ОБ ОДНОМ ПОДХОДЕ К ОПТИМИЗАЦИИ НА ДИСКРЕТНО-НЕПРЕРЫВНОМ МНОЖЕСТВЕ

А. Ш. Абакаров, Ю. А. Сушков (Санкт-Петербург)

Предлагается подход к решению задач оптимизации на дискретно-непрерывном множестве (mixed discrete-continuous optimization problems), базирующийся на комбинированном использовании адаптивного случайного поиска (СП) [1] и различных алгоритмов дискретной оптимизации, в частности, — жадных алгоритмов.

В общем виде задачу оптимизации на дискретно-непрерывном множестве можно представить следующим образом:

$$F(\lambda, s) \to \min_{\lambda \in \Lambda, s \in S}, \qquad (1)$$

где $\lambda \in \Lambda \subset \mathbb{R}^n$, $s \in S$ (S — некоторое дискретное множество).

В научных статьях, опубликованных за рубежом, для решения задач вида (1) в основном применяются генетические алгоритмы. Проведенные на широком классе тестовых функций статистические исследования СП [1, 2] позволили сделать вывод о преимуществе последнего над генетическими алгоритмами. В результате имеются достаточные основания полагать о возможностях СП более эффективно решать задачи вида (1). Апробация предлагаемого подхода была проведена на задачах синтеза структурно управляемых систем [3].

На базе адаптивного случайного поиска и алгоритма Хука — Дживса разработана диалоговая программная система глобальной оптимизации "OPTIMUM 1.0" (программную систему планируется сделать доступной на Интернет-сайте: http://r-tech.narod.ru).

Работа выполнялась при финансовой поддержке гранта РФФИ — ГФЕН Китая (проект 04-01-39002ГФЕН2004а).

Список литературы

1. Сушков Ю. А. Метод, алгоритм и программа случайного поиска — Л.: ВНИИТрансМаш, 1969. — 43 с.

2. Абакаров А. Ш., Сушков Ю. А. Статистическое исследование случайного поиска // Математические модели. Теория и приложения. — СПб.: СПбГУ, 2002. — С. 87–101.

3. Абакаров А. Ш., Сушков Ю. А. О синтезе структурно управляемых систем // Математические модели. Теория и приложения. — СПб.: СПбГУ, 2003. — С. 3–23.

О КВАНТОВОЙ СЛОЖНОСТИ БУЛЕВОЙ ФУНКЦИИ «ЗАДАЧА О СКРЫТОЙ ПОДГРУППЕ»

Ф. М. Аблаев, А. Ф. Хасьянов (Казань)

Пусть G — конечная группа, а K — ее нормальная подгруппа. Пусть X — конечное множество. Пусть функция $g : G \to X$ принимает различные значения на элементах из различных смежных классов группы G по подгруппе K и принимает одинаковые значения на элементах принадлежащих одному смежному классу. Задача определения (в том или ином смысле) подгруппы K по функции g называется задачей о скрытой подгруппе (см., например книгу [2]). Целый ряд задач (в частности задачи факторизации и дискретного логарифма) являются задачами о скрытой подгруппе [2].

Мы определяем булевскую функцию $HSP_{G,K,X}$ (булевский вариант задачи о скрытой подгруппе) и рассматриваем сложность ее реализвции в квантовых OBDD. Модель квантовой OBDD определена в работе [1]. Результат реализации вычисления в квантовой OBDD — вероятностный. В квантовой OBDD вершины разбиты на уровни. Ширина $width(P)$ квантовой OBDD P — это максимальное число вершин на уровнях P.

ТЕОРЕМА. Функция $HSP_{G,K,X}(\sigma)$ вычислима с ошибкой ≤ 0.4 квантовыми один раз читающими бинарными программами ширины $O(\log|X||G/K|)$.

Для группы G, ее подгруппы K обозначим $CCN(G,K)$ число общих смежных классов.

ТЕОРЕМА. Пусть K — нетривиальная подгруппа конечной группы G. Пусть X — некоторое конечное множество. Пусть квантовая OBDD P вычисляет $HSP_{G,K,X}$ с ошибкой ≤ 0.4. Тогда $width(Q) \in \Omega(\log|X|CCN(G,K) + |G/K|)$.

Работа выполнена при финансовой поддержке РФФИ (проект 03-01-00769).

Список литературы

1. Ablayev F., Gainutdinova A., Karpinski M. On computational power of quantum branching programs // Proceedings of FCT-2001. — Lecture Notes in Computer Science. — Springer-Verlag, 2001. — № 2138.

2. Nielsen M. A., Chuang I. L. Quantum computation and quantum information. — Cambridge University Press, 2000.

О СИММЕТРИИ И ТОЧНЫХ РАСШИРЕНИЯХ ГРАФОВ

М. Б. Абросимов (Саратов)

Граф $G^* = (V^*, \alpha^*)$ называется точным вершинным (реберным) k-расширением графа $G = (V, \alpha)$, если G изоморфен каждому подграфу графа G^*, получающемуся удалением любых k вершин (ребер). В данной работе рассматривается случай $k = 1$. Точные вершинные расширения графов впервые были введены Харари и Хейзом в работе [1]. В работе [2] получены результаты, связывающие точные вершинные расширения графов и свойство дополнительности расширения графа. Далее приводятся результаты, устанавливающие связь между точными расширениями и симметрическими графами.

Две вершины u и v графа G называются подобными, если для некоторого автоморфизма f этого графа $f(u) = v$. Два ребра $e_1 = \{u_1, v_1\}$ и $e_2 = \{u_2, v_2\}$ называются подобными, если существует такой автоморфизм f графа G, что $f(\{u_1, v_1\}) = \{u_2, v_2\}$.

Граф называется вершинно-симметрическим, если любая пара его вершин подобна, и реберно-симметрическим, если любая пара его ребер подобна. Граф называется симметрическим, если он вершинно- и реберно-симметрический.

ТЕОРЕМА 1 [1]. Граф G является точным вершинным 1-расширением тогда и только тогда, когда он является вершинно-симметрическим.

Удалось получить следующий результат в этом направлении:

ТЕОРЕМА 2. Всякий однородный граф G является точным реберным 1-расширением тогда и только тогда, когда он является реберно-симметрическим.

С учетом известной связи между реберно-симметрическими и вершинно-симметрическими графами можно установить связь между точными реберными и вершинными 1-расширениями.

ТЕОРЕМА 3. Пусть однородный граф G является точным реберным 1-расширением, тогда он является либо точным вершинным 1-расширением, либо двудольным графом.

Список литературы

1. Harary F., Hayes J. P. Node fault tolerance in graphs // Networks. — 1996. — V. 27. — P. 19–23.

2. Абросимов М. Б. Минимальные расширения дополнений графов // Теоретические проблемы информатики и ее приложений. — Саратов: СГУ, 2001. — Вып. 4. — С. 11–19.

ОПТИМАЛЬНЫЕ МЕТОДЫ УПРАВЛЕНИЯ FIFO-ОЧЕРЕДЯМИ В ПАМЯТИ ОДНОГО УРОВНЯ

Е. А. Аксёнова, А. В. Соколов (Петрозаводск)

Для представления очереди в памяти компьютера используются два основных способа хранения — связанное и последовательное представления. Также, возможен промежуточный способ, когда очередь представлена в виде связанного списка страниц одной длины. В случае связанного представления работа продолжается до полного исчерпания свободной памяти, но часть памяти тратится на связи. В случае последовательного представления при переполнении очереди часть памяти остается свободной.

В данной работе предлагаются математические модели, предназначенные для анализа методов представления трех очередей в памяти одного уровня. Для описания процесса представления трех очередей предложены модели в виде случайного блуждания в трехмерном пространстве. Для решения задач использовались результаты теории конечных поглощающих цепей Маркова. Предложены алгоритмы нумерации состояний процессов блуждания. Доказаны теоремы, описывающие структуру матриц переходных вероятностей для рассмотренных случайных блужданий. Разработаны алгоритмы и программы, с помощью которых вычисляется среднее время до переполнения выделенного объема памяти и определяется оптимальное разбиение памяти для представления структур данных. Вычисления проводились на многопроцессорной машине IBM pSeries 690 (Regatta).

Список литературы

1. Кнут Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы. — М.: Вильямс, 2001.

2. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М: Наука, 1970.

3. Соколов А. В. Математические модели и алгоритмы оптимального управления динамическими структурами данных. — Петрозаводск, 2002.

4. Феллер В. Введение в теорию вероятностей и ее приложения. — М.: Мир, 1964.

ОЦЕНКИ НАДЕЖНОСТИ СХЕМ В БАЗИСЕ $\{x \vee y \vee z, x\&y\&z, \bar{x}\}$ ПРИ ОДНОТИПНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в базисе $\{x\&y\&z, x\vee y\vee z, \bar{x}\}$ [1]. Предполагается, что входы элементов схемы независимо друг от друга переходят в неисправные состояния типа 0. Эти неисправности характеризуются тем, что поступающий на вход элемента нуль не искажается, а единица — с вероятностью γ ($\gamma < 1/2$) может превратится в нуль.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей функцию $f(\tilde{x})$ при входном наборе $\tilde{a}$. Ненадежность $P(S)$ схемы S есть максимальное из чисел $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах $\tilde{a}$. Надежность схемы равна $1 - P(S)$. Обозначим $P(f) = \inf P(S)$, где S — схема из ненадежных элементов, реализующая функцию f. Схему S, реализующую функцию f, назовем асимптотически наилучшей по надежности, если $P(S) \sim P(f)$ при $\gamma \to 0$.

Очевидно, функцию x_i, $i = 1, 2, ..., n$, можно реализовать абсолютно надежно. Нетрудно построить схемы, реализующие константы 0 и 1 сколь угодно надежно. Ответ на вопрос об оценках ненадежности "наилучшей" схемы для произвольной булевой функции f содержат следующие теоремы.

ТЕОРЕМА 1. При $\gamma \leq 1/8$ любую булеву функцию $f(x_1, ..., x_n)$ можно реализовать схемой A такой, что $P(A) \leq \gamma^3 + 5\gamma^4$.

ТЕОРЕМА 2. Для любой функции $f(x_1, ..., x_n)$, отличной от констант 0, 1 и функций x_i ($i = 1, 2, ..., n$), и любой схемы B, реализующей f, при $\gamma < 1/2$ верно неравенство $P(B) \geq \gamma^3$.

Из теоремы 2 следует, что схемы из теоремы 1 являются асимптотически наилучшими по надежности для функций $f(x_1, ..., x_n)$, отличных от x_i ($i = 1, 2, ..., n$) и констант, и функционируют с ненадежностью, асимптотически равной γ^3 при $\gamma \to 0$.

Исследование выполнено при финансовой поддержке научной программы «Университеты России» (проект 04.01.032).

Список литературы

1. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

ВЕРХНЯЯ ОЦЕНКА НЕНАДЕЖНОСТИ СХЕМ В БАЗИСЕ $\{x \vee y, \bar{x}\}$ ПРИ ИНВЕРСНЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина, В. В. Чугунова (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в базисе $\{x \vee y, \bar{x}\}$ [1]. Предполагается, что входы элементов схемы независимо друг от друга подвержены инверсным неисправностям. Эти неисправности характеризуются тем, что поступающее на вход элемента значение a, ($a \in \{0, 1\}$) с вероятностью ε ($\varepsilon < 1/2$) может превратится в $\bar{a}$.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей функцию $f(\tilde{x})$ при входном наборе $\tilde{a}$. Ненадежность $P(S)$ схемы S есть максимальное из чисел $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах $\tilde{a}$. Надежность схемы равна $1-P(S)$.

Нетрудно проверить, что ненадежности базисных элементов дизъюнктора и инвертора соответственно равны $2\varepsilon - \varepsilon^2$ и ε.

Справедлива следующая теорема.

ТЕОРЕМА. При $\varepsilon \leq 1/640$ любую булеву функцию $f(x_1, ..., x_n)$ можно реализовать схемой S такой, что $P(S) \leq 4\varepsilon + 86\varepsilon^2$.

Результат теоремы получается так же как верхние оценки ненадежности схем в работе [2]. Заметим, что схемы, построенные при доказательстве теоремы, являются надежными, причем ненадежность этих схем не больше ненадежности дизъюнктора в два с половиной раза и не больше ненадежности инвертора в пять раз. Отметим также, что полученная оценка ненадежности справедлива для функций любого числа переменных n.

Исследование выполнено при финансовой поддержке научной программы «Университеты России» (проект 04.01.032).

Список литературы

1. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

2. Алехина М. А. Верхние оценки ненадежности схем при однотипных константных неисправностях на входах элементов // Материалы VII Международного семинара "Дискретная математика и ее приложения" (29 января – 2 февраля 2001 г.). — Ч. 1. — М.: Изд-во центра прикл. исслед. при механ.-матем. фак-те МГУ, 2001.

СЛОЖНОСТЬ КОНТРОЛЯ БЛОКОВ УПРАВЛЯЕМЫХ ПЕРЕСТАНОВОК

Е. Н. Анисимова (Донецк)

Новый криптографический примитив класса высокоскоростных шифров — блок управляемых перестановок (БУП). Анализу их работоспособности не уделяется достаточного внимания ни в криптографии, ни в технической диагностике. Поэтому разработка тестов, основанных на максимальном использовании структуры БУП — актуальная задача. Неисправности — константные неисправности ($\equiv 0, \equiv 1$) и короткое замыкание на линиях схемы. Сложность схемы S — число C_S всех линий схемы, а сложность минимального теста L_a равна $C_S^a = дл(L_a) \cdot шир(L_a)$,$(a \in (обн, лк))$ ($дл(L_a)$ и $шир(L_a)$ — длина и ширина L_a). Пусть m и n — размерность управляющего и информационного векторов. Сложность БУП $M_{n,m}$ с матричной и послойной структурой при $n \to \infty$ равна $C_{M_{n,m}} = O(n \cdot 2^m)$ и $C_{P_{n,m}} = O(n \cdot l)$ $(l = 2 \cdot m \cdot n^{-1})$.

ТЕОРЕМА 1. $C^a_{M_{n,m}} = O(4^m \cdot C_{M_{n,m}})$ при $n \to \infty$.

ТЕОРЕМА 2. $C^{обн}_{P_{n,m}} = O(C_{P_{n,m}})$ при $n \to \infty$, $C^{лк}_{P_{n,m}} = O(m^2)$ при $m \to \infty$.

Сложность рекурсивной модели БУП $R_{2n,2m+n}$ $(n = 2^k)$ с послойной структурой равна $C_{R_{2n,2m+n}} = O(n^2)$ при $n \to \infty$.

ТЕОРЕМА 3. Для одиночных неисправностей схемы $R_{2n,2m+n}$ $C^a_{R_{2n,2m+n}} = O(C_{R_{2n,2m+n}})$ при $n \to \infty$.

Таким образом, в рассмотренных случаях сложность обнаружения либо локализации неисправностей асимптотически линейна от размера схемы. Эта сложность — верхняя оценка сложности обеспечения работоспособности сети Клоса, схем Бенеша и Ваксмана, применяемых при синтезе высокоскоростных блочных шифров.

Список литературы

1. Молдовян А. А. и др. Криптография: скоростные шифры. — СПб.: БХВ-Петербург, 2002. – 496 с.

2. Скобелев В. Г., Анисимова Е. Н. Сложность локализации неисправностей блока управляемых перестановок // Искусственный интеллект. — 2004. — № 4. — С. 794–803.

3. Анисимова Е. Н, Скобелев В. Г. Анализ послойных блоков управляемых перестановок // Искусственный интеллект. — 2005. — № 1. — С. 4–10.

О РАСЩЕПЛЯЕМОСТИ p-ИЧНЫХ ФУНКЦИЙ

М. И. Анохин (Москва)

Пусть V — ненулевое n-мерное векторное пространство над полем F из p элементов, где p — простое число. Пусть также φ — произвольная функция из V в F. Предположим, что V является прямой суммой множества $\mathcal{S}$ своих ненулевых подпространств. Назовем множество $\mathcal{S}$ расщепляющим (для φ), если φ представима в виде $\varphi(\sum_{U\in\mathcal{S}} x_U) = \sum_{U\in\mathcal{S}} \varphi_U(x_U)$ $(x_U \in U, U \in \mathcal{S})$ для некоторых функций $\varphi_U \colon U \to F$. Легко видеть, что все такие функции φ_U имеют вид $\varphi|_U + c_U$ для произвольного семейства констант $c_U \in F$, удовлетворяющих равенству $\sum_{U\in\mathcal{S}} c_U = (1 - |\mathcal{S}|)\varphi(0)$. Таким образом, по заданному расщепляющему множеству $\mathcal{S}$ можно легко найти вышеуказанное представление функции φ.

Функция φ называется расщепляемой, если она обладает расщепляющим множеством, отличным от $\{V\}$ или, что эквивалентно, двухэлементным расщепляющим множеством.

ТЕОРЕМА 1. Существует полиномиальный от $\log p^{p^n}$ детерминированный алгоритм, который по произвольной функции $\varphi\colon V \to F$ (заданной таблицей своих значений) проверяет, является ли она расщепляемой, и в случае расщепляемости φ находит двухэлементное расщепляющее множество для φ.

Теорема 1 дает решение задачи 2.17 из книги [1] (поставленной там в случае, когда $p = 2$).

Расщепляющее множество $\mathcal{S}$ для φ называется полным, если для любого $U \in \mathcal{S}$ функция $\varphi|_U$ нерасщепляема. Представляет интерес нахождение условий, при которых полное расщепляющее множество единственно (существование его тривиально). Очевидно, что к таким условиям относится нерасщепляемость функции φ. Другое условие дается в следующей теореме.

ТЕОРЕМА 2. Если не существует $v \in V \setminus \{0\}$ такого, что производная φ по направлению v аффинна, то полное расщепляющее множество для φ единственно.

Автор благодарит О. А. Логачёва, А. А. Сальникова и В. В. Ященко за постановку задачи и полезные обсуждения.

Список литературы

1. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

СВЕДЕНИЕ СИСТЕМЫ ЛИНЕЙНЫХ НЕРАВЕНСТВ ТРАНСПОРТНОГО ТИПА К ЗАДАЧЕ ПОИСКА МАКСИМАЛЬНОГО ПОТОКА В СЕТИ ПРИ ДОПОЛНИТЕЛЬНЫХ ОГРАНИЧЕНИЯХ

Л. Г. Афраймович (Нижний Новгород)

При решении задачи распределения однородного ресурса в иерархических системах [1] необходимо проверять на совместность системы линейных неравенств транспортного типа:

$$b_i^- \le \sum_{j=1}^{n} a_{ij}x_j \le b_i^+,\ i=\overline{1,m},$$

где $a_{ij} \in \{1,0,-1\}$, $i=\overline{1,m}$, $j=\overline{1,n}$. Исследование совместности рассматриваемой системы линейных неравенств сводится к поиску максимального потока транспортной сети при дополнительных ограничениях: пусть $N=(s,t,V,A,b,\varphi)$ — транспортная сеть, в основе которой лежит (n,m) орграф $G=(V,A)$, s — исток, t — сток, $s,t \in V$, b — m-мерный вектор дуговых ограничений, φ — некоторое бинарное отношение эквивалентности, заданное на множестве дуг. Обозначим через B матрицу инцидентности орграфа G; v — величину потока; d — вспомогательный n-мерный вектор, $d_i=0$ при $i \ne s,t$, $d_s=-1$, $d_t=1$. Тогда задача заключается в поиске m-мерного вектора потока f, i-я компонента которого означает величину потока на соответствующей дуге x_i, $x_i \in A$, $i=\overline{1,m}$, такого, что выполняются ограничения: $Bf+dv=0$; $0 \le f \le b$; $f_i=f_j$, если имеет место $x_i \varphi x_j$, $x_i,x_j \in A$; и принимает максимальное значение величина потока v. Рассматриваемая задача является задачей линейного программирования. Применив к ней прямо-двойственный алгоритм [2], получаем, что поток f^1 величины v_1 является максимальным в том и только в том случае, если не существует m-мерного вектора f^2 такого, что поток f^1+f^2 величины v_2 удовлетворяет условиям задачи и $v_2 > v_1$.

Список литературы

1. Прилуцкий М. Х. Многокритериальное распределение однородного ресурса в иерархических системах // Автоматика и телемеханика. — 1996. — № 2. — С. 24–29.

2. Пападимитриу Х., Стайглиц К. Комбинаторная оптимизация. Алгоритмы и сложность. — М.: Мир, 1985. — 510 с.

МЕТОД ОБЕСПЕЧЕНИЯ ПЛАНИРУЕМОСТИ ЗАДАЧ НА СИСТЕМАХ С ДИНАМИЧЕСКИМ ПЛАНИРОВАНИЕМ

В. В. Балашов (Москва)

При разработке вычислительной системы (ВС) реального времени часто возникает проблема непланируемости набора вычислительных задач (ВЗ), т. е. невозможности обеспечить при заданной производительности ВС гарантированное выполнение ВЗ на ВС в рамках директивных сроков. В таком случае разработчик ВС должен повысить производительность ВС или снизить вычислительную нагрузку на ВС. Снижение вычислительной нагрузки может быть достигнуто посредством сокращения наихудшего времени выполнения отдельных ВЗ и/или уменьшения частоты их выполнения.

В докладе предложен метод определения изменений времён и частот выполнения ВЗ (далее — параметры ВЗ), достаточных для обеспечения планируемости заданного непланируемого набора ВЗ, предназначенного для выполнения на ВС. Метод разработан для ВС с динамическим планированием ВЗ с фиксированными приоритетами. При работе в рамках метода разработчик ВС указывает для каждой ВЗ рамки допустимого изменения её параметров, а также значения штрафов, накладываемых на эти изменения. По этим входным данным вычисляются требуемые изменения параметров ВЗ с учётом требования минимальности суммы штрафов. Определение планируемости набора ВЗ осуществляется по формулам из работы [1].

Задача поиска требуемых изменений параметров ВЗ с учётом штрафов на изменения является оптимизационной. Для её решения автором разработаны алгоритмы на основе жадных алгоритмов и алгоритмов имитации отжига, учитывающие специфику задачи (в частности, влияние параметров высокоприоритетных задач на соблюдение директивных сроков низкоприоритетных задач). Выполнена реализация этих алгоритмов в виде программного средства. В докладе будут приведены результаты исследования работы реализованных алгоритмов с точки зрения оптимальности находимого решения и времени поиска этого решения.

Работа выполнена при финансовой поддержке РФФИ.

Список литературы

1. K. W. Tindell. An Extendible Approach for Analysing Fixed Priority Hard Real-Time Tasks. // University of York, England, 1994

ДИСКРЕТНАЯ ХАРАКТЕРИЗАЦИЯ ПОЧТИ КОНТАКТНЫХ МЕТРИЧЕСКИХ ГИПЕРПОВЕРХНОСТЕЙ AH-МНОГООБРАЗИЙ

М. Б. Банару (Смоленск), Т. Л. Мелехина (Москва)

Одним из наиболее интересных и важных примеров почти контактной метрической структуры является структура на ориентируемой гиперповерхности почти эрмитова (almost Hermitian, AH-) многообразия. Ранее [1–3] предпринимались попытки характеризации некоторых видов таких гиперповерхностей в терминах их типового числа (type number). Такого рода характеризация гиперповерхностей в последнее время активно разрабатывалась известным японским математиком Риоши Такаджи и его учениками главным образом для гиперповерхностей комплексного проективного пространства, а также комплексных пространственных и кватернионных пространственных форм (см., например, [4, 5]).

Отметим однако, что в упомянутых выше работах [1–3] дается характеризация лишь для некоторых специальных видов почти контактной метрической структуры (косимплектической, слабо косимплектической, сасакиевой, структуры Кенмоцу) на гиперповерхности AH-многообразия. В докладе предполагается обобщить полученные ранее результаты в данном направлении и представить ряд новых фактов, касающихся дискретной характеризации почти контактных метрических гиперповерхностей общего вида.

Список литературы

1. Банару М. Б. О типовом числе слабо косимплектических гиперповерхностей приближённо келеровых многообразий // Фундаментальная и прикладная математика. — 2002. — Т. 8, вып. 2. — С. 357–364.

2. Банару М. Б. Две теоремы о косимплектических гиперповерхностях 6-мерных эрмитовых подмногообразий алгебры Кэли // Известия вузов. Математика. — 2002. — № 1 (476). — С. 9–12.

3. Банару М. Б. О сасакиевых гиперповерхностях 6-мерных эрмитовых подмногообразий алгебры Кэли // Математический сборник. — 2003. — Т. 194, № 8. — С. 13–24.

4. Kurihara H., Takagi R. A note on the type number of real hypersurfaces in $P(C)_n$ // Tsukuba J. Math. — 1998. — V. 22. — P. 793–802.

5. Kurihara H. The type number on real hypersurfaces in a quaternionic space form // Tsukuba J. Math. — 2000. — V. 24. — P. 127–132.

ОРТОГОНАЛЬНЫЕ ГИПЕРКУБЫ И МНОГОМЕСТНЫЕ АЛГЕБРАИЧЕСКИЕ ОПЕРАЦИИ

Г. Б. Белявская (Кишинев)

Пусть d-гиперкуб ($d \geq 2$) порядка n — это $n \times n \times ... \times n$ таблица с n^d позициями, заполненными n символами [1].

Два d-гиперкуба порядка n ортогональны, если при их наложении каждая из n^2 упорядоченных пар символов появляется n^{d-2} раз [1].

Множество из $t \geq 2$ гиперкубов ортогонально, если каждая пара различных гиперкубов ортогональна (кратко, МОНС).

Гиперкубы и МОНС связаны с аффинными схемами, аффинными и проективными геометриями, ортогональными таблицами, (k, n)-сетями и (t, m, s)-сетями, графами, кодами и шифрами и т. д.

Пусть H — d-мерный гиперкуб, заданный на множестве Q порядка n, тогда d-операция A на Q, соответствующая H, может быть определена следующим образом: $A(x_1^d) = a$, если в позиции $(x_1, x_2, \ldots, x_d)$ в H находится элемент $a \in Q$.

Две d-операции A и B порядка n, заданные на множестве Q, ортогональны, если пара уравнений $A(x_1^d) = a$ и $B(x_1^d) = b$ имеет точно n^{d-2} решений для любых элементов $a, b \in Q$.

Назовем k-набор $< A_1, A_2, \ldots, A_k >$, $1 \leq k \leq d$, различных d-операций, заданных на множестве Q, ортогональным, если система $\{A_i(x_1^d) = a_i\}_{i=1}^k$ имеет точно n^{d-k} решений для любых $a_1^k \in Q^k$.

Множество $\Sigma = \{A_1, A_2, \ldots, A_t\}$ из d-операций называется k-кратно ортогональным, $1 \leq k \leq d$, $t \geq k$, если каждый k-набор $< A_{i_1}, A_{i_2}, \ldots, A_{i_k} >$ различных d-операций из Σ ортогонален.

ТЕОРЕМА 1. Если множество $\Sigma = \{A_1, A_2, \ldots, A_t\}$, $t \geq k$, d-операций порядка n, заданных на множестве Q, является k-кратно ортогональным, $1 \leq k \leq d$, то множество Σ является l-кратно ортогональным для любого l, $1 \leq l < k$.

ТЕОРЕМА 2. Любой ортогональный k-набор $< A_1^k >$ d-операций может быть вложен в ортогональный d-набор $< A_1^k, B_{k+1}^d >$ d-операций, где $1 \leq k \leq d$.

Работа выполнена при финансовой поддержке MRDA и CRDF (проект MM1-3040-CH-02).

Список литературы

1. Kishen K. On the construction of latin and hyper-graeco-latin cubes and hypercubes // J. Ind. Soc. Agric. Statist. — 1950. — V. 2. — P. 20–48.

АЛГОРИТМ С ЖЕСТКИМ ПОРЯДКОМ ПРОВЕРОК ПОСТРОЕНИЯ РЕШАЮЩИХ ДЕРЕВЬЕВ ДЛЯ ЗАДАЧИ ИНТЕРВАЛЬНОГО ПОИСКА НА БУЛЕВОМ КУБЕ

Т. Д. Блайвас (Москва)

Рассматривается следующая задача поиска. Задано некоторое k-элементное подмножество n-мерного булевого куба, называемое библиотекой. Для произвольного интервала данного булевого куба (запроса) требуется определить, какие элементы библиотеки попадают в этот интервал-запрос. Задача решается в классе информационных деревьев над базовым множеством переменных. В качестве критерия сложности алгоритма рассматривается среднее количество шагов алгоритма, где на одном шаге может быть вычислено значение одной переменной.

Предложен алгоритм построения информационных деревьев по библиотеке и произвольной перестановке координат $\sigma \in S_n$, названный алгоритмом с жестким порядком проверок.

Обозначим через $T(D)$ сложность информационного дерева D, а через $\mathcal{D}_I$ — множество деревьев, решающих задачу поиска I. Тогда $T(I) = \min_{D\in\mathcal{D}_I} T(D)$. Пусть $\mathcal{I}(n,k)$ — множество задач на n-мерном булевом кубе, мощность библиотек которых равна k. Обозначим через $A(I,\sigma)$ информационное дерево, полученное алгоритмом с жестким порядком проверок для задачи I и перестановки $\sigma \in S_n$. Положим $\bar{T}(n,k) = \mathbf{M}_{I\in\mathcal{I}(n,k),\sigma\in S_n} A(I,\sigma)$.

ТЕОРЕМА. При $n\to\infty$, $k\to\infty$, $n = \bar{o}(2^k)$, $k = \bar{o}(2^n)$ выполнено $\bar{T}(n,k) \asymp \left(\frac{k}{\log_2 k}\right)^{\log_2 \frac{4}{3}}$.

Таким образом показано, что алгоритм с жестким порядком проверок в среднем строит решающие деревья со сложностью, лучшей по порядку, чем сложность сбалансированных деревьев [1].

Автор выражает благодарность Э. Э. Гасанову за постановку задачи.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 05-01-00709).

Список литературы

1. Блайвас Т. Д. Асимптотика сложности интервального поиска на булевом кубе в классе сбалансированных деревьев // Дискретная математика. — 2004. — Т. 16, вып. 4. — С. 65–78.

СТАТИСТИЧЕСКИ ТОЧНЫЙ АЛГОРИТМ РЕШЕНИЯ ЗАДАЧИ О ДИАДИЧЕСКОМ ДЕРЕВЕ

Е. В. Бобылева (Днепропетровск)

Задача о диадическом дереве является представителем подкласса NP-трудных задач об остовных деревьях ограниченной степени [1].

Под диадическим деревом (ДД) понимается дерево, в котором все невисячие вершины имеют степень, равную 3. Если рассмотреть это понятие в терминах теории фрактальных графов, то ДД является предфрактальным деревом, порожденным 3-вершинной звездой [2].

Рассматриваемая в данной работе задача формулируется следующим образом. Пусть задан n-вершинный граф $G = (V,E)$ с нечетным числом вершин $n = |V|$, в котором каждому ребру $e \in E$ приписан вес $w(e) > 0$. Допустимым решением задачи о диадическом дереве на графе G является всякий остовный подграф $x = (V, E_x), E_x \subset E$, который представляет собой корневое диадическое дерево; $X = X\{G\} = \{x\}$ — множество всех допустимых решений (МДР) на графе G. На МДР X определена целевая функция (ЦФ)

$$F(x) = \textstyle\sum_{e\in E_x} w(e) \to \min.$$

Необходимо найти оптимальное решение $x^* \in X$, такое, что $F(x^*) = \min_{x\in X} F(x)$.

Предлагается малотрудоемкий приближенный алгоритм решения сформулированной задачи. Данный алгоритм исследован на вероятностных графах. Получены достаточные условия его статистической эффективности, то есть условия, при выполнении которых алгоритм "почти всегда" находит оптимальное решение.

Список литературы

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

2. Перепелица В. А., Сергиенко И. В., Кочкаров А. М. К проблеме распознавания фрактальных графов // Кибернетика и системный анализ. — 1999. — № 4. — С. 72–89.

ЛОГИКО-СТРУКТУРНОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ УПРАВЛЕНИЯ

А. С. Богомолов (Саратов)

Проблемы оптимизации управления процессами исследований, разработками и производством интеллектуально-технической продукции (приборов, технических элементов систем управления) особенно актуальны в настоящее время в силу возрастания сложности и многообразия этих процессов. Из-за разнообразия этих процессов и их взаимодействий они не поддаются унифицированному описанию. Поэтому возникает проблема выбора формального аппарата для адекватного описания указанных процессов и их взаимодействий. При выборе формального аппарата описания следует исходить из того, что как технические элементы и механизмы, так и интеллектуальные субъекты (специалисты и разработчики), участвующие в реализации процессов преобразования материальных и информационных потоков различной природы по своим функционально-структурным признакам аналогичны дискретным преобразователям информации и таким образом имеют общую логико-структурную модель.

Логической основой данного положения является то, что технические механизмы и интеллектуальные элементы могут находиться в двух устойчивых состояниях (способность к выполнению требуемых функций или неспособность к указанным действиям), что позволяет описывать данные процессы в рамках аппарата алгебры логики. С другой стороны, различные процессы преобразований потоков (материальных, информационных) определяются необходимыми и достаточными условиями, которые можно представить логико-структурной схемой и таким образом поведение дискретных преобразователей (как моделей) описывается в рамках логико-структурной универсальной модели, имеющей конечный алфавит.

В сообщении рассматривается задача выявления функциональных операций, необходимых для установления зависимостей между логическими условиями и технологическими или интеллектуальными операторами. С этой целью проанализированы различные комбинации используемых схем алгоритмов, на основе которых выявлены основные функциональные зависимости и разработаны логико-структурные блоки, составляющие основу аппарата формализации производственных процессов.

ЧИСЛО ПЕРЕСЕЧЕНИЙ ПОЛНЫХ r-ДОЛЬНЫХ ГРАФОВ

Н. С. Большакова (Мурманск)

Для графов используем терминологию принятую Харари [1]. Граф $r\overline{K}_n$ — полный r-дольный граф, где мощность всех долей равна n. Граф $\Gamma(V,E)$ называется графом пересечений на множестве U, если существует инъекция φ: $V\to 2^U-\{\emptyset\}$ такая, что $\{a,b\}\in E$ равносильно $\varphi(a)\cap\varphi(b)\neq\emptyset$ для всех $a,b\in V$. Числом пересечений графа Γ называется наименьшее число $n=nin(\Gamma)$ такое, что Γ является графом пересечений на n-элементном множестве U. Понятие графа пересечений введено в работе Марчевского [2]. В [3] доказано, что $nin(r\overline{K}_2)\sim\log_2 r$, при $r\to\infty$. В [4] анонсирован результат: $nin(r\overline{K}_2+K_m)$ равно наименьшему $s\in N$ такому, что $m+r\leq 2^{s-1}$, $r\leq\binom{s-1}{[s/2]-1}$.

Латинские квадраты C и D порядка n называются псевдоортогональными, если любые две строки матриц C и D имеют в точности один общий элемент. Если $n=p^k$, где $p>0$ — простое число, $k\in N$, то существует семейство из $n-1$ псевдоортогонального $n\times n$ латинского квадрата. Пусть $n=p_1^{k_1}\ldots p_r^{k_r}$ — каноническое разложение числа $n\geq 2$ на простые множители, $t=\min\{p_1^{k_1}-1,\ldots,p_r^{k_r}-1\}$. Тогда существует множество из t псевдоортогональных $n\times n$ латинских квадратов.

Пусть $npols(n)=t$ — наибольшее число, для которого существует множество из t псевдоортогональных $n\times n$ латинских квадратов. Например: $npols(6)=1$, $npols(10)\geq 2$, $npols(12)\geq 5$.

ТЕОРЕМА 1. Пусть $n>1$ и $r\geq 3$. Существование $r-2$ попарно псевдоортогональных $n\times n$ латинских квадратов равносильно $nin(r\overline{K}_n)=n^2$.

ТЕОРЕМА 2. Если $2\leq r\leq npols(n)+2$, $0\leq m\leq 2^{n^2-n}$, то число пересечений графа $r\overline{K}_n+K_m$ равно n^2.

Список литературы

1. Харари Ф. Теория графов. — М.: Мир, 1973.

2. Marczewski E. Sur deux proprietes des classes d'ensembles. — Fund. Math. — 1945. — V. 33. — P. 303–307.

3. Schinerman E. R., Trenk A. N. On the fractional intersection number of graph // Graph and Comb. — 1999. — № 3. — P. 341–351

4. Маренич Е. Е. Число пересечений графа // Материалы VIII Международного семинара "Дискретная математика и ее приложения". — М.: Изд-во механико-математического ф-та МГУ, 2004. — С. 216–219.

