплициальные вершины: $x_1, x_2, ..., x_l$.

2) Если $l<2$, то исходный граф не триангулирован.

В противном случае перейти к п. 3.

3) Если $X\neq\varnothing$, то обозначить $L(X\setminus\{x_1, x_2, ..., x_l\})$ через $L(X)$ и перейти к п. 1.

В противном случае исходный граф триангулирован.

Оценим сложность алгоритма $g(n)$. Будем предполагать, что граф задан матрицей смежности. За единицу сложности алгоритма возьмем простейшую операцию (сложение, умножение, сравнение) над двоичными символами. Тогда для проверки каждой вершины n-вершинного графа на симплициальность потребуется $\leqslant n^2$ операций. Поиск и исключение всех симплициальных вершин в одной итерации потребует, следовательно, выполнения $\sim n^3$ операций. Если учесть теперь, что алгоритм прекращает работу не далее чем через n итераций, то становится ясно, что

$$g(n)\sim n^4.$$

ЛИТЕРАТУРА

1. Зыков А. А. Теория конечных графов. Новосибирск, Наука, 1969.

2. Erdös P., Goodman A. W., Posa L., The representation of a graph by set intersection, Canad. T. Math. **18**, № 1, 106—112, (1966).

3. Алексеев В. Е. О сжимаемых графах. Сб. Проблемы кибернетики, М., Наука, 1979, вып. 36 (в печати).

4. Rose D. T., A graph-theoretic study of the numerical solution of sparse positive definite systems of linear equations. Сб. «Graph theory and computing», edited by Ronald C. Read, Academic Press, New Gork. and London, 1972, p. 183—217.

5. Миркин Б. Г., Родин С. Н. Графы и гены. М., Наука, 1977.

Горьковский государственный университет

[28/XII 1977]

ВЫПУКЛЫЕ МНОГОГРАННЫЕ КОНУСЫ, СИСТЕМЫ СРАВНЕНИЙ И ПРАВИЛЬНЫЕ ОТСЕЧЕНИЯ В ЦЕЛОЧИСЛЕННОМ ПРОГРАММИРОВАНИИ

В. Н. Шевченко

1. Обозначим через R, Z, R_+, Z_+ множества рациональных, целых, неотрицательных рациональных и неотрицательных целых чисел соответственно; а через R^m, Z^m, R_+^m, Z_+^m — m-ю декартову степень соответствующего множества. Пусть $A=(a_{ij})$ — целочисленная матрица размеров $m\times n$; $a_1, ..., a_n$ — ее столбцы; $b\in Z^m$, $c_j\in Z$ $(j=1, ..., n)$, $u=(u_1, ..., u_m)$ — вектор переменных. Рассмотрим задачу целочисленного линейного программирования относительно u

$$\max u\,b, \tag{1}$$

$$u\,a_j\leqslant c_j \quad (j=1, ..., n), \tag{2}$$

$$u\in Z^m. \tag{3}$$

Ограничения (2) можно переписать в матричном виде, обозначив через c строку, j-я компонента которой равна c_j:

$$u\,A\leqslant c. \tag{4}$$

Множество u из R^m, удовлетворяющих (4), обозначим через $M(A, c)$. Обозначим через $A^{\angle}$ (или в более подробной записи через $\{a_1, \ldots a_n\}^{\angle}$) выпуклый многогранный конус, порожденный столбцами A, т. е.

$$A^{\angle} = \{a \mid a = \sum_{j=1}^{n} \lambda_j a_j,\ \lambda_j \in R_+ \quad (j = 1, \ldots, n)\}.$$

Относительно задачи (1)—(3) сделаем следующие предположения:

а) ранг матрицы A равен m,

б) $M(A, c) \neq \varnothing$,

в) $b \in A^{\angle}$,

что, как известно из теории линейного программирования (см., например, [1]), гарантирует существование крайней точки в $M(A, c)$ и оптимального плана в задаче (1), (2).

2. Обозначим через $L(A, c)$ выпуклую оболочку множества $M(A, c) \cap Z^m$ и через $N(A, c)$ — множество крайних точек множества $L(A, c)$. Из [2] легко получается следующая

Лемма 1. Для того чтобы $v \in N(A, c)$, необходимо и достаточно существование такой линейно независимой системы векторов $b^1, \ldots, b^m$ из Z^m, чтобы для всякой $u \in L(A, c) \setminus \{v\}$ выполнялись неравенства $ub^i < vb^i$ $(i = 1, \ldots, m)$. В [3] доказана (см. также [4]) следующая

Теорема 1. Если $a_{ij} \in R$, то $N(A, c)$ конечно и $L(A, c)$ — выпуклое многогранное множество, т. е. найдется такое натуральное число n', такая целочисленная матрица A' размерами $m \times n'$ и такой вектор $c' \in Z^{n'}$, что $L(A, c) = M(A', c')$.

Если $M(A, c)$ ограничено, то этот факт тривиален при любых действительных a_{ij} в силу конечности $M(A, c) \cap Z^m$ (см., например, [5]). Если же $M(A, c)$ не ограничено, то предположение о рациональности коэффициентов матрицы A существенно, в чем нетрудно убедиться, взяв, например, $A = \begin{pmatrix} -1 & -1 \\ \sqrt{2} & 0 \end{pmatrix}$ и $c = (0, 1)$. Здесь $N(A, c)$ бесконечно и $L(A, c)$ нельзя описать конечной системой неравенств [4].

Заметим, что, несмотря на конструктивность доказательства теоремы 1, удобных алгоритмов для нахождения $L(A, c)$ (или матрицы A' и вектора c', о которых говорится в теореме 1) пока не известно.

3. *Определение.* Неравенство $ua \leqslant \alpha$ называется правильным отсечением точки w от M, если $wa > \alpha$ и для всякой $v \in M \cap Z^m$ $va \leqslant \alpha$.

Пусть d — натуральное число. Рассмотрим систему линейных сравнений

$$\sum_{j=1}^{n} a_{ij} x_j \equiv 0 \ (d) \quad (i = 1, \ldots, m). \tag{5}$$

Для записи системы (5) будем использовать также векторную форму $\sum_{j=1}^{n} a_j x_j \equiv 0 \ (d)$ и матричную форму $Ax \equiv 0 \ (d)$, положив $x = (x_1, \ldots, x_n)^T$. Через $[\alpha]$ будем обозначать наибольшее целое число, не превосходящее α.

Лемма 2. Если вектор x удовлетворяет системе (5), $a = \frac{Ax}{d}$ и $\alpha = \left[\frac{cx}{d}\right]$, то для всякой точки v из $M(A, c) \cap Z^m$ выполняется $va \leqslant \alpha$.