АДДИТИВНАЯ ЗАДАЧА ПЕРЕЧИСЛЕНИЯ ПЕРЕСТАНОВОК

Л. Н. Бондаренко (Пенза)

При нечетном n операция сложения "$\oplus$" двух перестановок из S_{n-1} определяется как их поэлементное сложение по mod n, причем результатами являются наименьшие положительные вычеты. Перестановки $\sigma, \overline{\sigma} \in S_{n-1}$ называются дополнительными относительно "$\oplus$", если $\sigma \oplus \overline{\sigma} = \pi$, где $\varepsilon \in S_{n-1}$ — единичная перестановка, а $\varepsilon \oplus \pi = 0$, $\pi \in S_{n-1}$ [1]. Комплекс K перестановок, имеющих дополнение, замкнут относительно операций дополнения и обращения, причем $\left(\overline{\sigma^{-1}}\right)^{-1} = \overline{(\overline{\sigma})^{-1}}$. Поэтому и множества вида $U = \left\{\sigma, \overline{\sigma}, \sigma^{-1}, \overline{\sigma^{-1}}, (\overline{\sigma})^{-1}, \left(\overline{\sigma^{-1}}\right)^{-1}\right\}$, содержащие не обязательно разные перестановки рассматриваемого комплекса, замкнуты относительно операций дополнения и обращения.

Рассмотрим случай, когда $U = U_2$ содержит только две различные (четные) перестановки, и обозначим $b_{n-1} = \#\{U_2 : U_2 \subset K\}$.

ТЕОРЕМА. 1) $b_{n-1} = 0$ при $n \equiv 3; 5 \pmod 6$; 2) $2b_{n-1} = 2^{(n-1)/3} bq_{n-1}$ при $n \equiv 1 \pmod 6$, где bq_{n-1} — количество таких разбиений числа $n(n-1)/2$ ровно с $n-1$ различными частями, каждая из которых не превосходит $n-1$, причем эти разбиения можно представить в виде объединения $(n-1)/3$ разбиений чисел n и $2n$ ровно с $(n-1)/6$ различными частями, не превосходящими, соответственно, $n-3$ — для числа n и n — для числа $2n$.

В частности, $bq_7 = 1$, $bq_{13} = 5$, $bq_{19} = 52$, $bq_{25} = 1055$, $bq_{31} = 31814$.

Так как рассматриваемые перестановки $\sigma \in S_{n-1}$ относятся к цикловому классу $3^{(n-1)/3}$, то $bq_{n-1} < 6^{(1-n)/3}(n-1)!/((n-1)/3)!$, но эта оценка представляется сильно завышенной. Точное соотношение для чисел bq_{n-1} или их оценку, вероятно, следует разыскивать на основании теоретико-числовых соображений. Так, для простого числа $p = 6k+1$ имеется только одна перестановка класса $3^{(p-1)/3}$, у которой все элементы каждого цикла являются квадратичными вычетами или невычетами и образуют указанные в пункте 2) теоремы разбиения.

Список литературы

1. Бондаренко Л. Н. Перманенты и "аддитивные" задачи перечисления перестановок // Материалы VII Международного семинара "Дискретная математика и ее приложения" (Москва, 29 января – 2 февраля 2001 г.). Часть III. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ, 2001. — С. 335–338.

О ЧИСЛЕ ПРИМЕНЕНИЙ ПРАВИЛ СТОХАСТИЧЕСКОЙ КС-ГРАММАТИКИ

А. Е. Борисов (Нижний Новгород)

Рассматривается стохастическая КС-грамматика

$$G = \langle V_T, V_N, R, s \rangle,$$

где V_T и V_N — множества терминальных и нетерминальных символов, $s \in V_N$ — аксиома, R — конечное множество правил вида

$$r_{ij} : A_i \xrightarrow{p_{ij}} \beta_{ij},\ j = 1, \ldots, n_i, \text{ где } A_i \in V_N, \beta_{ij} \in (V_T \cup V_N)^*,$$

p_{ij} — вероятность применения правила r_{ij}, удовлетворяющая условиям: $p_{ij} > 0$ и $\sum_j p_{ij} = 1$.

В работе рассматривается грамматика с двумя нетерминальными символами — A_1, A_2, где A_1 — аксиома, причем матрица A первых моментов [1] имеет вид

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

и ее перронов корень равен 1.

При этом возможны три случая: $a = c = 1$, $a < c = 1$ и $c < a = 1$.

Через $S_{ij}(t)$ обозначим общее число применений правила r_{ij} в дереве вывода высоты t; $S_{ij}(t)$ — случайная величина.

ТЕОРЕМА. Пусть G — стохастическая КС-грамматика с матрицей первых моментов вида (1). Тогда при $t \to \infty$ выполняются следующие асимптотические равенства:

1) $M(S_{1j}(t)) \sim p_{1j} b_{22}^2 t/4b$, $M(S_{2j}(t)) \sim p_{2j} b_{22}^2 t^2/4$ для $a = c = 1$;

2) $M(S_{ij}(t)) \sim p_{ij} v_i b_{11}^1 t^2/6$ для $0 < c < a = 1$, где $v = (v_1, v_2) = (1, b/(1-c))$;

3) $M(S_{1j}(t)) \sim p_{1j} b_{11}^1/(1-a)^2 + p_{1j}/(1-a)$, $M(S_{2j}(t)) \sim p_{2j} b_{22}^2 t^2/6$ для $0 < a < c = 1$ (здесь b_{jk}^i — вторые моменты грамматики).

Список литературы

1. Фу К. Структурные методы в распознавании образов. — М.: Мир, 1977.

РАВНОМЕРНАЯ НЕПРЕРЫВНОСТЬ СИГНАТУРНЫХ ОПЕРАЦИЙ ТАБЛИЧНЫХ АЛГЕБР

Д. Б. Буй, Ю. И. Брона, Н. Д. Кахута (Киев)

Сообщение посвящено применению характеристического свойства равномерной непрерывности в исследовании взаимной производности сигнатурных операций табличных алгебр, построенных на основе известных реляционных алгебр Кодда, и выступающих основной моделью манипуляций над реляционными структурами [1–3].

ОПРЕДЕЛЕНИЕ. Табличную операцию F назовем равномерно непрерывной, если существует натуральное число m, такое, что для всех таблиц $t_1, ..., t_n$ и строк s выполняется эквивалентность $s \in F(t_1, ..., t_n) \Leftrightarrow \exists\ t'_n ... \exists\ t'_n (|t'_1| \le m \wedge ... \wedge |t'_n| \le m \wedge t'_1 \subseteq t_1 \wedge ... \wedge\ t'_n \subseteq t_n \wedge s \in F(t_1, ..., t_n))$.

Содержательная интерпретация равномерной непрерывности операции: при вычислении любой строки в таблице-результате надо обратиться не более чем m раз к таблицам-аргументам.

ПРЕДЛОЖЕНИЕ. Операции объединения, пересечения, селекции, проекции, соединения, переименования равномерно непрерывны; операции вычитания, деления, насыщения и активного дополнения не являются таковыми. Селекторные операции и константные операции равномерно непрерывны; класс равномерно непрерывных операций замкнут относительно суперпозиции.

СЛЕДСТВИЕ. Операция вычитания (деления, насыщения, активного дополнения) не является производной относительно операций объединения, пересечения, селекции, проекции, соединения, переименования и произвольных констант.

Работа выполнена при финансовой поддержке Государственного Фонда Фундаментальных Исследований Украины (проект 01.07/105).

Список литературы

1. Кренке Д. Теория и практика построения баз данных. 8-е изд. — Санкт-Петербург: Питер, 2003. — 800 с.

2. Редько В. Н., Буй Д. Б. К основаниям теории реляционных моделей баз данных // Кибернет. и системн. анализ. — 1996. — № 4. — С. 3–12.

3. Редько В. Н., Брона Ю. И., Буй Д. Б. Взаимная непроизводность и выразительная сила операций реляционных алгебр // Доклады НАН Украины. — 1996. — № 11. — С. 84–88.

ОБ УСТОЙЧИВОСТИ ВЕКТОРНОЙ ДИСКРЕТНОЙ ЗАДАЧИ С ПРИНЦИПОМ ОПТИМАЛЬНОСТИ, ОБОБЩАЮЩИМ ПАРЕТОВСКИЙ И ЛЕКСИКОГРАФИЧЕСКИЙ

С. Е. Бухтояров, В. А. Емеличев (Минск)

Пусть на конечном множестве $X \subset \mathbb{R}^m$, $m \ge 2$, задан векторный критерий

$$f(x, C) = (C_1 x, C_2 x, ..., C_n x) \to \min\limits_{x \in X},\ n \ge 1,$$

где C_i — i-я строка матрицы $C \in \mathbb{R}^{n \times m}$. Для каждого разбиения $I_1, I_2, \ldots, I_s$ множества N_n на $s \ge 1$ непустых непересекающихся подмножеств (групп) определим множество $(I_1, I_2, ..., I_s)$-оптимальных решений

$$G^n(C, I_1, I_2, ..., I_s) = \{x \in X\ :\ \zeta(x, C) = \emptyset\},$$

где

$$\zeta(x, C) = \{x' \in X\ :\ f(x, C)\ \Omega^n(I_1, I_2, \ldots, I_s)\ f(x', C)\},$$

$$y\ \Omega^n(I_1, I_2, \ldots, I_s)\ y' \ \Leftrightarrow\ \left(y_{I_k} \ge y'_{I_k}\ \&\ y_{I_k} \ne y'_{I_k}\right),$$

$$k = \min\{j \in N_s\ :\ y_{I_j} \ne y'_{I_j}\},$$

y_{I_k} и y'_{I_k} — проекции соответственно векторов y и y' на координатные оси пространства $\mathbb{R}^n$ с номерами группы I_k. Таким образом, критерии разбиты на s групп так, что каждая предыдущая группа критериев важнее любой последующей. Тогда $G^n(C, N_n)$ есть множество Парето, а $G^n(C, \{1\}, \{2\}, \ldots, \{n\})$ — множество лексикографически оптимальных решений.

Получены нижняя и верхняя оценки предельного уровня возмущений коэффициентов частных линейных критериев в чебышевской метрике, не приводящих к появлению новых $(I_1, I_2, ..., I_s)$-оптимальных решений.

О СЛОЖНОСТИ АЛГОРИТМОВ ДЛЯ РАЗРЕЖЕННЫХ ПОЛИНОМОВ

Ю. Д. Валеев (Тамбов)

Пусть W — коммутативная область, элементы которой могут храниться в машинном слове. Назовем полиномом типа (m, α) случайный полином $\sum_{i=0}^{m-1} c_i x^i$ из $W[x]$, каждый коэффициент которого отличен от нуля с вероятностью α.

Оценки математического ожидания числа операций сложения и умножения коэффициентов в полиномиальных алгоритмах с такими полиномами изучались в [1]. В настоящей работе получены оценки сложности полиномиальных алгоритмов, как математического ожидания времени вычисления. При этом учитывается время выполнения следующих операций: T_a, T_m и T_c — сложения, умножения и сравнения двух чисел из W, T_l — логической операции и T_{rw} — операции чтения или записи элементов массива. Предполагается, что ненулевые коэффициенты полиномов упорядочены по степеням и хранятся в виде вектора степеней и вектора коэффициентов.

ТЕОРЕМА 1. Сложность алгоритма сложения двух полиномов типа (m, α) и (m, β) равна $T = m(3\alpha + 4\beta - 3\alpha\beta)T_c + m\alpha\beta T_a + m(\alpha + \beta - \alpha\beta)T_l + m(6\alpha + 8\beta - 5\alpha\beta)T_{rw} + m(2\alpha + 2\beta - \alpha\beta)T_i$.

ТЕОРЕМА 2. Сложность стандартного алгоритма умножения двух полиномов типа (m, α) и (m, β) равна $T = (m\alpha + m\beta - 1 + 2n + 2N_a + 2N_c)T_c + (m\alpha + m\beta - 1 + 3n)T_i + (m^2\alpha\beta + N_a)T_a + m^2\alpha\beta T_m + (5m^2\alpha\beta + 2m\beta + 12n + 7N_a + 5N_c)T_{rw}$, где $n = \sum_{i=1}^{m} \pi_i^{m,m}$, $N_c = (\sum_{k=2}^{m} \sum_{i=k}^{k+m-1} \pi_i^{k,m} + m)\beta$, $N_a = m^2\alpha\beta - n$, $N_m = m^2\alpha\beta$, $\pi_i^{m,k} = 1 - (1 - \alpha\beta)^{t_i^{m,k}}$ при $1 \le i \le 2m - 1$, $t_i^{m,k} = i$ при $1 \le i \le k$, $t_i^{m,k} = k$ при $k \le i \le m$, $t_i^{m,k} = m + k - i$ при $m \le i \le m + k - 1$.

Работа выполнена при частичной поддержке грантов РФФИ (проект 04-07-90268), Human Capital Foundation (проект 23-03-24) и программы «Университеты России» (проект УР.04.01.464).

Список литературы

1. Валеев Ю. Д., Малашонок Г. И. О сложности алгоритмов умножения полиномов // Труды VI Международной конференции "Дискретные модели в теории управляющих систем". — М.: Изд-во ВМиК МГУ, 2004. — С. 13–19.

ОДИН МЕТОД ВЫЧИСЛЕНИЯ ЭЛЕМЕНТАРНЫХ ФУНКЦИЙ С ИСПОЛЬЗОВАНИЕМ ТАБЛИЦ

Я. В. Вегнер (Москва)

ТЕОРЕМА. Пусть зафиксирован отрезок $[a, b]$ и функция $f \in C^5[a, b]$. Пусть также зафиксирован натуральный параметр n. Тогда существует алгоритм построения схемы для приближённого вычисления значения f на отрезке $[a, b]$, такой что:

1. Схема имеет $4n$ битов входного числа X после запятой. В зависимости от отрезка $[a, b]$ могут иметься дополнительные биты входа для передачи целой части значения X.

2. Схема имеет $6n$ битов выхода и вычисляет f с погрешностью, меньшей 2^{6n-c}, где константа c зависит от f и $[a, b]$ и не зависит от n.

3. Схема имеет сложность $324 \cdot 2^{2n} + 54n \log 2n \cdot 2^{n/2} + O(n^2)$ и глубину $4n + 2{,}574 \log n + 24$.

4. Схема использует 13 таблиц с шириной входа $2n$ и суммарной шириной выхода $54n$. Если расчитывать сложность и глубину схемы без учёта этих таблиц, то сложность не превосходит велиины

$$23n \log n + 393n + 92 \log n + 1782,$$

а глубина — величины

$$4{,}574 \log n + 20.$$

Реальная погрешность оказывается меньше теоретической оценки. Для функции $1/x$ на отрезке $[1, 2]$ она меньше в 8 раз, для функции $\sqrt{x}$ на отрезке $[1, 2]$ она меньше примерно в 64 раза. При $n = 5$ фактическая точность вычисления $\sqrt{x}$ становится равной 2^{-32}.

Список литературы

1. Wong W. F., Goto E. Fast evaluation on the elementary functions in single precision // IEEE Transactions on Computers. — 1995. — V. 44, №. 3.

О ХОПФОВОЙ СТРУКТУРЕ КОДОВ РИДА — СОЛОМОНА

А. Б. Верёвкин (Ульяновск)

Пусть α — примитивный элемент конечного поля F_q и $k<q-1$. Расширенным кодом Рида — Соломона $\overline{RS}(k,\,q)$ называется k-мерный идеал конечной алгебры $R = F_q[x]/((x^{q-1}-1))$, порождённый многочленом вида $g(x)=(x-\alpha^0)(x-\alpha)\dots(x-\alpha^{q-k-2})$. Исправление m ошибок в коэффициентах многочлена $P(x)\in R$ связано с решением в F_q системы алгебраических уравнений:

$$\sum_{i=1}^{m} x_i z_i^j = b_j\,,\ j = 0, 1, \dots,\ q-k-2, \quad \text{где} \quad b_j = P(\alpha^j).$$

Алгебра R изоморфна групповой алгебре циклической группы порядка $q-1$ и поэтому является алгеброй Хопфа, то есть, имеет алгебраическую структуру на пространстве R^*, связанную с R [1, гл. 1]. Решение этой системы эквивалентно нахождению функционала $\phi \in R^*$, имеющего синдромное значение на коидеале $<x^j;\ j = 0,\ 1,\ \dots,\ q-k-2>$ в R: $\phi(x^j) = b_j$ и порождающего коидеал в R^* размерности не выше m. Иначе говоря, ϕ должен иметь разложение:

$$\phi = \sum\nolimits_{a\in F^*}^{(m)} x_a \delta_a^*, \quad \text{где} \quad \delta_a^*(P(x)) = P(a).$$

Исходя из этого соображения можно обобщать коды Рида — Соломона, используя некоммутативные конечные алгебры Хопфа.

Работа выполнена при частичной финансовой поддержке грантов РФФИ 04-01-00739 и УР 04.01.054 № 214.

Список литературы

1. Montgomery S. Hopf algebras and their actions on rings // Regional Conference Series in Mathematics. — Providence: CBMS, 1992. — № 82.

НЕКОТОРЫЕ ОЦЕНКИ СЛОЖНОСТИ УГАДЫВАЮЩЕГО АВТОМАТА

А. Г. Вереникин, Э. Э. Гасанов (Москва)

Пусть $\{0,1\}^\infty$ — множество сверхслов в алфавите $\{0,1\}$. Пусть $a = a(1)a(2)a(3)\dots$, $b = b(1)b(2)b(3)\dots \in \{0,1\}^\infty$. Пусть V — некоторый автомат, на вход которого поступает сверхслово a, а на выходе получается сверхслово b. Скажем, что этот автомат угадывает сверхслово a, если существует такое натуральное число N, что для любого $t \geq N$ выполнено $a(t) = b(t+1)$. Автомат угадывает множество $\mathcal{A} \subset \{0,1\}^\infty$, если он угадывает каждое сверхслово из этого множества. Множество сверхслов угадываемо, если существует угадывающий его автомат. Под сложностью автомата понимается число его состояний. $w(\mathcal{A})$ — минимальное количество состояний, достаточное автомату, чтобы угадать $\mathcal{A} \subset \{0,1\}^\infty$.

ТЕОРЕМА 1. Множество сверхслов $\mathcal{A} \subset \{0,1\}^\infty$ угадываемо тогда и только тогда, когда оно состоит из периодических сверхслов с ограниченной длиной периода.

ТЕОРЕМА 2. Если $\mathcal{A}_n \subset \{0,1\}^\infty$ — множество всех периодических сверхслов с длиной периода n, то $w(\mathcal{A}_n) = 2^{n-1}$.

ТЕОРЕМА 3. Если $\mathcal{B}_n \subset \{0,1\}^\infty$ — множество всех периодических сверхслов с минимальной длиной периода n, то $w(\mathcal{B}_n) \sim 2^{n-1}$ при $n \to \infty$, причем если n — простое, то $w(\mathcal{B}_n) = 2^{n-1} - 1$.

ТЕОРЕМА 4. Если $\mathcal{C}_n \subset \{0,1\}^\infty$ — множество всех периодических сверхслов с длиной периода не большей чем n и нулевой длиной предпериода, то $2^n \lesssim w(\mathcal{C}_n) \lesssim 3 \cdot 2^{n-1}$ при $n \to \infty$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 05-01-00709).

О ЧИСЛЕ OP-КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ

С. Ф. Винокуров, А. С. Казимиров (Иркутск)

В работе рассматривается группа отображений булевых функций, сохраняющая сложность в операторных полиномиальных формах. Оператор t можно представить последовательностью $t_1 ... t_n$, где $t_i \in \{d, e, p\}$, компонента t_i определяет действие оператора по переменной x_i. Подробно операторы описаны в [1].

Пусть P — полная группа подстановок на множестве $\{d, e, p\}$. Пусть φ — последовательность $\varphi_1\varphi_2 \dots \varphi_n$, где $\varphi_i \in P$. Тогда φ действует на оператор $a_1 \dots a_n$ так: $\varphi(a_1 \dots a_n) = \varphi_1(a_1) \dots \varphi_n(a_n)$.

Отображение φ операторов продолжается на функции по их операторным представлениям: $\varphi(f) = \sum_{i=1}^{s} \varphi(a^i)(x_1 \cdot \dots \cdot x_n)$.

ОПРЕДЕЛЕНИЕ. OP-отображением функций назовем композицию введенного отображения и отображения, задаваемого перестановками переменных.

Легко показать, что OP-отображения образуют группу. Можно заметить, что группа Джевонса [2] образует подгруппу в группе OP-отображений.

ОПРЕДЕЛЕНИЕ. Функции f и g называются OP-эквивалентными, если существует OP-отображение φ такое, что $g = \varphi(f)$.

Интерес к таким отображениям связан с тем, что все функции, попадающие в один класс эквивалентности относительно этой группы, имеют одинаковую сложность (сложность как число слагаемых в операторной форме) [1].

ТЕОРЕМА. Почти все функции порождают класс эквивалентности мощности $6^n n!$.

СЛЕДСТВИЕ. Число классов OP-эквивалентности K_n асимптотически равно: $K_n \sim \frac{2^{2^n}}{6^n n!}$.

Работа выполнена при финансовой поддержке РФФИ (проект 04-07-90178в).

Список литературы

1. Винокуров С. Ф., Казимиров А. С. Верхняя оценка сложности булевых функций в классе ПНФ // Алгебра и теория моделей. Вып. 4. Новосибирск: Изд-во Новосиб. гос. тех. ун-та, 2003. — С. 160–165.

2. Поваров Г. Н. О групповой инвариантности булевых функций // Применение логики в науке и технике. — М.: АН СССР, 1961. — С. 263–340.

О НАХОЖДЕНИИ МИНИМАЛЬНЫХ ПОЛИНОМОВ В ОПЕРАТОРНЫХ ФОРМАХ

С. Ф. Винокуров, А. Н. Маркович (Иркутск)

В настоящее время имеется большое количество работ по нахождению минимальных полиномиальных нормальных форм (ПНФ) булевых функций. В [1] показано, что задача нахождения минимальной ПНФ для булевой функции $f(x_1, ..., x_n)$ может быть сведена к задаче нахождения подходящего операторного пучка, действующего на базисную функцию $g(x_1, ..., x_n) = x_1 \cdot ... \cdot x_n$. Это сведéние позволило расширить задачу минимизации в ПНФ до минимизации в операторных формах, в которых базисная функция $g(x_1, ..., x_n) \neq x_1 \cdot ... \cdot x_n$.

В данной работе предложен метод нахождения минимальной (по числу слагаемых) операторной формы по любой базисной функции g. Все необходимые определения и свойства операторов имеются в [1].

Рассмотрим операторное представление для функции f:
$f(x_1, ..., x_n) = \bigoplus_{\tilde{\tau}} \alpha_{\tilde{\tau}} \mathbf{a}^{\tilde{\tau}} g(x_1, ..., x_n)$, где $\tilde{\tau} = (\tau_1, ..., \tau_n)$, $\tau_i \in \{0, 1\}$, $\alpha_{\tilde{\tau}} \in \{0, 1\}$, $\mathbf{a}^{\tilde{\tau}}$ — операторы некоторого пучка.

Пусть $\phi : F^n \to F^n$ — линейное отображение, индуцированное отображением $\phi(g(x_1, ..., x_n)) = x_1 \cdot ... \cdot x_n$. Для базисных функций такое отображение всегда можно построить; отображение ϕ — обратимо. Тогда функция $\phi(f(x_1, ..., x_n))$ имеет следующую ПНФ:
$\phi(f(x_1, ..., x_n)) = \bigoplus_{\tilde{\tau}} \alpha_{\tilde{\tau}} \mathbf{a}^{\tilde{\tau}} \phi(g(x_1, ..., x_n)) = \bigoplus_{\tilde{\tau}} \alpha_{\tilde{\tau}} \mathbf{a}^{\tilde{\tau}} (x_1 \cdot ... \cdot x_n)$.

Пусть для функции $\phi(f(x_1, ..., x_n))$ найдена минимальная ПНФ
$\phi(f(x_1, ..., x_n)) = \bigoplus_{\tilde{\tau}} \beta_{\tilde{\tau}} \mathbf{b}^{\tilde{\tau}} (x_1 \cdot ... \cdot x_n)$.

ТЕОРЕМА. Операторное представление

$$f(x_1, ..., x_n) = \bigoplus_{\tilde{\tau}} \beta_{\tilde{\tau}} \mathbf{b}^{\tilde{\tau}} g(x_1, ..., x_n)$$

является минимальным для функции f в операторных формах по базисной функции $g(x_1, ..., x_n)$.

Эта теорема позволяет использовать алгоритмы минимизации в ПНФ для минимизации в операторных формах по произвольной базисной функции.

Работа выполнена при финансовой поддержке РФФИ (проект 04-07-90178в).

Список литературы

1. Избранные вопросы теории булевых функций // Под ред. Винокурова С. Ф. и Перязева Н. А. — М.: Физматлит, 2001. — 192 с.

О НИЖНЕЙ ОЦЕНКЕ ПОРОГА 4-ВЫПОЛНИМОСТИ

Ф. Ю. Воробьев (Москва)

Назовем k-буквенной скобкой дизъюнкцию вида $(x_{i_1}^{\sigma_{i_1}} \vee x_{i_2}^{\sigma_{i_2}} \vee \ldots \vee x_{i_k}^{\sigma_{i_k}})$. Пусть $F_k(n,m)$ — k-КНФ, полученная путем случайного равновероятностного и независимого выбора m скобок из числа $2^k C_n^k$ всех k-буквенных скобок над множеством из n переменных. Пусть $S_k(n,r)$ — вероятность того, что $F_k(n,nr)$ выполнима. Определим

$$r_k \equiv \sup\{r : \lim_{n\to\infty} S_k(n,r) = 1\},$$
$$r_k^* \equiv \inf\{r : \lim_{n\to\infty} S_k(n,r) = 0\}.$$

Предположение о пороге выполнимости заключается в том, что $r_k = r_k^*$.

В работе [1] была получена наилучшая из известных верхних оценок для r_4, равная 10.23. В [2] были получены нижние оценки для r_k с помощью применения метода второго момента к случайной величине вида

$$X = \sum_{\sigma\in\{0,1\}^n} \gamma^{H(\sigma,F)} 1_{F(\sigma)=1},$$

где $H(\sigma,F)$ — разность числа букв формулы F, обращающихся в единицу на наборе σ, и числа букв, обращающихся в ноль. Так, для r_4 была получена оценка 7.91 — наилучшая из известных оценок. В настоящей работе доказывается применимость метода второго момента к более широкому классу случайных величин. Для r_4 удается улучшить результаты, полученные в [2].

ТЕОРЕМА. $r_4 \geq 8.09$.

Список литературы

1. Dubois O., Boufkhad Y. A general upper bound for the satisfiability threshold of random r-SAT formulae // J. Algorithms. — 1997. — V. 24, № 2. — P. 395–420.

2. Achlioptas D., Peres Y. The threshold for random k-SAT is $2^k \ln 2 - O(k)$ // STOC. — 2003. — P. 223–231.

ОЦЕНКИ ДЛИНЫ ПРОВЕРЯЮЩИХ ТЕСТОВ ДЛЯ БЕСПОВТОРНЫХ ФУНКЦИЙ В ОСНОВНЫХ БАЗИСАХ

А. А. Вороненко (Москва)

Рассматривается следующая задача: для заданной булевой функции, выразимой бесповторной формулой в некотором базисе и существенно зависящей от переменных $x_1, \ldots, x_n$, требуется построить проверяющий тест на множестве всех бесповторных в этом базисе функций, существенно зависящих от некоторых переменных из множества $\{x_1, \ldots, x_n\}$. В работе [1] обоснован выбор именно такой постановки тестовой задачи и приведены достаточно нетрудные доказательства вырожденности ряда других естественных постановок. Рассматриваются базисы $B_0 = \{0, 1, \&, \vee, \neg\}$, $B_2 = \{0, 1, \&, \vee, \neg, \oplus\}$ и B_3 — базис всех функций трех переменных. В докладе приводятся следующие результаты:

$$n + 1 \leq T_{B_0}(n) < 3.5n, \text{ где } n \geq 2;$$

$$\frac{n(n+1)}{2} + 1 \leq T_{B_2}(n) \leq 2n(n-1), \text{ где } n \geq 2;$$

$$\frac{n^3}{6} \leq T_{B_3}(n) \leq \frac{4}{3}n^3, \text{ где } n \geq 3.$$

Работа выполнена при финансовой поддержке РФФИ (проекты 04-01-00359 и 05-01-01000)

Список литературы

1. Вороненко А. А. О проверяющих тестах для бесповторных функций // Математические вопросы кибернетики. Вып. 11. — 2002. — С. 163–176.

О СЛОЖНОСТИ СХЕМ ДЛЯ УМНОЖЕНИЯ И ИНВЕРТИРОВАНИЯ В НЕКОТОРЫХ КОНЕЧНЫХ ПОЛЯХ ХАРАКТЕРИСТИКИ ДВА

С. Б. Гашков (Москва)

Рассматривается задача о построении из двухвходовых булевых функциональных элементов логических схем, реализующих операции умножения и инвертирования в конечных полях порядка 2^n. Сложность (число элементов) схемы, реализующей умножение в данном базисе B поля $GF(2^n)$, обозначим $M(n) = M_B(n)$. Сложность схемы, реализующей операцию инвертирования (т. е. вычисления $1/x$ при $x \neq 0$) обозначим $I(n) = I_B(n)$.

Справедливы следующие утверждения.

Пусть для любых натуральных m, s и $k < s$ выбрано наименьшее r такое, что $2^{m^r} \geq 2m^k - 1$ и $r = s \bmod k$. Тогда для $n = m^s$ и некоторого базиса в $GF(2^n)$

$$M(n) = m^{O(k)} n^{\log_{m^k} 3(2m^k-1)}, \quad I(n) = O(km^k \log_2 m) M(n).$$

При подходящем выборе k можно получить, что для любого $\varepsilon > 0$ и любого m справедливы при $n = m^s$ и $s \geq s_\varepsilon$ неравенства

$$M\left(GF(2^n)\right) < n^{1+\varepsilon/2}, \quad I(n) < n^{1+\varepsilon}.$$

В частности, при $n = 2 \cdot 3^k$

$$M(n) < 2.75 n^{\log_3 8} < 2.75 n^{1.9}, \quad I(n) < 8.9 n^{\log_3 8} + 990,$$

$$M(n) < n(\log_3 n)^{(\log_2 \log_3 n)/2 + O(1)}, \quad I(n) < n(\log_3 n)^{(\log_2 \log_3 n)/2 + O(1)},$$

при $n = 4 \cdot 3^k$

$$I(n) = O\left(n^{\log_3 7}\right), \quad M(n) = O\left(n^{\log_3 7}\right),$$

при $n = 8 \cdot 3^k$

$$I(n) = O\left(n^{\log_3 5}\right), \quad M(n) = O\left(n^{\log_3 5}\right),$$

$M(162) \leq 19525$, $I(162) \leq 106278$, $M(486) \leq 158468$, $I(486) \leq 481789$,

$M(36) \leq 1881$, $I(36) \leq 3204$, $M(108) \leq 19071$, $I(108) \leq 69649$,

$M(216) \leq 61170$, $I(216) \leq 196050$, $M(324) \leq 151209$, $I(324) \leq 659196$.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1) и программы «Университеты России» (проект УР.04.02.528).

ОЦЕНКА СЛОЖНОСТИ АЛГОРИТМА ОПРЕДЕЛЕНИЯ СОВМЕСТНОСТИ СИСТЕМ ЛИНЕЙНЫХ ДВУЧЛЕННЫХ НЕРАВЕНСТВ

А. С. Герасимов, Н. К. Косовский (Санкт-Петербург)

Уточнен и реализован алгоритм определения совместности систем линейных двучленных неравенств с целочисленными коэффициентами, предложенный в [2]. Получены оценки временной сложности алгоритма и длины чисел, используемых в работе алгоритма.

Алгоритм заключается в последовательном исключении переменных ([3], с. 239–242) с одновременным удалением избыточных неравенств так, что количество неравенств, содержащих любые 2 переменные, ограничено константой. В [2] показано, что предложенный там алгоритм является истинно полиномиальным ([3], с. 304) и требует $O(n^3 + m)$ арифметических операций над числами длины $O(I)$, где m — число неравенств, n — число неизвестных, I — длина входа.

Алгоритм реализован на языке программирования Java [1]. При этом часто встречается (при удалении избыточных неравенств) операция — выбор всех неравенств, содержащих 2 данные переменные. Эта операция эффективно реализована путем введения линейного порядка на множестве неупорядоченных пар переменных и использования сбалансированного дерева поиска для хранения неравенств.

ТЕОРЕМА. Реализованный на языке Java алгоритм имеет временную сложность $O(m \log n + mL^2 + n^3 \log n + n^3 L^2)$, где L — сумма длин всех чисел, входящих в систему. Реализация алгоритма выполняет арифметические операции (только сложение, умножение и сравнение) над числами длины не более $4L$.

Список литературы

1. Арнольд К., Гослинг Дж., Холмс Д. Язык программирования Java. — М.: Издательский дом "Вильямс", 2001.

2. Давыдок Д. В. О совместности систем двучленных линейных неравенств // Логики конечнозначных предикатов на основе неравенств — СПб: Изд-во СПбГУ, 2000. — С. 246–268.

3. Схрейвер А. Теория линейного и целочисленного программирования — М.: Мир, 1991.

СИНТАКСИЧЕСКАЯ КЛАССИФИКАЦИЯ ФУНКЦИЙ, ВЫЧИСЛИМЫХ ЗА ЛИНЕЙНОЕ ВРЕМЯ

М. А. Герасимов (Санкт-Петербург)

Предлагается способ классификации алгоритмов, работающих в линейное время на основе специальной синтаксической иерархии, построенной аналогично иерархии А. Гжегорчика. Предлагаемая классификация функций позволяет использовать синтаксические способы оценки их сложности.

В рассматриваемом случае применяется подход, впервые описанный в работе А. Гжегорчика [3]. В соответствии с этим подходом предъявляется синтаксическое описание классов функций, вычислимых на сублинейной зоне машины Тьюринга [4]. Применяя определенные ограничения на структуру порождаемых термов можно добиться расслоения исходного класса на множества функций, вычислимых за линейное время.

Полученные следствия позволяют получить априорные оценки сложности алгоритмов рассматриваемых классов и вычислять соответствующие константы.

Рассматриваемые подклассы класса функций, вычислимых за линейное время могут быть использованы для оценки качества реализации линейных алгоритмов. Полученные результаты допускают алгоритмическое представление в виде профайлеров для структурированных языков программирования. Особенно важными представляются возможности использования этого подхода для оценок сложности алгоритмов реального времени.

Список литературы

1. Ахо А., Хопкрофт Дж., Ульман Дж., Построение и анализ вычислительных алгоритмов. —М., 1979. — 536 с.

2. Бельтюков А. П. Малые классы, основанные на ограниченной рекурсии // Вычислительная техника и вопросы кибернетики. — Л., 1979. — С. 75–85.

3. Гжегорчик А. Некоторые классы рекурсивных функций // Проблемы математической логики. Сложность алгоритмов и классы вычислимых функций. — М.: Мир, 1970. — С. 9–49.

4. Минский М. Вычисления и автоматы. —М.: Мир, 1971. — 364 с.

МОДЕЛЬ ПРОЦЕССА ДЫХАНИЯ ЖИВЫХ ОРГАНИЗМОВ

Ю. Г. Гераськина (Москва)

Лёгкие живых организмов при огрублённом подходе могут рассматриваться как древовидная структура бронхов, в которых имеются ворсинки, играющие роль эскалаторного механизма вывода как внутреннего секрета, так и поступающего извне в лёгкие вещества во внешнюю среду. Бронхи имеют разные пропускные способности и разную эффективность ворсинок. Чем выше от альвеол, то есть самых мелких бронхов, тем мощнее механизм передачи вещества изнутри вовне.

Возникает задача построения модели лёгочного механизма самоочищения как в случае чистой среды, так и в условиях возможной её запыленности. В [1] построена подобная модель в предположении чистой среды и найдена временная сложность такого очищения.

В данной работе указанная модель распространяется на случай запыленной среды и решается задача описания всех возможных воздействующих квазислов (слов и сверхслов), каждая буква которых означает количество поступающего в лёгкие вещества извне в заданный момент времени и при этом требуется, чтобы общая запыленность лёгкого не превышала предельно допустимого порога. Конструктивно описываются все такие квазислова, называемые допустимыми. Это описание сводится к указанию всех предельно допустимых квазислов (соответственно, слов и сверхслов). Все допустимые квазислова являются в точности побуквенно монотонными в обычном смысле “предшественниками” квазислов из этого семейства. Квазислова описываются также с помощью специальных алгебр слов и сверхслов, близких к алгебрам Клини и МакНотона.

Рассматривается сложностной аспект задачи определения принадлежности слова длины m множеству допустимых (предельно допустимых) слов. Вводятся функция Шеннона, которая равна минимально достаточному числу шагов для определения принадлежности любого заданного слова длины m множеству допустимых слов, и аналогичная функция для определения предельной допустимости слов. Показывается, что эти функции линейно зависят от m.

Список литературы

1. Гераськина Ю. Г. Модель самоочищения лёгочных структур // Интеллектуальные системы — 2002–2003. — Т. 7, вып. 1–4, — С. 41–54.

МЕТОДЫ ОБОСНОВАНИЯ ГИПОТЕЗ О РАСПРЕДЕЛЕНИИ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В КОМПАКТНЫХ ОБЛАСТЯХ

Н. М. Глазунов (Киев)

Рассмотрено порождение, эксперименты и методы обоснования гипотез о псевдослучайных последовательностях. Последовательностью называем отображение бесконечного подмножества натурального ряда в метрическое пространство. Рассматриваются метрические пространства, являющиеся компактными подмножествами вещественной прямой, а также некоторые другие. Доклад содержит четыре раздела.

1. Методы генерации. Рассматриваются методы генерации псевдослучайных последовательностей, имеющие теоретико-числовую природу и связанные с числом точек алгебраических многообразий над конечными полями, а также с дискретными преобразованиями Фурье.

2. Функции распределения и плотности распределения. Построение функций распределения и функций плотности распределения, исходя из последовательностей.

3. Экспериментальное исследование и проверка гипотез о плотностях функций распределения.

4. Методы доказательства гипотез о функциях плотности распределения последовательностей. Будут представлены результаты, которые являются математической основой строгого доказательства свойств последовательностей.

Изложение иллюстрируется экспериментальными и теоретическими результатами об избранных последовательностях.

Список литературы

1. Глазунов Н. М. О пространствах модулей, равнораспределенности, оценках и рациональных точках алгебраических кривых // Укр. мат. журнал. — 2001. — Т. 53, № 9. — С. 1174–1183.

2. Glazunov N. M. Categorification of Fourier transform, efficient computation and computing intelligence // Nuclear Instruments & Methods in Physics Research. — 2004. — V. 534. — P. 324–328.

3. Глазунов Н. М. Постникова Л. П., Шор Н. З. Арифметическое моделирование случайных процессов и эргодическая теория // Кибернетика и системный анализ. — 2004. — № 4. — С. 73–86.

БИНАРНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ ЗНАКА ЧИСЛА ИЗ ПРОСТОГО АЛГЕБРАИЧЕСКОГО РАСШИРЕНИЯ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Д. В. Груздев (Нижний Новгород)

Пусть α является единственным на интервале (l_0, r_0) вещественным корнем неприводимого над полем рациональных чисел Q многочлена $\varphi(x) = \sum_{i=0}^{n} a_i x^i \in Z[x]$, где $a_n \neq 0$, $2^q l_0 \in Z$ и $2^q(r_0 - l_0) = 1$ при некотором $q \in N$. Положим $L_\varphi = \sum_{i=0}^{n} |a_i|$, $H_\varphi = \max\{|a_0|, \ldots, |a_n|\}$ и $M_\varphi = 1 + \lceil H_\varphi / |a_n| \rceil$. Задача определения знака числа из простого алгебраического расширения $Q(\alpha) = \{h(\alpha) : h(x) = \sum_{j=0}^{n-1} c_j x^j \in Q[x]\}$ поля Q может быть поставлена как задача определения знака числа $f(\alpha)$, где $f(x) = \sum_{i=0}^{k} b_i x^i \in Z[x]$, $k < n$ и $b_k \neq 0$ при $k > 0$.

В сборнике [1, с. 240] приведен метод решения поставленной задачи, основанный на разложения числа α в цепную дробь, для которого не удается получить оценку временной сложности, конкурентоспособную с таковыми для представленных в [2] методов, лучшая из которых не превосходит $O(\,n^5 \log^3(L_\varphi + L_f)\,)$. Здесь предлагается являющийся модификацией метода из [1] бинарный метод решения поставленной задачи, который при $f \neq 0$ строит такую последовательность интервалов (l_j, r_j), содержащих α, что $r_j - l_j = (r_{j-1} - l_{j-1})/2$, полагая $\alpha_j = (r_j + l_j)/2$, и делает это до тех пор, пока при некотором $j = j^*$ не будет выполнен критерий останова $|f(\alpha_j)| \geq H_f \left(\sum_{t=1}^{k} t M_\varphi^{t-1}\right) (r_0 - l_0)/2^j$. Тогда знаком числа $f(\alpha)$ является знак числа $f(\alpha_{j^*})$.

ТЕОРЕМА. Временная сложность бинарного метода не превосходит $O(\,n^2(n \log L_\varphi + k \log L_f)^3)\,)$.

Работа выполнена при финансовой поддержке Министерства образования РФ (СПбКЦ, грант А04-2.8-893).

Список литературы

1. Вычисления в алгебре и теории чисел. — М.: Мир, 1976.

2. Rump S. On the sign of a real algebraic number // Proceedings of the 1976 ACM symposium on symbolic and algebraic computation. — 1976. — P. 238–241.

ОБ ОТЛИЧИМОСТИ ПЛОСКИХ ЛАБИРИНТОВ

В. И. Грунская (Димитровград)

Рассматривается задача распознавания прямоугольных лабиринтов [1, 2] и их обобщения — s-лабиринтов, с помощью порождаемых ими слов. Эта задача возникла из задач автоматического распознавания и отображения среды.

Каждой вершине v лабиринта L поставлено в соответствие множество слов λ_v, соответствующих всевозможным путям, начинающимся в вершине v. Вершины v лабиринта L и v' лабиринта L' названы неотличимыми, если множества λ_v и λ'_v совпадают. Лабиринт L назван приведенным, если любая пара его вершин отличима. Лабиринты L и L' названы эквивалентными, если для любой вершины лабиринта L найдется неотличимая от нее вершина лабиринта L' и для любой вершины лабиринта L' найдется неотличимая от нее вершина лабиринта L. Лабиринты L и L' названы изоморфными, если существует взаимно однозначное соответствие между множествами их вершин, сохраняющее смежность и отметки вершин и исходящих из них дуг.

ТЕОРЕМА 1. 1) Две вершины v и v' s-лабиринта L, $v \neq v'$, неотличимы тогда и только тогда, когда они неотличимы никаким словом длины $|L| - |A_L| + 1$, где L и A_L — множества вершин лабиринта L и их отметок, соответственно.

2) Две вершины прямоугольного лабиринта L неотличимы тогда и только тогда, когда они неотличимы никаким словом длины $[|L|/2]+1$.

ТЕОРЕМА 2. Любой прямоугольный лабиринт является приведенным.

ТЕОРЕМА 3. Для прямоугольных лабиринтов L и L' следующие утверждения эквивалентны:

1) некоторые вершины v лабиринта L и v' лабиринта L' неотличимы;

2) лабиринты L и L' эквивалентны;

3) лабиринты L и L' изоморфны.

Список литературы

1. Килибарда Г., Кудрявцев В. Б., Ушчумлич Щ. Независимые системы автоматов в лабиринтах // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 3–39.

2. Килибарда Г., Кудрявцев В. Б., Ушчумлич Щ. Коллективы автоматов в лабиринтах // Дискретная математика. — 2003. — Т. 15, вып. 3. С. 3–40.

АЛГОРИТМ ПОСТРОЕНИЯ ОДНОПРОЦЕССОРНЫХ РАСПИСАНИЙ ДЛЯ СИСТЕМЫ РАБОТ С ИНДИВИДУАЛЬНЫМИ ДИРЕКТИВНЫМИ СРОКАМИ ВЫПОЛНЕНИЯ

Е. С. Гурьянов, В. А. Костенко (Москва)

Задача построения расписания выполнения работ рассматривается в следующем варианте постановки. Задан набор независимых работ. Для каждой работы заданы: время ее выполнения и директивные сроки (директивный интервал), в течении которых работа должна быть выполнена. Расписание выполнения работ это — упорядоченный список непересекающихся по времени выполнения работ, в котором каждая работа определяется временем старта и временем окончания.

Для формирования ограничений на корректность расписания введем понятие цепочки работ. Цепочка работ — последовательность работ, следующих непрерывно друг за другом. Расписание корректно, если выполнены следующие ограничения: 1) не нарушены директивные сроки выполнения работ; 2) длина любой цепочки работ в расписании не превосходит исходно заданной максимально допустимой длины; 3) свободный интервал времени (не запланированы никакие работы) между любыми двумя последовательными цепочками работ не меньше исходно заданной минимально необходимой величины.

Критерием оптимальности расписания является максимальное число работ (из исходно заданного набора), размещенных в расписание без нарушения ограничений. Данная постановка задачи построения расписаний возникла в связи с необходимостью построения статического расписания обменов по централизованному каналу обменов (шине) в бортовых системах реального времени. Ограничения 2 и 3 на корректность расписания обусловлены допустимыми режимами работы бортовой системы и типом контроллера шины.

В основу алгоритма построения расписания выполнения работ положены жадный принцип распределения работ в расписание в соответствии с локальным критерием "самый ранний срок возможного завершения выполнения работы" и проверка на каждом шаге оптимальности этого критерия. Если этот критерий на некотором шаге не является оптимальным, то осуществляется вызов эвристической процедуры выбора очередной работы для размещения в расписание.

АВТОМАТНОЕ РАСПОЗНАВАНИЕ ЗАШУМЛЕННЫХ КУСОЧНО-ЛИНЕЙНЫХ КОНТУРОВ

Ю. Б. Деглина, В. А. Козловский (Донецк)

Задача распознавания и описания контуров плоских фигур является одной из базовых задач распознавания и сжатого описания изображений. Эти задачи созвучны также задачам распознавания лабиринтов автоматами [1]. В работе расматривается подход к анализу и синтезу растровых изображений кусочно-линейных контуров на основе автоматных моделей.

Полагаем, что предъявляемый к распознаванию образ представляет собой прямоугольное поле размера $m \times n$, разбитое на единичные квадраты, окрашенные белым (0) или черным (1) цветом. Описание объектов составляется на основе варианта цепочечного кодирования Фримена. Для удобства рассматриваем только прямые с углом наклона, не превышающим $\pi/4$. Переход к описанию остальных прямых осуществляется простой перекодировкой. В работе [2] рассмотрен случай идеального описания отрезков дискретизированных прямых, на основе которого были предложены схемы алгоритмов их распознавания и синтеза, и выписан в явном виде автомат, порождающий слова описания прямых.

Реальные изображения обычно сопровождаются некоторыми "шумами". Шумом считаем такие изменения в изображении, которые генерируют описания, близкие в некотором смысле к идеальным. Рассмотрены два типа шумов: 1) шумы, искажающие подслова длины, не превышающей длину периода идеального слова k; при этом между двумя подсловами, являющимися шумом, всякий раз находится подслово идеального слова P длиной не меньше k; 2) случай, когда слово описания прямой составлено из подслов, принадлежащих множеству циклических перестановок периода p идеального слова P. Для обоих типов шумов построены распознающие их автоматы и описаны соответствующие алгоритмы распознавания.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов — М.: Наука, 1985. — 320 с.

2. Деглина Ю. Б., Козловский В. А., Костогрыз К. А. Автоматное распознавание оцифрованных многоугольников // Искусственный интеллект, 2004. — № 3. — С. 443–452.

ТЕОРИЯ УПРАВЛЯЕМЫХ СЕТЕЙ И ЕЕ ПРИМЕНЕНИЕ

А. И. Дивеев (Москва)

Управляемой сетью называется конечное множество частичных подсетей

$$\mathbf{G} = \{G_1(V, E_1), G_2(V, E_2), \ldots, G_k(V, E_k)\},$$

где $E = \bigcup_{i=1}^{k} E_i$, $G(V, E)$ — базовая сеть, $V = \{v_1, \ldots, v_n\}$ — множество узлов базовой сети, $E = \{e_1, \ldots, e_m\}$ — множество дуг базовой сети.

Для управляемой сети определено правило выбора частичной подсети

$$G(\mathbf{u}): \quad \mathbf{U} \to \mathbf{G},$$

где $\mathbf{u}$ — вектор управления, $\mathbf{U}$ — множество допустимых управлений, $\mathbf{u} \in \mathbf{U}$.

Для дуг базовой сети заданы ограниченные величины пропускной способности b_{ij}, $i, j = \overline{1,n}$, $i \neq j$, а для узлов — величины вместимостей, b_{ii},$i = \overline{1,n}$.

В сети задан поток $\mathbf{w}^j = [w_1^j \ldots w_n^j]^T$, где j — такт управления, который определяет состояние сети в момент j.

Предполагается, что в каждый такт управления поток может переместиться по сети только по конечному числу дуг. Распределение потока в каждом узле сети по нескольким дугам, выходящим из данного узла, определяются свойствами потока.

Теория управляемых сетей рассматривает вопросы управления потоком в сети за счет выбора на каждом такте конфигурации базовой сети из множества $\mathbf{G}$ частичных подсетей.

Важным свойством управляемой сети является перегрузка — это такое состояние сети, при котором любая конфигурация из $\mathbf{G}$, приводит к превышению допустимой величины вместимости хотя бы в одном узле.

Рассматривается также задача оптимального управления потоком в сети. В качестве критерия управления используется максимум пропускной способности сети за конечное число тактов управления. Разработан эффективный алгоритм решения задачи оптимального управления потоком в сети на базе комбинации методов генетического алгоритма и динамического программирования.

ТАБЛИЦЫ СВЯЗЕЙ ГРУПП ПРОСТОЙ ЭКСПОНЕНТЫ СТУПЕНИ 2 И РЕГУЛЯРНЫЕ ГИПЕРБОЛИЧЕСКИЕ (3,4)-ПЛОСКОСТИ

А. И. Долгарев (Пенза)

Рассматриваются нильпотентные группы N_p простого периода p ступени 2 [1] с 8 образующими $a_i, i = \overline{1,8}$, и удовлетворяющие условиям: (1) $Z(N_p) = C(N_p)$; (2) всякие два элемента a_i, a_j неперестановочны; (3) для всякого фиксированного j коммутаторы $[a_i, a_j] = c_k$ таковы, что $\langle c_k\rangle \cap \langle c_l\rangle = \langle e\rangle$; некоторые коммутаторы образующих группы N_p являются образующими коммутанта $C(N_p)$, а остальные являются степенями этих коммутаторов; (4) среди коммутаторов образующих в каждой из циклических подгрупп $\langle c_k\rangle$ содержится по 4 коммутатора; (5) множество пар с различными индексами $[i, j]$ образующих a_i, входящих в подгруппы $\langle c_k\rangle$, разбиваются значениями коммутаторов $[a_i, a_j]$ на классы эквивалентности.

Для группы составляется таблица связей: размеры таблицы 8x8, на пересечении i-ой строки и j-го столбца расположен номер образующего элемента коммутанта, являющийся коммутатором образующих группы $[a_i, a_j]$.

Установлены следующие свойства: 1) коммутант группы порождается 7 элементами, группа имеет порядок p^{15}; 2) таблица связей определяет группу, при $p = 2$ единственную; 3) таблица связей является симметричным латинским квадратом [2], ее восьмой элемент — пустая клетка; распадается на 4 латинских квадрата 4x4; 4) имеется не менее четырех видов таблиц связей, не преобразующихся одна в другую, и четыре вида попарно неизоморфных групп N_p. Это количество не связано с числом ортогональных квадратов размеров 4x4.

На основании таблиц связей рассматриваемых групп построены таблицы инцидентности регулярных гиперболических $(3, 4)$-плоскостей, [3]. На каждой прямой содержится по 3 точки; через каждую точку вне прямой проходит по 4 прямые, не пересекающие данную прямую. Плоскости содержат по 15 точек, 35 прямых, через каждую точку проходит по 7 прямых.

До сих пор неизвестны неизоморфные гиперболические $(3, 4)$-плоскости. Нами получено 4 попарно неизоморфных плоскости.

Список литературы

1. Курош А. Г. Теория групп. — М.: Наука, 1967. — 648 с.
2. Холл М. Комбинаторика. — М.: Мир, 1970. — 424 с.
3. Картеси Ф. Введение в конечные геометрии. — М.: Наука, 1960. — 320 с.

КОНЕЧНЫЕ КОАЛИЦИОННЫЕ ИГРЫ: ПАРАМЕТРИЗАЦИЯ КОНЦЕПЦИИ РАВНОВЕСИЯ И УСТОЙЧИВОСТЬ ОБОБЩЕННО-ЭФФЕКТИВНЫХ СИТУАЦИЙ

В. А. Емеличев, К. Г. Кузьмин (Минск)

Пусть $X_i \subseteq \mathbb{R}$, — конечное множество стратегий игрока $i \in N_n = \{1, 2, \ldots, n\}$, $n \geq 2$, $f_i(x) = C_i x$, — функция выигрыша игрока i, определенная на множестве ситуаций $X = \prod\limits_{i \in N_n} X_i$, $|X_i| \geq 2$; C_i — i-я строка матрицы $C = [c_{ij}]_{n\times n} \in \mathbb{R}^{n\times n}$, $x = (x_1, x_2, \ldots, x_n)^T$, $x_i \in X_i$, $i \in N_n$.

Пусть множество игроков N_n разбито на $s \in N_n$ непересекающихся коалиций $(J_1, J_2, \ldots, J_s)$ и пусть внутри каждой коалиции отношения игроков строятся на основе лексикографического принципа максимизации. Возникающая таким образом параметрическая концепция равновесия (принцип оптимальности) порождает множество обобщенно-эффективных (или иначе $(J_1, J_2, \ldots, J_s)$-эффективных) ситуаций $H^n(C, J_1, J_2, \ldots, J_s)$. В частности, $H^n(C, N_n)$ — множество лексикографически максимальных ситуаций, а $H^n(C, \{1\}, \{2\}, \ldots, \{n\})$ — множество ситуаций равновесия по Нэшу.

Радиусом устойчивости $(J_1, J_2, \ldots, J_s)$-эффективной ситуации $x^0 \in H^n(C, J_1, J_2, \ldots, J_s)$, как обычно [1], назовем число $\rho^n(x^0, C, J_1, J_2, \ldots, J_s) = \sup \Xi$ при $\Xi \neq \emptyset$ и $\rho^n(x^0, C, J_1, J_2, \ldots, J_s) = 0$ при $\Xi = \emptyset$, где $\Xi = \{\varepsilon > 0 : \ \forall\, C' \in \Omega(\varepsilon) \ \big(x^0 \in H^n(C + C', J_1, J_2, \ldots, J_s)\big)\}$, $\Omega(\varepsilon) = \{C' \in \mathbb{R}^{n\times n} : ||C'|| < \varepsilon\}$, $C' = [c'_{ij}]_{n\times n}$.

Выведена формула радиуса устойчивости ситуации $x^0 \in H^n(C, J_1, J_2, \ldots, J_s)$ при любом разбиении $(J_1, J_2, \ldots, J_s)$, а также частные случаи этой формулы для лексикографической и равновесной ситуации в случае метрик l_1 и l_∞.

Список литературы

1. Емеличев В. А., Кузьмин К. Г. Анализ устойчивости строго эффективного решения одной векторной задачи булева программирования в метрике l_1 // Дискретная математика. — 2004. — Т. 16, вып. 4. — С. 14–19.

ОПТИМИЗАЦИЯ ДРОБНО-ЛИНЕЙНОЙ ФУНКЦИИ НА РАЗМЕЩЕНИЯХ ПРИ ДОПОЛНИТЕЛЬНЫХ ОГРАНИЧЕНИЯХ

О. А. Емец, Т. Н. Барболина, О. А. Черненко (Полтава)

Рассматривается задача максимизации функции

$$F(x^*) = \max_{x \in R^m} \frac{\sum\limits_{j=1}^{m} c_j x_j + c_0}{\sum\limits_{j=1}^{m} d_j x_j + d_0}$$

при комбинаторном условии принадлежности решения множеству размещений, т. е. $x \in E^k_{\eta n}(G) \subset R^m$, и линейных ограничениях $\sum\limits_{j=1}^{m} a_{ij} x_j \le b_i$, где $c_j, d_j, c_0, d_0, a_{ij}, b_i \in R, j \in J_m = \{1, 2, ..., m\}, i \in J_p$. Считаем, что $\sum\limits_{j=1}^{m} d_j x_j + d_0 > 0$. Предлагаемый подход к решению основывается на замене условия $x \in E^k_{\eta n}(G)$ релаксирующим условием $x \in conv E^k_{\eta n}(G)$ и переходе к линейной задаче путем преобразования $y_0 = 1 / \left(\sum\limits_{j=1}^{m} d_j x_j + d_0 \right)$. Если полученное решение релаксирующей задачи не удовлетворяет условию $x \in E^k_{\eta n}(G)$, то осуществляется лексикографический перебор λ-классов — элементов фактор-множества по лексикографической эквивалентности относительно размещений [1]. Перебор проводится как в направлении лексикографического убывания (т. е. переход к лексикографически меньшему λ-классу), так и в направлении лексикографического возрастания. С целью сокращения перебора из рассмотрения исключаются λ-классы, на представителях которых значение целевой функции меньше F^*, где F^* было получено на одной из предыдущих итераций. Это ограничение, как показано авторами, может быть записано в виде линейного.

Список литературы

1. Емец О. А., Барболина Т. Н. Решение задач евклидовой комбинаторной оптимизации методом построения лексикографической эквивалентности // Кибернетика и системный анализ. — 2004. — № 5. — С. 115–125.

ЗАДАЧИ НА ПЕРЕСТАНОВКАХ ИГРОВОГО ТИПА

О. А. Емец, Н. Ю. Устьян (Полтава)

Рассмотрим матаметическую модель: найти $\vartheta = F(X_{i_1}, Y_{j_2})$, где X_{i_1} находится из выражения $F(X_{i_1}, Y_{j_1}) = \max\limits_i \min\limits_j F(X, Y)$; Y_{j_2} — из выражения $F(X_{i_2}, Y_{j_2}) = \min\limits_j \max\limits_i F(X, Y)$;

$$F(X,Y) = \sum_{j=1}^{n} y_j \sum_{i=1}^{m} a_{ij} x_i, A = (a_{ij}), i = \overline{1,m}, j = \overline{1,n};$$

$$X = (x_1, x_2, ..., x_m) \in E_m(P^x), \quad Y = (y_1, y_2, ..., y_n) \in \overline{Y};$$

$$P^x = (P_1^x, P_2^x, ..., P_m^x) : \forall i = \overline{1,m} \quad P_i^x \ge 0; \sum_{i=1}^{m} P_i^x = 1.$$

Если $\overline{Y} = R^n$ и вектор $Y = (y_1, y_2, ..., y_n)$ удовлетворяет условиям $\sum\limits_{j=1}^{n} y_j = 1,\ y_j \ge 0\ \forall j = \overline{1,n}$, то назовем такую модель моделью 1, а если $\overline{Y} = E_n(P^y) \in R^n$, где $P^y = (P_1^y, P_2^y, ..., P_n^y)$ — заданный вектор, для которого выполняется $\sum\limits_{j=1}^{n} P_j^y = 1,\ P_j^y \ge 0\ \forall j = \overline{1,n}$, — моделью 2.

Задачи, которые описываются моделями 1 и 2, назовем задачами на перестановках игрового типа [1], X_{i_1} и Y_{j_2} — оптимальными стратегиями первого и второго игроков соответственно, ϑ — ценой игры.

Для нахождения оптимальной стратегии Y_{j_2} модель 1 была сведена к задаче линейной оптимизации и при небольшой размерности может быть решена симплекс-методом, а для нахождения X_{i_1} — к линейной задаче комбинаторной оптимизации на перестановках, которая в отдельных случаях решается методом комбинаторного отсечения [2]. Модель 2 была сведена к матричной игре. Для решения задач размерности $2 \times n$ и $m \times 2$ был модифицирован графический метод теории игр.

Список литературы

1. Емець О. О., Устьян Н. Ю. Ігрова комбінаторна модель однієї задачі сільськогосподарського виробництва // Матеріали VII Міжн. наук.-практ. конф. «Наука і освіта, 2004». — Дніпропетровськ: Наука і освіта, 2004. — Т. 70. — С. 46–49.

2. Емець О. О., Емець Е. М. Відсікання в лінійних частково комбінаторних задачах евклідової комбінаторної оптимізації // Доповіді НАН України. — 2000. — № 9. —С. 105–109.

О СТОИМОСТИ КОДИРОВАНИЯ И ЭНТРОПИИ СТОХАСТИЧЕСКОГО ЯЗЫКА

Л. П. Жильцова (Нижний Новгород)

В [1] исследовалась зависимость между стоимостью оптимального двоичного кодирования и энтропией стохастического языка. В настоящей работе эта зависимость устанавливается для q-ичного кодирования ($q \geq 2$). Пусть L — произвольный бесконечный язык в некотором алфавите и P — распределение вероятностей на множестве слов языка L. Пара $\mathcal{L} = (L, P)$ называется стохастическим языком.

Кодированием языка $\mathcal{L}$ в q-ичном алфавите A будем называть инъективное отображение $f : L \to A^+$. Через $F(L)$ обозначим класс всех инъективных отображений из L в A^+.

Пусть $f \in F(L)$. Величину

$$C(\mathcal{L}, f) = \lim_{N\to\infty} \sum_{\alpha\in L, |\alpha|\leq N} p(\alpha)\cdot \mid f(\alpha) \mid$$

назовем стоимостью кодирования f (здесь $\mid x \mid$ — длина слова x).

Под стоимостью оптимального кодирования будем понимать величину

$$C_0(\mathcal{L}) = \inf_{f\in F(L)} C(\mathcal{L}, f)$$

и под q-энтропией языка $\mathcal{L}$ — величину

$$H_q(\mathcal{L}) = \lim_{N\to\infty} \sum_{\alpha\in L, |\alpha|\leq N} (-p(\alpha) \cdot \log_q p(\alpha)).$$

ТЕОРЕМА. Пусть $\mathcal{L}$ — бесконечный стохастический язык, для которого существует конечное значение $H_q(\mathcal{L})$. Тогда $C_0(\mathcal{L})$ имеет конечное значение и удовлетворяет неравенствам

$$\tfrac{1}{\log_q 2} H_q(\mathcal{L}) \leq C_0(\mathcal{L}) < H_q(\mathcal{L}) + 1.$$

Работа выполнена при финансовой поддержке РФФИ (проект 04-01-00374) и программы поддержки ведущих научных школ.

Список литературы

1. Zhiltsova L. On Entropy and optimal coding cost for stochastic language // Fundamenta Informaticae. — 1998. — V. 36. — P. 285–305.

О РАЗМЕЩЕНИИ МАКСИМАЛЬНОГО ЧИСЛА ЗАДАНИЙ С РАЗЛИЧНЫМИ ВРЕМЕНАМИ ОКОНЧАНИЯ

С. Н. Жук (Москва)

В [1] рассмотрена задача о размещении n независимых многопроцессорных заданий с единичными временами выполнения и заданными временами окончания, в которой требовалось максимизировать число размещенных заданий. В данной работе исследовалось обобщение этой задачи на случай, когда задания могут иметь произвольные времена работы.

Пусть $T = \{T_1, T_2, \ldots, T_n\}$ — множество заданий, которые должны быть выполнены на m процессорах. Для каждого T_j заданы $h(T_j)$, $w(T_j)$ и $d(T_j)$ — время выполнения задания, требуемое число процессоров и время, до которого задание должно быть выполнено.

Множество R пар $(T_j, t(T_j))$ будем называть размещением множества заданий T, если: 1) каждое задание T_j входит в R не более одного раза; 2) $t(T_j) \in [0, d(T_j) - h(T_j)]$, $\forall (T_j, t(T_j)) \in R$; 3) для всех h справедливо неравенство

$$\sum_{\substack{(T_j,t(T_j))\in R \\ h\in(t(T_j),t(T_j)+h(T_j))}} w(T_j) \leq m.$$

Требуется найти размещение R, содержащее наибольшее количества заданий (то есть имеющее наибольшее значение $|R|$).

Рассматриваемая задача является NP-трудной (даже для случая когда все времена выполнения равны 1), поэтому вряд ли можно ожидать, что она имеет эффективное решение. В данной работе получен приближенный полиномиальный алгоритм, позволяющий решить эту задачу с логарифмической точностью.

Будем обозначать: $R_O(T)$ — одно из оптимальных размещений T, $R_A(T)$ — размещение, получаемое с помощью алгоритма A. Тогда величина $r_A(T) = \frac{|R_O(T)|}{|R_A(T)|}$ является мультипликативной точностью алгоритма A.

ТЕОРЕМА. Существует полиномиальный алгоритм A, такой что для любого множества заданий T выполняется неравенство

$$r_A(T) \leq 6 \log_2 n + 216.$$

Список литературы

1. Fishkin A., Zhang G. On maximizing the throughput of multiprocessor tasks // Theoretical Computer Science. — 2003. — V. 302. — P. 319–335.

СТАТИСТИЧЕСКИЕ ОЦЕНКИ ЛИНЕЙНОЙ СЛОЖНОСТИ МАРКОВСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПО КРИТЕРИЮ ЭНТРОПИИ

В. М. Захаров, Б. Ф. Эминов (Казань)

Линейная сложность $L(l)$ (ЛС) является важным параметром анализа случайных и псевдослучайных последовательностей. Одной из проблемных исследовательских задач является разработка методов увеличения ЛС последовательностей через усложнение их аналитического строения. В работе исследуется ЛС марковских последовательностей (МП), классифицируемых по критерию энтропии $H(P)$ матрицы переходов P. Цель исследования — определение взаимосвязей ЛС и $H(P)$. $L(l)$ вычисляется по алгоритму Берлекэмпа — Месси. МП рассматриваются как реализации конечной длины l однородных простых и сложных цепей Маркова (ЦМ), задаваемых матрицами P из класса регулярных матриц. Решаются следующие задачи:

— определение оценок математического ожидания $M(L(l))$ и дисперсии $D(L(l))$ МП, моделируемых по P, с заданной $H(P)$;

— определение $M(L(l))$ и $D(L(l))$ как характеристик определенных подклассов МП, классифицируемых по критерию $H(P)$;

— определения линейного профиля МП, отражающего поведение $L(l)$ от длины последовательностей генерируемой реализации ЦМ.

Введен критерий получения требуемой длины l реализации ЦМ, позволяющий сопоставить для P МП длины l, с заданной точностью. Вычислены выборочные среднее $M(L(l))$ и дисперсия $D(L(l))$ при заданных значениях $H(P)$ и объемах выборок реализаций ЦМ.

Было получено, что $M(L(l)) \to c + l/2$, $D(L(l)) \to 86/81$, $c < 1$, c зависит от $H(P)$, с нормальным законом распределения при $H(P) = [0,5H_{max}(P);\ \ 0,9H_{max}(P)]$, где $H_{max}(P) = \log_2 m$, m — размерность P. При $H(P) \to 0$ у последовательностей выявляется период N: $L(l) \to \log_2 N$, плотность распределений $L(l)$ представляет собой разрозненные выбросы.

ЛС реализаций сложных ЦМ больше или равна ЛС для простых ЦМ из-за избыточности кодирования. ЛС обладает инвариантностью по отношению к размерности матрицы. Профиль ЛС может состоять из множества горизонтальных отрезков, при аппроксимации стремящихся к прямой вида $L(l) = l/2$.

О СИММЕТРИЧЕСКИХ ПРОСТРАНСТВАХ ГРАФОВ

Д. В. Захарова (Нижний Новгород)

Множество обыкновенных графов назовем симметрическим пространством графов, если оно замкнуто относительно изоморфизма и сложения графов по модулю 2. Нетривиальными примерами симметрических пространств являются класс ED всех графов, у которых степени всех вершин четны (квазициклов) и класс CB всех полных двудольных графов. С этими двумя классами связаны пространства циклов и разрезов: для каждого графа G его пространством циклов является множество $ED \cap S(G)$, а пространством разрезов — множество $CB \wedge S(G)$, где $S(G)$ обозначает множество всех остовных подграфов графа G, а $X \wedge Y = \{G \cap H : G \in X, H \in Y\}$. Представляет интерес вопрос о существовании других симметрических пространств графов. Доказывается, что имеется ровно 14 таких пространств.

О НИЖНЕЙ ОЦЕНКЕ СЛОЖНОСТИ ОПЕРАТОРНЫХ ПОЛИНОМИАЛЬНЫХ ФОРМ ДЛЯ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

А. С. Зинченко, В. И. Пантелеев (Иркутск)

При изучении полиномиальных форм оказался удобным операторный подход, рассмотренный в [1] для булевых функций. Для функций k-значной логики (k — простое число, $k \geq 2$) будем рассматривать полиномиальные представления, которые имеют вид многоместной суммы по модулю k, в которых слагаемые есть операторные образы системы функций G по оператору t. Все необходимые определения можно посмотреть например в [2].

Пусть

$$G = \{x_1^0 \cdot \ldots \cdot x_n^0, \ldots, x_1^{k-1} \cdot \ldots \cdot x_n^{k-1}\},$$

$$D = (d^{i_1} \ldots d^{i_n} | (i_1, \ldots, i_n) \in E_k^n)\}.$$

Тогда справедлива следующая

ТЕОРЕМА. $L_D^G(n) \geq (\frac{k+1}{2})^n$, $k \geq 3$.

Работа выполнена при частичной финансовой поддержке РФФИ (код проекта 04–07–90178в).

Список литературы

1. Избранные вопросы теории булевых функций / Под редакцией Винокурова С. Ф., Перязева Н. А. — М.: Физматлит, 2001.

2. Зинченко А. С., Пантелеев В. И. О представлении функций конечнозначной логики пучками операторов // Алгебра, логика и кибернетика: Материалы международной конференции. — Иркутск: Издательство ГОУ ВПО "Иркутский государственный педагогический университет", 2004. — С. 139–142.

О СЛОЖНОСТИ АЛГОРИТМОВ УМНОЖЕНИЯ МАТРИЦ НАД ПОЛИНОМАМИ

М. С. Зуев (Тамбов)

Пусть R — коммутативная область. Полином $\sum_{i=1}^m c_i x^{i-1} \in R[x]$, у которого коэффициент c_i отличен от нуля с вероятностью α_i, назовем полиномом типа (m, α_i). Если $\alpha_i = \alpha$ для всех i, то обозначаем тип (m, α). Назовем матрицей типа (n, ρ, m, α_k) случайную $n \times n$ матрицу, каждый элемент которой отличен от нуля с вероятностью ρ, а каждый ненулевой элемент — это полином типа (m, α_k). Будем обозначать $\mathcal{EA}$ и $\mathcal{EM}$ математическое ожидание числа операций сложения и умножения в алгоритме, а также $\phi_{a,b} = a + b - ab$ (см. [1]).

ТЕОРЕМА 1. При сложении матриц типа (n, ρ, m, α) и (n, σ, m, β) сумма имеет тип $(n, \phi_{\rho,\sigma}, m, \phi_{\rho\alpha,\sigma\beta})$ и $\mathcal{EA} = \phi_{\rho\alpha,\sigma\beta} m n^2$.

ТЕОРЕМА 2. При умножении матриц типа (n, ρ, m, α) и (n, σ, m, β) произведение имеет тип $(n, 1-(1-\rho\sigma)^n, 2m-1, \eta_i)$ где $\eta_i = 1 - \sum_{k=0}^n \binom{n}{k} \rho^k \sigma^k (1-\pi_i)^k (1-\rho\sigma)^{n-k}$. Если при этом применяется стандартный алгоритм умножения, то $\mathcal{EM} = \alpha\beta\rho\sigma n^3 m^2$ и $\mathcal{EA} = \mathcal{EM} + n^2 \sum_{i=1}^{2m-1} \sum_{j=2}^n (1-(1-\rho\sigma\pi_i)^j)$.

Здесь обозначено $\pi_i = 1 - (1-\alpha\beta)^{t_i^m}$, $t_i^m = i$ при $1 \leq i \leq m$ и $t_i^m = 2m - i$ при $m \leq i \leq 2m-1$.