Действительно, так как $x \geqslant 0$ и $vA \leqslant c$, то $va \leqslant \frac{vAx}{d} \leqslant \frac{cx}{d}$, откуда, в силу целочисленности v и a, следует требуемое неравенство.

Итак, неотрицательные решения системы (5) могут использоваться для построения таких неравенств, добавление которых к системе (2) не меняет множества целочисленных решений этой системы. Поскольку вектору a, полученному таким способом, могут соответствовать и другие решения системы (5) (может быть, и для других d), естественно пытаться найти наименьшее α.

Лемма 3. Если $M(A,c)\neq\varnothing$ и множество $T(a)$ решений системы $Ax=a$, $x\geqslant 0$ не пусто, то функция $[cx]$ достигает своего минимума на крайней точке множества $T(a)$, в которой достигает своего минимума и функция cx.

Для доказательства рассмотрим пару двойственных задач линейного программирования

$$\left.\begin{matrix}\max ua,\\ uA\leqslant c\end{matrix}\right\} \text{ и } \left.\begin{matrix}\min cx,\\ x\geqslant 0,\ Ax=a\end{matrix}\right\}.$$

По теореме двойственности [1] обе задачи имеют оптимальные планы, причем существует такая крайняя точка p множества $T(a)$, что для любой $x\in T(a)$ выполняется $cp\leqslant cx$, а значит, и $[cp]\leqslant[cx]$.

Замечание. Точка p может быть получена какой-нибудь конечной модификацией симплекс-метода, например, лексикографическим его вариантом. В этом случае (напомним, что ранг A равен m) получим не только p, но и множество $T=\{s_1,\ldots,s_m\}$ такое, что матрица $B=(a_{s_1},\ldots,a_{s_m})$ не вырождена, $a\in B^{\angle}$ и решение w системы

$$wa_{s_i}=c_{s_i}\quad (i=1,\ldots,m), \tag{6}$$

является крайней точкой $M(A,c)$.

Положим $\Delta=\det B$ и $\bar{c}=(c_{s_1},\ldots,c_{s_m})$.

Лемма 4. Если существует натуральное число d и вектор x из Z^m такие, что $Bx\equiv 0(d)$ и Н.О.Д. $(d,\Delta)=\delta$, то $\dfrac{\delta x}{d}\in Z^m$.

Действительно, так как Н.О.Д $(d,\Delta)=\delta$, то найдутся такие целые числа α и β, что $\delta=\alpha\Delta+\beta d$. Пусть $da=Bx$. Тогда $\delta x=\alpha\Delta x+\beta dx=\alpha\Delta dB^{-1}a+\beta dx=d(\alpha\Delta B^{-1}a+\beta x)$. Так как в скобках стоит, очевидно, целочисленный вектор, то лемма доказана.

4. Итак, вместо системы (5) достаточно рассматривать лишь системы вида

$$Bx\equiv 0(\Delta),\quad x\in Z^m, \tag{7}$$

где B — некоторая невырожденная подматрица матрицы A.

Вместе с системой (7) будем рассматривать систему

$$uB\leqslant\bar{c}. \tag{8}$$

Множество ее решений $M(B,\bar{c})=\{u/u=\bar{c}B^{-1}-\lambda B^{-1},\ \lambda\in R_+^m\}$, очевидно, имеет единственную крайнюю точку $w=\bar{c}B^{-1}$, в которой для любого $b\in B^{\angle}$ достигается максимум функции ub. Понятен интерес, который вызывает асимптотическая [6, 7] задача целочисленного линейного программирования (в [8] она называется элементарной)

$$\left.\begin{matrix}\max ub,\\ u\in M(B,\bar{c})\cap Z^m\end{matrix}\right\}. \tag{9}$$

Обозначим множество решений системы (7) через S. Приведем ряд утверждений из [3], связывающих множество S с правильными отсечениями w от $M(B,\bar{c})$.

Лемма 5. $S=\{x/x=\Delta B^{-1}a,\ a\in Z^m\}$.

Лемма 6. $w\in Z^m$ тогда и только тогда, когда для всякого $x\in S$ $\bar{c}x\equiv 0(\Delta)$.

Лемма 7. Если $x\in S$, $x\geqslant 0$ и $\bar{c}x\not\equiv 0(\Delta)$, то неравенство

$$\frac{uBx}{|\Delta|}\leqslant\left[\frac{cx}{|\Delta|}\right] \tag{10}$$

является правильным отсечением w от $M(B,\bar{c})$.

Положим $v=\bar{c}-uB$ и $x_0=\mathrm{res}_\Delta\,\bar{c}\,x$ (т. е. x_0 равно остатку от деления числа $\bar{c}x$ на число Δ). Тогда неравенство (10) можно переписать как

$$\frac{vx}{|\Delta|}\geqslant\frac{x_0}{|\Delta|}. \tag{11}$$

Пусть $y\geqslant 0$, $y\in S$, $y_0=\mathrm{res}_\Delta\,\bar{c}y$. Естественно поставить вопрос о сравнении отсечений (ср. [9]) $\dfrac{vy}{|\Delta|}\geqslant\dfrac{y_0}{|\Delta|}$ и (11).

Лемма 8. Для того чтобы неравенство $\dfrac{vy}{|\Delta|}\geqslant\dfrac{y_0}{|\Delta|}$ являлось следствием системы неравенств (8) и (10), необходимо и достаточно существование такого $\lambda\geqslant 0$, что $y\geqslant\lambda x$ и $y_0\leqslant\lambda x_0$.

Последнее утверждение позволяет ограничиться лишь теми $x=(x_1,\ldots,x_m)^T$ из S, для которых $0\leqslant x_i<|\Delta|$.

Обеспечить выполнение последнего условия можно, заменив соответствующую компоненту остатком от деления ее на $|\Delta|$.

Из лемм 5—8 следует

Теорема 2. Если $\bar{c}B^{-1}\in Z^m$, то система

$$Bx\equiv 0(\Delta),\ \bar{c}x\not\equiv 0(\Delta),\ 0\leqslant x_i<|\Delta|\ \ (i=1,\ldots,m) \tag{12}$$

совместна. Для каждого решения системы (12) неравенство, получаемое по формуле (10), является правильным отсечением точки w от $M(B,\bar{c})$.

Б [10] рассмотрена связь неравенств (10) с отсечениями Р. Гомори.