Получены также выражения для математического ожидания числа сложений и умножений в случае применения алгоритма Штрассена для умножения матриц.

Работа выполнена при частичной поддержке грантов РФФИ (проект 04-07-90268), Human Capital Foundation (проект 23-03-24) и программы Университеты России (проект УР.04.01.464).

Список литературы

1. Зуев М. С., Малашонок Г. И. О сложности алгоритмов умножения полиномиальных матриц // Труды VI Международной конференции "Дискретные модели в теории управляющих систем". — М.: Изд-во ВМиК МГУ, 2004. — С. 32–40.

ОБ ОДНОМ РАСШИРЕНИИ ПРОПОЗИЦИОНАЛЬНОЙ ЛОГИКИ ЛИНЕЙНОГО ВРЕМЕНИ

А. С. Иванов (Москва)

Пропозициональная логика линейного времени ($PLTL$) - это логика с модальными операторами $\circ$ ("в следующий момент времени"), $\Box$ ("всегда в будущем") и U ("до тех пор, пока"). Известно, что задачи проверки выполнимости и проверки выполнимости на модели для $PLTL$ разрешимы за время, экспоненциальное от размера формулы и полиномиальное от размера модели.

В работе рассматривается язык $PLTL^e$ линейной темпоральной логики, дополненный операторами $\Box^{\leq n}$ (верно на протяжении последующих n шагов) и $\circ^n$ (верно через n шагов). В качестве моделей рассматриваются автоматы, в которых каждый переход занимает некоторое фиксированное время, и для успешности перехода необходимо, чтобы входная буква автомата принадлежала некоторому множеству на протяжении всего этого времени. Известно, что формулы и модели $PLTL^e$ можно перевести в формулы и модели $PLTL$, но это приведет к экспоненциальному увеличению их размера.

ТЕОРЕМА. Для любой $PLTL^e$-формулы ϕ можно построить такую эквивалентную ей $PLTL$-формулу ψ, что $|\psi| = poly(|\phi|)$ и при этом в ψ содержится $O(|\phi|)$ новых переменных.

ТЕОРЕМА. Для любого автомата Бюхи A с n состояниями и любой $PLTL^e$-модели M с m вершинами существует автомат B размера $O(mn)$, который непуст тогда и только тогда, когда непусто пересечение языков, порождаемых автоматом A и моделью M.

Эти две теоремы дают способ построения алгоритма проверки выполнимости формулы ϕ на модели M для $PLTL^e$ со сложностью, не превосходящей полинома от сложности алгоритма проверки на модели для $PLTL$: вначале ϕ преобразуется в эквивалентную формулу ψ, далее согласно методу построения канонической модели, описанному в [1], строится автомат A_ψ, после чего по A_ψ и M строится автомат B. Если B непуст, то ответ о выполнимости положительный, иначе — отрицательный.

Список литературы

1. Э. М. Кларк, О. Грамберг, Д. Пелед. Верификация моделей программ — model checking. — М.: МЦНМО, 2002.

ЗАДАЧИ ДЕЛЬСАРТА ДЛЯ ПЕРИОДИЧЕСКИХ ПОЛОЖИТЕЛЬНО ОПРЕДЕЛЕННЫХ ФУНКЦИЙ

В. И. Иванов (Тула)

Пусть $0 < h \leqslant 1/2$, $K_D(h)$ — класс 1-периодических, непрерывных, четных, положительно определенных функций $f(x)$, для которых $f(x) \leqslant 0$, $h \leqslant |x| \leqslant 1/2$.

Интегральная задача Дельсарта состоит в вычислении величины

$$A_D(h) = \sup_{f \in K_D(h)} \int_{-1/2}^{1/2} f(x)dx.$$

Поточечная задача Дельсарта состоит в определении функции

$$A_D(x,h) = \sup_{f \in K_D(h)} f(x), \quad |x| \leq h.$$

Задачи Дельсарта с успехом применяются при решении многих задач дискретной математики.

Вычисление величины $A_D(h)$ для рациональных h сводится к решению дискретной задачи Фейера о наибольшем значении четного дискретного неотрицательного полинома с фиксированным нулевым коэффициентом. Для определения функции $A_D(x,h)$ для рациональных x и h необходимо найти наибольшие значения коэффициентов таких полиномов.

В докладе будет идти речь о подходах к решению дискретных задач Фейера. Первую дискретную задачу Фейера удалось решить полностью.

Работа выполнена при финансовой поддержке РФФИ (проект 03-01-00647).

λ-РЕАЛИЗАЦИЯ СЕТИ И СХОДИМОСТЬ λ-ЭКСТРЕМАЛЬНЫХ СЕТЕЙ ПРИ $\lambda \to \infty$

Д. П. Ильютко (Москва)

В данной работе рассматриваются λ-экстремальные сети, т.е. критические точки функционала нормированной длины, где единичная окружность для нормы совпадает с правильным 2λ-угольником. *Сеть* — это произвольное плоское дерево Γ с множеством вершин $V(\Gamma)$, причем у сети выделено некоторое множество $\partial\Gamma$ его вершин. Вершины из $\partial\Gamma$ называются *граничными*, а вершины из $V(\Gamma) \setminus \partial\Gamma$ — *внутренними*. Ребра сети являются прямолинейными отрезками.

ОПРЕДЕЛЕНИЕ. Сеть называется *деревом Штейнера*, если степени всех вершин не больше 3, а все вершины степени 1 — граничные. Сеть называется *бинарной*, если все ее граничные вершины имеют степень 1, а внутренние — 3. Будем говорить, что сеть Γ *допускает планарную λ-реализацию*, если существует планарно эквивалентная ей λ-экстремальная сеть Γ'.

ТЕОРЕМА 1. Сеть Γ допускает планарную λ-реализацию, где $\lambda \neq 2, 3, 4, 6$, тогда и только тогда, когда Γ является деревом Штейнера.

Рассмотрим на плоскости произвольную сеть Γ и последовательность сетей $\{\Gamma_n\}_{n=1}^{\infty}$, планарно эквивалентных сети Γ.

ОПРЕДЕЛЕНИЕ. Последовательность $\{\Gamma_n\}_{n=1}^{\infty}$ *сходится к* Γ, если последовательность вершин, составленная из вершин сетей Γ_n, которые при планарной эквивалентности переходят друг в друга, сходится к соответствующей вершине из Γ. Последовательность $\{\Gamma_n\}_{n=1}^{\infty}$ *строго сходится к* Γ, если она сходится и границы всех сетей совпадают.

ТЕОРЕМА 2. Для любой (бинарной) экстремальной сети Γ на стандартной евклидовой плоскости существует последовательность λ-экстремальных сетей, (строго) сходящаяся к Γ при $\lambda \to \infty$.

Автор выражает глубокую благодарность профессорам А. О. Иванову и А. А. Тужилину за постоянное внимание к работе.

Работа выполнена при частичной поддержке грантов Президента РФ НШ–1988.2003.1, МД–263.2003.01, а также гранта РФФИ 04–01–00682.

Список литературы

1. Иванов А. О, Тужилин А. А. Теория экстремальных сетей. — Москва-Ижевск: Институт компьютерных исследований, 2003.

ТЕОРЕТИКО-МНОЖЕСТВЕННОЕ ОПИСАНИЕ ПОДГРАФОВ ГРАНЕЙ ПЛАНАРНЫХ ГРАФОВ

М. А. Иорданский (Нижний Новгород)

Рассматриваются связные планарные графы. Подграф G' графа G, вершины и ребра которого образуют границу некоторой грани в плоской укладке графа G, называется графом грани графа G. Произвольный подграф графа грани G' называется подграфом грани графа G. Оболочкой графа грани G' в графе G называется подграф, порожденный ребрами множества $E(G)\backslash E(G')$. Грань графа G называется максимальной, если оболочка соответствующего ей графа грани G' обладает следующими свойствами:

1) никакая компонента связности оболочки графа грани G' не может пересекаться с графом грани G' по одной вершине;

2) цепи из оболочки графа грани G' не могут соединять вершины v_i и v_j из $V(G')$, если все ребра цепи, соединяющей вершины v_i и v_j в $E(G')$, не принадлежат циклам из G'.

При задании графов используется конструктивный подход [1]. Граф G реализуем Q-суперпозицией графов из P, если его можно получить из графов множества P путем последовательного применения операций склейки по графам из множества Q.

ТЕОРЕМА. G' является графом максимальной грани графа G тогда и только тогда, когда:

1. G' реализуем $K1$-суперпозицией над $P = \{K_2, C_1, C_2, ...\}$;

2. G' выбирается в G таким образом, что

a) оболочка G' состоит из множества цепей, соединяющих пары вершин, принадлежащих одному циклу в G';

b) никакие 3 вершины одного цикла из G' не образуют большую долю подграфа графа G, гомеоморфного $K_{2,3}$;

c) никакие 4 вершины одного цикла из G' не образуют подграф графа G, гомеоморфный K_4.

Работа выполнена при финансовой поддержке РФФИ (проект 04-01-00374).

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 4. — С. 35–63.

КОНЕЧНОРАЗНОСТНЫЙ ДВОЙСТВЕННЫЙ РЕГУЛЯРИЗОВАННЫЙ МЕТОД В ЗАДАЧЕ УПРАВЛЕНИЯ ГИПЕРБОЛИЧЕСКОЙ СИСТЕМОЙ

А. З. Ишмухаметов, Р. Махроус (Москва)

Рассматривается задача оптимального управления

$$J(u,v)=\int_0^l (|w(x,T;u,v)-y_0(x)|^2+|w_t(x,T;u,v)-y_1(x)|^2)dx\to\inf,$$

$$w_{tt}-(a(x)\cdot w_x(x,t))_x=d(x)\cdot u(t)+f(x,t),\ (x,t)\in Q,$$

$$w_x(0,t)=v(t),\ w_x(l,t)=0,\ t\in[0,T],$$

$$w(x,0)=\varphi_0(x),\ w(_t(x,0)=\varphi_1(x),\ x\in[0,l],$$

где управления $(u(t),v(t))\in L_2(0,T)\times L_2(0,T)$:

$$|u(t)|_{L_2(0,T)}\le R_1,\ \ |v(t)|_{L_2(0,T)}\le R_2.$$

Здесь $Q=(0,l)\times(0,T)$; $a(x)\in C^1[0,l]$, $a(x)>0$, $f\in L_2(Q)$, $y_0(x)$, $\varphi_0(x)\in W^1(0,l)$, $d(x)$, $y_1(x)$, $\varphi_1(x)\in L_2(0,l)$.

Данной задаче ставится в соответствие конечноразностная задача. Для решения конечноразностных задач применяется двойственный регуляризованный метод [1], который является развитием обобщенного метода моментов [2]. Используя методику исследования свойств аппроксимаций задач оптимального управления [3], для данного метода выведены условия и оценки сходимости по функционалу и по управлению.

Работа выполнена при финансовой поддержке РФФИ (проект 04-01-00619).

Список литературы

1. Ишмухаметов А. З. Двойственный метод решения одного класса выпуклых задач минимизации // ЖВМ и МФ. — 2000. — Т. 40, № 7. — С. 1045–1060.

2. Васильев Ф. П., Ишмухаметов А. З., Потапов М. М. Обобщенный метод моментов в задачах оптимального управления. — М.: Изд-во МГУ, 1989.

3. Ишмухаметов А. З. Вопросы устойчивости и аппроксимации задач оптимального управления системами с распределенными параметрами. — М.: ВЦ РАН, 2001.

СИСТЕМА ОПЕРАЦИЙ ПРЕОБРАЗОВАНИЯ РАСПИСАНИЙ, ЕЕ СВОЙСТВА И ИСПОЛЬЗОВАНИЕ ДЛЯ ПОСТРОЕНИЯ ИТЕРАЦИОННЫХ АЛГОРИТМОВ

А. В. Калашников, В. А. Костенко (Москва)

Будем рассматривать задачу построения расписания в следующем варианте постановки. Исходными данными для построения расписания являются: 1) множество работ, на котором определено отношение частичного порядка, задающее ограничения на допустимую последовательность выполнения работ, 2) множество ресурсов, 3) критерий оптимальности расписания и функция его вычисления. Расписание выполнения заданного множества работ определено, если для каждой работы заданы: 1) привязка к одному из ресурсов; 2) порядковый номер выполнения на ресурсе. Расписание является корректным, если выполнены следующие ограничения: 1) каждая работа должна быть назначена на ресурс и лишь на один ресурс; 2) частичный порядок, заданный на исходном множестве работ не должен нарушаться в расписании; 3) расписание должно быть беступиковым.

Для получения нового варианта расписания используется две операций преобразования расписания: 1) $O1(p_i,R_m,R_k,c)$ — операция изменения привязки работ переносит работу p_i с ресурса R_m на ресурс R_k (порядковый номер работы на ресурсе R_k становится равным c); 2) $O2(p_i,SP_m,c)$ — операция изменения порядка работ на одном ресурсе изменяет порядковый номер работы p_i на ресурсе R_m (порядковый номер работы становится равным c).

ТЕОРЕМА. Если H и H' произвольные корректные варианты расписания, то существует конечная цепочка операций $\{O_i\}_{i=1}^K, O_i\in\{O1,O2\}$, переводящая расписание H в H', такая, что все K промежуточных расписаний являются корректными и $K\le 2N$, где N — количество планируемых работ.

УТВЕРЖДЕНИЕ. Сложность нахождения множества значений c, при которых применение операций $O1$ и $O2$ приводит к корректным вариантам расписания, не больше чем $O(N)$.

На основании сформулированных теоремы и утверждения можно сделать вывод, что существует (но неизвестен) итерационный алгоритм перехода от произвольного корректного расписания к оптимальному расписанию, сложность которого равна $O(N^2)$ и алгоритм на каждой итерации получает корректные варианты расписания.

ОБ АНОРМАЛЬНЫХ ЗАДАЧАХ С НЕРАВЕНСТВАМИ

Д. Ю. Карамзин (Москва)

В пространстве $X = \mathbb{R}^n$ рассмотрим задачу

$$f(x) \to \min, \quad F(x) \in C, \tag{1}$$

где $C = \{y \in Y : y^j = 0, j \in J_1,\ y^j \le 0, j \in J_2\}$, $Y = \mathbb{R}^k$. Точка $\hat{x}$ локального минимума в задаче (1) называется *нормальной*, если $\operatorname{Im} F'(\hat{x}) = Y$, и *анормальной* в противном случае. Рассмотрим функцию $\mathcal{L} : \mathbb{R}^n \times \mathbb{R}^{k+1} \to \mathbb{R}^1$

$$\mathcal{L}(x, \lambda) = \lambda_0 f(x) + \langle y, F(x) \rangle, \quad \lambda = (\lambda_0, y),\ \lambda_0 \in \mathbb{R}^1,\ y \in Y.$$

Обозначим через $\Lambda(\hat{x})$ множество векторов $\lambda = (\lambda_0, y)$ таких, что $\frac{\partial \mathcal{L}}{\partial x}(\hat{x}, \lambda) = 0$, $\lambda_0 \ge 0$, $y \in N_C(0)$, $\lambda \ne 0$. Здесь $N_C(0)$ — нормальный конус к C в нуле. Для $r = 1, 2, ...$ обозначим через $\Lambda_r(\hat{x})$ множество векторов $\lambda \in \Lambda(\hat{x})$, для которых существует подпространство $\Pi = \Pi(\lambda) \subseteq \ker F'(\hat{x})$ такое, что $\operatorname{codim} \Pi \le r$ и $\frac{\partial^2 \mathcal{L}}{\partial x^2}(\hat{x}, \lambda)[h, h] \ge 0\ \forall\, h \in \Pi$.

ТЕОРЕМА. Пусть $\hat{x}$ — анормальная точка локального минимума в задаче (1). Тогда $\Lambda_{k-1}(\hat{x}) \ne \varnothing$.

При $C = \{0\}$ теорема доказана в [2]. В [3] теорема доказана при $f'(0) = 0$, $F'(0) = 0$. Здесь задача решается с помощью методов алгебраической геометрии [1].

Работа выполнена при финансовой поддержке гранта РФФИ, проект № 04-01-00619.

Список литературы

1. Bochnak J., Coste M., Roy M. F. Real algebraic geometry // Springer: A series of modern surveys in mathematics. — 1998.

2. Арутюнов А. В., Ячимович В. К теории экстремума для анормальных задач // Вестник МГУ. Сер. 15. ВМиК. — 2000. — № 1. — С. 34–40.

3. Карамзин Д. Ю. К необходимым условиям экстремума в анормальных задачах с ограничениями типа равенств и неравенств // Сб. ВЦ РАН. — 2004. — С. 88–99.

О ГЛУБИНЕ БУЛЕВЫХ ФУНКЦИЙ НАД БЕСКОНЕЧНЫМИ БАЗИСАМИ

О. М. Касим-Заде (Москва)

Рассматривается реализация булевых функций схемами из функциональных элементов над произвольным базисом B. Под базисом понимается любое функционально полное множество булевых функций. Базис называется бесконечным, если число существенных переменных входящих в него функций не ограничено, т. е. для любого числа m найдется базисная функция, существенно зависящая не менее чем от m переменных. В противном случае базис называется конечным.

Глубиной схемы S называется наибольшее число $D(S)$ функциональных элементов этой схемы, составляющих ориентированную цепь, ведущую от входов схемы к ее выходу. Обычным образом вводится соответствующая базису B функция Шеннона глубины $D_B(n) = \max_f \min_S D(S)$, где максимум берется по всем булевым функциям f от n переменных, минимум — по всем реализующим функцию f схемам S над базисом B.

Известно, что для любого конечного базиса B функция Шеннона глубины при $n \to \infty$ имеет асимптотику вида $D_B(n) = \alpha n + o(n)$, где α — зависящая от базиса положительная постоянная [1]. В данной работе найден вид асимптотики функции Шеннона глубины для всех бесконечных базисов.

ТЕОРЕМА. Для любого бесконечного базиса B выполняется одно из соотношений: либо существует такая постоянная $\beta > 0$, что $D_B(n) = \beta$ при всех достаточно больших n, либо существуют такие постоянные $\gamma > 0$ и δ, что $\gamma \log_2 n \le D_B(n) \le \gamma \log_2 n + \delta$ при всех n.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00994), программы поддержки ведущих научных школ РФ (проект НШ-1807.2003.1), программы "Университеты России" (проект УР.04.02.528) и программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Оптимальный синтез управляющих систем").

Список литературы

1. Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. — М.: Наука, 1970. — С. 43–81.

УСТАНОВОЧНЫЕ ЭКСПЕРИМЕНТЫ ДЛЯ ЧАСТИЧНЫХ АВТОМАТОВ

А. Е. Кирнасов (Москва)

Автомат $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ с частично определёнными функциями φ и ψ называется частичным [1].

Рассмотрена задача о длине кратчайшего установочного эксперимента в классе частичных автоматов.

Пусть $\mathfrak{A} = (A, Q, B, \varphi, \psi)$ — частичный автомат. Если существует хотя бы один условный установочный эксперимент для множества состояний Q_0 автомата $\mathfrak{A}$, то длину кратчайшего такого эксперимента обозначим $l(\mathfrak{A}, Q_0)$. В противном случае положим $l(\mathfrak{A}, Q_0) = 0$. Положим $l(\mathfrak{A}, r) = \max\limits_{Q_0 \subset Q, |Q_0| = r} l(\mathfrak{A}, Q_0)$. Обозначим через K класс частичных автоматов, у которых любые два состояния отличимы. Положим $l(n, r) = \max\limits_{\mathfrak{A} \in K : |Q| = n} l(\mathfrak{A}, r)$. Остаточной степенью отличимости автомата назовем максимальную из кратчайших длин слов, остаточно отличающих пары состояний автомата.

ТЕОРЕМА 1. Если $m \geq 2$ и $k \geq 2$, то найдется константа $C > 0$ такая, что равномерно (по диаграммам переходов [2]) для почти всех частичных автоматов с m входными, k выходными символами и n состояниями остаточная степень отличимости ограничена сверху величиной $C \log_k^2 n$ при $n \to \infty$.

ТЕОРЕМА 2. Если $\frac{r(n)}{n} \to 0$ при $n \to \infty$, то

$$l(n, r) \sim C_n^r.$$

Если $\frac{r(n)}{n} < \frac{1}{2} - \varepsilon$, $0 < \varepsilon < \frac{1}{2}$, то

$$l(n, r) \asymp C_n^r.$$

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М: Наука, 1985.

2. Бардзинь Я. М. О расшифровке автоматов // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 103–114.

ДВОЙНОЕ ОТНОШЕНИЕ КАК ПРОСТОЕ

Л. М. Коганов (Москва)

Как представляется автору, по всей видимости, впервые детально рассмотрено действие симметрических групп S_4 и S_3 на буквах-символах, входящих в двойное и, соответственно, в простое отношение 4-х (соответственно 3-х) букв [1; разд. 9.5, с. 152] с целью решения при помощи элементарной абстрактной теории групп, минуя прямой перебор, следующей известной задачи: [2; гл. 11, с. 235] или [3; предл. 6.2, с. 68–69]. В работе установлена причина того известного факта, что дробно-линейные выражения, составляющие орбиту простого отношения 3-х букв при действии S_3, сами образуют группу относительно операции суперпозиции [4; пр. 1, с. 4–5], причем изоморфную S_3. То есть индуцированное действие на орбите простого отношения является точным.

ЛЕММА. Двойное отношение представимо в виде простого: $\frac{x_1 - x_3}{x_2 - x_3} : \frac{x_1 - x_4}{x_2 - x_4} = \frac{\varphi_4 - \varphi_2}{\varphi_3 - \varphi_2}$ от 3-х полиномов — алгебраических выражений: $\varphi_2 = x_1 x_2 + x_3 x_4$; $\varphi_3 = x_1 x_3 + x_2 x_4$; $\varphi_4 = x_1 x_4 + x_2 x_3$.

СЛЕДСТВИЕ. С помощью переноса действия S_4 на основных буквах x_1, x_2, x_3, x_4 на индуцированное действие S_3 на $\varphi_2, \varphi_3, \varphi_4$, путём пересечения стабилизаторов (достаточно пересечь 2 из 3-х) указанных выражений φ_i; $i = 2, 3, 4$, получается клейновская группа (Vierergruppe) V_4 как ядро гомоморфизма (эпиморфизма) $S_4 \to S_3$. Тем самым значительно проще интерпретируется естественный изоморфизм $S_4/V_4 \cong S_3$, нежели это демонстрируется, например, в [5, с. 220].

Список литературы

1. Веселов А. П., Троицкий Е. В. Лекции по аналитической геометрии. — СПб–М.–Краснодар: Лань, 2003.

2. Брус Дж., Джиблин П. Кривые и особенности. — М.: Мир, 1988.

3. Гельфанд И. М., Граев М. И., Ретах В. С. Гипер-геометрические функции над произвольным полем // Успехи математических наук. — 2004. — Т. 59, вып. 5 (359). — С. 27–100.

4. Окунев Л. Я. Основы современной алгебры. — М.: Учпедгиз, 1941.

5. Проскуряков И. В. Сборник задач по линейной алгебре (4-е изд.). — М.: Наука, 1970.

ЗАДАЧИ О ДВУХ РАНЦАХ

Д. И. Коган, А. Н. Федорин (Нижний Новгород)

Вводится система математических моделей, описывающих задачу о двух ранцах в различных постановках — с наложением и без наложения условий недробимости предметов; в предположениях зависимости или независимости весов и стоимостей предметов от ранцев, в которые они кладутся; с возможным наличием несовместимых пар предметов (если предметы Π_i и Π_j несовместимы, то в один ранец они, целиком или частично, помещены быть не могут). Показатели $K_1(X)$ и $K_2(X)$ выражают суммарную стоимость помещенных в первый и, соответственно, второй ранец предметов при реализации решения X. Рассматриваются однокритериальные задачи синтеза решений, максимизирующих: а) взвешенную сумму $K_1(X)$ и $K_2(X)$; б) минимальное из значений $\{K_1(X), K_2(X)\}$. Изучаются вопросы синтеза полных совокупностей эффективных оценок или достаточно представительных (в том либо ином смысле) подмножеств таких оценок в возникающей бикритериальной задаче с недробимыми предметами. Для задач с дробимыми предметами дополнительно рассматриваются вопросы синтеза оптимальных решений, в которых минимально возможное число предметов делится на части. Строятся решающие алгоритмы. Для задач с недробимыми предметами процедуры синтеза решений базируются на схемах ветвей и границ и динамического программирования (включая многокритериальные аналоги этих схем). Отмечается, что применение рекуррентных соотношений многокритериального динамического программирования для синтеза представительной совокупности эффективных оценок гарантирует получение искомого результата лишь в случаях, когда используемый оператор выбора представительного подножества оценок обладает вводимым в сообщении свойством консервативности. В связи с этим приводятся результаты исследования ряда операторов выбора (выделения разреженных подмножеств оценок; крайних или квазикрайних оценок; подмножеств оценок, удовлетворяющих пороговым ограничениям; оценок, получаемых линейной сверткой критериев при варьируемых параметрах свертки) на предмет обладания ими свойством консервативности. Излагаются результаты вычислительных экспериментов.

БИПОЛИГОНЫ И МУЛЬТИПОЛИГОНЫ НАД НЕКОТОРЫМИ КЛАССАМИ ПОЛУГРУПП

И. Б. Кожухов, М. Ю. Максимовский (Москва)

В алгебраической интерпретации понятие абстрактного автомата тождественно понятию *полигона над полугруппой* [1], т. е. множества X, на котором действует полугруппа S и $(xs)t = x(st)$ при $x \in X$, $s, t \in S$. Интересными обобщениями полигона являются *биполигон* и *мультиполигон*. Биполигон ${}_SX_T$ над полугруппами S и T — это множество X, на котором действует полугруппа S слева и T справа и выполняется аксиома $(sx)t = s(xt)$ (наряду с аксиомами S- и T-полигонов). *Мультиполигон* — это множество X, на котором действуют полугруппы S_i некоторого семейства полугрупп $\{S_i | i \in I\}$ и их действия перестановочны. Мультиполигоны можно интерпретировать как автоматы с несколькими входными алфавитами.

Авторами получено описание биполигонов над произвольной группой. Строение унитарного мультиполигона над семейством групп сведено к полигону над дискретным прямым произведением групп. С помощью результатов из [2] получено описание биполигонов ${}_LX_R$ и ${}_RX_L$, где L и R — полугруппы левых и правых нулей соответственно. В частности, доказана

ТЕОРЕМА. Пусть X, Q, R — непустые множества, σ_1, σ_2 — разбиения множества X, $\tau = \sup\{\sigma_1, \sigma_2\}$ и для $q \in Q$, $r \in R$ Y_q, Z_r — множества представителей классов σ_1, σ_2, т.е. $|Y_q \cap x\sigma_1| = |Z_r \cap x\sigma_2| = 1$ при всех $x \in X$. Пусть также выполнены условия: (i) для любого τ-класса K существует $a \in K$ такое, что $Z_r \cap K \subseteq a\sigma_1$ и $Y_q \cap K \subseteq a\sigma_2$; (ii) $\forall c, x, y \in X$ $(x \in Y_q \cap c\sigma_1 \,\&\, y \in Z_r \cap c\sigma_2 \Rightarrow x = y)$. Определим умножение в Q и R, полагая $qq' = q'$, $rr' = r'$, и действия Q и R на множестве X: $qx \in Y_q \cap x\sigma_1$, $xr \in Z_r \cap x\sigma_2$. Тогда Q и R — полугруппы правых нулей, а X — биполигон над Q и R. Наоборот, всякий биполигон над полугруппами правых нулей изоморфен биполигону, построенному таким способом.

Список литературы

1. Kilp M., Knauer U., Mikhalev A. V. Monoids, acts and categories. — Berlin — New York: W. de Gruyter, 2000.

2. Avdeev A. Yu., Kozhukhov I. B. Acts over completely 0-simple semigroups // Acta Cybernetica. — 2000. — V. 14. — C. 523–531.

О ПЕРИОДИЧЕСКИХ СВОЙСТВАХ ПОЛИНОМИАЛЬНОГО ГЕНЕРАТОРА НАД КОНЕЧНЫМ ЦЕПНЫМ КОЛЬЦОМ.

О. А. Козлитин (Москва)

Рассмотрим конечное цепное, вообще говоря, некоммутативное кольцо S простой характеристики p. Такие кольца с точностью до изоморфизма описаны в работе [1]. Пусть J — радикал кольца S, $\bar{S} = S/J$ — поле из q элементов, e — индекс нильпотентности идеала J, m — некоторое натуральное число.

Допустим, $a \in S$, и функция F над кольцом S сопоставляет любому набору значений своих аргументов элемент a. В этой ситуации будем отождествлять функцию F с элементом a. Полиномиальными называются функции из замыкания класса k–значных функций $\{+, \cdot\} \cup S$. Семейство всех биективных полиномиальных отображений из S^m в S^m обозначим через $B_m(S)$.

Если $a \in S^m$, $F \in B_m(S)$, обозначим через $T_F(a)$ длину цикла отображения F, на котором лежит точка a. Отображение, граф которого состоит из одного цикла, назовем транзитивным. Следуя [2], обозначим через $GL(q, m)$ полную линейную группу обратимых матриц $m \times m$ над полем из q элементов, а через $\exp(GL(q, m))$ — экспоненту этой группы.

ТЕОРЕМА. Во введенных обозначениях

1) Для любых $a \in S^m$, $F \in B_m(S)$ справедливо соотношение

$$T_F(a) \,|\, T_{\bar{F}}(\bar{a}) \cdot \exp(GL(q, m)) \cdot p^{e-1}.$$

2) Если $p < q$ и $e \geq 2$, семейство $B_m(S)$ не содержит транзитивных отображений.

Автор выражает признательность А. А. Нечаеву за постановку задачи и обсуждение полученных результатов.

Работа выполнена при поддержке гранта НШ 2358.2003.9 Президента Российской Федерации поддержки ведущих научных школ.

Список литературы

1. Нечаев А. А. Конечные кольца главных идеалов // Математический сборник. — 1973. — Т. 6. — С. 350–366.

2. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. — М.: Гелиос, 2003.

РАСПОЗНАВАНИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ДИСКРЕТНО-ГЕОМЕТРИЧЕСКОГО ПОДХОДА

В. Н. Козлов (Москва)

Работа относится к распознаванию образов и может быть интерпретирована применительно к компьютерному зрению и стереовосприятию.

Рассматривается подход к распознаванию геометрических фигур (изображений), образованных конечными множествами точек на плоскости или в пространстве. Подход существенным образом опирается на введение внутренней кодировки фигур, инвариантной к аффинным их преобразованиям.

В плоском и объемном случаях внутренний код фигур вводится так. Нумеруются точки фигуры; с учетом ее размерности рассматривается множество всех симплексов, образованных точками фигуры; для каждого симплекса вычисляется мера. Код фигуры образует множество всех троек, состоящих из двух симплексов и числа, являющегося отношением их ненулевых мер.

Для каждой из размерностей показано, что фигуры с точностью до перенумерации их точек имеют один и тот же код тогда и только тогда, когда они аффинно эквивалентны.

Сравнение (и распознавание) произвольных фигур A и B основывается на следующем. Порождаются множества A^* и B^* всех фигур, получаемых из A и B преобразованиями из некоторого класса (в общем случае аффинными). Рассматривается множество величин $r(A', B')$, где A' из A^*, B' из B^*, являющихся расстоянием между множествами A' и B' (расстояние Хаусдорфа). Показывается, что минимум на этом множестве достигается на конечном подмножестве, что и позволяет его вычислить. Этот минимум и служит мерой сходства и различия фигур.

Рассмотрено восстановление объемных фигур по их плоским проекциям (моделирование стереовосприятия).

К настоящему времени имеются две компьютерные реализации подхода: по распознаванию фигур и по стереовосприятию.

Список литературы

1. Козлов В. Н. Элементы математической теории зрительного восприятия — М.: Издательство Центра прикладных исследований при механико-математическом факультете МГУ, 2001. — 128 с.

СЛОЖНОСТНОЙ АНАЛИЗ ПРЕДСТАВЛЕНИЙ АВТОМАТОВ

В. А. Козловский (Донецк)

Рассматривается задача определения сложности распознавания свойства "быть представлением автомата" (обобщением контрольного эксперимента) [1] относительно заданного класса автоматов.

Пусть A — автомат с выходом (рассматриваются приведенные с точностью до изоморфизма автоматы в одних и тех же входном и выходном алфавитах). Частичный автомат определяет множество $F(R)$ всех таких автоматов, что R гомоморфно отображается в каждый из них, т. е. для них автомат R является фрагментом. Фрагмент R автомата A называется представлением автомата A относительно класса автоматов F ($A \in F$), если справедливо равенство $F(R) \bigcap F = \{A\}$. Задача распознавания непустоты множества $(F(R) \bigcap F) - A$ и есть задача распознавания представления. Ее сложность для тройки (R, A, F) определяется в рамках теории NP-полноты и определяется в следующие три этапа для так называемых m-плотных классов [2].

1. На множестве состояний автомата R определяются два отношения: σ, требующее отождествления состояний, и ρ, запрещающее такое отождествление при любых гомоморфизмах R в автоматы из класса F. По ним строится обыкновенный неорграф $G_R(\sigma, \rho)$ [2].

2. Для автоматов, чьи свойства подобным образом выразимы, показывается, что эффективность проверки свойства "быть представлением" определяется эффективностью проверки свойства однозначной раскрашиваемости графа $G_R(\sigma, \rho)$.

3. Доказывается, что задача раскрашиваемости такого графа либо NP-полна, либо полиномиально разрешима.

На основе предложенного подхода была доказана NP-полнота задачи распознавания представлений как ранее рассмотренных классов, так и новых.

Список литературы

1. Грунский И. С., Козловский В. А. Синтез и идентификация автоматов. — Киев: Наук. думка, 2004. — 246 с.

2. Козловский В. А., Копытова О. М. Представления автоматов относительно m-плотных классов // Материалы VIII Международного семинара «Дискретная математика и ее приложения» (2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 277–280

О МАКСИМАЛЬНЫХ НЕПОРОЖДЕННЫХ КВАДРАТАХ

Р. М. Колпаков (Москва)

Пусть $w = a_1 \dots a_n$ — конечное слово. Через $w[i..j]$ обозначается подслово $a_i \dots a_j$ слова w. Два подслова $w[i'..j']$, $w[i''..j'']$ слова w, где $i' \le i''$, называются *смежными*, если $j' \ge i'' - 1$. Натуральное число p является периодом слова w, если $a_i = a_{i+p}$ для любого $i = 1, \dots, n-p$. Мы обозначаем через $p(w)$ минимальный период слова w и через $e(w)$ отношение $\frac{|w|}{p(w)}$.

Периодичностью в слове w называется любое подслово r такое, что $e(r) \ge 2$. Частным случаем периодичности является *квадрат*, т. е. периодичность, преставимая как uu для некоторого слова u. Под периодом такого квадрата понимается длина слова u. Любое подслово периодичности r, имеющее длину $p(r)$, называется *периодическим*. Две периодичности с одинаковым минимальным периодом называются *однокоренными*, если эти периодичности имеют одинаковые периодические подслова. Периодичность $r = w[i..j]$ в слове w называется *максимальной*, если выполняются два условия: 1) $a_{i-1} \ne a_{i-1+p(r)}$ при $i > 1$; 2) $a_{j+1-p(r)} \ne a_{j+1}$ при $j < n$.

Пусть $r' = w[i'..j']$, $r'' = w[i''..j'']$, где $i' < i''$, — две смежных однокоренных максимальных периодичности с минимальным периодом p в слове w и $v = w[i..j]$ — квадрат такой, что $i' \le i < i''$ и $j' < j \le j''$. Обозначим через p_v период квадрата v. Квадрат v называется *порожденным*, если $i'' \le i + p_v \le j' + 1$. В [1] показано, что если $p_v \ge 2p$, то квадрат v является порожденным. В данной работе мы усиливаем этот результат следующим образом.

ТЕОРЕМА. Если $p_v \ge p$, то квадрат v является порожденным.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1) и программы «Университеты России» (проект УР.04.02.528).

Список литературы

1. Gasieniec L., Kolpakov R. M., Potapov I. Space efficient search for maximal repetitions // Proceedings of 4th International Conference on Combinatorics on Words. — TUCS General Publication, 2003. — № 27. — P. 269–281.