5. Отождествим в множестве S те решения x и x', для которых $x\equiv x'(\Delta)$, и положим $G=\{x\in S\mid 0\leqslant x_i<|\Delta|\}$. Если под сложением векторов понимать их покомпонентное сложение по модулю Δ (будем обозначать такую операцию знаком $+$, а результат ее s-кратного применения — через $s\circ x$), то очевидно, что G — группа. Вопрос о ее строении был изучен Р. Гомори в [11] (см. также [6] и [3]. Пусть D — нормальная диагональная форма (употребителен также термин «нормальная форма Смита») матрицы B, $d_i\,(i=1,\ldots,m)$ — ее диагональные элементы, P и $Q=(q_{ij})$ — такие унимодулярные матрицы, что $D=PBQ$, $\bar{q}_{ij}=\mathrm{res}_\Delta\,q_{ij}$, $\bar{Q}=(\bar{q}_{ij})$, $\bar{q}_1,\bar{q}_2,\ldots,\bar{q}_m$ — столбцы матрицы $\bar{Q}$, $r_i=|\Delta|/d_i\circ\bar{q}_i$ $(i=1,\ldots,m)$.

Теорема 3 [3]. Формула

$$x=\beta_1\circ r_1\oplus\ldots\oplus\beta_m\circ r_m \tag{13}$$

взаимно однозначно отображает множество векторов $\beta=(\beta_1,\ldots,\beta_m)$ таких, что $\beta_i\in Z$, $0\leqslant\beta_i\leqslant d_i-1$ $(i=1,\ldots,m)$ на множество G.

Следствие 1. Порядок группы G равен $|\Delta|$.

Следствие 2. Пусть κ такое, что $d_1=\cdots=d_\kappa=1$ и $d_{\kappa+1}\geqslant 2$. Тогда G — прямая сумма циклических групп $G_i\,(i=\kappa+1,\ldots,m)$, где G_i имеет порядок d_i и порождается вектором $r_i\,(i=\kappa+1,\ldots,m)$.

Следствие 3. G — циклическая тогда и только тогда, когда Н.О.Д. миноров $(m-1)$-го порядка матрицы B равен единице.

Следствие 4. Н.О.Д. миноров $(m-1)$-го порядка матрицы $(a_{s_1},\ldots,a_{s_{i-1}},a_{s_{i+1}},\ldots,a_{s_m})$ равен наименьшему из положительных значений, принимаемых x_i при $x\in S$.

Рассмотрим множество $V(G,\bar{c})$ решений системы

$$v\bar{q}_i\equiv\bar{c}\bar{q}_i(d_i)\ \ (i=1,\ldots,m),\ v\in Z_+^m \tag{14}$$

и множество $N(G,\bar{c})$ крайних точек $\mathrm{Co}\,V(G,\bar{c})$ (здесь и дальше через $\mathrm{Co}\,M$ обозначается выпуклая оболочка множества M).

Теорема 4. Формула $v=\bar{c}-uB$ взаимно однозначно отображает множество $M(B,\bar{c})\cap Z^m$ на множество $V(G,\bar{c})$, при этом множество $N(B,\bar{c})$ взаимно однозначно отображается на множество $N(G,\bar{c})$.

Действительно очевидно, что условия $u\in M(B,\bar{c})$ и $v\geqslant 0$ равносильны. Далее, если $u\in Z^m$, то $v\in Z^m$, и, кроме того, умножив равенство $v=\bar{c}-uB$ на $\bar{q}_i$, получим, что $v\bar{q}_i=\bar{c}\,q_i-uB\,\bar{q}_i$, откуда следует, что $v\bar{q}_i\equiv\bar{c}\,\bar{q}_i(d_1)$ $(i=1,\ldots,m)$. С другой стороны, если $v\bar{q}_i\equiv\bar{c}\bar{q}_i(d_i)$ $(i=1,\ldots,m)$, то для каждого $x\in S$ $vx\equiv\bar{c}x(\Delta)$, откуда по лемме 6 следует, что $u\in Z^m$. Теперь очевидно и второе утверждение теоремы.

Рассмотрим вопрос о соотношении между задачей (9) и задачей групповой минимизации (ЗГМ), введенной Р. Гомори [11] и служажей предметом изучения большого числа статей (см. библиографию в [6, 12]). Она может быть поставлена следующим образом: найти вектор $v=(v_1,\ldots,v_m)\in Z_+^m$, минимизирующий $v\beta$ при заданном $\beta\in R_+^m$ и удовлетворяющий групповому соотношению

$$\sum_{j=1}^{m} v_j g_j=g_0,\quad v_j\in Z_+\ (j=1,\ldots,m), \tag{15}$$

где $g_0,g_1,\ldots,g_m$ — элементы некоторой абелевой группы g (записываемой аддитивно) порядка δ. Теорема 4позволяет свести задачу (9) к ЗГМ, если положить $B^{-1}b=\beta$. В этом случае группа g является прямой суммой $(m-\kappa)$ циклических групп порядков $d_{\kappa+1},\ldots,d_m$ (элементы g можно отождествить с $(m-\kappa)$-мерными векторами, i-е компоненты которых складываются по модулю d_i, причем (15) совместно при любом g_0, поскольку для (14) это выполняется в силу унимодулярности матрицы Q).

Оказывается, что последнее условие является не только необходимым, но и достаточным для того, чтобы от ЗГМ можно было прийти к такой задаче (9), для которой $|\det B|=\delta$ и система (14) равносильна соотношению (15). Действительно, так как абелева группа изоморфна прямой сумме циклических групп, а циклическая группа из d элементов изоморфна группе вычетов по модулю d [14], то (15) равносильно некоторой системе

$$\sum_{j=1}^{m} v_j\alpha_{ji}\equiv\alpha_{0i}(\delta_i)\ \ (i=1,\ldots,s),\ v_j\in Z_+\ (j=1,\ldots,m), \tag{16}$$

причем можно считать, что сравнения независимы и $\prod_{i=1}^{m}\delta_i=\delta$.

Рассмотрим блочную матрицу $\Gamma'=\begin{pmatrix}\Gamma\\ \Lambda\end{pmatrix}$, где $\Gamma=\begin{pmatrix}\alpha_{11}\cdots\alpha_{1s}\\ \cdot\ \ \cdot\ \ \cdot\\ \alpha_{m1}\cdots\alpha_{ms}\end{pmatrix}$ и $\Lambda=\begin{pmatrix}\delta_1\ 0\ \cdots\ 0\\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\\ 0\ \ 0\ \cdots\ \delta_s\end{pmatrix}$. Так как система (16) совместна при любых $\alpha_{0i}\in Z$, то найдутся такие унимодулярные матрицы R и T, что $R\Gamma' T=\begin{pmatrix}E_s\\ 0\end{pmatrix}$, где E_s — единичная матрица s-го порядка, а 0 — нулевая $m\times s$-матрица. Разбив матрицу R на блоки $R=\begin{pmatrix}R_{11}R_{12}\\ R_{21}R_{22}\end{pmatrix}$ соответствующих размеров (в частности R_{21} — квадратная m-го порядка), получим, как нетрудно проверить, что $|\det R_{21}|=\delta$ и $R_{21}\Gamma+R_{22}\Lambda=0$. Очевидно теперь, что за искомую матрицу B можно взять R_{21}, а в качестве $\bar{c}$ — любое решение системы (16).