О ВОССТАНОВЛЕНИИ ПЕРЕСТАНОВОК СО ЗНАКАМИ

Е. В. Константинова (Новосибирск)

Исследуется множество перестановок со знаками $\{+,-\}$ на n элементах с реверсальной метрикой. Реверсальное расстояние между двумя перестановками со знаками определяется минимальным числом обращений интервалов перестановки, необходимое для того, чтобы перевести одну перестановку со знаками в другую. Обращением интервала называется подстановка, меняющая порядок элементов интервала и их знаки. В работе рассматривается задача восстановления неизвестной перестановки со знаками из перестановок, находящихся от данной на реверсальном расстоянии не более 1. Доказано, что для любого $n \geq 2$ любая неизвестная перестановка со знаками восстанавливается из 3 перестановок со знаками, находящихся от нее на реверсальном расстоянии не более 1. Неизвестная перестановка со знаками восстанавливается из 2 перестановок со знаками с вероятностью $p_2 \sim \frac{1}{3}$ при $n \to \infty$. Данные результаты получены на основе анализа структурных свойств графа G_n, вершинами которого являются перестановки со знаками, с реверсальной метрикой. В частности, доказывается, что G_n не содержит циклов длины три и пять и двудольных подграфов $K_{2,3}$ и описываются все его циклы длины четыре. Также показано, что для однозначного восстановления неизвестной перестановки со знаками, вообще говоря, не достаточно $n(n+1)$ перестановок со знаками, находящихся от нее на реверсальном расстоянии не более 2. Задача восстановления перестановок без знаков рассмотрена в [1].

Работа выполнена при поддержке гранта РФФИ 04–01–00122 и гранта NSF–CCR–0310832.

Список литературы

1. Константинова Е. В. Восстановление подстановок, искаженных одиночными реверсальными ошибками // Дискретные модели в теории управляющих систем. Труды VI Международной конференции (Москва, Москва, 7–11 декабря 2004 г.). — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2004. —С. 238–241.

О ПОСЛЕДОВАТЕЛЬНОМ АЛГОРИТМЕ ПОИСКА ЭКСТРЕМУМА В КЛАССАХ ФУНКЦИЙ, ОПРЕДЕЛЯЕМЫХ КУСОЧНО-СТЕПЕННЫМИ МАЖОРАНТАМИ

А. Г. Коротченко (Нижний Новгород)

Рассматриваются функции вида

$$Q(X) = \max_{j=\overline{1,m}} Q_j(X),$$

$X \in D, D = \{X \in R^n | a_i \leq x_i \leq b_i, a_i < b_i, i = \overline{1,n}\}$, где каждая функция $Q_j(X)$ такова, что для любой точки $X^0 \in D$ и любого ненулевого вектора $H \in R^n$ функция $q_j(x) = Q_j(X^0 + xH)$ принадлежит одному из функциональных классов, описанных в [1]. Здесь $x \in [a,b]$, где $a(b)$ есть минимальное (максимальное) значение x, при котором $X^0 + xH \in D$. В частности указанному требованию удовлетворяют вогнутые функции $Q_j(X)$, $X \in D$, $j = \overline{1,m}$.

Для решения задачи $Q(X) \Rightarrow \max$, $X \in D$ предлагаются стратегии, основанные на алгоритме решения задачи

$$q(x) = \max_{j=\overline{1,m}} q_j(x) \Rightarrow \max, x \in [a,b].$$

Данный алгоритм описан в [1] и основан только на вычислении значений функции $q(x)$ в некоторых точках отрезка $[a,b]$.

В сообщении рассматриваются его модификации, причем вычисления организуются таким образом, чтобы, если это возможно, при вычислении функции $q(x)$ в точке x не вычислялись значения тех функций $q_j(x)$, которые заведомо не могут реализовать значение $q(x)$.

Список литературы

1. Коротченко А. Г., Бобков А. Н. О последовательном алгоритме поиска максимума в классах многоэкстремальных функций, определяемых кусочно-степенными мажорантами // Вестник Нижегородского университета. Сер. Математика. — 2004. — Вып. 1 (2). – С. 116–125.

ОБ ОДНОМ СИМВОЛЬНОМ МЕТОДЕ ВЕРИФИКАЦИИ КРИПТОГРАФИЧЕКИХ ПРОТОКОЛОВ

А. А. Корчевский, В. А. Захаров (Москва)

Предложен новый символьный алгоритм проверки свойств целостности и конфиденциальности для некоторых классов криптографических протоколов. Проверяемые протоколы представляются в виде процессов spi-исчисления [1], в котором наряду с коммуникационными примитивами отправления и приема сообщений, а также операциями последовательной и параллельной композиции, недетерминированного выбора и репликации используются криптографические примитивы шифрования и дешифрования, цифровой подписи и др. Операционная семантика spi-исчисления определяется правилами редукции, которые задают отношение редукции $\rightarrow_*$. Два процесса P и Q считаются *тестово эквивалентными* ($P \sim Q$) [2], если для некоторого процесса T (противника) выполняется $T \parallel P \rightarrow_* \Omega \parallel P'$ и $T \parallel Q \not\rightarrow_* \Omega \parallel Q'$, где Ω — специальный сигнальный процесс. Известно [2], что задачи проверки целостности и конфиденциальности протоколов сводится к проблеме проверки тестовой эквивалентности spi-процессов. Для ее решения вводится понятие *сценария поведения противника*, взаимодействующего с заданным spi-процессом, и *отношение неотличимости* сценариев. Первый из разработанных нами алгоритмов позволяет для каждого spi-процесса P (без репликаций) построить конечное множество $E(P)$ сценариев поведения противника, взаимодействующего с процессом P.

ТЕОРЕМА. $P_0 \sim P_1$ тогда и только тогда, когда для любого сценария поведения S_i из множества $E(P_i)$, $i = 0,1$, существует сценарий поведения S_{1-i} из множества $E(P_{1-i})$, неотличимый от S_i.

Второй из разработанных нами алгоритмов позволяет для любой пары сценариев поведения противника проверить их неотличимость.

Работа выполнена при поддержке РФФИ (проект 03-01-00312).

Список литературы

1. Abadi M., Gordon A. D. A calculus for cryptographic protocols: the spi calculus // Information and Computation. — 1998. — V. 148. — P. 1–70.

2. Durante L., Sisto R., Valenzano A. Automatic testing equivalence verification of spi calculus specifications // ACM Transactions on Software Engineering and Methodology. — 2003. — V. 12. — P. 222–284.

РАЗЛИЧИЯ МЕЖДУ КЛАССОМ LIN-SPACE И РЯДОМ ДРУГИХ КЛАССОВ СЛОЖНОСТИ

Т. М. Косовская, Н. К. Косовский (Санкт-Петербург)

Пусть LIN-SPACE — класс предикатов, вычислимых на машине Тьюринга с линейной от длины записи исходных данных лентой.

ТЕОРЕМА 1 [1]. LIN-SPACE $\neq$ P.

ТЕОРЕМА 2. LIN-SPACE $\subset$ P тогда и только тогда, когда P = P-SPACE

СЛЕДСТВИЕ. Если LIN-SPACE $\subseteq$ P, то P = NP.

Пусть Δ_i^p — классы полиномиальной иерархии [1].

ТЕОРЕМА 3. Для каждого i, если $i \geq 2$, то LIN-SPACE $\neq \Delta_i^p$.

Доказательство этой теоремы основывается на следующих леммах.

Пусть Q^* — класс предикатов. Посредством $P(Q^*)$ будем обозначать класс всех предикатов, вычислимых за полиномиальное время на машине Тьюринга с оракулом из класса Q^*.

ЛЕММА 1. $P(P(Q^*)) = P(Q^*)$.

ЛЕММА 2. Для каждого положительного целого числа i $P(\Delta_{i+1}^p) = \Delta_{i+1}^p$.

СЛЕДСТВИЕ. P(PH) = PH.

ЛЕММА 3. P(LIN-SPACE) = P-SPACE.

Пусть FLIN-SPACE и FP — классы всех алгоритмов,вычислимых на машине Тьюринга на линейной зоне и за полиномиальное время соответственно.

СЛЕДСТВИЕ ТЕОРЕМЫ 3. FLIN-SPACE $\neq$ FP.

ТЕОРЕМА 4. Для каждого i LIN-SPACE $\subseteq \Delta_i^p$ тогда и только тогда, когда Δ_i^p = P-SPACE.

ТЕОРЕМА 5. LIN-SPACE $\subseteq$ PH тогда и только тогда, когда PH = P-SPACE.

ТЕОРЕМА 6. LIN-SPACE $\neq$ PH.

Список литературы

1. Du D., Ko K. Theory of computational complexity. —John Wiley & sons, Inc., 2000.

О ВЫЧИСЛЕНИИ ИНВАРИАНТОВ ПРОГРАММ

Е. В. Костылев (Москва)

При решении задач верификации программ требуется нахождение инвариантных соотношений между данными, то есть таких соотношений, которые выполняются при любых вычислениях программы, проходящих через заданные точки. Некоторые инварианты имеют вид равенств $x = t$, где x — переменная, а t — терм. Для порождения инвариантов равенства применяются методы статического анализа программ на основе абстрактных интерпретаций, в которых в качестве области абстрактных данных используются подстановки — формальные синтаксические конструкции, представляющие арифметические или логические выражения. Основная трудность состоит в том, что операция взятия точной нижней грани в решетке подстановок не удовлетворяет закону левой дистрибутивности относительно операции композиции. Поэтому данный метод нельзя эффективно применять для анализа программ с вызовами функций.

Нами предлагается другой метод вычисления инвариантов, в котором используются метаподстановки [1] — особые конструкции, обобщающие понятие подстановки. Метаподстановки представляются в виде формальных языков, что позволяет использовать теорию автоматов в алгоритмах вычисления инвариантных соотношений. Так как для множества метаподстановок выполняются оба закона дистрибутивности, этот метод может быть эффективно примененен к задаче вычисления инвариантов для программ с вызовами функций. Нами разработан новый алгоритм вычисления инвариантов равенства в программах с рекурсивными процедурами, основанный на преобразованиях метаподстановок. Отличительная особенность алгоритма состоит в том, что вычисление инвариантов проводится в два этапа — сначала внутри отдельных модулей (параллельно) и затем между модулями на основе графа вызовов функций.

Работа выполнена при поддержке гранта РФФИ 03-01-00312.

Список литературы

1. Костылев Е. В., Захаров В. А. Об одном обобщении подстановок применительно к задаче синтеза инвариантов программ // Материалы VIII Международного семинара «Дискретная математика и ее приложения»(Москва, 2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 134–137.

ОБ АДДИТИВНОЙ СЛОЖНОСТИ ПАР ВЕКТОРОВ ДЛИНЫ 2

В. В. Кочергин (Москва)

Обобщение известной задачи об аддитивных цепочках (см., например, [1]) на случай, когда вычисляется не одно число, а система векторов, в общем случае может быть сформулировано следующим образом.

Пусть $n_{ij} \in \mathbb{Z}$, $n_{ij} \geq 0$, $i = 1, ..., p$, $j = 1, ..., q$. Аддитивной цепочкой для системы векторов
$n_1 = (n_{11}, n_{12}, ..., n_{1q}), n_2 = (n_{21}, n_{22}, ..., n_{2q}), ..., n_p = (n_{p1}, n_{p2}, ..., n_{pq})$,
называется последовательность q-мерных векторов вида
$a_1 = (1, 0, ..., 0), a_2 = (0, 1, ..., 0), ..., a_q = (0, 0, ..., 1), a_{q+1}, a_2, ..., a_{q+r}$,
удовлетворяющая условиям: 1) каждый вектор a_i, $i = q + 1, ..., q + r$, представляется в виде (покомпонентной) суммы каких-либо двух (не обязательно различных) предшествующих элементов последовательности; 2) $\{n_1, n_2, ..., n_p\} \subseteq \{a_1, a_2, ..., a_{q+r}\}$. Число r называется длиной такой аддитивной цепочки векторов. Задача состоит в нахождении аддитивной сложности $L(\{n_1, n_2, ..., n_p\})$ данной системы векторов, т. е. минимальной длины аддитивной цепочки для этой системы.

Некоторые оценки аддитивной сложности (или в мультипликативной постановке — сложности вычисления систем одночленов) можно найти в [2, 3].

В данной работе исследуется случай $p = q = 2$.

ТЕОРЕМА. Пусть a_n, b_n, c_n, d_n $(n = 1, 2, ...)$ — целые неотрицательные числа, $\max\{a_n, b_n, c_n, d_n\} = a_n$, и $a_n \to \infty$ при $n \to \infty$. Тогда
$$L((a_n, b_n), (c_n, d_n)) = \log_2(a_n + |b_n c_n - a_n d_n|)(1 + o(1)).$$

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1) и программы «Университеты России» (проект УР.04.02.528).

Список литературы

1. Кнут Д. Е. Искусство программирования для ЭВМ. Т. 2 — М.: Мир — 1977.

2. Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — V. 9, № 2. — P. 230–250.

3. Кочергин В. В. О некоторых обобщениях задачи об аддитивных цепочках // Дискретная математика и ее приложения. Сборник лекций. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ, 2001. — С. 59–83.

НЕКОТОРЫЕ КОМБИНАТОРНЫЕ СВОЙСТВА МНОГОГРАННИКА ТРЕХИНДЕКСНОЙ АКСИАЛЬНОЙ ЗАДАЧИ О НАЗНАЧЕНИЯХ

В. М. Кравцов (Минск)

Исследованию r-нецелочисленных вершин (т. е. вершин, число дробных компонент у которых равно r) многогранника $M(3,n)$ трехиндексной аксиальной задачи о назначениях порядка n, $n \geq 2$, посвящен ряд публикаций (см., например, [1]).

В настоящем докладе приводятся следующие новые комбинаторные свойства многогранника $M(3,n)$:

1) диаметр многогранника $M(3,n)$ не меньше числа $3n-2$;

2) для любого числа $r \in \{2n,\ 2n+1,\ ...,\ 3n-2\}$, и только для него, у многогранника $M(3,n)$ существуют полностью r-нецелочисленные вершины, т. е. r-нецелочисленные вершины, не содержащие целых положительных компонент;

3) количество полностью $(2n)$-нецелочисленных вершин многогранника $M(3,n)$, $n \geq 3$, не меньше числа $2^{n-3}6^n(n-1)!$;

4) опровержение гипотезы из [1], согласно которой значения ненулевых элементов любой матрицы, представляющей $(3n-2)$-нецелочисленную вершину типа A многогранника $M(3,n)$, $n \geq 3$, не зависят от числа n и принадлежат множеству $\{\frac{1}{3}, \frac{2}{3}\}$;

5) у многогранника $M(3,n)$, $n \geq 6$, существует $(3n-2)$-нецелочисленная вершина, содержащая компоненту, равную $\frac{1}{n^2-5n+6}$;

6) у многогранника $M(3,n)$, $n \geq 7$, существует $(3n-2)$-нецелочисленная вершина, содержащая компоненту, равную $\frac{n^2-7n+10}{n^2-7n+12}$.

Последние два свойства опровергают высказанное в [1] предположение о том, что для любого натурального n наименьшая (наибольшая) положительная компонента среди всех $(3n-2)$-нецелочисленных вершин многогранника $M(3,n)$ равна $\frac{1}{n}$ $(\frac{n-1}{n})$.

Список литературы

1. Кравцов М. К., Кравцов В. М., Лукшин Е. В. О типах $(3n-2)$-нецелочисленных вершин многогранника трехиндексной аксиальной задачи выбора // Известия вузов. Математика. — 2002. — № 12. — С. 84–90.

ВЫЧИСЛИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ОДНОГО ПРИБЛИЖЕННОГО АЛГОРИТМА ДЛЯ ТРЕХИНДЕКСНОЙ ПЛАНАРНОЙ ПРОБЛЕМЫ ВЫБОРА

М. К. Кравцов, С. А. Дичковская (Минск)

В [1] предложен полиномиальный алгоритм α нахождения асимптотически оптимального решения трехиндексной планарной проблемы выбора (3-планарной ПВ), являющейся NP-трудной и имеющей многочисленнные применения. Постановка 3-планарной ПВ заключается в минимизации целевой функции $f(X) = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{t=1}^{n} c_{ijt}x_{ijt}$ при условиях $\sum_{i=1}^{n} x_{ijt} = 1 \quad \forall (j,t) \in N_n^2$, $\sum_{j=1}^{n} x_{ijt} = 1 \quad \forall (i,t) \in N_n^2$, $\sum_{t=1}^{n} x_{ijt} = 1 \quad \forall (i,j) \in N_n^2$, $x_{ijt} = 0$ или $1 \quad \forall (i,j,t) \in N_n \times N_n \times N_n$, где $N_n = \{1,2,\ldots,n\}$, $N_n^2 = N_n \times N_n$, $C = ||c_{ijt}||_n$ — заданная трехиндексная матрица с действительными элементами, $X = ||x_{ijt}||_n$ — исходный план 3-планарной ПВ.

Алгоритм α нахождения асимптотически оптимального решения 3-планарной ПВ программно реализован на языке Object Pascal (в среде Delphi) с использованием компьютера Pentium 4, 512 Mb RAM, ОС Win2000 и по нему проведены вычислительные эксперименты, исходная информация (матрица C) для которых формировалась с помощью датчика случайных чисел, настроенного на работу с целыми числами из отрезка $[1,r]$, где $2 \leq r \leq n$. Проверка плана X^*, построенного с помощью алгоритма α на оптимальность осуществлялась на основе утверждения: если элементы матрицы C принимают целочисленные значения из отрезка $[1,r]$, то план X 3-планарной ПВ, для которого выполняется равенство $f(X) = n^2$, является оптимальным. Всего было решено 30000 задач (по 1000 задач для каждого $n \in \{200, 250, 300, 350, 400\}$ и $r \in \{2, [\sqrt{n}], [n/4], [n/2], [3n/4], n\}$).

В результате проведенных вычислительных экспериментов установлено, что доля оптимальных решений 3-планарной ПВ порядка n, $n \geq 200$, находимых посредством алгоритма α составляет не менее 94,7% , если $r = 2$; не менее 82,8% , если $r = [\sqrt{n}]$; не менее 65,6%, если $r = [n/4]$; не менее 49,2%, если $r = [n/2]$; не менее 35,0%, если $r = [3n/4]$ и не менее 13,6%, если $r = n$, причем с ростом n их доля увеличивается.

Список литературы

1. Кравцов М. К., Крачковский А. П. О полиномиальном алгоритме нахождения асимптотически оптимального решения трехиндексной планарной проблемы выбора // Журнал вычислительной математики и математической физики. — 2001. — Т. 41, № 2. — С. 342–345.

АНТРОПОЦЕНТРИЧЕСКИЙ ГОМОМОРФИЗМ ВИЗУАЛЬНЫХ СОБЫТИЙ

О. А. Криводубский, Р. Т. Газимов (Донецк)

В работе рассматриваются принципы технической реализации механизмов запоминания визуальных событий, основанных на человеческом восприятии. Выделены процессы получения, распознавания и запоминания событий на основе введенных определений: «визуальное событие», «изображение события», «размещение изображений в памяти технических систем (ТС)» в большом и малом. Ключевой задачей работы при технической реализации механизмов запоминания, является «размещение изображений». Для ее решения предложен способ организации визуальной памяти ТС как «гиперпространства изображений», конструктивно представляющего систему координатных пространств: «проективного», «концептуального» и «относительного».

Проективное пространство представлено топологией модифицированного Гильбертова пространства и отражает положение фиксированного события в пространстве-времени. Концептуальное пространство представлено множеством подпространств (схожих по представлению с проективным) отдельных изображенных предметов, содержащих их характеристики. Относительное пространство представлено аналогично проективному и отображает характеристики пространственных отношений между отдельными изображенными предметами.

Формальное описание рассматриваемого в работе «гиперпространства изображений», осуществлено с использованием реляционной модели. При технической реализации механизмов антропоцентрического запоминания визуальных событий, предложено организовать визуальную память ТС через совокупность R-отношений как реляционную базу знаний, что позволяет создать СУБД, имеющую преимущества относительно степени детализации запросов на поиск изображений в БД. Система предусматривает формирование запросов на поиск сложных сцен: в привязке к заданным месту и времени; причем задаются не только параметры предметов сцены, но и параметры их взаимодействия в сцене. Разработанная форма представления также позволяет реализовать на ее основе алгоритмы оптимального размещения и поиска изображений в БД.

НИЖНИЕ ОЦЕНКИ ДЛЯ НЕКОТОРОГО КЛАССА ON-LINE АЛГОРИТМОВ УПАКОВКИ

Н. Н. Кузюрин, А. И. Поспелов (Москва)

В [1] рассмотрен класс шельфовых алгоритмов упаковки прямоугольников в полубесконечную полосу.

Высоты шельфов выбираются из некоторого заданного множества $\{r_n\}$, а прямоугольники упаковываются в минимальный по высоте шельф, в который они входят. При этом упаковка в шельфы заданной ширины осуществляется некоторой одномерной эвристикой упаковки в контейнеры [2]. В [1] показано, что в предположении, что для каждого прямоугольника высота h_i и ширина w_i имеют равномерное распределение на отрезке $[0, 1]$ и независимы в совокупности, то для математического ожидания Σ площади, незаполненной прямоугольниками, между основанием полосы и верхней границей самого верхнего шельфа справедлива оценка $\Sigma = O\left(N^{2/3}\log^{1/2} N\right)$.

ТЕОРЕМА. В классе шельфовых алгоритмов с $r_n = (1-\delta)^n$, где δ — параметр, $0 < \delta < 1$, с произвольной одномерной on-line эвристикой упаковки в контейнеры справедлива оценка $\Sigma = \Omega\left(N^{2/3}\right)$.

Работа выполнена при поддержке РФФИ.

Список литературы

1. Кузюрин Н. Н., Поспелов А. И. Вероятностный анализ шельфовых эвристик упаковки прямоугольников в полосу // Дискретная математика (принято к печати).

2. Baker B. S., Schwartz J. S. Shelf algorithms for two-dimensional packing problems // SIAM J. Computing. — 1983. — V. 12. — P. 508–525.

РЕГУЛЯРНЫЕ И ИНВЕРСНЫЕ РЕШЕТОЧНЫЕ МАТРИЦЫ

В. Г. Кумаров (Мурманск)

Пусть $(P, \leq)$ — решетка с операцией взятия верхней грани $\vee$ и операцией взятия нижней грани $\wedge$; $\overline{a}$ — дополнение к $a \in P$, если оно существует; $P^{m\times n}$ — множество всех $m \times n$ матриц с элементами из P; A^t — матрица, транспонированная к A, $\bar{A} = ||\bar{a}_{ij}||$. Введем на множестве $P^{m\times n}$ частичный порядок $\leq$: $A \leq B$ равносильно тому, что $a_{ij} \leq b_{ij}$ для всех i, j. Определим произведение решеточных матриц $A \in P^{m\times k}$, $B \in P^{k\times n}$: $AB = || \vee_{r=1}^{k} (a_{ir} \wedge b_{rj})||_{m\times n}$.

Если для заданных элементов $a, b \in P$ в множестве решений неравенства $a \wedge x \leq b$ существует наибольший элемент, то он называется относительным псевдодополнением элемента a в b и обозначается $b : a$. Решетка $(P, \leq)$, в которой для любых $a, b \in P$ существует $b : a$, называется брауэровой [1]. Любая дистрибутивная решетка с дополнениями является брауэровой решеткой, в которой $b : a = b \vee \bar{a}$.

ТЕОРЕМА. Пусть $(P, \leq)$ — дистрибутивная решетка с дополнениями, $A \in P^{m\times k}$, $B \in P^{l\times n}$, $C \in P^{m\times n}$. Уравнение $AXB = C$ разрешимо тогда и только тогда, когда ему удовлетворяет матрица $\overline{A^t \cdot \overline{C} \cdot B^t}$. Матрица $\overline{A^t \cdot \overline{C} \cdot B^t}$ является наибольшей среди всех решеточных матриц X, таких что $AXB \leq C$.

СЛЕДСТВИЕ 1. Пусть $(P, \leq)$ — дистрибутивная решетка с дополнениями, $A \in P^{n\times n}$. Матрица A регулярна тогда и только тогда, когда $A \cdot \overline{A^t \cdot \overline{A} \cdot A^t} \cdot A = A$.

Для $P = \{\widetilde{0}, \widetilde{1}\}$ следствие 1 доказано в работе [2].

СЛЕДСТВИЕ 2. Пусть $(P, \leq)$ — дистрибутивная решетка с дополнениями, $A \in P^{n\times n}$. Если матрица A регулярна, то среди всех инверсных к ней матриц существует наибольшая, равная

$$\overline{A^t \cdot \overline{A} \cdot A^t} \cdot A \cdot \overline{A^t \cdot \overline{A} \cdot A^t}.$$

Список литературы

1. Биркгоф Г. Теория решеток. — М.: Наука, 1984.

3. Schein B. M. Regular elements of the semigroup of all binary relations // Semigroup Forum, 13. — 1976.

ПЕРИОДИЧЕСКИЕ ФУНКЦИИ НА МНОЖЕСТВЕ СЛОВ

В. Л. Куракин (Москва)

Пусть X — конечное, M — произвольное множества, X^* — множество слов в алфавите X, $l(\bar{x})$ — длина слова $\bar{x}$. Зададим действие полугруппы X^* на множестве функций $u\colon X^* \to M$. Левым и правым сдвигами функции u на слово $\bar{y} \in X^*$ назовем функции $\bar{y}u, u\bar{y}\colon X^* \to M$, определяемые соотношениями

$$\bar{y}u(\bar{x}) = u(\bar{x}\bar{y}),\ u\bar{y}(\bar{x}) = u(\bar{y}\bar{x}),\ \bar{x} \in X^*.$$

Функцию $u\colon X^* \to M$ назовем периодичной слева (справа), если множество ее левых (правых) сдвигов конечно.

Отметим, что функции u можно сопоставить функцию $\widehat{u}\colon X^* \to M^*$, действующую по правилу

$$\widehat{u}(x_1x_2\dots x_n) = u(x_1)u(x_1x_2)\dots u(x_1x_2\dots x_n).$$

Тогда $\widehat{u}$ — детерминированная функция и $\widehat{u\bar{y}}$ — ее остаточная функция, так что u периодична справа тогда и только тогда, когда $\widehat{u}$ — ограниченно детерминированная функция.

ТЕОРЕМА. Произвольная функция $u\colon X^* \to M$ периодична слева тогда и только тогда, когда она периодична справа.

Введенные понятия возникают при изучении регистров сдвига на некоммутативной полугруппе.

АЛГОРИТМЫ РАСПРЕДЕЛЕНИЯ ПОТОКА ОБЪЕКТОВ ДЛЯ ОБСЛУЖИВАНИЯ В СИСТЕМЕ ИДЕНТИЧНЫХ ПРОЦЕССОРОВ

А. В. Куранов (Нижний Новгород)

Рассматривается модель однофазного обслуживания детерминированного потока Z объектов $\{z_1, z_2, \ldots, z_n\}$ в системе Ξ идентичных процессоров $\{P_1, P_2, \ldots, P_m\}$. Каждый объект z_i потока подлежит обслуживанию без прерываний одним из процессоров системы Ξ и характеризуется следующими параметрами: моментом t_i поступления в систему, требуемой продолжительностью обслуживания τ_i и функцией штрафа $\varphi_i(t)$ от момента завершения обслуживания объекта. Считаем, что $t_1 \leq t_2 \leq \ldots \leq t_n$. Обслуживание объектов каждым процессором производится в порядке возрастания их индексов.

Расписание обслуживания объектов ρ определяется как набор $(p_1, p_2, \ldots, p_n)$, где $p_i \in \{1, 2, \ldots, m\}$ — индекс процессора, обслуживающего объект z_i. По расписанию обслуживания однозначно определяются моменты начала и завершения обслуживания каждого объекта. Если $\overline{t}_i$ — момент завершения обслуживания объекта z_i, то штраф по этому объекту есть $\varphi_i(\overline{t}_i)$.

В рамках рассматриваемой модели изучаются задачи синтеза расписаний обслуживания, минимизирующих 1) суммарный штраф по всем объектам потока и 2) максимальное из значений индивидуальных штрафов. Так как число допустимых расписаний обслуживания оценивается велечиной m^n, то поиск оптимального расписания путем полного перебора зачастую неприемлем на практике в силу ограниченности времени, выделяемого на решение задач подобного рода в оперативной обстановке.

Предлагаются алгоритмы синтеза оптимальных расписаний для задач 1 и 2 на основе соотношений динамического программирования. Вводится понятие ситуации в момент принятия решения и функции минимального штрафа для ситуации. Относительно данной функции записываются соотношения динамического программирования, позволяющие вычислять ее значения. При принятии ограничений, зачастую выполняющихся на практике, предлагаемые алгоритмы имеют полиномиальную вычислительную сложность.

В докладе приводятся результаты вычислительных экспериментов и оценки сложности предлагаемых алгоритмов.

Т-НЕПРИВОДИМЫЕ РАСШИРЕНИЯ ДЛЯ ОРИЕНТИРОВАННЫХ ГРАФОВ

С. Г. Курносова (Саратов)

Известны две оптимальные конструкции расширений для неориентированных графов: минимальные расширения (P. Hayes [1]) и T-неприводимые расширения (В. Н. Салий [2]). В настоящем сообщении одна из этих конструкций — T-неприводимое расширение — обобщается на ориентированные графы. Описываются все T-неприводимые расширения для ориентированной цепи.

Тривиальным расширением ориентированного графа G называется граф, полученный из G добавлением вершины v и соединением ее входящими и исходящими дугами с каждой вершиной графа G. Под T-неприводимыми расширениями для ориентированного графа G понимают графы, полученные из тривиального расширения графа G удалением максимального числа дуг, не нарушающим свойство расширения.

Ориентированной цепью называют граф $\overrightarrow{P}_n = (V, \alpha)$, где $V = \{v_1, ..., v_n\}$, $\alpha = \{(v_i, v_{i+1}) | i = \overline{1, n-1}\}$.

ТЕОРЕМА (о T-неприводимых расширениях для ориентированной цепи). Ориентированная цепь $\overrightarrow{P}_n$ имеет точно два неизоморфных T-неприводимых расширения: $H_1 = (V \bigcup \{v\}, \alpha \bigcup \alpha_1)$ и $H_2 = (V \bigcup \{v\}, \alpha \bigcup \alpha_2^n)$, где $\alpha_1 = \{(v, v_1), (v_n, v)\}$, $\alpha_2^2 = \{(v_1, v), (v, v_2)\}$, $\alpha_2^3 = \{(v_1, v), (v_2, v), (v, v_3)\}$, $\alpha_2^4 = \{(v_1, v), (v_2, v), (v, v_3), (v, v_4)\}$, а при $n > 4$ $\alpha_2^n = \{(v_1, v), (v_2, v), (v, v_{n-1}), (v, v_n)\} \bigcup \{(v, v_i), (v_i, v) | i = \overline{3, n-2}\}$.

Список литературы

1. Hayes P. A graph model for fault-tolerant computing system // IEEE Trans. Comput. — 1976. — V. C-25, № 9. — P. 875–884.

2. Салий В. Н. Доказательства с нулевым разглашением в задачах о расширениях графов // Вестник Томского гос. ун-та. Приложение 6. — Сентябрь, 2003. — С. 63–65.

О РАЗРЕШИМОСТИ ОБРАТИМОСТИ ДЛЯ ОДНОРОДНЫХ СТРУКТУР

И. В. Кучеренко (Москва)

К основным задачам теории однородных структур (ОС) относится задача о связи локальных свойств ОС, то есть свойств шаблона соседства и локальной функции переходов, и ее глобального поведения [1]. Примером такой задачи является распознавание обратимости однородной структуры [2]. В работе [3] установлено, что в общей постановке она является алгоритмически неразрешимой.

Автором было исследовано расслоение задачи распознавания обратимости за счет рассмотрения некоторых подклассов класса всех однородных структур. Пусть $S_1(k,V)$ — множество всех k-мерных ОС с шаблоном соседства V; $S_2(n)$ — множество двухмерных однородных структур с n состояниями ячейки и шаблоном соседства в виде прямоугольника $\{(v_1,v_2) \in \mathbf{Z}^2 \setminus \{0\} || v_2| < l, |v_2| < 2\}$, где $l \in \mathbf{N}$; $S_3(n)$ — множество двухмерных ОС с n состояниями ячейки и шаблоном соседства вида $\{(0,1),(1,0),(2,0),\ldots,(l,0)\}$, где $l \in \mathbf{N}$. Для этих классов были доказаны следующие утверждения.

ТЕОРЕМА 1. Для однородных структур из $S_1(k,V)$ свойство обратимости разрешимо тогда и только тогда, когда ранг системы векторов, образующих V, равен единице.

ТЕОРЕМА 2. При $n > 1$ для ОС из $S_2(n)$ свойство обратимости алгоритмически неразрешимо.

ТЕОРЕМА 3. Существует n_0, $n_0 \leq 1248^6$, такое, что при $n \geq n_0$ для ОС из $S_3(n)$ свойство обратимости алгоритмически неразрешимо.

Работа выполнена при финансовой поддержке РФФИ (проект 02–01–00162).

Список литературы

1. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

2. Кучеренко И. В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы (в печати).

3. Kari J. Reversibility of $2D$ cellular automata is undecidable // Physica D. — 1990. — V. 45. — P. 379–385.

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ ТРЕМЯ СТЕКАМИ В ПАМЯТИ ОДНОГО УРОВНЯ

А. А. Лазутина, А. В. Соколов (Петрозаводск)

Пусть в памяти объема m единиц мы должны работать с тремя стеками [1] и известны вероятности включения и исключения элементов в стеки в каждый момент дискретного времени. Рассматривается два способа представления трех стеков в памяти одного уровня.

Первый способ — связанное представление [1, 2], где для хранения одного элемента стека нужно два элемента памяти, так как один элемент тратится под данные и один — на связь. В качестве математической модели в этом случае предложено блуждание по целочисленной решетке внутри пирамиды в трехмерном пространстве.

Во втором способе представления трех стеков [3] один из стеков начинает расти из точки k навстречу одновременно двум другим. Нужно решить какой стек расположить по центру, и каким должно быть k, чтобы среднее время до завершения работы было максимальным. Для решения задачи строится математическая модель в виде случайного блуждания по целочисленной решетке в четырехмерном пространстве.

Предложены алгоритмы нумерации состояний процессов, доказаны теоремы, которые определяют вид матриц переходных вероятностей соответствующих поглощающих цепей Маркова [4, 5], разработаны алгоритмы решения задач, приводятся результаты численных экспериментов, где изложенные методы представления стеков сравниваются со способом, в котором два стека растут навстречу друг другу, а третий расположен отдельно [3].

Список литературы

1. Кнут Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы. — М.: Вильямс, 2001.

2. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. — МЦНМО, 2001.

3. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М: Наука, 1970.

4. Соколов А. В. Математические модели и алгоритмы оптимального управления динамическими структурами данных. — Петрозаводск, 2002.

5. Феллер В. Введение в теорию вероятностей и ее приложения. — М: Мир, 1964.

О ДИНАМИЧЕСКИХ БАЗАХ ДАННЫХ С КОНСТАНТНОЙ В СРЕДНЕМ СЛОЖНОСТЬЮ ПОИСКА И ВСТАВКИ

И. С. Лапшов (Москва)

В работе рассматриваются динамические базы данных, представленные в виде информационных графов (см. [1]) вместе с набором процедур, реализующих основные операции (такие как поиск элемента и вставка элемента в базу данных). Введено понятие сложности этих операций (в худшем случае и в среднем).

Записями базы данных являются элементы некоторого множества X. В частности, в качестве этого множества может выступать множество натуральных чисел или множество действительных чисел, расположенных на отрезке $[0, 1]$.

Предметом исследования являются базы данных, предназначенные для поиска идентичных объектов (поиска по ключу), в которых основными операциями являются операция поиска записи и операция вставки записи. В случае поиска записи запрос к базе данных представляет собой элемент множества X, а результатом поиска является ответ "да", если такая запись содержится в базе, или "нет" в противном случае. Результатом вставки записи $x \in X$ является добавление x к множеству записей базы данных.

Рассматривается модель с двумя взаимодействующими вычислителями (процессорами), в которой один вычислитель выполняет основные операции, а второй занимается постоянной перестройкой (оптимизацией) базы данных.

ТЕОРЕМА. В рамках рассматриваемой модели с двумя взаимодействующими вычислителями существует структура базы данных, в которой средняя сложность операций поиска и вставки записи не превышает константу.

Автор выражает благодарность Э. Э. Гасанову за постановку задачи и помощь в работе. Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 05-01-00709).

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

КОДЫ, ПРЕДОТВРАЩАЮЩИЕ КОНФЛИКТЫ ПРИ МНОГИХ АКТИВНЫХ ПОЛЬЗОВАТЕЛЯХ

В. И. Левенштейн (Москва)

Рассматривается комбинаторная задача, связанная с передачей по каналам множественного доступа [1]. Требуется построить код, состоящий из максимального числа $M = M(n, w)$ двоичных векторов длины n с w единицами и $n - w$ нулями, $M \geq w$, такой, что каждая матрица размера $w \times n$, составленная из любых циклических сдвигов w его различных векторов содержит перестановочную матрицу порядка w в качестве минора. Предполагается следующая схема передачи информации. Каждому из M пользователей ставится в соответствие кодовый вектор, который периодически повторяется. Единицы в этой последовательности указывают моменты, когда этот пользователь делает попытки передать пакет информации по каналу. Моменты синхронизированы, но каждый пользователь может начать попытки в любой момент. Если в каждый момент времени активны не более w пользователей, то указанное свойство обеспечивает возможность по крайней мере одной передачи в течение n последовательных моментов каждым из них без коллизии с другими активными пользователями. Эта задача при $w = 3$ рассмотрена в [2].

ТЕОРЕМА. Для любого простого p ($p \geq 3$) и любого целого r ($r \geq 2$) имеет место $M(n.w) \geq \frac{n-1}{2(w-1)}$, когда $n = p^r$ и $w = \frac{p+1}{2}$.

Построение использует точки проективной геометрии $PG(r - 1, p)$, как и в случае совершенных кодов, исправляющих сдвиги единиц [3]. Имеется предположение, что построенные коды максимальны, которое в настоящее время доказано при любом $r \geq 2$ для $p = 3, 5, 7$.

Работа выполнена при поддержке гранта РФФИ 04–01–00122 и гранта NSF 0310632.

Список литературы

1. Цыбаков Б. С, Рубинов А. Р. Некоторые конструкции кодов, избегающих конфликтов // Проблемы передачи информации. — 2002. — Т. 38, № 4. — С. 268–279.

2. Левенштейн В. И., Тончев В. Об оптимальных кодах, предотвращающих конфликты // Дискретные модели в теории управляющих систем. Труды VI Межд. конф. — М.: Изд. отдел ф-та ВМиК МГУ, 2004. — С. 242–246.

3. Levenshtein V. I., Vinck A. J. H. Perfect (d, k)-codes capable of correcting single peak shifts //IEEE Trans. Inform. Theory. — 1993. — V. 39, №. 2 . — P. 656–662.

ОБ АЛГОРИТМИЧЕСКОЙ КЛАССИФИКАЦИИ ЧИСЕЛ

Л. П. Лисовик, Т. А. Карнаух (Киев)

Среди множества всех определимых действительных чисел, кроме вычислимых чисел, можно выделить и другие подклассы:

— Z-числа — числа, двоичная запись которых вычислима машиной Тьюринга (генератором), выходная лента которой функционирует по принципу магазина.

— D-числа — числа, являющиеся значениями производных (при условии существования) в нуле вычислимых действительных функций (вычислимая функция понимается в смысле теории R-преобразователей [1]: машина Тьюринга последовательно перерабатывает входное двоичное представление, при этом результат, быть может с использованием символов переполнения, записывается на выходную ленту, функционирующую по принципу нестирающего магазина).

ТЕОРЕМА 1. Множества Z-чисел и D-чисел совпадают.

Ограничения на структуру рабочей ленты существенно влияют на возможности задания вычислимых чисел. С помощью генераторов с магазинной или конечной памятью можно задать в точности множество рациональных чисел [2], использование гнездовой стековой памяти позволяет задавать трансцендентные числа [3]. В случае Z-чисел аналогия частична.

ТЕОРЕМА 2. Множество Z-чисел, задаваемых генераторами с конечной памятью, в точности есть множество рациональных чисел.

ТЕОРЕМА 3. Множество Z-чисел, задаваемых генераторами с одним счетчиком, в точности есть множество всех Z-чисел.

Список литературы

1. Лисовик Л. П. Логические свойства частично непрерывных функций // Тр. Ин-та математики СО АН СССР. — Математическая логика и алгоритмические проблемы. — Новосибирск: Наука, 1989. — Т. 12. — С. 39–72.

2. Лисовик Л. П., Шкаравская О. Ю. Функции, определяемые преобразователями с магазинной памятью // Докл. НАН Украины. — 1995. — № 2. — С. 82–93.

3. Карнаух Т. О. Обчислюваність трансцендентних чисел генераторами з гніздовою стековою пам'яттю // Вісник Київського університету. Серія: фіз.-мат. науки. — 2003. — № 3. — С. 216–220.

О СООТНОШЕНИИ МЕЖДУ СЛОЖНОСТЬЮ И ПЛОЩАДЬЮ КЛЕТОЧНЫХ ДЕШИФРАТОРОВ

С. А. Ложкин (Москва)

Рассматривается модель клеточных схем из функциональных и коммутационных элементов (КСФЭ), вложенных в плоские прямоугольные решетки [1–3]. Исследуются соотношения между сложностью $L(S)$ КСФЭ S и площадью $A(S)$ занимаемой ею решетки. В [1] установлен порядок вида 2^n для функции Шеннона $A(n)$, связанной с площадью схемы. При этом в [2] обнаружено, что для «типичной» функции алгебры логики ФАЛ $f(x_1, \ldots, x_n)$ площадь любой реализующей ее КСФЭ S_f такой, что $L(S_f)$ по порядку не больше $\frac{2^n}{n}$, растет существенно быстрее, чем 2^n. В настоящей работе аналогичное явление «антагонизма» устанавливается для дешифратора порядка n, площадь которого асимптотически равна $n2^{n-1}$ (см. [3]). В работе доказано, что площадь $A(S_n)$ любой КСФЭ S_n, реализующей дешифратор Q_n порядка n и такой, что $L(S_n)$ по порядку не больше, чем 2^n, имеет порядок роста не меньше, чем $2^{(3n)/2}$, причем указанные оценки достигаются на некоторой последовательности КСФЭ S_n.

Работы выполнена при поддержке гранта РФФИ 05–01–01000.

Список литературы

1. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. Вып. 19. — 1967. — С. 274–284.

2. Albrecht A. Zur Kompliziertheit der Realisierung Boolescher Functionen F-V-Schemata // EIK 15. — 1979. — P. 159–171.

3. Ложкин С. А., Пашковский А. М. О сложности реализации некоторых систем функций алгебры логики клеточными и планарными схемами // Проблемы теоретической кибернетики. Тезисы докладов IX Всесоюзной конференции (1990). Часть I. — 1991. — С. 28.

МОДЕЛИРОВАНИЕ ФУНКЦИОНАЛЬНО-ПЕРЕКЛЮЧАТЕЛЬНЫХ СХЕМ СРЕДСТВАМИ ЛОГИЧЕСКОГО ПРОГРАММИРОВАНИЯ

А. Е. Люлькин (Минск)

В докладе предлагается предикатное описание функционально-переключательных КМОП-структур, содержащих как функциональные элементы, так и фрагменты, представленные на переключательном уровне (уровень транзисторов). Полученное описание позволяет выполнить логическое моделирование схемы с учетом задержек элементов на основе логического вывода.

Моделирование транзисторных структур выполняется в семизначном алфавите, позволяющем учесть емкостные свойства КМОП-схем. Это значительно повышает точность моделирования и делает возможным его применение для решения задач анализа неисправностей (типичные неисправности в КМОП-схемах можно проверить с использованием емкостных сигналов). При моделировании функциональных элементов в целях повышения быстродействия используется троичный алфавит.

Для представления функциональных элементов строятся предикаты, описывающие функции многозначной логики, реализуемые элементами.

Кроме функциональных элементов, функционально-переключательные КМОП-структуры содержат транзисторы n- и p-типа, играющие роль ключей с прямым и инверсным упралением, соответственно. Для моделирования транзисторов предлагаются предикаты, описывающие функционирование транзисторов в выбранном алфавите. Для выполнения моделирования схемы в целом строятся также различные вспомогательные предикаты: для перехода от семизначного алфавита к троичному, для описания результата объединения нескольких сигналов в узле схемы и др.

В заключение приводятся примеры описания конкретных схем множествами предикатов и их реализация с помощью системы логического программирования Visual Prolog.

ЗАДАЧИ И РЕАЛИЗАЦИЯ ЛИНГВИСТИЧЕСКОГО АНАЛИЗА В ПОИСКОВОЙ СИСТЕМЕ MEDSEARCH

И. В. Люстиг (Москва)

Поисковая система MEDSEARCH разрабатывается для получения справочной информации о лекарственных препаратах из их описаний в электронном виде. Система ориентирована на запросы следующих типов: общие сведения о лекарственном препарате (ЛекП); перечень ЛекП для лечения заболевания; побочные эффекты от ЛекП; характер побочных эффектов с учетом особенностей пациента. Использование поиска по ключевым словам не дает приемлемого результата. Для интеллектуализации поиска осуществляется семантико-синтаксический анализ документов. Для этого используется лингвистическая база данных, включающая лексико-семантический словарь и совокупность семантико-синтаксических шаблонов конструкций естественного языка (ЕЯ). Методологической основой для построения этих шаблонов является теория K-языков, предложенная В. А. Фомичевым. Эта теория описывает математическую модель, задающую такие 10 операций на концептуальных структурах, с помощью которых можно строить семантические представления предложений и сколь угодно сложных связных текстов на ЕЯ, в том числе текстов по медицине. Для ответа на запросы достаточно использовать семантико-синтаксические модели смысловых отношений между словами. В формальных конструкциях смысловых отношений фигурируют лишь ядерные понятия или слова — слова, наличие которых обязательно для реализации отношения и между ними нет слов-отрицаний. При ответе на некоторые запросы используется база знаний о медицине для определения сопутствующих недугу явления.

Список литературы

1. Люстиг И. В., Фомичев В. А. Принципы формального отображения семантики лексических единиц, предложений и дискурсов в интеллектуальной поисковой системе MEDSEARCH // Компьютерная лингвистика и интеллектуальные технологии: Тр. междунар. конференции Диалог'2004 («Верхневолжский», 2–7 июня 2004 г.). — М.: Наука. — 2004. — С. 431–435.

2. Fomichov V. A. A mathematical model for describing structured items of conceptual level // Informatica. — V. 20, № 1. — P. 5–32.

АЛГОРИТМИЧЕСКАЯ НЕРАЗРЕШИМОСТЬ АВТОМАТНЫХ УРАВНЕНИЙ С ТРЕМЯ НЕИЗВЕСТНЫМИ

И. В. Лялин (Москва)

Пусть S — автоматная схема, в которой автоматы X, Y, Z и $A_1, \ldots, A_n$ как-то связаны друг с другом при помощи операций суперпозиции и обратной связи. Пусть вместо автоматов X, Y и Z можно подставлять любые другие автоматы с тем же числом входов и выходов, при этом автоматная схема будет реализовывать различные автоматы. Если при этом требуется чтобы схема реализовала некий автомат h, то возникает уравнение $S(X,Y,Z) = h$. Данное уравнение называется автоматным уравнением с тремя неизвестными (X, Y и Z), его решениями являются такие тройки автоматов, при подстановке которых вместо X, Y и Z схема S реализует автомат h.

Ранее [1] был найден способ решения автоматных уравнений с одной неизвестной. Возникает вопрос решения автоматных уравнений с большим количеством неизвестных. Следующая теорема в некотором смысле дает ответ на этот вопрос.

ТЕОРЕМА. Задача о нахождении решения автоматного уравнения с тремя неизвестными алгоритмически неразрешима.

То есть не существует алгоритма, который для любого автоматного уравнения вычисляет, имеет ли оно решение или нет.

Из данной теоремы следует что автоматные уравнения с количеством неизвестных больше чем три также неразрешимы. Таким образом, неисследованным остается только случай двух переменных.

Список литературы

1. Petrenko A., Yevtushenko N. Solving asynchronous equations. Formal description techniques // Protocol specification, testing and verification. — Kluwer Academic Publishers, 1998. — P. 125–140.

ДЕФРАГМЕНТАЦИЯ МАТРИЦ ПЕРЕСТАНОВОК С СОХРАНЕНИЕМ НАБОРОВ ЭЛЕМЕНТОВ В ЛИНИЯХ

А. М. Магомедов (Махачкала)

Алгоритмы дефрагментации матриц востребованы в задачах сжатия информации, улучшения размещения информации на дисках, оптимизации расписаний.

ОПРЕДЕЛЕНИЯ. Элемент $M[i,j]$ матрицы M будем называть дефектом, если $M[i,j] = 0, \exists v,w, v < j < w : M[i,v] \neq 0, M[i,w] \neq 0$. Под k-дефрагментацией матрицы будем понимать приведение ее к матрице с k дефектами с сохранением наборов элементов в каждой линии.

ОБОЗНАЧЕНИЯ. Далее: n, m, L — заданные целые положительные числа, $L > n$; $[n,m]$-матрица M — матрица $L \times m$, содержащая в каждом столбце перестановку элементов $1, ..., n$ и $L-n$ нулей; $\Sigma(i)$ — множество номеров строк матрицы M, каждая из которых содержит в точности i ненулевых элементов, $\sigma(i)$ — мощность множества $\Sigma(i)$; $\alpha(i,j)$ — количество вхождений числа i в строку с номером j.

РЕЗУЛЬТАТЫ. 1. Для матрицы $sign(M)$ доказана NP-полнота задачи 0-дефрагментации, разработан псевдополиномиальный алгоритм решения (известно, что задача проверки возможности сплошного расположения единиц в строках (0-1)-матрицы путем перестановки столбцов допускает решение за полиномиальное время).

2. С привлечением потоковых методов получены необходимые и достаточные условия 0-дефрагментации при $m = 3, 4, 5$ (за исключением случаев $\sigma(1) \neq 0$) и $m = 6$ (за исключением случаев $\sigma(1) \neq 0$, $\sigma(3) \neq 0$); рассмотрены частные случаи при $m > 6$. При $m = 4$, например, для 0-дефрагментации $[n,m]$-матрицы M необходимо и достаточно существование допустимого потока в следующей сети с заданными двухсторонними потоковыми ограничениями для дуг:

3. С использованием теоремы о факторизации графа, установлено, что при четном m разреженная $[n,m]$-матрица M (матрица, где $\sigma(i) = 0$ при $i > 2$) всегда допускает 0-дефрагментацию. Получены модификации теоремы о факторизации, позволившие исследовать задачи k-дефрагментации ($k = 0, 1$) разреженных матриц при нечетных m.

ОЦЕНКИ КОММУНИКАЦИОННОЙ СЛОЖНОСТИ PIR-ПРОТОКОЛОВ С МАЛЫМИ СЛУЧАЙНЫМИ ЧИСЛАМИ

Г. А. Майлыбаева (Москва)

Протоколы извлечения информации без раскрытия запроса, PIR-протоколы, позволяют пользователю получить один бит из базы данных, копия которой хранится на k несообщающихся серверах таким образом, что администраторы базы данных не узнают номер запрашиваемого бита. Предполагаем, что пользователь может генерировать случайные числа для вычисления запросов к серверам. Если k — это количество серверов, n — количество бит в базе данных x, s — максимальное значение генератора случайных чисел, m — количество бит в запросе пользователя, p — суммарное количество бит в ответах серверов, то (k,n,s,m,p)-*PIR-протоколом* называется набор из $k+2$ функций $I = \langle Q, A^1, \ldots, A^k, R\rangle$, где Q — функция, которую использует пользователь для построения запросов, $A^j, j \in \{1,\ldots,k\}$ — функция, которую использует сервер S_j для построения ответов, R — реконструирующая функция, которую использует пользователь для вычисления значения искомого бита. В этих терминах, коммуникационная сложность протокола определена как число $C(I) = km + p$. Получена точная оценка коммуникационной сложности для класса PIR-протоколов при $k = 2$, малых значениях параметра s и ограничениях, наложенных на класс возможных функций ответов. Обозначим через $\mathcal{I}(k,n,s)$ класс всех (k,n,s,m,p)-PIR-протоколов, где $m \geq 0, p > 0$. Пусть $\mathcal{A} \subseteq \mathcal{I}(k,n,s)$. Положим $C(k,n,s,\mathcal{A}) = \min\{C(I) : I \in \mathcal{A}\}$.

ТЕОРЕМА. Если множество $\mathcal{A} \subseteq \mathcal{I}(2,n,s)$, $s < \sqrt{n}$, такое, что для любого протокола $I \in \mathcal{A}$ функция ответов имеет вид

$$A(j,x,q^j) = \begin{cases} (x_{i_1^1} \oplus x_{i_1^2}, \ldots, x_{i_{l_1}^1} \oplus x_{i_{l_1}^2}), & \text{если } j = 1 \\ (x_{i_1}, \ldots, x_{i_{l_2}}), & \text{если } j = 2 \end{cases},$$

где $x = (x_1,\ldots,x_n)$ — база данных, q^j — запрос к серверу j, $i_r^1 = i_r^1(q^1), i_r^2 = i_r^2(q^1) \in \{1,\ldots,n\}$, $r \in \{1,\ldots,l_1\}$, $i_t = i_t(q^2) \in \{1,\ldots,n\}$, $t \in \{1,\ldots,l_2\}$, $l_1 + l_2 = p$, то справедливо равенство

$$C(2,n,s,\mathcal{A}) =]\tfrac{s+1}{2s}n[.$$

Автор выражает благодарность Э. Э. Гасанову за постановку задачи.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 05-01-00709).

РАСШИРЕННЫЙ БАЗИСНЫЙ КОНЕЧНЫЙ АВТОМАТ ДЛЯ ЗАДАННОГО РЕГУЛЯРНОГО ЯЗЫКА

Б. Ф. Мельников (Тольятти)

Расширенные (обобщённые) конечные автоматы определяются согласно [1]; но, в отличие от [1], мы специально сужаем описательные возможности данного класса автоматов — дуги, не являющиеся циклами, помечены буквами (а не регулярными языками). Базисные конечные автоматы и некоторые другие обозначения определяются согласно [2] (см. также другие ссылки, имеющиеся в той статье).

Определим расширенный базисный конечный автомат для заданного регулярного языка L — недетерминированный конечный автомат $BE(L)$, который строится согласно следующему определению. Пусть $\binom{A}{X}$ — некоторое состояние автомата $BA(L)$ [2]. Определим функцию переходов-циклов расширенного автомата $\zeta_{BE(L)} : Q_{BE(L)} \to \mathcal{P}(\Sigma^*)$ таким образом. Пусть $K = (Q,\Sigma,\delta,S,F)$ — произвольный недетерминированный конечный автомат, определяющий L, а $q \in Q$ — некоторое его состояние, такое что $f_K^{in}(q) \ni A$ и $f_K^{out}(q) \ni X$. Пусть также $u \in \mathcal{L}_K^{io}(q)$; тогда мы также полагаем, что $u \in \zeta_{BE(L)}\binom{A}{X}$. Ничто иное не является словом языка $\zeta_{BE(L)}\binom{A}{X}$.

ТЕОРЕМА. $\mathcal{L}(BE(L)) = L$.

Возможности применения данного класса автоматов — следующие: для более удобного описания специальных алгоритмов эквивалентного преобразования обычных конечных автоматов; для описания практических алгоритмов реального времени проблем минимизации автоматов; а также для упрощения некоторых доказательств.

Часть работ по данной теме, связанная с построением алгоритмов реального времени, выполняется при финансовой поддержке РФФИ (проект 04-01-00863).

Список литературы

1. Han Y.-S., Wood D. The generalization of generalized automata: expression automata // The 9th international conference on implementation and application of automata. — Canada, London, 2004. — P. 114–122.

2. Melnikov B., Sciarini-Guryanova N. Possible edges of a finite automaton defining a given regular language // The Korean journal of computational and applied mathematics. — 2002. — V. 9, №. 2. — P. 475–485.

СУЩЕСТВОВАНИЕ ПУТЕВЫХ ЯДЕР И РАЗБИЕНИЙ В НЕОРИЕНТИРОВАННЫХ ГРАФАХ

Л. С. Мельников, И. В. Петренко (Новосибирск)

Пусть $\tau(G)$ — количество вершин в наиболее длинном пути неориентированного графа G. Подмножество K множества вершин V графа G называется P_n-ядром графа G, если $\tau(G[K]) \leq n-1$ и каждая вершина из множества $V(G \setminus K)$ смежна с вершиной, которая является конечной вершиной для пути длины n в графе G. Для пары натуральных чисел a, b таких, что $a+b = \tau(G)$, разбиение $\{A, B\}$ множества $V(G)$ называется (a,b)-*разбиением*, если $\tau(G[A]) \leq a$ и $\tau(G[B]) \leq b$. Если в графе G имеется (a,b)-разбиение для любой пары чисел (a,b) такой, что $a+b = \tau(G)$, то граф G называется τ-разбиваемым. Наличие P_n–ядра в графе G означает, что G является $(\tau(G)-n+1, n-1)$-разбиваемым. Высказываются гипотезы (например, в [1]) о том, что произвольный граф является τ-разбиваемым. Решения этой проблемы в общем виде не получено.

В [2] доказано существование P_8-ядра в произволном неориентированном графе. Взаимосвязь существования путевых ядер и длин циклов продемонстрирована в [3], где доказано, что если G — неориентированный связный граф с длиной наибольшего цикла $c(G) = m$, тогда в графе G имеется P_{m+2}-ядро. Данный результат позволяет обобщить выводы о τ-разбиваемости графов, в которых $\tau(G) \leq 2c(G) + 3$.

Авторами доказано существование P_9-ядра в произвольном неориентированном графе G, из чего следует τ-разбиваемость графа G с $\tau(G) \leq 17$.

Работа авторов поддержана грантами РФФИ (коды проектов 02-01-00039 и 02-01-01153).

Список литературы

1. Dunbar J. E., Frick M. Path kernels and partitions // J. Combin. Math. Combin. Comput. — 1999. — V. 31. — P. 137–149.

2. Мельников Л. С., Петренко И. В. Путевые ядра и разбиения в неориентированных графах // Дискретный анализ и исследование операций. Сер. 1. — 2002. — Т. 9, № 2. — С. 21–35.

3. Мельников Л. С., Петренко И. В. Путевые ядра и длины циклов в неориентированных графах // Современные проблемы конструирования программ. Сб. Института систем информатики им. А. П. Ершова. — Новосибирск, 2002. — С. 222–231.

О СУЩЕСТВОВАНИИ ГУСЕНИЧНЫХ ФАКТОРИЗАЦИЙ

О. В. Мироненко (Кировоград)

Под T-факторизацией полного графа K_n понимается разложение этого графа на подграфы, каждый из которых изоморфен дереву T порядка n. Задача Л. Байнеке состоит в выделении класса T деревьев, для которых существуют T-факторизации. Необходимыми для существования T-факторизации порядка n являются условия $n = 2k$, k натуральное, и $\Delta(T) \leq k$. Количество компонент в T-факторизации порядка $n = 2k$ равно k.

Мы решаем задачу Л. Байнеке для класса гусениц. Под гусеницей G_n порядка n здесь понимается дерево порядка n, у которого, кроме концевых вершин, есть только вершины степени 3, причем подграф, индуцированный множеством неконцевых вершин, является цепью. Легко понять, что в гусенице порядка n имеется ровно $t = (n-2)/2$ вершин степени 3. Для гусеничной факторизации порядка n обозначим $s(x)$ количество компонент, в которых вершина x основного графа имеет степень 3.

ЛЕММА. $s(x) \geq (n-2)/4$ для некоторой вершины x.

ТЕОРЕМА 1. Если $n = 2k, k = 2m, m \in N$, то G_n-факторизаций не существует.

Доказательство. Предположим противное — в условиях теоремы существует G_n-факторизация. Рассмотрим вершину x основного графа. Она является вершиной степени 3 в $3s(x)$ компонентах и концевой вершиной в остальных $k - s(x)$ компонентах, а всего в вершине x сходятся $2k-1$ ребер. Следовательно, $3s(x)+k-s(x) = 2k-1$, откуда $2s(x) = k-1$, то есть число k нечетно. Это противоречит условию $k = 2m$ теоремы.

ТЕОРЕМА 2. Если $n = 2k, k = 2m-1, m \in N$, то G_n-факторизации существуют.

Доказательство. Дерево G_n в этом случае является полусимметричным [1]. Для него легко строится базовая компонента полувращательной G_n-факторизации [1] и сама эта факторизация, чем теорема доказана.

Список литературы

1. Петренюк А. Я. Півобертові деревні факторизації повних графів // Український математичний журнал. — 2001. — Т. 53, № 5. — С. 710–716.

О СВЯЗНОСТИ ГРАФОВ, ГИПЕРГРАФОВ И МАТРОИДОВ

А. В. Митропольский (Санкт-Петербург)

С появлением гиперграфов (естественного обобщения графов) встал вопрос о перенесении основных понятий теории графов на новые структуры. Обобщение понятия связности было сделано двумя способами. Первый способ является перенесением на гиперграфы понятия связности матроидов (описанного, например, в [1]). Такой подход получил широкое распространение, особенно за границей. Существуют также обобщения понятия n-связности на матроиды, а следовательно и на гиперграфы [2–4]. Второй способ (названный структурная связность) был сформулирован в [5] и применялся для синтеза многорежимных систем со структурныи управлением. Он также был обобщен на матроиды.

В данной работе установлено соответствие между указанными способами определения связности на уровне гиперграфов и на уровне матроидов.

Также в работе введено понятие структурной n-связности и исследована ее взаимосвязь с соответствующими понятиями n-связности матроидов.

Работа выполнена при финансовой поддержке РФФИ — ГФЕН КИТАЯ 2004 (проект 04-01-39002ГФЕН2004а).

Список литературы

1. Айгнер М. Комбинаторная теория. — М., 1982. — 556 с.

2. Cunningham W. H. On Matroid Connectivity // Journal of Combinatorial Theory. Series B. — 1981. — V. 30. — P. 94–99.

3. Oxley J. G. On a matroid generalization of graph connectivity // Math. Proc. Camb. Phil. Soc. — 1981). — V. 90. — P. 207–214.

4. Tutte W. T. Connectivity in matroids // Canad. J. Math. — 1966. — V. 18. — P. 1301–1324

5. Сушков Ю. А. Связность в гиперграфах и матроидах // Исследование операций и статистическое моделирование. — 1994. — Вып. 6. — С. 111–138.

СЛОВА ШТУРМА И МНОГООБРАЗИЯ ЛИНЕЙНЫХ АЛГЕБР

С. П. Мищенко (Ульяновск)

Одной из важных числовых характеристик при исследовании тождественных соотношений линейной алгебры A является экспонента $EXP(A)$ соответствующего многообразия (см., например, [1]). Известно, что для классических классов алгебр, например, ассоциативных или лиевских, $EXP(A) = 1$ или $EXP(A) \geq 2$.

Рассмотрим бесконечное слово $w = w_1 w_2 \cdots$ в алфавите $\{0, 1\}$. Функция, задаваемая числом различных подслов слова w длины n, называется сложностью слова. По определению, слова Штурма имеют сложность равную $n+1$. Пусть $\pi(w)$ предел отношения числа единиц в начальном подслове к его длине. Для рационального $0 < \alpha < 1$ можно построить периодическое слово, а для иррационального существует слово Штурма w [2] такое, что $\pi(w) = \alpha$. Зафиксируем натуральное m и определим последовательность чисел k_i, причем $k_i = m$, если $w_i = 0$ и $k_i = m+1$, если $w_i = 1$. Обозначим через $A(m, w)$ линейную алгебру с базисом $\{a, b\} \cup Z_1 \cup Z_2 \cup \ldots$, где $Z_i = \{z_j^{(i)} \mid 1 \leq j \leq k_i\}$, $i = 1, 2, \ldots$, и таблицей умножения $z_1^{(i)} a = z_2^{(i)}$, $\ldots$, $z_{k_i-1}^{(i)} a = z_{k_i}^{(i)}$, $i = 1, 2 \ldots$, $z_{k_i}^{(i)} b = z_1^{(i+1)}$, $i = 1, 2, \ldots$, причем, не определенные произведения равны 0.

Для формулировки результата нам понадобиться непрерывная монотонно возрастающая функция $\Phi(x) = \frac{1}{x^x (1-x)^{1-x}}$, которая полуинтервал $(0; \frac{1}{2}]$ отображает на полуинтервал $(1; 2]$.

ТЕОРЕМА. Пусть w бесконечное периодическое или слово Штурма, причем $\pi(w) = \alpha$, $0 < \alpha < 1$. Если $m \geq 2$, то $EXP(A(m, w)) = \Phi(\beta)$, где $\beta = \frac{1}{m+\alpha}$.

Работа выполнена при финансовой поддержке РФФИ (проект 04-01-00739-а).

Список литературы

1. Мищенко С. П. Рост многообразий алгебр Ли // УМН. — 1990. —Т. 45. — № 6 (276). — С. 25–45.

2. Lothaire M. Algebraic combinatorics on words // Encyclopedia of Mathematics and Its Applications. Vol. 90. — Cambridge: Cambridge University Press, 2002.

О НЕОБХОДИМЫХ УСЛОВИЯХ ОПТИМАЛЬНОСТИ ДЛЯ НЕЛИНЕЙНЫХ СИСТЕМ С ИНТЕГРАЛЬНЫМИ УСЛОВИЯМИ

Г. Г. Моллаи (Баку)

Рассматривается задача минимизации функционала

$$J(u) = \sum_{i=0}^{N} \varphi\left(x(t_i)\right), \tag{1}$$

при ограничениях

$$\dot{x} = f(t,x,u), \;\; t \in [t_0,T], \;\; \int_{t_0}^{T} n(t)x(t)dt = A, \tag{2}$$

$$u = u(\cdot) \in U = \{u(t) \in L_2^r[t_0,T] : u(t) \in V \subset R^r, \text{ п.в. } t \in [t_0,T]\}. \tag{3}$$

Здесь $t_0 \le t_1 < t_2 < \cdots < t_N \le T$ — фиксированные моменты времени, $x \in R^n$ — фазовая переменная, $u \in R^r$ — управления; $((n(t)-n)\times n)$-мерная матрица-функция, $n(t) \in L_\infty^{n\times n}[t_0,T]$, $\widetilde{n}(t) = \int_0^t n(\tau)d\tau$, $\det \widetilde{n}(T) \neq 0$.

В работе при некоторых условиях на данные задачи доказана

ТЕОРЕМА. Пусть в задаче (1)–(3) допустимый процесс (x^*,u^*) является оптимальным. Тогда

$$\int_{t_0}^{T} \left\langle \bigtriangledown_u H\left(t,x(t,u^*),u^*,u^*(t),\psi(t,u^*)\right), u(t)-u^*(t)\right\rangle dt \le 0$$

при всех $u \in U$. Если u^* — внутренняя точка U, то

$$\bigtriangledown_u H\left(t,x(t,u^*),u^*,u^*(t),\psi(t,u^*)\right) = 0, \; t_0 \le t \le T.$$

Здесь $\psi(t,u^*)$ — решение сопряженной системы, соответствующее управлению $u^* \in U$:

$$\psi(t) = -\int_{t_0}^{t} \bigtriangledown_x H\left(\tau,x...\right) d\tau + \left(\widetilde{n}^{-1}(T)\widetilde{n}(t)\right)' \int_{t_0}^{T} \bigtriangledown_x H\left(\tau,x...\right) d\tau +$$

$$+ \sum_{i=1}^{N} \left[E\chi\left(t-t_i\right) - \left(\widetilde{n}(T)\widetilde{n}(t)\right)' \bigtriangledown \varphi\left(x(t_i)\right)\right],$$

где E — $(n\times n)$-мерная единичная матрица, $H(t,x,...) = \left\langle \psi(t), f(t,x,u)\right\rangle$, $\chi\left(t\right)$ — функция Хевисайда.

Доказательство проводится с помощью метода из [1] (см. с. 524).

Список литературы

1. Васильев Ф. П. Методы оптимизации — М.: Факториал, 2002.

О РАСПОЗНАВАНИИ ЯЗЫКОВ ПРОИЗВОЛЬНЫХ СЛОВ КОНЕЧНЫМИ ПОЛУГРУППАМИ

В. А. Молчанов, Т. П. Молчанова (Саратов)

В работе [1] доказано, что при изучении распознаваемых конечными автоматами языков естественно возникает задача исследования языков произвольных слов, содержащих как конечные, так и бесконечные в любую сторону слова. В этом случае класс распознаваемых автоматами языков совпадает с классом так называемых обобщенно рациональных языков, которые определяются рациональными выражениями с помощью четырех специальных операций (объединение, тернарное произведение и бесконечная итерация).

В настоящей работе с помощью методов нестандартного анализа [2] разрабатывается естественный подход к теории языков произвольных слов, распознаваемых конечными полугруппами. Показано, как любое отображение φ алфавита A в произвольную конечную полугруппу S можно канонически продолжить на множество $W(A)$ всех слов над этим алфавитом. Реализация такого продолжения приводит к каноническому расширению исходной полугруппы S до четырехсортной алгебры $\overline{S}$, элементами которой интерпретируются все слова над алфавитом A. Этот результат позволяет естественно ввести понятие языка произвольных слов, распознаваемого конечными полугруппами и доказать следующий принципиально важный факт.

ТЕОРЕМА. Любой обобщенно рациональный язык $L \subset W(A)$ распознается конечными полугруппами.

Полученные результаты позволяют описать класс всех языков произвольных слов, распознаваемых конечными полугруппами.

Работа выполнена при поддержке INTAS, грант № 99–1224.

Список литературы

1. Molchanov V. A. Nonstandard approach to general rational languages // Contributions to General Algebra. — 2001. — V. 13. — P. 233–244.

2. Альбеверио С., Фенстад Й., Хеэг-Крон Р., Линдстрем Т. Нестандартные методы в стохастическом анализе и математической физике. — М.: Мир, 1990.

О ТОЖДЕСТВЕННЫХ ПРЕОБРАЗОВАНИЯХ В НЕКОТОРЫХ КЛАССАХ ФОРМУЛ

Д. Г. Мотин (Москва)

Тождественные преобразования формул, порожденных конечным набором булевых функций, играют важную роль в приложениях и, прежде всего, в синтезе процессоров. Одной из проблем является вопрос существования конечной полной системы тождеств, осуществляющей эти преобразования. В работе [1] указано, в частности, что такая система существует для всех классов формул, порожденных базисом, состоящим из одной ассоциативной и коммутативной функции k-значной логики от двух переменных.

Кроме того, в случае наличия конечной полной системы тождеств очень важной проблемой является сложность рассматриваемых тождественных преобразований. Автором был исследован этот вопрос для некоторых частных классов формул k-значной логики.

ТЕОРЕМА. Пусть функция $L^I_Б(n)$ характеризует сложность перевода произвольных равных формул меры не более n над некоторым множеством $Б$ друг в друга с помощью конечной полной системы тождеств I, а $x \circ y$ — некоторая квазисущественная функция k-значной логики от двух переменных, коммутативная, ассоциативная и такая, что из равенства формул $(f(x) \circ g(y)) = (m(x) \circ n(y))$ следуют равенства $f(x) = m(x)$ и $g(y) = n(y)$ ($f(x), g(y), m(x), n(y)$ — формулы над $\{x \circ y\}$), а из равенства $(f(x) \circ g(y)) = m(x)$ — равенства $f(x) = m(x)$ и $(x \circ g(y)) = x$. Если $Б = \{x \circ y\}$, тогда для любой полной для $Б$ системы тождеств I при $n \to \infty$ функция $L^I_Б(n)$ имеет порядок роста, равный $n \log n$.

Работа выполнена при финансовой поддержке РФФИ (проект 02–01–00162).

Список литературы

1. Перкинс П. Базисы для эквациональных теорий полугрупп // Кибернетический сборник. Вып 11 (н. с.). — М.: Мир, 1974. — С. 5–23.

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

ЖАДНЫЙ АЛГОРИТМ ПОСТРОЕНИЯ ЧАСТИЧНЫХ ПОКРЫТИЙ

М. Мошков, М. Пилищук, Б. Зелёско (Сосновец, Польша)

Рассмотрим непустое конечное множество A и такое семейство $S = \{B_1, \ldots, B_m\}$ его подмножеств, что $\bigcup_{i=1}^m B_i = A$. Пусть α такое действительное число, что $0 \le \alpha < 1$. Подсемейство $\{B_{i_1}, \ldots, B_{i_t}\}$ семейства S назовем частичным покрытием множества A с ошибкой α если $\left|\bigcup_{j=1}^t B_{i_j}\right| \ge (1-\alpha)\,|A|$. Число t назовем мощностью этого частичного покрытия. Через $C^\alpha_{\min}$ обозначим минимальную мощность частичного покрытия с ошибкой α.