Доказанная равносильность ЗГМ и задачи (9) позволяет перенести методы решения одной из них на другую, например, ЗГМ можно решать методами отсечений. Привлечение идей динамического программирования позволило Р. Гомори и его последователям [6, 13] получить для решения ЗГМ алгоритмы с числом операций, пропорциональным δ^2 или $m\delta$. Однако подход к решению задачи (1)—(3), связанный с решением задачи (9) (так называемый ассимптотический подход [11]), где матрица B выбирается так, чтобы $b\in B$, имеет существенный минус, связанный с тем, что решение w задачи (9) может не принадлежать множеству $M(A,c)$. Вычислительный эксперимент [15] показал, что $w\in M(A,c)$ приблизительно в 70% случаев.

Если вместе с точкой w получим такую унимодулярную матрицу $F=(f_1,\ldots,f_m)$ и такой вектор $f_0=(f_{10},\ldots,f_{m0})\in Z^m$, что 1) $wF=f_0$, 2) $b\in F^<$, 3) $uf_i\leqslant f_{i0}$ $(i=1,\ldots,m)$ — правильные отсечения w от $M(B,\bar c)$, то, как показано в [3], можно продолжать счет полностью целочисленным алгоритмом Гомори [5, 6] и в случае, когда $w\in \overline{\in M(A,c)}$. В дипломной работе А. И. Шевчук реализовал этот подход и провел небольшой вычислительный эксперимент, показавший неплохие результаты, однако оценить число шагов полностью целочисленного алгоритма не удалось. Последняя трудность преодолена в [8, 16] за счет более сложного построения исходной матрицы F, однако хороших оценок самого этого построения не получилось.

6. Приведем еще способы использования x из S для получения правильных отсечений w от $M(B,\bar c)$.

Лемма 9. Если а) $w=\bar c B^{-1}\in Z^m$, б) $x\in S$, $x\geqslant 0$, $\bar cx\equiv 0(\Delta)$, $x_i>0$ $(i\in I)$ и в) система $ua_{s_i}=c_{s_i}$ $(i\in I)$ не совместна в целых числах, то

$$\frac{uBx}{|\Delta|}\leqslant\frac{\bar cx}{|\Delta|}-1 \tag{17}$$

является правильным отсечением w от $M(B,\bar c)$.

Доказательство. Во-первых, $\frac{wBx}{|\Delta|}=\frac{\bar cx}{|\Delta|}>\frac{\bar cx}{|\Delta|}-1$. Во-вторых, если $u\in M(B,\bar c)$, то $\frac{uBx}{|\Delta|}\leqslant\frac{\bar cx}{|\Delta|}$. Так как $\bar cx\equiv 0(\Delta)$, то для $u\in M(B,\bar c)\cap Z^m$, либо $\frac{uBx}{|\Delta|}\leqslant\frac{\bar cx}{|\Delta|}-1$, либо $uBx=\bar cx$. Если $uBx=\bar cx$, то $\sum\limits_{i=1}^{m}x_i(ua_{s_i}-c_{s_i})=0$, и следовательно, $x_i(ua_{s_i}-c_{s_i})=0$ $(i=1,\ldots,m)$, откуда следует, что $ua_{s_i}=c_{s_i}$ $(i\in I)$, что противоречит предположению в).

Следствие [10]. Если $\bar cB^{-1}\in\overline{Z^m}$ и существует такое $x\in S$, что $x>0$ и $\bar cx\equiv 0(\Delta)$, то неравенство (17) является правильным отсечением.

В частности, если в (17) положить $x_i=|\Delta|$ $(i=1,\ldots,m)$, то получится отсечение Данцига, которое можно переписать в виде $\sum\limits_{i=1}^{m}v_i\geqslant 1$.

Определение. Назовем циклическим следующий процесс:
шаг 0: положить $A^1=A$, $c^1=c$, $i=1$ и перейти к шагу $2i-1$; шаг $2i-1$: найти точку $u^i\in M(A^i,c^i)$, максимизирующую линейную форму ub; если $u^i\in Z^m$, то остановиться, в противном случае перейти к шагу $2i$, шаг $2i$: построить $ua\leqslant\alpha$ правильное отсечение u^i от $M(A^i,c^i)$, поло-

жить $A^{i+1}=(A^i, a)$, $c^{i+1}=(c^i, \alpha)$, увеличить i на единицу и перейти к шагу $2i$—1.

Существуют примеры, показывающие, что если на шаге $2i$ использовать лишь отсечения Данцига, то циклический процесс бесконечен [5]. В [10] было высказано предположение о конечности циклического процесса, если на шаге $2i$ использовать лишь отсечения, получаемые по теореме 2. В своей курсовой работе Н. М. Моржаков это предположение опроверг, приведя соответствующий пример. Известно (см., например, [5, 6]), что Гомори удалось, детерминировав циклический процесс при помощи лексикографии, получить такой способ решения задачи (1)—(3), для которого доказана конечность. Однако указать верхние оценки, близкие к достижимым, даже для простейшей задачи (9) пока не удается (ср. [17]).

Другой способ использования $x\in S$ для построения правильных отсечений связан с отказом от неотрицательности x. Пусть

$$x=(x_1, \ldots, x_m)\in S,\ J=\{j \mid x_j>0\},\ x_0=\operatorname{res}_\Delta \bar{c}x>0,$$

$$a(x)=\frac{|\Delta|-x_0}{|\Delta|}\sum_{i\in J} x_i a_{s_i}-\frac{x_0}{|\Delta|}\sum_{i\in \bar{J}} x_i a_{s_i}, \tag{18}$$

$$\alpha(x)=\frac{|\Delta|-x_0}{|\Delta|}\sum_{i\in J} x_i c_{s_i}-\frac{x_0}{|\Delta|}\sum_{i\in \bar{J}} x_i c_{s_i}-\frac{x_0(|\Delta|-x_0)}{|\Delta|}. \tag{19}$$

Лемма 10 [18]. Неравенство

$$ua(x)\leqslant\alpha(x) \tag{20}$$

является правильным отсечением w от $M(B, \bar{c})$; при этом $a(x)\in Z^m$, $\alpha(x)\in Z$.

В [18] обсуждается связь неравенств вида (20) с отсечениями, используемыми во втором алгоритме Р. Гомори [5], который может применяться и для задач частично целочисленного программирования.