Рассмотрим жадный алгоритм построения частичного покрытия с ошибкой α. Найдем в S подмножество B_{j_1} максимальной мощности и добавим его к строящемуся покрытию. Если число покрытых элементов множества A не меньше чем $(1-\alpha)\,|A|$, то алгоритм прекращает работу. В противном случае находим в S новое подмножество B_{j_2}, которое покрывает максимальное число непокрытых элементов, и добавляем его к строящемуся покрытию, и т. д.

Обозначим через C^α_{greedy} мощность частичного покрытия с ошибкой α, построенного рассмотренным жадным алгоритмом.

ТЕОРЕМА. Пусть $0 < \beta \le \alpha < 1$. Тогда

$$C^\alpha_{\text{greedy}} \le C^{\alpha-\beta}_{\min} \ln\left(\frac{1-\alpha+\beta}{\beta}\right) + 1.$$

Полученная оценка используется в исследованиях частичных тестов и частичных решающих правил для таблиц решений.

ИЕРАРХИЯ КЛАССОВ СЛОЖНОСТИ, ЯВЛЯЮЩИХСЯ РАСШИРЕНИЕМ РЕГУЛЯРНЫХ ЯЗЫКОВ

Р. Г. Мубаракзянов (Казань)

Настоящая работа является обзором исследований, посвященным сложности различных моделей, вычисляющих булевы функции. Известно, что класс функций, вычислимых конечными детерминированными автоматами, или класс регулярных языков, не расширяется при рассмотрении конечных недетерминированных автоматов, а также при рассмотрении конечных вероятностных автоматов с изолированной точкой сечения. При расширении класса вычислительных моделей, соответствующие классы сложности могут различаться [1]. Вычисления конечными автоматами являются вычислениями бинарными программами очень специального вида, а именно упорядоченными программами константной ширины, читающими переменные в естественном порядке. Нами рассматриваются вычислительные модели, получаемые как расширение класса автоматов путем последовательного снятия ограничений на бинарные программы [2].

Исследуются детерминированные, недетерминированные, вероятностные без ошибки, вероятностные с ограничением на ошибку и без ограничения на ошибку бинарные программы. При фиксировании класса вычислительных моделей показаны соотношения между соответствующими класса сложности [1, 3]. Кроме того, доказано собственное включение одних классов сложности в другие при переходе к более широким классам вычислительных моделей.

Работа выполнена при поддержке гранта РФФИ (проект 03-01-00769).

Список литературы

1. Ablayev F., Karpinski M., Mubarakzjanov R. On BPP versus $NP \cup coNP$ for ordered read-once branching programs // Theoretical Computer Science. — 2001. — V. 264. — P. 127–137.

2. Мубаракзянов Р. Г. О классах сложности, определяемых бинарными программами ограниченной ширины // Дискретный анализ и исследование операций. Серия 1. — 2000. — Т. 7, вып. 5. — С. 67–78.

3. Мубаракзянов Р. Г. Детерминированные и вероятностные без ошибки упорядоченные один раз читающие бинарные программы равномощны // Дискретный анализ и исследование операций. Серия 1. — 2004. — Т. 11, вып. 2. — С. 80–90.

О СЛОЖНОСТИ СЛЕПОЙ ИДЕНТИФИКАЦИИ ОБЪЕКТОВ

А. С. Нагорный (Москва)

Графом Z^n ($n \geq 1$) назовем бесконечный граф, вершинами которого являются упорядоченные наборы из n целых чисел, а дуга между двумя такими вершинами проводится тогда и только тогда, когда соответствующие наборы являются соседними. Пусть $G = (V, E)$ — подграф графа Z^n, индуцированный произвольным конечным множеством V вершин графа Z^n. Обозначим через m число компонент связности в графе G ($m \geq 1$), p_i — число вершин в i-й компоненте связности ($i = 1, 2, \ldots, m$), p — число вершин во всем графе G, т. е. $p = |V|$. Далее рассмотрим s объектов [1], $1 \leq s \leq p$.

Задача слепой идентификации s объектов состоит в следующем. Пусть известно значение n ($n \geq 1$), а также количество объектов s ($1 \leq s \leq p$), расположенных в вершинах графа G. Ни граф G, ни позиции объектов не известны. Требуется, используя команды move(b,j,d), описанные в [1], определить (с точностью до сдвига) структуру каждой компоненты связности графа G, а также выяснить текущие координаты всех s объектов в некоторый момент времени. Сложность задачи идентификации — наименьшее количество команд move в худшем случае.

Обозначим через s_i количество объектов, находящихся на i-й компоненте связности графа G, $i = 1, 2, \ldots, m$. Граница dG графа G — множество всех вершин v графа Z^n таких, что v не является вершиной графа G, но v смежна (в Z^n) хотя бы с одной вершиной G.

ТЕОРЕМА. Если для каждого $i = 1, 2, \ldots, m$ выполняется условие $1 \leq s_i \leq p_i - 1$, то задача слепой идентификации s объектов на графе G разрешима, причем ее сложность L удовлетворяет следующему двойному неравенству $p + r - m \leq L \leq 2p + l_s r + s^2 + (2n+1)s - 3$, где $r = |dG|$, $l_s = 1$ при $s = 1$ и $l_s = 2s + 1$ при $s \geq 2$.

Работа выполнена при поддержке РФФИ (проект 03-01-00783).

Список литературы

1. Нагорный А. С. О сложности задачи идентификации объектов, передвигающихся по k-значному n-мерному кубу // Синтез и сложность управляющих систем. Материалы XIII международной школы-семинара (Пенза, 14–20 октября 2002 г.). Часть II. — М.: Изд-во центра прикладных исследований при механико-математическом факультете МГУ, 2002. — С. 172–176.

ВЕСОВОЙ СПЕКТР ОДНОГО ПОДКОДА КОДА $RM(3,n)$

М. С. Никифоров, А. В. Покровский (Москва)

ОПРЕДЕЛЕНИЕ. Обозначим через K множество булевых функций от n переменных степени не выше третьей такое, что любая кубичная функция из K содержит один фиксированный моном третьей степени.

Несложно видеть, что K — подкод кода Рида — Маллера третьего порядка, обозначаемого $RM(3,n)$.

ТЕОРЕМА. Весовой спектр кода K при $n \geq 6$ равен:

вес функции	количество функций
$2^{n-1}-2^{n-1-k}$	$O_{f_{1,2}}(k)\cdot s_1$
$2^{n-1}-3\cdot 2^{n-3-k}$	$O_{f_{1,2}}(k)(s_2+s_1)$
$2^{n-1}-2^{n-2-k}$	$O_{f_{1,2}}(k)(s_3+s_2)+O_{f_3}(k)\cdot s'_1$
$2^{n-1}-2^{n-3-k}$	$O_{f_{1,2}}(k)(s_4+s_3)+O_{f_3}(k)\cdot s'_2$
$2^{n-1}-2^{n-4-k}$	$O_{f_{1,2}}(k)\cdot s_5+O_{f_3}(k)\cdot s'_3$
2^{n-1}	$2\cdot O_{f_{1,2}}(k)s_4+O_{f_3}(k)\cdot s'_4$
$2^{n-1}+2^{n-4-k}$	$O_{f_{1,2}}(k)\cdot s_5+O_{f_3}(k)\cdot s'_3$
$2^{n-1}+2^{n-3-k}$	$O_{f_{1,2}}(k)(s_3+s_4)+O_{f_3}(k)\cdot s'_2$
$2^{n-1}+2^{n-2-k}$	$O_{f_{1,2}}(k)(s_2+s_3)+O_{f_3}(k)\cdot s'_1$
$2^{n-1}+3\cdot 2^{n-3-k}$	$O_{f_{1,2}}(k)(s_1+s_2)$
$2^{n-1}+2^{n-1-k}$	$O_{f_{1,2}}(k)\cdot s_1$

где $k=\overline{0,\lfloor\frac{n-3}{2}\rfloor}$, $s_1=2^{6k}$, $s_2=7\cdot 2^{6k}$, $s_3=21\cdot 2^{6k}+112\cdot 2^{6k}(2^{n-3-2k}-1)$, $s_4=35\cdot 2^{6k}+336\cdot 2^{6k}(2^{n-3-2k}-1)+448\cdot 2^{6k}(2^{n-3-2k}-1)(2^{n-3-2k}-2)$, $s_5=128\cdot 2^{6k}(2^{n-3-2k}-1)(2^{n-3-2k}-2)(2^{n-3-2k}-4)$, $s'_1=56\cdot 2^{6k}$, $s'_2=672\cdot 2^{6k}(2^{n-3-2k}-2)+224\cdot 2^{6k}$, $s'_3=448\cdot 2^{6k}(2^{n-3-2k}-2)(2^{n-3-2k}-4)$, $s'_4=128(2^{3(n-3)}-7\cdot 2^{2k+2(n-3)}+21\cdot 2^{4k+n-3}-21\cdot 2^{6k})+1344\cdot 2^{6k}(2^{n-3-2k}-2)+336\cdot 2^{6k}$, $O_{f_{1,2}}(0)=1$, $O_{f_3}(0)=2^{n-2}-2$, при $k>0$ $O_{f_3}(k)$ — мощность орбиты, на которой лежит функция $f_3(x_1,\ldots,x_{n-3})=x_1x_2\oplus\ldots\oplus x_{2k-1}x_{2k}\oplus x_{2k+1}$ относительно действия аффинной группы на аргументы квадратичных форм от $n-3$ переменных,

$$O_{f_{1,2}}(k)=2^{k(k+1)}\frac{(2^{n-3}-1)(2^{n-4}-1)\ldots(2^{n-2k-2}-1)}{(2^{2k}-1)(2^{2k-2}-1)\ldots(2^2-1)}.$$

Список литературы

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

ГЕНЕРАТОРЫ КОНЦЕПТОВ В ПРОБЛЕМЕ РАСПОЗНАВАНИЯ ОБРАЗОВ

В. Е. Новиков (Саратов)

В работах немецких математиков Р. Вилле, Б. Гантера и др. построена теория формального концептуального анализа [1]. Настоящая работа посвящена продолжению исследования [2] взаимосвязи между концептуальным анализом, теорией отношений и проблемой распознавания образов с целью описания общего принципа выбора класса решающих правил в концептуальном анализе.

Пусть $\rho \subseteq M_1\times\cdots\times M_n$ — n-арное отношение. Обозначим $\bar{n} := (1,2,\ldots,n)$ и $\bar{i}_k := (i_1,i_2,\ldots,i_k)$, $x_{\bar{i}_k} := (x_{i_1},x_{i_2},\ldots,x_{i_k})$, $M_{\bar{i}_k} := M_{i_1}\times M_{i_2}\times\cdots\times M_{i_k}$ для произвольных $1\leq i_1<\ldots<i_k\leq n$. Будем говорить, что k-система $x_{\bar{i}_k}$ *входит в отношение* ρ, если существует n-система $x_{\bar{n}}$, для которой $x_{i_1},x_{i_2},\ldots,x_{i_k}$ являются её соответствующими компонентами. Для $\bar{i}_s,\bar{j}_k\subseteq\bar{n}$, $a_{\bar{i}_s}\in M_{\bar{i}_s}$, $X\subseteq M_{\bar{i}_s}$ обозначим: $\pi_{\bar{j}_k}(\rho) := \{y_{\bar{j}_k}\in M_{\bar{j}_k} \mid y_{\bar{j}_k}$ входит в $\rho\}$; $\sigma_{\{a_{\bar{i}_s}\}}(\rho) := \{x_{\bar{n}}\in\rho \mid a_{\bar{i}_s}$ входит в $x_{\bar{n}}\}$; $\rho_{\bar{j}_k}\langle x_{\bar{i}_s}\rangle := \pi_{\bar{j}_k}(\sigma_{\{x_{\bar{i}_s}\}}(\rho))$;

$$\widehat{\rho}_{\bar{j}_k}(X) := \cap\{\rho_{\bar{j}_k}\langle x_{\bar{i}_s}\rangle : x_{\bar{i}_s}\in X\};\quad \widehat{\rho}_{\bar{i}_s\bar{j}_k}(X) := \widehat{\rho}_{\bar{i}_s}(\widehat{\rho}_{\bar{j}_k}(X)).$$

Если $X=\widehat{\rho}_{\bar{i}_s\bar{j}_k}(X)$ и $\widehat{\rho}_{\bar{i}_s}(Y)=X$ для $Y\subseteq M_{\bar{j}_k}$, то X называется *$\bar{i}_s$-концептом по $\bar{j}_k$* и Y — *$\bar{j}_k$-генератором $\bar{i}_s$-концепта X*.

ТЕОРЕМА. Функция $R(Y)=|\widehat{\rho}_{\bar{i}_s}(Y)|$ $(Y\subseteq M_{\bar{j}_k})$ обладает следующими свойствами:

1) R постоянна на множестве немаксимальных $\bar{j}_k$-генераторов одного и того же $\bar{i}_s$-концепта;

2) Если Y максимальный $\bar{j}_k$-генератор $\bar{i}_s$-концепта X, то для любого $Y'\supset Y$ выполняется $R(Y')<R(Y)$.

Таким образом, приближение функции R ступенчатыми функциями устанавливает общий принцип выбора класса решающих правил в концептуальном анализе.

Список литературы

[1] Wille R. Introduction to formal concept analysis // Technische Hochschule Darmstadt. — Oktober, 1996.

[2] Новиков В. Е. Определения понятий на n-арных отношениях. — Саратов, 2004. — Деп. в ВИНИТИ 17.02.04, № 266-В2004.

СТРУКТУРНЫЕ АВТОМАТНЫЕ МОДЕЛИ ГЕНЕРАТОРОВ МАРКОВСКИХ ФУНКЦИЙ

Ш. Р. Нурутдинов (Казань)

Процессы, порождаемые автономными вероятностными автоматами (АВА) с выходом можно рассматривать как функции конечных однородных цепей Маркова (марковские функции (МФ)). Опишем один из таких типов АВА [1].

ТЕОРЕМА. Последовательность состояний случайного процесса, описываемого МФ $\{Z_t\}$, представима последовательностью значений функции $\psi_2 = f_2 \cdot f_1$ — суперпозиции двух полиномов над полем $GF(2^n)$, где n зависит от размерности автоматных алфавитов.

ОПРЕДЕЛЕНИЕ 1. Автономным вероятностным автоматом типа A_2 будем называть систему $A_2 = ((A_1), Z, \mu(z/y))$.

ОПРЕДЕЛЕНИЕ 2. Автономным вероятностным автоматом типа A_1 будем называть систему $A_1 = (S, P, Y, \lambda(s), \pi_0)$,
где $Y = \{y_1, y_2, \ldots, y_k\}$ — конечный выходной алфавит, $\lambda(s) : S \to Y$ — функция выхода, отображающая S на Y, Z — тот же математический объект, что и в A_2, $\mu(z/y)$ — вероятностная функция, задаваемая аналогично функции $\mu(z/s)$ стохастической матрицей $P_{(z/y)}$ размера $k \times d$, где элемент p_{ij}, $i = \overline{1,k}$, $j = \overline{j=1,d}$ определяет вероятность появления буквы z_j на выходе при условии, что на выходе автомата A_2 появилась буква y_i.

Процесс $\{Z'_t\}$ зададим в соответствии с определением автомата A_2 [2]. Поэтому полиномиальную модель марковской функции вида $\{Z'_t\}$ можно определить на основе теоремы. При этом необходимо учитывать, что разложение стохастической матрицы $P_{(z/y)}$ размера $k \times d$ имеет вид $\sum_{i=1}^{l_2} p_i M(u'_i)$, где $l_2 \le k \cdot d - k + 1$.

СЛЕДСТВИЕ. Последовательность состояний процесса $\{Z'_t\}$, заданного автоматом A_2, разбиением на множестве S и функцией $\mu(z/y)$, можно представить последовательностью значений функции $\Psi_3 = f_3 \cdot f_2 \cdot f_1$ — суперпозиции трех полиномов: f_1, f_3 и f_2.

Работа выполнена при финансовой поддержке РФФИ (проект 03-01-00769).

Список литературы

1. Нурутдинов Ш. Р. Моделирование цепей Маркова в полях Галуа // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 136–147.

2. Zacharov V. M., Kuznetsov S. E. Complexity of the problem of approximation of stochastic matrix by rational elements // FCT'87. — Berlin: Springer-Verlag, 1987. — V. 278. — P. 483–487.

О ЧИСЛЕ НЕЗАВИСИМЫХ МНОЖЕСТВ В «ПОВРЕЖДЕННЫХ» ГРАФАХ КЭЛИ

К. Г. Омельянов (Москва)

Обозначим через $I(\Gamma)$ семейство независимых множеств графа Γ. Для любых действительных чисел p и q обозначим через $[p,q]$ множество натуральных чисел x таких, что $p \le x \le q$. Обозначим через $\sigma(G)$ наибольшую из степеней вершин графа G. Класс графов $G = (V, E)$, таких, что $|V| = n$, $|E| = m$ и $\sigma(G) \le 2$, обозначим через $\mathcal{G}_2(n,m)$. Графом Кэли, порожденным множеством A, назовем граф $\Gamma_A(V)$ на множестве натуральных чисел V, такой, что пара чисел $(u,v) \in V \times V$ является ребром тогда и только тогда, когда $|u-v| \in A$ или $u+v \in A$. Рассматриваемые в данной работе графы Кэли возникли при вычислении констант в асимптотиках из гипотезы Камерона — Эрдеша. Теоремой 1 оценивается число независимых множеств в графах Кэли $\Gamma_A(V)$, таких, что $A = \{\lceil \frac{n}{2} \rceil - t, \lceil \frac{n}{2} \rceil - f\}$, $V \subseteq [\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + t] \cup [n - t + 1, n]$, где $n, t, f \in \mathbb{N}$ и $f < t < \frac{n}{4}$. Такие графы удобно воспринимать как графы Кэли на объединении двух соответствующих отрезков натуральных чисел, "поврежденные" удалением части вершин. Теоремой 2 описывается граф с наибольшим количеством независимых множеств среди всех графов в классе $\mathcal{G}_2(n,m)$. Это является частичным решением соответствующей задачи, поставленной Н. Алоном.

ТЕОРЕМА 1. Пусть $n, t, f \in \mathbb{N}$ и $f < t < \frac{n}{4}$, положим $A = \{\lceil \frac{n}{2} \rceil - t, \lceil \frac{n}{2} \rceil - f\}$, $V = [\lfloor \frac{n}{2} \rfloor + 1, \lfloor \frac{n}{2} \rfloor + t] \cup [n - t + 1, n]$. Пусть граф $\Gamma_A^m(V)$ получен из графа $\Gamma_A(V)$ удалением произвольных m вершин. Тогда

$$|I(\Gamma_A^m(V))| \le \left(\frac{7+3\sqrt{5}}{2\sqrt{5}}\right)^t \left(\frac{2\sqrt{5}}{3+\sqrt{5}}\right)^f \left(\frac{4}{3+\sqrt{5}}\right)^m.$$

ТЕОРЕМА 2. Наибольшим количеством независимых множеств в $\mathcal{G}_2(n,m)$ при $m \ge 4$ обладает единственный граф Γ, состоящий из $n-m$ изолированных вершин и из

1) $\frac{m}{4}$ циклов длины 4, если $m \equiv 0 \pmod 4$,
2) $\lfloor \frac{m}{4} \rfloor - 1$ циклов длины 4 и цикла длины 5, если $m \equiv 1 \pmod 4$,
3) $\lfloor \frac{m}{4} \rfloor - 1$ циклов длины 4 и цикла длины 6, если $m \equiv 2 \pmod 4$,
4) $\lfloor \frac{m}{4} \rfloor - 1$ циклов длины 4 и цикла длины 7, если $m \equiv 3 \pmod 4$.

Работа выполнена при поддержке РФФИ (проект 04-01-00359).

ОБ ИСПОЛЬЗОВАНИИ СВОЙСТВ ЭЛЕМЕНТОВ СХЕМ

В. А. Орлов (Москва)

Назовем I-элементом (O-элементом) элемент схемы такой, что для любого его входного (выходного) набора существует входной набор схемы, порождающий этот входной (выходной) набор элемента.

Схему, почти все элементы которой являются I-элементами (O-элементами), назовем I-схемой (O-схемой). Скажем, что I-схема (O-схема) получена с использованием первого (второго) принципа максимального использования элементов (ПМИЭ).

Вначале рассмотрим случай булевых базисов, элементы которых имеют один выход.

ТЕОРЕМА. Для любого базиса и почти любой функции существует реализующая ее асимптотически наилучшая схема, в которой почти все элементы не являются I-элементами.

Однако, при реализации наилучших схем для "узких" классов функций может понадобиться применение ПМИЭ1.

Из [1] следует, что для случая k-значных, $k \geq 3$, базисов, элементы которых имеют один выход, при реализации почти всех функций можно не применять даже ПМИЭ2. Из [2] следует, что для случая булевых базисов, элементы которых могут иметь более одного выхода, ситуация аналогична.

На примере рассмотренной в [3, с. 60] задачи показано, что применение ПМИЭ1 позволило улучшить в два раза полученную в [3] оценку. Доказанная оптимальность полученных схем показывает, что применение ПМИЭ может оказаться весьма эффективным.

Работа выполнена при финансовой поддержке гранта поддержки ведущих научных школ РФ (проект НШ-1807.2003.1).

Список литературы

1. Орлов В. А. Реализация функций из P_k схемами в произвольном базисе из функциональных элементов // Докл. РАН. — 1998. — Т. 359, № 3. — С. 308–309.

2. Марковский А. В., Редькин Н. П. О реализации булевых функций схемами из блоков // Проблемы кибернетики. Вып. 28. — М.: Физматгиз, 1974. — С. 81–100.

3. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Физматгиз, 1965. — С. 31–110.

О ФУНКЦИОНАЛЬНОЙ СЛОЖНОСТИ МНОГОМЕРНОЙ ЗАДАЧИ О МАНХЭТТЕНОВСКОЙ БЛИЗОСТИ

Е. Н. Остроухова (Москва)

Пусть $X = [0,1]^n$ — множество запросов, $Y = [0,1]^n$ — множество записей, V — конечное подмножество Y. Отношение поиска ρ^n_{man} на $X \times Y$ задается соотношением $x\rho^n_{man}y \Longleftrightarrow \sum_{i=1}^n |x_i - y_i| \leq r$, где $x \in X$, $y \in Y$, $0 < r < n$. Задача о манхэттеновской близости состоит в перечислении для произвольного $x \in X$ тех и только тех $y \in V$, для которых $x\rho^n_{man}y$. При оценке алгоритмов поиска обычно используют три основных характеристики: объем памяти, время поиска в худшем случае и среднее время поиска. Зависимость времени поиска от объема памяти называется функциональной сложностью алгоритма. Будем называть алгоритм поиска $(f(k), g(k), h(k))$-алгоритмом, если объем памяти, время поиска в худшем случае (без времени на перечисление ответа) и среднее время поиска (без времени на перечисление ответа) есть $O(f(k))$, $O(g(k))$ и $O(h(k))$ соответственно при $k \to \infty$, где $k = |V|$. В данной работе по методу, описанному в [1], получен алгоритм решения многомерной задачи о манхэттеновской близости, зависящий от некоторого параметра m $(1 \leq m \leq \ln k)$. Вариация этого параметра позволяет оценить функциональную сложность в некоторой последовательности точек. Полученный алгоритм есть $(m^q k^{1+q/m}, m^q \log_2 k, m^q)$-алгоритм, где $q = 2^{n-1} - 1$.

Автор выражает благодарность Э. Э. Гасанову за постановку задачи и помощь в работе.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 05-01-00709).

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации — М.: Физматлит, 2002.

ЯЗЫКОВЫЕ УРАВНЕНИЯ: ПОПЫТКА КЛАССИФИКАЦИИ

А. С. Охотин (Турку, Финляндия)

Языковым уравнением, в широком смысле, называется всякое формальное высказывание о взаимоотношении между языками, содержащее неизвестные языки. Их изучение началось с работ Гинзбурга и Райса [1] и Бондарчука [2], представивших, соответственно, контекстно-свободные грамматики и конечные автоматы двумя классами систем уравнений вида $X_i = \varphi_i(X_1, \ldots, X_n)$ $(1 \leq i \leq n)$, разрешённых относительно неизвестных. Позднее изучалась выразительная мощность многих других классов уравнений [3–8], а также была установлена сложность распознавания ряда их свойств [3,7].

Первый опыт классификации языковых уравнений принадлежит автору [6], выделившему 8 разновидностей уравнений с различными базисами булевых операций. В этом докладе предлагается дальнейшее развитие классификации, распространённой на неразрешённые уравнения и учитывающей основные виды ограничений на конкатенацию, что позволяет представить классические работы [1, 2] и результаты последних лет [3–8] в рамках общей модели.

Список литературы

1. Ginsburg S. Rice H. G. Two families of languages related to ALGOL // Journal of the ACM. — 1962. — V. 9. — P. 350–371.

2. Бондарчук В. Г. Системы уравнений в алгебре событий // Журнал выч. математики и мат. физики. — 1963. — Т. 3, № 6. — С. 1077–1088.

3. Baader F., Küsters R. Solving linear equations over regular languages // UNIF 2001 (Siena, Italy, June 18–19, 2001). — P. 27–31.

4. Kunc M. The power of commuting with finite sets of words // STACS 2005 (Stuttgart, Germany). — LNCS 3404. — P. 569–580.

5. Охотин А. С. Конъюнктивные грамматики и системы языковых уравнений // Программирование. — 2002. — Т. 28, № 5. — С. 3–11.

6. Охотин А. С. Системы языковых уравнений и замкнутые классы функций алгебры логики // Дискретные модели в теории управляющих систем: V Международная конференция (Ратмино, 2003). — С. 56–64.

7. Okhotin A. Decision problems for language equations with Boolean operations // ICALP 2003 (Eindhoven, Holland). — P. 239–251.

8. Охотин А. С. Языковые уравнения и модели вычислений // Дискретные модели в теории управляющих систем: VI Международная конференция (Москва, 7–11 декабря 2004 г.). — С. 129–134.

УСЛОВИЯ РЕАЛИЗУЕМОСТИ ФУНКЦИЙ НА ПОЛУРЕШЁТКАХ ПЕРЕКЛЮЧАТЕЛЬНЫМИ СХЕМАМИ

И. А. Панкратова (Томск)

Недостающие определения и обозначения см. в [1]. Рассматриваются функции состояний на полурешётке I, где $I = (\tilde{E}_3)^2$, и переключательные схемы с двухполюсным источником питания, в которых проводимости между выходным полюсом и полюсами питания реализуются переключательными сетями без общих элементов.

Пусть заданы множество переключательных элементов (базис) B и функция состояний $f : U_f \subseteq I^n \to I$. Обозначим $G_B = \{g_1, ..., g_r\}$ множество функций проводимости всех элементов в B при всевозможных отождествлениях их управляющих полюсов с входными полюсами схемы. Определим бинарное отношение $\Gamma_{f,B} \subseteq \tilde{E}_3^{\,r} \times I$, положив $((g_1(a), ..., g_r(a)), f(a)) \in \Gamma_{f,B} \Leftrightarrow a \in U_f$.

ТЕОРЕМА 1. Если функция f реализуется в базисе B, то отношение $\Gamma_{f,B}$ квазимонотонно.

Определим бинарное отношение γ на $\tilde{E}_3$ как $(a, b) \in \gamma \Leftrightarrow (a \leq 1' \wedge b \leq 0') \vee (a \cap b \neq \oslash)$. Пусть далее B — множество элементов, проводимости в которых принимают значения в $\tilde{E}_2$, и R — резистор.

ТЕОРЕМА 2. Функция f реализуется схемой глубины 2 в базисе $B \cup \{R\}$, если отношение $\Gamma_{f,B}$ квазимонотонно и B содержит элемент с функцией проводимости, не сохраняющей отношения γ.

Пару наборов (a, b) назовём (0,1)-разделимой множеством функций G, если $(g(a), g(b)) = (0, 1)$ для некоторой $g \in G$.

ТЕОРЕМА 3. Функция f реализуется схемой глубины 1 в базисе $B \cup \{R\}$, если и только если для каждой функции $h \in \{f_0, f_1\}$, где $(f_0, f_1) = f$, выполнены условия:

а) для любых $a, b \in U_f$ если $h(a) = 0$ и $h(b) \leq 0'$, или $h(a) \leq 1'$ и $h(b) = 1$, то пара (a, b) (0,1)-разделима множеством G_B;

б) для любых $a_0, a_1, b \in U_f$ если $h(a_0) \leq 1'$, $h(a_1) \leq 0'$ и $h(b) = X'$, то хотя бы одна из пар (a_0, a_1), (a_0, b) или (b, a_1) (0,1)-разделима G_B.

ТЕОРЕМА 4. Для функции, не реализуемой схемой глубины 1, условия теоремы 2 являются необходимыми и достаточными для её реализуемости в базисе $B \cup \{R\}$.

Список литературы

1. Агибалов Г. П. Дискретные автоматы на полурешетках. — Томск: Изд-во Том. ун-та, 1993.

РАЗЛОЖЕНИЕ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ В СУММУ ПРОИЗВЕДЕНИЙ СОБСТВЕННЫХ ПОДФУНКЦИЙ

В. И. Пантелеев, Н. А. Перязев (Иркутск)

Рассматриваем $n \times m$-матрицы над произвольным полем P. Пусть $M_{n\times m}(P)$ — множество всех таких матриц.

На $M_{n\times m}(P)$ определим операцию $\circ$ следующим образом: если $A = (a_{i,j})$, $B = (b_{i,j})$, то $A \circ B = C = (c_{i,j}) \in M_{n\times m}(P)$ и $c_{i,j} = a_{i,j} \cdot b_{i,j}$ ($\cdot$ — умножение в поле P).

Для $i \in \{1, ..., n\}$ ($j \in \{1, ..., m\}$) через A_i (A^j) обозначим матрицу, полученную из $A \in M_{n\times m}(P)$, заменой всех строк (столбцов) на строку (столбец) с номером i (j).

ТЕОРЕМА. Для любой матрицы $A \in M_{n\times m}(P)$ справедливо

$$A = \sum_{i=1}^{n} \sum_{j=1}^{m} \sigma_{ij} A_i \circ A^j \quad (\sigma_{ij} \in P)$$

Пусть $k = p^\alpha$, p — простое число, $E_k = \{0, ..., k-1\}$, $f(x_1, \ldots, x_n)$ — функция k-значной логики, $\tilde{u}, \tilde{v}$ — некоторое разбиение множества переменных $\{x_1, \ldots, x_n\}$ на две части, $\tilde{\sigma}_1, \tilde{\sigma}_2$ — наборы констант из E_k, причем $|\tilde{\sigma}_1| = |\tilde{u}|, |\tilde{\sigma}_2| = |\tilde{v}|$

СЛЕДСТВИЕ. Для любой функции k-значной логики $f(\tilde{u}, \tilde{v})$ имеет место разложение

$$f(\tilde{u}, \tilde{v}) = \sum_{\tilde{\sigma}_1, \tilde{\sigma}_2} \alpha_{\tilde{\sigma}_1 \tilde{\sigma}_2} f(\tilde{\sigma}_1, \tilde{v}) \cdot f(\tilde{u}, \tilde{\sigma}_2),$$

где сложение и умножение выполняются в поле $GF(k)$, $\alpha_{\tilde{\sigma}_1 \tilde{\sigma}_2} \in E_k$.

Справедливость данного результата при $k = 2$ показана в [1].

Работа выполнена при частичной финансовой поддержке РФФИ (проект 04-07-90178в).

Список литературы

1. Винокуров С. Ф., Перязев Н. А. Разложение булевых функций в сумму произведений собственных подфункций // Дискретная математика. — 1993. — Т. 5, № 3. — С. 121–123.

ОБ ОТЛИЧИМОСТИ АВТОМАТОВ ПРИ ИСКАЖЕНИЯХ НА ВХОДЕ

П. А. Пантелеев (Москва)

Рассматривается задачи отличимости состояний конечного автомата при искажении входных слов. Два состояния называются k-кратно отличимыми, если существует такое слово α, что оно и любое его искажение не более чем в k позициях отличает их. Рассмотрим функцию Шеннона $L(n, k)$ — минимальную длину α на множестве всех автоматов с не более чем n состояниями для всех их пар k-кратно отличимых состояний.

ТЕОРЕМА 1. При $n \to \infty$ имеет место соотношение

$$L(n, k) \leq n^2 2^{kn^2}.$$

ТЕОРЕМА 2. Для каждого натурального $n > 1$ существует автомат с n состояниями и двумя входными символами такой, что у него найдутся два состояния q_1, q_2, для которых длина минимального 1-кратно отличающего слова экспоненциальна по n.

Назовем автомат кратно-приведенным, если любая пара его различных состояний 1-кратно отличима. Оказывается, что у кратно-приведенного автомата все состояния k-кратно отличимы для любого $k = 0, 1, 2, \ldots$. Рассмотрим соответствующую функцию Шеннона $L_C(n, k)$ для класса кратно-приведенных автоматов.

ТЕОРЕМА 3. Имеет место равенство $L_C(n, k) = n - 1 + k\frac{n(n-1)}{2}$.

Список литературы

1. Пантелеев П. А. Об отличимости состояний автоматов // Дискретная математика. — 2003. — Т. 15, вып. 3.

2. Panteleev P. A. On modification of a distingiushability of an automaton states // V international congress on mathematical modelling (Dubna, 2002). — V 2. — P. 120.

3. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: Изд-во МГУ, 1978.

ВЕРХНЯЯ ОЦЕНКА РОДА ПЕРЕПЛЕТЁННЫХ ГРАФОВ

В. И. Петренюк (Кировоград)

Задача заключается в определении эйлерового рода φ-образа [1] плоских графов G_1, G_2, заданного на множествах точек M_1, M_2 с числом достижимости большим 1, следующим φ-преобразованием: $\varphi(G_1 + G_2, \sum_{i=1}^{n} a_i + g_i) \to (G, \{a_i^*\}_1^n)$, где $M_1 = \{a_i\}_1^n, t_{G_1}(M_1) = t_1$, $M_2 = \{g_i\}_1^n, t_{G_2}(M_2) = t_2$ — заданные множества точек графов G_1,G_2 с числами достижимости t_1, t_2. Частным случаем этой будет задача оценки рода апекс-графа. Возможные различные варианты такого φ-преобразования графа $G_1 + G_2$ на граф G, который будем называть переплетённым, где $G_i \in \{K_4, K_{2,3}\}$, имеют место когда, либо вершины отождествляются с внутренними точками рёбер (в том числе с вершинами), либо отождествляется ребро одного графа с ребром (частью ребра) другого графа. Получены следующие результаты:

1. Пусть G — плоский граф с заданным множеством точек X, обладающим числом достижимости t, $t > 1$, и задано K — множество из $t - 1$ графа, изоморфного K_4 или $K_{2,3}$, где $G_1 \doteq K_4$ или $G_1 \doteq K_{2,3}$. Определён подграф $G[X]$ как φ-образ множества K при φ-преобразовании описанным графом $L(K, G[X])$. Если цикломатическое число графа $L(K, G[X])$ ненулевое, то граф переплетения $G + G_1$ имеет род, равный $\gamma(G) + 1$, иначе $\gamma(G)$.

2. Обозначим через P_1, P_2 графы, полученные путём удаления вершины степени 2 из графа $K_{2,3}$ или двух внутренних точек несмежных рёбер графа $\{K_4\}$. Пусть G — плоский граф с заданным подмножеством вершин X, обладающим числом достижимости t, $t > 1$ и разбитым на t непустых подмножеств X_i . Если задано φ-преобразование графа $G + \{P_1 i\}_i = 1_1^t + \{P_2 i\}_i = 1_2^t$ на переплетённый граф J описанным выше способом, то $\gamma(J) \le \gamma(G) + 2(t_1 + t_2)$.

Список литературы

1. Хоменко Н. П. φ-преобразования графов. — Препринт ИМ АН УССР. — Киев, 1973. — 320 с.