Покажем, как неравенство (20) можно использовать для частично целочисленных задач. Пусть $I\subseteq\{1, .., m\}$, $\bar{I}=\{1, \ldots, m\}\setminus I$, $w=(w_1, \ldots, w_m)=\bar{c}B^{-1}$, $L(I)=\{u=(u_1, \ldots, u_m)\in M(B, \bar{c})/u_i\in Z\ (i\in I)\}$. Рассмотрим систему линейных соотношений

$$\left.\begin{aligned}&\sum_{\nu=1}^{m} a_{is_\nu}x_\nu\equiv 0\ (\Delta)\quad (i\in I),\\ &\sum_{\nu=1}^{m} a_{is_\nu}x_\nu=0\quad (i\in\bar{I}),\\ &x=(x_1, \ldots, x_m)\in Z^m.\end{aligned}\right\} \tag{21}$$

Лемма 11. Если существует такое $i\in I$, что $w_i\in\overline{Z}$, то найдется такое решение x системы (21), для которого $\bar{c}x\not\equiv 0\ (\Delta)$.

Для доказательства достаточно взять i-й столбец матрицы ΔB^{-1} в качестве требуемого x.

Лемма 12. Если x удовлетворяет системе (21), $\bar{c}x\not\equiv 0\ (\Delta)$, $a(x)$ получено по формуле (18), $\alpha(x)$ — по формуле (19), то неравенство (20) является правильным отсечением w от $L(I)$; $a(x)\in Z^m$, $\alpha(x)\in Z$.

Для доказательства положим $q_0=\frac{1}{|\Delta|}(\bar{c}x-x^0)$ и $q=\frac{1}{|\Delta|}Bx$. Очевидно, что $q=(q_1, \ldots, q_m)\in Z^m$ и $q_i=0\ (i\in\bar{I})$. Таким образом, для всякой $u\in L(I)$ либо

$$uq\leqslant q_0, \tag{22}$$

либо

$$uq\geqslant q_0+1. \tag{23}$$

Из (18) и (19) имеем $a(x)=(|\Delta|-x_0)q-\sum_{j\in\bar{J}} a_{s_j}x_j=\sum_{j\in J} a_{s_j}x_j-$

$-x_0 q$, $\alpha(x)=(|\Delta|-x_0)q_0-\sum\limits_{j\in J} c_{s_j}x_j=\sum\limits_{j\in J} c_{s_j}x_j-x_0(q+1)$, откуда следует целочисленность $a(x)$ и $\alpha(x)$. Кроме того, из этих же формул видно, что если выполнено (22), то неравенство (20) является следствием неравенств системы (8), соответствующих тем s_j, для которых $x_j<0$, и неравенства (22). Если же выполнено (23), то (20) следует из (23) и неравенств системы (8), соответствующих тем s_j, для которых $x_j>0$. Поскольку проверка условия $w\,a(x)>\alpha(x)$ тривиальна, то лемма доказана.

7. Получим верхние оценки для числа крайних точек выпуклой оболочки множества целочисленных решений в общей задаче целочисленного программирования и в ее частных случаях: задаче о рюкзаке и ЗГМ (см. также [19]). Такого рода результаты могут оказаться весьма полезными для оценки эффективности алгоритмов решения соответствующих задач. Получим сначала следующий результат комбинаторного характера. Мощность множества M будем обозначать через $|M|$.

Теорема 5. Пусть $D_i=\{0, 1, ..., \Delta_i-1\}$, $P=D_1\times\cdots\times D_{m-1}\times Z$ и κ — натуральное число, $\kappa\geqslant 2$. Если в P не существует таких точек p и q $(p\neq q)$, что $p\leqslant\kappa q$, то $|P|\leqslant\prod\limits_{i=1}^{m-1}\delta_i$, где $\delta_i=1+[\log_\kappa((\Delta_i-1)(\kappa-1)+1)]$ и $\prod\limits_{i=1}^{0}\delta_i=1$.

Доказательство проведем индукцией по m, положив $P=(p_{ij})$ $(i=1, ..., m;\ j=1, ..., n)$. При $m=1$, $n=|P|\leqslant 1$, так как в противном случае должно было бы выполняться $p_{11}>\kappa p_{12}$ и $p_{12}>\kappa p_{11}$. Допустим, что теорема доказана для $m-1$, и рассмотрим множества $J_\nu=\left\{j \;\middle/\; \frac{\kappa^\nu-1}{\kappa-1}\leqslant p_{1j}\leqslant\frac{\kappa^{\nu+1}-1}{\kappa-1}-1\right\}$. Так как $p_{1j}\leqslant\Delta_1-1$, то $\frac{\kappa^\nu-1}{\kappa-1}\leqslant\Delta_1-1$, откуда $\nu\leqslant\log_\kappa((\kappa-1)(\Delta_1-1)+1)$ и, следовательно, $\nu\leqslant\delta_1-1$.

Рассмотрим множество p_{ij} $(i=2, ..., m;\ j\in J_\nu)$. Для любых j и l таких, что $j\in J_\nu$, $l\in J_\nu$, $j\neq l$, найдется такое $i\in\{2, ..., m\}$, что $p_{ij}\geqslant\kappa p_{il}+1$, так как $\max\limits_{j\in J_\nu} p_{1j}\leqslant\frac{\kappa^{\nu+1}-1}{\kappa-1}-1=\kappa\frac{\kappa^\nu-1}{\kappa-1}\leqslant\kappa\min\limits_{j\in J_\nu} p_{1j}$. Следовательно, по предположению индукции $|J_\nu|\leqslant\prod\limits_{i=2}^{m-1}\delta_i$ и $n=\sum\limits_{\nu=0}^{\delta_1-1}|J_\nu|\leqslant\prod\limits_{i=1}^{m-1}\delta_i$, что и требовалось.

Пусть M — множество решений системы $Ax=b$, $x\in Z^n$ а N — множество крайних точек $\mathrm{Co}\,M$.

Лемма 13. Если $p^1, ..., p^{s+1}$ — различные точки из M $(s\geqslant 1)$ и существуют такие положительные числа $\lambda_1, ..., \lambda_s$, что $\sum\limits_{\nu=1}^{s}\lambda_\nu=s$, $\sum\limits_{\nu=1}^{s}\lambda_\nu p^\nu\in Z^n$ и $(s+1)p^{s+1}\geqslant\sum\limits_{\nu=1}^{s}\lambda_\nu p^\nu$, то $p^{s+1}\overline{\in} N$.

Для доказательства положим $p^0=(s+1)p^{s+1}-\sum\limits_{\nu=1}^{s}\lambda_\nu p^\nu$. Очевидно, что $p^0\in M$ и $p^{s+1}=\frac{1}{s+1}p^0+\sum\limits_{\nu=1}^{s}\frac{\lambda_\nu}{s+1}p^\nu$, т. е. p^{s+1} является выпуклой

комбинацией точек из M, среди которых есть различные, и, следовательно, $p^{s+1}\overline{\in}N$.

Следствие. Если $p^i=(p_1^i, \ldots, p_n^i)\in N$ $(i=1,2)$ и $p^1\neq p^2$, то найдется такое j, что $2p_j^1<p_j^2$.

Отсюда и из теоремы 5 следует

Теорема 6. Если для всякой $(p_1, \ldots, p_n)$ из N справедливо $p_j\leqslant\Delta_j-1$ $(j=1, \ldots, n-1)$, то $|N|\leqslant\prod_{j=1}^{n-1}(1+[\log_2\Delta_j])$.

Пусть теперь G — аддитивная абелева группа порядка Δ, $\alpha_j\in G$ $(j=0,1, \ldots, n)$, $M(G,n,\alpha_0)$ — множество таких $x=(x_1, \ldots, x_n)$, что

$$\sum_{j=1}^{n}\alpha_j x_j=\alpha_0,\ x_j\in Z_+\ (j=1, \ldots, n),$$

$N(G,n,\alpha_0)$ — множество крайних точек $\mathrm{Co}\,M(G,n,\alpha_0)$. Известно [20], что $|N(G,n,\alpha_0)|\leqslant\Delta^{n-1}$. Кроме того (см. [6]), если $x\in N(G,n,\alpha_0)$, то

$$\sum_{j=1}^{n}x_j\leqslant\Delta-1 \tag{24}$$

и

$$\prod_{j=1}^{n}(x_j+1)\leqslant\Delta. \tag{25}$$

Обозначим через $\varphi_n(\Delta)$ число точек $x\in Z_+^n$, удовлетворяющих (25), и положим $\psi_n(\Delta)=\sum_{\alpha_0\in G}|N(G,n,\alpha_0)|$. Тогда [4] $|N(G,n,\alpha_0)\leqslant$ $\leqslant\psi_n(\Delta)\leqslant\varphi_n(\Delta)\leqslant\Delta\,h(\log\Delta)$, где $h(t)$ — многочлен от t степени $n-1$. Последнее неравенство в этой цепочке по-видимому было известно еще Дирихле [21]. Аналогично лемме 13 доказывается

Лемма 14. Если $p^1, \ldots, p^{s+1}$ — различные точки из $N(G,n,\alpha_0)$ и $(s+1)p^{s+1}\geqslant\sum_{\nu=1}^{s}p^\nu$, то $p^{s+1}\overline{\in}N(G,n,\alpha_0)$.

Следствие. Если $p^i=(p_1^i, \ldots, p_n^i)\in N(G,n,\alpha_0)$ $(i=1,2)$ и $p^1\neq p^2$, то найдется такое j, что $2p_j^1+1\leqslant p_j^2$.

Отсюда и из теоремы 5 следует (ср. предположение в [4]) оценка

$$|N(G,n,\alpha_0)|\leqslant(1+[\log_2\Delta])^{n-1}. \tag{26}$$

Этот результат нетрудно уточнить, учитывая (25) и полагая $\delta=1+$ $+[\log_2\Delta]$ и $\binom{n}{\kappa}=\frac{n!}{\kappa!(n-\kappa)!}$ следующим образом.

Теорема 7. $|N(G,n,\alpha_0)|\leqslant\binom{\delta+n-2}{n-1}$.

Заметим, что, в силу теоремы 4, эти оценки справедливы и для $|N(B,\bar{c})|$.

Рассмотрим теперь ограничения задачи о рюкзаке

$$\sum_{j=1}^{n}a_j x_j\leqslant a_0,\ x_j\in Z_+\ (j=1, \ldots, n), \tag{27}$$

где $a_j\in Z$ и $a_j>0$ $(j=0,1, \ldots, n)$. Обозначим через $M(a)$ множество решений (27) и через $N(a)$ — множество крайних точек $\mathrm{Co}\,M(a)$. Вводя $x_{n+1}=a_0-\sum_{j=1}^{n}a_j x_j$, из теоремы 6 получим оценку

$$|N(a)|\leqslant\prod_{i=1}^{n}\left(1+\left[\log_2\left(\frac{a_0}{a_i}+1\right)\right]\right). \tag{28}$$

Получим теперь оценку для $|N(a)|$, не зависящую от a_0, что важно, если a_0 много больше, чем $a=\max\{a_1, ..., a_n\}$. Для $i\in\{1, ..., n\}$ обозначим через M_i множество решений системы

$$\sum_{j=1}^{n} a_j x_j \leqslant a_0, \quad x_j\in Z_+ \ (j=1, ..., i-1, i+1, ..., n), \tag{29}$$

через N_i — множество крайних точек $\mathrm{Co}\, M_i$ и положим $N_0=\{0\}$. Заметим, что (29) можно заменить на

$$a_1 x_1+\cdots+a_{i-1} x_{i-1}+a_{i+1} x_{i+1}+\cdots+a_n x_n+x_{n+1}\equiv a_0 (a_i)$$
$$x_j\in Z_+ \ (j=1, ..., i-1, \ i+1, ..., n+1).$$

Лемма 15. Если $a_0\geqslant a(a-1)$, то $N(a)=\bigcup\limits_{i=0}^{n} N_i$.

Действительно, пусть $p=(p_1, ..., p_n)\in N_i (i\neq 0)$ и $p_{n+1}=a_0-\sum\limits_{j=1}^{n} a_j p_j$. Из (24) следует, что $p_1+\cdots+p_{i-1}+p_{i+1}+\cdots+p_n+p_{n+1}\leqslant a_i-1$. Тогда

$$a_i p_i=a_0-\sum_{j\neq i} a_j p_j-p_{n+1}\geqslant a_0-a\sum_{j\neq i} p_j\geqslant a_0-a(a_i-1)\geqslant a_0-a(a-1),$$

следовательно, $p_i\geqslant 0$ и $p\in M(a)$. По лемме 1 найдется такой b, что $bx<bp$ для всякого $x\in M(a)\setminus\{p\}$, а следовательно, $p\in N(a)$.

Пусть теперь $p\in N(a)$, $p\neq 0$, тогда существует b такой, что $bx<bp$ для всякого $x\in M(a)\setminus\{p\}$. Обозначим через l_κ вектор, у которого κ-я компонента равна единице, а остальные — нулю. Найдем такое $i\in\{1, ..., n\}$, что $b\in\{-l_1, ..., l_{i-1}, a, -l_{i+1}, ..., -l_n\}^\angle$, и такой $y\in N_i$, что $by\geqslant bx$ для всякого $x\in M_i$. Тогда $by\geqslant bp$, так как $p\in M(a)\subseteq M_i$. С другой стороны, по только что доказанному $y\in N(a)$ и значит либо $y=p$, либо $by<bp$, следовательно, $p=y=N_i$, что и требовалось.

Следствие. Если $a_0\geqslant a(a-1)$, то $|N(a)|\leqslant 1+\sum\limits_{i=1}^{n}\binom{\delta_i+n-2}{n-1}$, где $\delta_i=1+[\log_2 a_i]$ $(i=1, ..., n)$.

8. Из полученных оценок (26) и (28) легко следует, что число крайних точек в задаче групповой минимизации и в задаче о рюкзаке заданной размерности n оценивается сверху многочленом n-й степени от длины входной информации N. Это позволяет надеяться на получение алгоритмов полиномиальной сложности для таких задач (например, для задачи о рюкзаке при $n=2$ такой алгоритм известен [22]). Однако при неограниченном n существуют примеры, в которых число крайних точек растет экспоненциально от N.

Пример 1. Рассмотрим две задачи групповой минимизации с ограничениями

$$x_1+2x_2+4x_3+\cdots+2^{\kappa-1} x_\kappa\equiv 2^\kappa-1 \ (2^\kappa) \tag{30}$$

и

$$x_1'+x_2+2x_3+\cdots+2^{\kappa-2} x_\kappa\equiv 2^{\kappa-1}-1 \ (2^{\kappa-1}), \tag{31}$$

соответственно и обозначим число $|N(G, \kappa, \alpha_0)|$ в первой из них через α_κ, а во второй — через β_κ. Тогда $\alpha_\kappa=\beta_\kappa$, так как из (30) следует, что $x_1\equiv 1$ (2), и подстановка $x_1=1+2x_1'$ переводит (30) в (31). Кроме того, очевидно, что $\beta_\kappa=2\alpha_{\kappa-1}$ и $\alpha_1=1$. Следовательно, $\alpha_\kappa=2^{\kappa-1}\cong 2^{\sqrt{N}}$.

Пример 2. Рассмотрим множество $N(a)$ задачи о рюкзаке с ограничением

$$x_1+2x_2+4x_3+\cdots+2^{\kappa-1} x_\kappa\leqslant 2^\kappa-1.$$

Нетрудно проверить, что $N(a)=\{0\}\cup N(G,\kappa,\alpha_0)$, где множество $N(G,\kappa,\alpha_0)$ соответствует ограничению (30). Аналогичный результат получается и для задачи о (0, 1)-рюкзаке.

Пример 3. Рассмотрим множество $N(\kappa)$ крайних точек множества $M(\kappa)$ таких $x=(x_1,\ldots,x_{2\kappa})$, что $x_j\in\{0,1\}$ $(j=1,2,\ldots,2\kappa)$ и

$$x_1+x_2+2x_3+2x_4+\cdots+2^{\kappa-1}x_{2\kappa-1}+2^{\kappa-1}x_{2\kappa}\leqslant 2^{\kappa}-1.$$

Положим $L=\{x\in Z_+^{2\kappa}\mid x_{2i-1}+x_{2i}=1\ (i=1,2,\ldots,\kappa)\}$. Нетрудно проверить, что $L\subseteq N(\kappa)$ и что $|L|=2^{\kappa}$.

ЛИТЕРАТУРА

1. Юдин Д. Б., Гольштейн Е. Г. Линейное программирование (теория и конечные методы). М., ФМ, 1963.

2. Рокафеллар Р. Выпуклый анализ. М., Мир, 1973.

3. Шевченко В. Н. Линейное программирование и теория линейных неравенств (учебное пособие) Горький, ГГУ, 1977.

4. Шевченко В. Н. О строении выпуклой оболочки множества целочисленных решений системы линейных неравенств. IV Всесоюз. конф. по преблемам теорет. кибернетики. (Тезисы докл.). Новосибирск, 1977, с. 81.

5. Корбут А. А., Финкельштейн Ю. Ю. Дискретное программирование. М., Наука, 1969.

6 Ху Т. Целочисленное программирование и потоки в сетях. М., Мир, 1974.

7. Gomory R. E. Some Polyhedra Related to Combinatorial Problems. J. Linear Algehra and Its Applications. **2**, N 451 (1969).

8. Шевченко В. Н. О решении элементарной задачи целочисленного линейного программирования. Сб. «Управляемые системы». Новосибирск, 1975, вып. 14, с. 69.

9. Piehler J. Gomory—Schnitte und diophantische Gleichungen, «Math. Operationsforsch. u. Statist». 5, Heft, N 4/5, 259 (1974).

10. Шевченко В. Н., Ремизова О. Л. О построении правильных отсечений в целочисленном лийнейном программировании. Учен. зап. ГГУ, Горький, 1973, вып. 166, с. 199.

11. Gomory R. E. On the Relation Between Integer and Non—Integer Solutions to Linear Programs, Proc. Nat. Acad. Sci. USA, **53**, N 2, 260 (1965).

12. Ковалев М. М. Дискретная оптимизация. Минск, Изд-во БГУ, 1977.

13. Glover F. Integer Programming over a Finite additive Group, SIAM J. Contr., N 7, 213 (1969).

14. Курош А. Г. Курс высшей алгебры. М., Наука, 1971.

15. Gorry G., Northup W., Shapiro T. Computational Experience with a Group Theoretic Integer Programming Algorithm, Math. Program, **4**, N 1, 171 (1973).

16. Вотяков А. А. О задачах инвариантных относительно z-округления. «Экон. и мат. методы», 7, № 2, 259 (1971).

17. Колоколов А. А. О длине лексикографически-монотонных последовательностей. — В кн.: Оптимизация территор. и отраслев. систем, методы решения эконом. задач. Новосибирск, 1973, с. 93.

18. Шевченко В. Н. О построении правильных отсечений. Труды 5-й зимней школы-симпозиума по мат. программированию и смежным вопросам, М., ЦЭМИ АН СССР, 1973, вып. 2, с. 266.

19. Шевченко В. Н. Оценки числа крайних точек в некоторых задачах целочисленного программирования. Тезисы докл. III Всесоюз. конф. по исслед. операций. Горький, 1978, с. 248.

20. J. Ch. Fiorot. Math. Program. N 3, 276 (1972).

21. Титчмарш Е. К. Теория дзета-функции Римана. М., ИЛ, 1953.

22. Hirschberg D. S., Wong C. K., A. Polinomial—Time. Algoritim for the Knapsack Problem wich Two. Variables, J. of ACM, **23**, N 1, 147 (1976).

Горьковский государственный университет

[11/XI 1977]

АННОТАЦИИ

УДК 519.72

Методы индексации. В. Е. Алексеев, А. П. Клевцов, А. А. Марков.
Дается обзор подходов к индексации массивов. Предложен новый метод адресации, использующий легко доступную информацию о массиве. Приводятся экспериментальные результаты сравнений различных методов. Библ. 6 назв., табл. 1.

УДК 519.72

О двоичных последовательностях с ограниченной автокорреляцией. В. Е. Алексеев, Н. А. Маслова.
Описан эвристический метод построения двоичных последовательностей с ограниченной автокорреляцией. Приводятся численные результаты, полученные этим методом на ЭВМ. Библ. 4 назв., табл. 1.

УДК 519.83

К вопросу об алгебраической разрешимости диадических игр. Н. Н. Воробьев.
По полиному весьма общего вида строится диадическая игра, для определения ситуации равновесия которой необходимо найти корни заданного полинома. Библ. 5 назв.

УДК 519.712
510.63

Об элементарных теориях некоторых дистрибутивных решеток с аддитивной мерой. Ю. В. Глебский, Е. И. Гордон.
В работе изучаются элементарные теории некоторых классов двуосновных моделей дистрибутивных решеток с аддитивной мерой. Установлена разрешимость некоторых классов таких решеток с относительным дополнением. Эти классы включают в себя многие известные решетки, например решетки ограниченных измеримых множеств с мерой Лебега. Библ. 9 назв.

УДК 519.17

Локальный алгоритм выделения блоков в графе. В. А. Евстигнеев.
В работе доказывается разрешимость задачи о выделении блоков и разделяющих вершин в неориентированном графе в класе локальных алгоритмов. Библ. 7 назв., рис. 7, табл. 1.

УДК 519.83

О сложности определеиия качества позиции в некоторых классах игр над словами.
Л. П. Жильцова, Д. И. Коган.
Выделен класс игр, для которых множество выигрышных позиций для каждого игрока распознается на машине Тьюринга за время n^2. Библ. 7 назв.

УДК 519.11

Оценки параметров д. н. ф. не всюду определенных (частичных) функций алгебры логики. Л. М. Караханян, А. А. Сапоженко.
Исследуются метрические соотношения между различными типами д. н. ф. частичных булевых функций. Для некоторых параметров д. н. ф. получены окончательные или близкие к окончательным оценки. Рассмотрены соотношения между максимальными значениями параметров всюду определенных и частичных функций. Библ. 9, рис. 4.

УДК 519.11

О некоторых асимптотически оптимальных упаковках. Н. Н. Кузюрин.
Получены оценки для упаковок и покрытий в решетках q-ичных векторов на основе подсчета числа решений систем сравнений. Библ. 6.

УДК 519.1
517.52

Одно многозначное разложение Лагранжа, выраженное через коэффициенты исходных рядов. А. В. Куприков.

Находится многозначное обращение (формула) голоморфного отображения вида

$$w_j=(z_j+\varphi_j\ (z))^{k_j}\cdot\psi_j\ (z),\ j=1,...,\ n \qquad (*)$$

Найдена формула разложения в ряд голоморфной функции от многозначного обратного отображения вида (*) через коэффициенты исходных функций. Библ. 6 назв.

УДК 519.712
510.66

Проблема следствия в некоторых подалгебрах алгебр действительных функций. М. Ю. Мошков.

Проблема следствия в различных подалгебрах алгебры функций действительного переменного возникает в связи с локализацией областей в параметрических задачах распознавания образов. Эта проблема исследуется в работе для некоторых важных подалгебр. В ряде случаев дана разрешающая процедура, в других доказана алгоритмическая неразрешимость проблемы. Библ. 9 назв.

УДК 519.714
519.72

Нижние оценки сложности реализации характеристической функции групповых кодов. А. К. Пулатов.

Изучается вопрос о сложности характеристических функций групповых кодов при реализации их параллельно-последовательными контактными схемами (П-схемами). Выявлен ряд случаев, когда характеристические функции групповых кодов при рассматриваемом способе реализации имеют нелинейную сложность и найдены соответствующие оценки. Получены результаты о структуре групповых кодов, а также даны ответы на некоторые вопросы, связанные с построением минимальных П-схем, реализующих булевые функции. Библ. 40 назв.

УДК 519.714.24
519.11

О количественных характеристиках логических формул. В. А. Таланов.

Дается обзор математических результатов об асимптотических характеристиках логических формул. Библ. 9 назв.

УДК 519.852.33

Об одном обобщении задачи о назначениях. В. А. Таланов, В. Н. Шевченко.

Отличие от известной задачи здесь состоит в том, что каждый исполнитель может быть назначен на несколько работ. Требуется определить максимальную суммарную эффективность при ограниченном суммарном числе совместительств. Задача сводится к определению максимального потока в специально построенной сети. Библ. 1 назв., табл. 1.

УДК 519.17

Представление и распознавание триангулированных графов. В. В. Усанов

Рассматривается один из способов представления триангулированных графов и описывается алгоритм распознавания графов этого класса. Библ. 5 назв., рис. 6.

УДК 519.854.3

Выпуклые многогранные конусы, системы сравнений и правильные отсечения в целочисленном программировании. В. Н. Шевченко.

Алгебраический подход к задаче целочисленного линейного программирования (ЗЦЛП) позволяет с единой точки зрения рассмотреть несколько методов решения ЗЦПЛ, получить качественное описание множества целочисленных решений системы линейных неравенств и множества правильных отсечений, а также оценить число крайних точек как в общей ЗЦЛП, так и в ее частных случаях. Библ. 17 назв.

СОДЕРЖАНИЕ

Заявки на сборник просим присылать по адресу: 603005, г. Горький, ул. Ульянова, 10, НИИ ПМК.

КОМБИНАТОРНО-АЛГЕБРАИЧЕСКИЕ МЕТОДЫ В ПРИКЛАДНОЙ МАТЕМАТИКЕ

Межвузовский сборник

Редактор **М. И. Карпович**

Сдано в набор 12.11.79 г. Подписано к печати 29.12.79 г. МЦ 11932.
Формат 70×108$^{1}/_{16}$. Бумага типографская № 2. Гарнитура литературная. Печать высокая. Усл. печ. л. 10,85. Уч.-изд. л. 10. Заказ 9258. Тираж 700 экз. Цена 1 р. 50 к.

Горьковский государственный университет им. Н. И. Лобачевского,
г. Горький, пр. Гагарина, д. 23

Дзержинская типография Горьковского областного управления издательств, полиграфии и книжной торговли