О ФАКТОРИЗАЦИЯХ r-РЕГУЛЯРНЫМИ ДЕРЕВЬЯМИ

Л. П. Петренюк, А. Я. Петренюк (Кировоград)

Для дерева T четного порядка n T-факторизацией [1] называют разложение полного графа K_n на подграфы, каждый из которых изоморфен дереву T. Задача состоит в том, чтобы выяснить, для каких деревьев существуют T-факторизации. Л. Байнеке установил необходимое условие $\Delta(T) \le k$ существования T-факторизации порядка n, где $n = 2k$, а $\Delta(T)$ означает наивысшую степень вершины в дереве T.

Дерево T называем r-регулярным, если оно может содержать, кроме концевых вершин, только вершины степени r, $r > 1$. Множество вершин степени r в r-регулярном дереве индуцирует поддерево T', которое мы называем определяющим поддеревом дерева T.

Обозначим t количество вершин степени r в дереве T, то есть порядок определяющего дерева. Размер дерева T равен, с одной стороны, $n - 1$, а с другой его можно выразить как $tr - (t - 1)$, или $t(k - 1) + 1$. Из равенства $t(r - 1) + 1 = n - 1$ непосредственно следует $t = (n - 2)/(r - 1)$. Отсюда получаем необходимое условие $n = 2 \mod (r - 1)$ существования r-регулярных деревьев порядка n.

Предположим, что для r-регулярного дерева $T_{n,r}$ порядка n существует $T_{n,r}$-факторизация Φ. Для вершины x основного графа K_n обозначим через $s = s(x)$ количество таких компонент факторизации Φ, у которых x — вершина степени k.

Среди $n-1$ ребер, инцидентных вершине x, $rs(x)$ ребер принадлежат тем компонентам, у которых x — вершина степени r, и $k - s(x)$ ребер, являющихся концевыми в остальных компонентах факторизации Φ. Из полученного равенства $rs(x) + k - s(x) = n - 1$, получаем $(r - 1)s(x) = k - 1$, откуда $s(x) = (k - 1)/(r - 1) = const$.

Из последнего соотношения вытекает

ТЕОРЕМА. Для существования $T_{n,r}$-факторизации необходимо, чтобы число $n - 2$ нацело делилось на $2(r - 1)$.

Список литературы

1. Petrenjuk A. J., On tree factorizations of K_{10} // Journal of Combinatorial Mathematics and Combinatorial Computing. — 2002. — V. 41. — P. 193–202.

ДИСКРЕТНО УПРАВЛЯЕМЫЕ СИСТЕМЫ МНОГОРЕСУРСНОГО СЕТЕВОГО ПЛАНИРОВАНИЯ

С. Ю. Петри (Нижний Новгород)

Пусть I и J — конечные множества мощностью m и n, $T = \{1 \dots T_0\}$. С помощью множеств $K(j) \subset J$, $j \in J$, определим отношение предшествования на множестве J: если элемент k непосредственно предшествует элементу j, то $k \in K(j)$ $(k \in J, j \in J)$. Обозначим через $\overrightarrow{c}(j)$ и $\overrightarrow{r}(j)$ — вектор-функции определенные, соответственно, на множествах J и T со значениями из R^m. Пусть: $S \times T = \{< \overrightarrow{s}, t > | \overrightarrow{s} \in R^m, t \in T\}$ — множество состояний системы, $U(< \overrightarrow{s}, t >)$, — множество управлений, допустимых в состоянии $< \overrightarrow{s}, t >$. Введем фиктивное управление λ, применение которого переводит систему из состояния $< \overrightarrow{s}, t >$ в состояние $< \overrightarrow{s} + \overrightarrow{r}(t+1), t+1 >$. При применении к системе управления j, $j \in U(< \overrightarrow{s}, t >)$, система из состояния $< \overrightarrow{s}, t >$ переходит в состояние $< \overrightarrow{s} - \overrightarrow{c}(j), t >$, приобретая при этом "доход", задаваемый функцией $g(\overrightarrow{s}, t, j)$. Стратегию управления системой будем отождествлять с функцией f определенной на множестве $S \times T$ и со значениями из J. Требуется найти такую стратегию управления системой, чтобы после окончания функционирования (при $t = T_0$) система получила максимальный суммарный доход [1]. Применив принцип оптимальности динамического программирования, строятся рекуррентные соотношения, позволяющие находить оптимальную стратегию управления рассматриваемой системой. В рамках построенной математической модели формализуются такие задачи многоресурсного сетевого планирования, как задачи логистического управления, задачи календарного планирования производства и др.

Список литературы

1. Прилуцкий М. Х. Дискретно управляемые системы распределения ресурсов в сетевых иерархических и канонических структурах // Математика и кибернетика. Сборник научных статей юбилейной научно-технической конференции факультета ВМК ННГУ и НИИ ПМК. — Н. Новгород, 2003. — С. 243–247.

О КОРДИАЛЬНОСТИ ДЕРЕВЬЕВ

Т. В. Петровская (Кировоград)

Для обыкновенного графа G $\{0,1\}$-разметкой вершин называют отображение $\Phi : V(G) \to \{0,1\}$. Множество вершин, отображающееся в 0 , обозначим V_0, и введем обозначения $V_1 = V(G) - V_0$, $v_0 = |V_0|$, $v_1 = |V_1|$. Разметка вершин графа G порождает $\{0,1\}$-разметку его ребер: ребро получает метку 0, если метки его концов одинаковы, и метку 1 в противоположном случае. Множество ребер, имеющих метки i, обозначим $E_i, i = 0, 1$.

$\{0,1\}$-разметка графа G кордиальна [1], если $|v_1 - v_0| \leq 1$ и одновременно $|e_1 - e_0| \leq 1$. Граф, допускающий кордиальную разметку, называется кордиальным.

Если в $\{0,1\}$-разметке графа G заменить нули единицами и наоборот, получим дополнительную разметку. Разметка, дополнительная к кордиальной, тоже кордиальна.

Легко видеть, что циклы $C_n (n \geq 3)$ кордиальны, полные же графы K_0 $(n \geq 3)$-некордиальны. Актуальная задача: кордиален ли заданный граф G?

ТЕОРЕМА 1. Все деревья — кордиальные графы.

Доказательство. Индукция по порядку дерева. При $n = 1, 2$ утверждение очевидно. Пусть $n > 2$, T_n — произвольное дерево порядка n, xy — ребро дерева T, где x — концевая вершина.

Рассмотрим дерево $T_n - x$. Его порядок $n-1$, и по предположению индукции существует кордиальная разметка Φ этого дерева.

Если n четно, то для этой разметки $e_0 = e_1$ и либо $v_0 = v_1 + 1$, либо $v_1 = v_0 + 1$. В первом случае полагаем $\Phi^*(x) = 1, \Phi^*(z) = \Phi(z)$ при всех $z \neq x$ и получаем кордиальную разметку Φ^* дерева T_n. Во втором случае построение разметки Φ^* сводим к первому, используя вместо Φ дополнительную к ней разметку.

В случае нечетного n для разметки Φ имеем $v_0 = v_1$ и либо $e_0 = e_1 + 1$ либо $e_1 = e_0 + 1$. В обоих случаях кордиальная разметка Φ^* дерева T строится так: $\Phi^*(x) \neq \Phi(x), \Phi^*(z) = \Phi(z)$ при всех $z \neq x$, и теорема доказана.

Список литературы

1. Стьожка І., Тодуа Л. Про кордіальні нумерації графів // Збірник матеріалів Четвертої Всеукраїнської студ. науково-практ. конференції. — Кіровоград, 2004. — С. 115–116.

О МНОЖЕСТВАХ, СВОБОДНЫХ ОТ ПРОИЗВЕДЕНИЙ

Т. Г. Петросян (Москва)

Множество A элементов группы G называется свободным от произведений (МСП), если уравнение $xy = z$ не имеет решений в множестве A. Семейство всех подмножеств группы G, свободных от произведений, обозначим через $\mathcal{P}(G)$. Пусть $p(n) = \max_G |\mathcal{P}(G)|$, где максимум берется по всем группам порядка n. Алон [1] получил оценку сверху для логарифма $p(n)$, имеющую вид

$$\log_2 p(n) \le n\big(1/2 + \varepsilon(n)\big), \qquad (1)$$

где $\varepsilon(n) \to 0$ при $n \to \infty$.

Сапоженко [2] и независимо Лев, Лучак и Шон [3] получили асимптотику числа множеств, свободных от сумм, в абелевых группах четного порядка.

ТЕОРЕМА 1 [2, 3]. Для любой группы G четного порядка n с числом подгрупп индекса 2, равным t,

$$t \cdot 2^{n/2} - 2^{(n/4)\left(1+\varepsilon(n)\right)} \le |\mathcal{P}(G)| \le t \cdot 2^{n/2} + 2^{n(1/2-c)},$$

где $c > 0,017$ и $\varepsilon(n) \to 0$ при $n \to \infty$.

В [4] была обобщена теорема 1 на случай произвольных групп, содержащих хотя бы одну подгруппу индекса 2. В данной работе получено улучшение оценки (1) из теоремы Алона [1] для конечных групп, содержащих нормальную подгруппу простого индекса большего, чем 2.

ТЕОРЕМА 2. Пусть G конечная группа порядка n, содержащая нормальную подгруппу H индекса p, $p > 2$, где p — простое число. Тогда верна оценка

$$|\mathcal{P}(G)| \le 2^{n(1/2-\delta)},$$

где $\delta > 0$.

Работы выполнена при поддержке гранта РФФИ 04-01-00359.

Список литературы

1. Alon N. Independent sets in regular graphs and Sum-Free Subsets of Finite Groups // Israel Journal of Math. — 1991. — V. 73, № 2. — P. 247–256.

2. Сапоженко А. А. О числе множеств, свободных от сумм, в абелевых группах // Вестник Моск. Ун-та. Сер. 1. Математика. Механика. — 2002. — № 4. — С. 14–17.

3. Lev V. F., Łuczak T., Schoen T. Sum-free sets in abelian groups // Israel Journal of Math. — 2001. — V. 125. — P. 347–367.

4. Петросян Т. Г. О числе множеств, свободных от произведений, в группах четного порядка // Дискретная математика. — 2005. — Т. 17, вып. 1.

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ПРОБЛЕМЫ ЭКВИВАЛЕНТНЫХ ПРЕОБРАЗОВАНИЙ

Р. И. Подловченко (Москва)

Проблема эквивалентных преобразований (э.п.) рассматривается в следующих моделях вычислений — схемы из функциональных элементов, автоматы, схемы программ. Объекты, принадлежащие этим моделям, задаются конечными размеченными графами. Каждой модели присуща процедура, которая всякому объекту приписывает порождаемое им множество. Объекты считаются эквивалентными, если совпадают порождаемые ими множества. Рассматриваемые системы преобразований состоят из пар эквивалентных объектов. Система называется полной, если ее замыкание совпадает с множеством всех пар эквивалентных объектов. Проблема э.п. в модели формулируется как поиск полной системы преобразований. Методика ее решения очерчена в [1] и предписывает создание формального исчисления с конечным множеством аксиом и единственным правилом вывода (правилом подстановки) с тем, чтобы аксиомы определяли систему преобразований объектов модели, а доказательство ее полноты осуществлялось выводимостью в данном исчислении из произвольного объекта модели любого ему эквивалентного объекта.

Эта методика применена нами для всех перечисленных выше моделей. Элементами создаваемых исчислений стали фрагменты, определяемые так, что объект-граф является частными случаем фрагмента. При этом используемые преобразования подразделяются на локальные и глобальные, а последние могут быть как безусловными, так и условными. Ранее было установлено, что для схем программ не существует конечной полной системы локальных преобразований, но существует конечная полная система глобальных преобразований. Нами обнаружен класс конечных автоматов, обладающий тем же свойством. Для уже построенных полных систем преобразований выполнена классификация их по типу преобразований и описаны стратегии построения выводов в используемых исчислениях.

Работа выполнена при поддержке РФФИ (проект 03-01-00312).

Список литературы

1. Подловченко Р. И. К вопросу об эквивалентных преобразованиях алгоритмов и программ // Математические вопросы кибернетики. Вып. 9. — М.: Физматлит, 2000. — С. 25–36.

ПРОВЕРКА ЭКВИВАЛЕНТНОСТИ ПРОГРАММ: МОДЕЛИ И АЛГОРИТМЫ

Р. И. Подловченко, В. А. Захаров (Москва)

Обзор посвящен анализу математических моделей и алгоритмов, используемых для проверки эквивалентности программ. Две программы считаются эквивалентными, если они имеют одинаковое поведение. Обоснованы интерес к изучению проблемы эквивалентности программ и выбор алгебраических моделей программ для проведения ее исследований. Описаны концепции, лежащие в основе алгебраических моделей программ. Объектами этих моделей являются схемы программ. Установлены необходимые и достаточные условия аппроксимации классов программ алгебраическими моделями. Отмечена связь алгебраических моделей программ со схемами Ляпунова — Янова, моделями Глушкова — Летичевского и др. Излагаются первые из установленных случаев разрешимости (Ю. И. Янов) и неразрешимости (А. А. Летичевский, М. Патерсон) проблемы эквивалентности. Проведены описание и классификация всех известных подходов к решению проблемы эквивалентности для различных алгебраических моделей программ. Среди описанных методов выделены:

— метод редукции к проблемам разрешимости в известных моделях вычислений (К. Ратледж);

— метод устранения несущественных ветвлений (А. А. Летичевский);

— метод совместных вычислений схем программ (В. А. Захаров);

— метод анализа структуры эквивалентных схем программ (Р. И. Подловченко);

— метод развертки по образцу (Р. И. Подловченко, В. Е. Хачатрян).

Продемонстрированы примеры применения перечисленных методов, а также описаны их основные характеристики (сложность разрешающих алгоритмов, получаемых на основе этих методов, классы моделей программ, к которым применимы данные методы, и др.). В заключение сформулированы направления дальнейших исследований проблемы эквивалентности в алгебраических моделях программ.

Работа выполнена при поддержке гранта РФФИ 03-01-00312.

КОМПОЗИЦИОННЫЙ ПОДХОД К ЗАДАНИЮ СЕМАНТИКИ ЯЗЫКА SQL

С. П. Поляков (Киев)

В соответствии с композиционным подходом [1] семантика языка SQL, выступающего стандартом для реляционных баз данных [2], определяется с помощью специальной программной алгебры. Ее носитель задается как множество функций, определенных на атомарных данных, записях, таблицах, конечных множествах таблиц и атомарных данных; сигнатура состоит из композиций полного образа, фильтрации, агрегирования [3]. Множество базовых функций (система порождающих) F состоит из: 1) операций объединения, пересечения, разности таблиц, объединения совместных строк; 2) операций внутреннего и внешнего соединения таблиц; 3) конъюнкции, дизъюнкции и отрицания трехзначной логики; 4) бинарных функций типа сложения, используемых композицией агрегирования; 5) специальных функций для построения упорядоченных таблиц и таблиц с группировкой; 6) функций именования и разименования на строках таблиц; 7) атомарных предикатов и функций, определенных на универсальном домене.

ОСНОВНОЙ РЕЗУЛЬТАТ. Множество функций, задающих семантику операторов манипулирования данными Select, Insert, Update, Delete языка SQL, принадлежит замыканию множества базовых функций F композициями полного образа, фильтрации и агрегирования.

Работа выполнена при финансовой поддержке Государственного Фонда Фундаментальных исследований Украины (проект 01.07/105).

Список литературы

1. Редько В. Н., Буй Д. Б. К основаниям теории реляционных моделей баз данных // Кибернет. и системн. анализ. — 1996. — № 4. — С. 3–12.

2. Кренке Д. Теория и практика построения баз данных. 8-е изд. — С-Пб: Питер, 2003. — 800 с.

3. Редько В. Н., Брона Ю. И., Буй Д. Б., Поляков С. А. Реляционные базы данных: табличные алгебры и SQL–подобные языки. — Киев: Академпериодика, 2001. — 196 с.

О ГРАФЕ, ОБЛАДАЮЩЕМ $(2t+r,3)-$СВОЙСТВОМ

О. П. Полякова (Ярославль)

В работах Дольникова [1, 2] были введены определения (p,q)-свойства для графов и гиперграфов:

Граф G обладает (p,q)-свойством, если каждый его подграф на p вершинах содержит пустой подграф на q вершинах, конечно $p \geq q$ и $n(G) \geq p$.

В докладе изучаются свойства графа, обладающего (p,q)-свойством. В работах [2–4] уже были получены определенные результаты на эту тему. Так, в статье [2] в этом направлении была доказана следующая

ЛЕММА. Если граф G обладает $(2q-2,q)$-свойством, то он обладает и $(2q-1,q+1)$-свойством и из множества его вершин можно так удалить $q-2$ вершины, что оставшееся множество будет независимо.

ТЕОРЕМА. Если граф G обладает $(2t+r,3)$-свойством, где $t > 2$, $r = -1, 0$, то из множества вершин графа G можно удалить $r+2$ вершины так, чтобы в результате остался граф без K_t.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 03-01-00801).

Список литературы

1. Дольников В. Л. Об одной задаче окрашивания // Сибирский математический журнал. — 1972. — XIII, № 6. — С. 1272–1283.

2. Дольников В. Л. Об одном обобщении теоремы Рамсея // ДАН СССР. — 1977. — Т. 232, № 6. — С. 1241–1244.

3. Полякова О. П. О поведении функции неплотности графа // Современные проблемы математики и информатики. Вып. 3: Сборник научных трудов молодых ученых, аспирантов и студентов. — Ярославль: Изд-во Яросл. гос. ун-та, 2000. — С. 52–61.

4. Полякова О. П. Оценка функции неплотности графа в точке $q+t$ // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.). — М.: Изд-во механико-математического ф-та МГУ, 2004. — С. 361–363.

РАНГ КОММУТАТИВНЫХ ГРУППОВЫХ АЛГЕБР НАД ПОЛЯМИ КОМПЛЕКСНЫХ И ВЕЩЕСТВЕННЫХ ЧИСЕЛ

А. Д. Поспелов (Москва)

Рассматриваются коммутативные групповые алгебры над полями комплексных и вещественных чисел, и изучается вопрос об их структурном представлении и сложности умножения в них. Доказано, что все алгебры указанного типа являются простыми алгебрами минимального ранга.

Доказано, что для любой абелевой группы G порядка n групповая алгебра $\mathbb{C}(G)$ изоморфна $\mathbb{C}^n$, и что $\operatorname{rk}\mathbb{C}(G) = n$.

Доказано, что для любой абелевой группы G порядка n групповая алгебра $\mathbb{R}(G)$ изоморфна $\mathbb{R}^{2^{e(G)}} \times (\mathbb{R}[x]/(x^2+1))^{\frac{n}{2}-2^{e(G)-1}}$, где $e(G)$ — число множителей чётного порядка в представлении G в виде прямого произведения циклических групп. Доказано, также, что $\operatorname{rk}\mathbb{R}(G) = \frac{3}{2}n - 2^{e(G)-1}$.

Очевидно, что для любого семейства коммутативных групповых алгебр над полем комплексных чисел константа асимптотики сложности равна 1. Описан весь спектр констант асимптотики сложности коммутативных групповых алгебр над полем вещественных чисел, а именно, доказано, что если для последовательности коммутативных групповых алгебр A_n над полем вещественных чисел существует предел $C = \lim_{n\to\infty} \frac{\operatorname{rk} A_n}{\dim A_n}$, то он равен либо $\frac{3}{2}$, либо $\frac{3}{2} - \frac{1}{2m}$ для некоторого натурального m, причём для всякой константы указанного вида соответствующая последовательность существует.

Автор выражает благодарность своему научному руководителю профессору В. Б. Алексееву.

Работа выполнена при поддержке РФФИ (проект 03-01-00783).

Список литературы

1. Алексеев В. Б., Поспелов А. Д. О ранге групповых алгебр // Математические методы решения инженерных задач. — 2004. — (В печати.)

2. Алексеев В. Б., Поспелов А. Д. Сложность умножения в групповой алгебре симметрий квадрата // Тезисы 6-ой Международной конференции «Дискретные модели в теории управляющих систем». — 2004. — С. 8–11.

3. Алексеев В. Б., Поспелов А. Д. Сложность умножения в некоторых групповых алгебрах // Дискретная математика. — 2005. — Т. 17, № 1. — (В печати.)

АЛГОРИТМИЧЕСКАЯ СЛОЖНОСТЬ СЛОВ ОТНОСИТЕЛЬНО СХЕМЫ КОНКАТЕНАЦИИ

В. Н. Потапов (Новосибирск)

Пусть A — конечный алфавит и $A^* = \cup_{i=0}^{\infty} A^i$. Программой будем называть частично рекурсивную функцию $P : \{0,1\}^* \to A^*$. Сложностью слова $w \in A^*$ относительно программы P будем называть величину $K_P(w) = \inf\{|x| \,|\, P(x) = w\}$. Схемой конкатенации слова w называется последовательность слов $v(1), \ldots, v(m) = w$ такая, что каждое слово $v(i)$ является буквой или конкатенацией двух предыдущих слов $v(j_1)$ и $v(j_2)$, т. е. $v(i) = v(j_1)v(j_2)$, где $j_1, j_2 < i$. Соответствующую схеме конкатенации программу обозначим через C. Системой множеств $\mathcal{B} = \{B_{n,r} \,|\, n \in N, r \in R_n\}$ будем называть совокупность рекурсивных множеств, где $B_{n,r} \subset A^n$.

Будем называть программу P оптимальной относительно системы $\mathcal{B}$, если при $n \to \infty$

$$\max_{w \in B_{n,r}} K_P(w) \le (\log |B_{n,r}| + \log |R_n|)(1 + o(1)).$$

Через $\mathcal{M}_k$ обозначим систему, состоящую из множеств с ограниченными частотами подслов длины k. Основываясь на результатах работы [1] доказана

ТЕОРЕМА. Программа C оптимальна относительно систем $\mathcal{M}_k$.

Символьная последовательность v имеет максимальную P-сложность относительно системы $\mathcal{B}$, если для ее префиксов v^n длины n справедливо $v^n \in B_{n,r(v)}$ и $K_P(v^n) \sim \max_{w \in B_{n,r(v)}} K_P(w)$ при $n \to \infty$. В [2] построены последовательности максимальной C-сложности для системы $\mathcal{M}_1$.

Работа выполнена при финансовой поддержке Министерства образования, программа "Университеты России" (проект 04.01.199).

Список литературы

1. Потапов В. Н. Аддитивная сложность слов с ограничениями на состав подслов // Дискрет. анализ и исслед. операций. Сер. 1. — 2004. — Т. 11, № 1. — С. 52–78.

2. Потапов В. Н. О максимальной длине двоичных слов с ограниченной частотой единиц и без одинаковых подслов заданной длины // Дискрет. анализ и исслед. операций. Сер. 1. — 2004. — Т. 11, № 3. — С. 48–58.

ЛЕКСИКОГРАФИЧЕСКИЕ СХЕМЫ РЕШЕНИЯ МНОГОКРИТЕРИАЛЬНЫХ МНОГОИНДЕКСНЫХ ЗАДАЧ РАСПРЕДЕЛЕНИЯ ОДНОРОДНОГО РЕСУРСА В ИЕРАРХИЧЕСКИХ СИСТЕМАХ

М. Х. Прилуцкий (Нижний Новгород)

Рассматриваются задачи распределения ресурса в иерархических системах, элементы которых могут производить, передавать или потреблять однородный ресурс. Требуется определить такие объемы ресурса, которые удовлетворяют сегментным ограничениям элементов системы, и соответствуют экстремальным значениям критериев оптимальности. В рассматриваемых задачах критерии задаются в виде ступенчатых функций со значениями из множества p натуральных чисел. В наиболее общем виде задача распределения ресурса может быть поставлена следующим образом. Заданы булевы матрицы A и B размерностей $m \times k$ и $n \times k$, действительный неотрицательный m-мерный вектор $\overrightarrow{c}$ и векторная функция $\overrightarrow{F(\overrightarrow{y})}$, отображающая пространство R^n на множество вершин n-мерного p-ичного куба. Требуется найти вектор $\overrightarrow{x}$, удовлетворяющий ограничениям $A\overrightarrow{x} \le \overrightarrow{c}$ и минимизирующий функционал $\overrightarrow{F(B\overrightarrow{x})}$. Полученная задача является n-критериальной задачей с линейными ограничениями и критериями оптимальности, вид которых зависит от вида функции $\overrightarrow{F(B\overrightarrow{x})}$. Для каждой компоненты i рассмотрим совокупность вложенных друг в друга сегментов $S_i(t)$, $t = 1, 2, \ldots, p$, $S_i(t) \subseteq S_i(t+1)$, $i = 1, 2, \ldots, n$. Тогда i-ая компонента векторной функции $\overrightarrow{F(B\overrightarrow{x})}$ принимает значение t, если значение i-ой компоненты вектора $B\overrightarrow{x}$ принадлежит сегменту $S_i(t)$. Для решения поставленной задачи разработаны два алгоритма — алгоритм проверки на совместность системы ограничений $A\overrightarrow{x} \le \overrightarrow{c}$ (в общем случае он является модификацией релаксационного метода ортогональных проекций Агмона — Моцкина [1]) и алгоритм поиска оптимальной вершины n-мерного p-ичного куба для монотонной двоичной функции при заданном лексикографическом порядке.

Список литературы

1. Прилуцкий М. Х. Многокритериальное распределение однородного ресурса в иерархических системах // Автоматика и телемеханика. — 1996. — № 2. — С. 24–29.

УРАВНОВЕШЕННЫЕ РАЗБИЕНИЯ ГРАФОВ

К. Д. Протасова (Киев)

Пусть $Gr(V,E)$ — конечный связный граф с множеством вершин V и множеством ребер E. Для всех $x,y \in V$ обозначим $d(x,y)$ — длина кратчайшего пути между x и y. Для всякого $A \subseteq V$, $A \neq \emptyset$, $r \in \omega$, положим $B(x,r) = \{y \in V : d(x,y) \leq r\}$, $B(A,r) = \bigcup_{a\in A} B(a,r)$, и обозначим через $\mathrm{ind}A$ минимальное число $m \in \omega$ такое, что $B(A,m) = V$.

ОПРЕДЕЛЕНИЕ. Пусть $|V| = n$, $n = rs+t$, $0 \leq t < r$. Разбиение $V = V_1 \bigcup V_2 \bigcup ... \bigcup V_r$ называется уравновешенным, если $|V_1| = |V_2| = ... = |V_t| = s+1$, $|V_{t+1}| = |V_{t+2}| = ... = |V_r| = s$.

По теореме 1.2 из [1] для каждого натурального числа $r \leq n$, существует уравновешенное разбиение $V = V_1 \bigcup V_2 \bigcup ... \bigcup V_r$ такое, что $\mathrm{ind}V_i \leq r$ для каждого $i \in \{1,2,...,r\}$.

ТЕОРЕМА 1. Для каждого конечного связного графа $Gr(V,E)$, $|V| > 1$, существует уравновешенное разбиение $V = V_1 \bigcup V_2$ такое, что $\mathrm{ind}V_1 = 1$, $\mathrm{ind}V_2 \leq 2$.

ТЕОРЕМА 2. Пусть $Gr(V,E)$ — конечный связный граф и пусть r — натуральное число такое, что $|B(x,1)| \geq r$ для каждого $x \in V$. Тогда существует уравновешенное разбиение $V = V_1 \bigcup V_2 \bigcup ... \bigcup V_r$ такое, что $\mathrm{ind}V_i \leq 3$ для каждого $i \in \{1,2,...,r\}$.

ВОПРОС. Пусть $Gr(V,E)$ — конечный связный граф и пусть r — натуральное число такое, что $|B(x,1)| \geq r$ для каждого $x \in V$. Существует ли уравновешенное разбиение $V = V_1 \bigcup V_2 \bigcup ... \bigcup V_r$ такое, что $\mathrm{ind}V_i \leq 2$ для каждого $i \in \{1,2,...,n\}$?

Рассмотрим два варианта игры $G_1(Gr)$ и $G_2(Gr)$ по теореме 1. В обеих играх два игрока по очереди закрашивают вершины V, $|V| > 1$, черным и оранжевым цветом. Игры окончены, когда все вершины закрашены. Обозначим $V(I)$ и $V(II)$ множества черных и оранжевых вершин. Мы утверждаем, что второй игрок выигрывает на $G_1(Gr)$, если $\mathrm{ind}V(II) \leq 2$. Мы утверждаем, что первый игрок выигрывает на $G_2(Gr)$, если $\mathrm{ind}V(I) = 1$.

ТЕОРЕМА 3. Для каждого графа Gr второй игрок имеет выигрышную стратегию на $G_1(Gr)$.

Список литературы

1. Protasov I., Banakh T. Ball structures and coloring of graphs and groups // Mat. Stud. Monogr. Ser. — Lviv: VNTL, 2003.

МАТРОИДЫ И ЖЕСТКОСТЬ ПЛАНАРНЫХ ФЕРМ

А. М. Ревякин (Москва)

Известно, что квадратная планарная ферма с набором диагональных стержней жестка, если связен двудольный граф $G = (V,E)$ с множеством вершин $V = \{x_1,\ldots,x_k,y_1,\ldots,y_l\}$ в котором x_i и y_j соединены ребром, если в квадрате, соответствующему i-строке и j-столбцу, размещен диагональный стержень (см. [1]).

Жесткость ферм, получаемых из $k \times l$ квадратной решетки удалением $s \times u$ фрагмента $(s,u \geq 2)$, изучены в [1, 2]. В работе получены необходимые и достаточные условия для жесткости ферм с несколькими параллельными удаленными фрагментами. В частности, доказано, что для $k \times l$ квадратной решетки с двумя удаленными параллельными прямоугольными $s \times u$ фрагментами $(s,u \geq 2)$ добавление к ней $k+l+2s+2u-5$ диагональных стержней сделает ее жесткой тогда и только тогда, когда добавленное множество станет базой циклического матроида графа $G_{k,l,2s,2u}$ после присоединения к нему по одному ребру каждого нового цвета. Граф $G_{k,l,2s,2u}$ получается из двудольного графа заменой вершин $y_{t+i}, i = 1,\ldots,u$, тройкой вершин, а x_j, над которыми есть удаленные клетки, парой вершин. Копии вершины x_j соединяем новыми ребрами разного цвета в зависимости от номера удаленного фрагмента. Аналогично поступаем с первой и второй парами копий вершины y_{t+i}. Ребра между вершинами без копий оставляем прежними. Вершины x_i, лежащие до (соответственно, между и после) вершин с копиями, соединяем ребрами с первыми (соответственно, со вторыми и третьими) копиями вершин y_j.

Предложен алгоритм построения всех баз циклического матроида графа $G_{k,l,2s,2u}$ с таким свойством, основанный на свойствах матриц представления матроидов. Получены различные обобщения этого результата.

Список литературы

1. Recski A. Matroid theory and its applications in electric network theory and in statics. — Budapest: Akad. Kiado, 1989.

2. Ревякин А. М., Речки А. Жесткость планарных квадратных ферм с удаленными фрагментами // Материалы VIII Международного семинара «Дискретная математика и ее приложения» (2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 222–224.

ПОЛНОТА ОБЪЕКТНО-ДИНАМИЧЕСКОГО ЯЗЫКА ЗАПРОСОВ ODQL ДИНАМИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ DIM

В. С. Рублев, Д. В. Чехранов, А. Р. Юсупов (Ярославль)

Ввод в динамическую информационную модель DIM [1] объектно-динамического языка запросов ODQL [2, 3] позволил получить доступ к манипулированию с объектами DIM в течение периода жизни этих объектов. Для задания динамики объектов и классов в язык вводятся дополнительные конструкции. Полноту языка ODQL по доступу к данным объектов, по динамике объектов и классов выражают следующие утверждения.

ТЕОРЕМА 1. Для любых множеств связных классов DIM, связных объектов этих классов и свойств этих объектов существует запрос ODQL, который выделяет заданные множества объектов и их свойств.

ТЕОРЕМА 2. Для любых множеств классов DIM, связных объектов этих классов, идентификационных свойств этих объектов и любого допустимого изменения этих свойств существует запрос ODQL, который определяет такое изменение свойств, порождая новые объекты-последователи и связывая их со старыми объектами-предшественниками отношениями истории объектов.

ТЕОРЕМА 3. Для любого изменения классов DIM и связанных с ними допустимых изменений объектов существует последовательность запросов ODQL, приводящая к этим изменениям.

Список литературы

1. Рублев В. С., Дерябин В. О., Лобачев Д. И., Юсупов А.Р. Базовые отношения объектов баз данных и гибкие таблицы // Моделирование и анализ информ. систем. — Ярославль, 2002. — Т. 9, № 2. — С. 16–27.

2. Рублев В. С., Лобачев Д. И., Юсупов А. Р. Языки запросов объектной динамической информационной модели DIM // Математика: Материалы Всероссийской научной конференции, посвященной 200-летию Ярославского государственного университета им. П. Г. Демидова. — Ярославль, 2003. — С. 134–143.

3. Юсупов А. Р. Языки объектно-динамических запросов и решение проблем доступа к информации в динамической информационной модели DIM // Современные проблемы математики и информатики: Сборник научных трудов молодых ученых, аспирантов и студентов. — Ярославль, 2004. — Вып. 6. — С. 157–163.

ПОЛНОТА ДИНАМИЧЕСКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ DIM

В. С. Рублев, А. Р. Юсупов (Ярославль)

Концепция динамической информационной модели DIM [1, 2] основана на выделении базовых отношений между объектами системы и между классами системы (наследования, включения, выбора, идентификации, истории и взаимодействия) и определении на этой основе понятий класс DIM, объект DIM, тип объектов DIM. Эта система предназначена для описания разнообразных дискретных детерминированных моделей, возникающих в различных областях науки, экономики, производства, и описываемых дискретным множеством объектов при помощи некоторого конечного набора свойств и детерминированными законами изменения этих объектов при их взаимодействии. Динамика объектов, при которой может изменяться тип объектов плохо описывается современными типами СУБД, что подтверждает актуальность введения системы DIM. Уверенность в возможности реализовать в этой системе описание любой дискретной детерминированной модели дает следующая теореиа о полноте.

ТЕОРЕМА. Любая дискретная детерминированная модель может быть описана при помощи DIM.

Для доказательства этой теоремы приводится алгоритм пошагового построения классов, объектов и связей между классами и между объектами, который может быть положен в основу проектирования описания дискретной модели.

Список литературы

1. Дерябин В. О., Лобачев Д. И., Рублев В. С., Юсупов А. Р. Базовые отношения объектов баз данных и гибкие таблицы // Проблемы теоретической кибернетики. Тезисы докладов XIII Международной конференции (Казань, 27–31 мая 2002 г.). Часть I. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ, 2002. — С. 55.

2. Рублев В. С., Дерябин В. О., Лобачев Д. И., Юсупов А. Р. Базовые отношения объектов баз данных и гибкие таблицы // Моделирование и анализ информ. систем. — Ярославль, 2002. — Т. 9, № 2. — С. 16–27.

КОНСТАНТЫ ДЖЕКСОНА В ПРОСТРАНСТВЕ $l_2(\mathbb{Z}_q)$

Ю. Д. Рудомазина (Тула)

Пусть $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$ — циклическая группа, $x \in \mathbb{Z}_q$, $d(x) = \min\{x, q-x\}$, $l_2(\mathbb{Z}_q)$ — евклидово пространство четных функций f на $\mathbb{Z}_q$ с нормой $||f||_2 = \left(\frac{1}{q}\sum\limits_{x\in\mathbb{Z}_q}|f(x)|^2\right)^{1/2}$, $E_k(f)_2 = \min_{a_s}\left\|f(x) - \sum\limits_{s=0}^{k-1} a_s \cos\frac{2\pi s x}{q}\right\|_2$ — величина наилучшего приближения функции f порядка k в пространстве $l_2(\mathbb{Z}_q)$, $\omega(d, f)_2 = \max\{||f(x+y) - f(x)||_2 : d(y) \le d\}$ — ее модуль непрерывности, $D(d,k)_2 = \sup_{f\in l_2(\mathbb{Z}_q)} \frac{E_k(f)_2}{\omega(d,f)_2}$, $d, k = 1, \ldots, [q/2]$, — дискретные константы Джексона.

Вычислением констант Джексона в пространстве $l_2(\mathbb{Z}_q)$ занимались А. Г. Бабенко, В. И. Иванов, А. А. Тюрюканов. Точные значения были известны только в случаях, когда $k \mid q$.

Нами константы Джексона $D([q/2], k)_2$ найдены для всех $k = 1, \ldots, [q/2]$. Их вычисление основано на решении дискретной задачи Фейера о наибольшем значении четного дискретного тригонометрического полинома с фиксированным нулевым коэффициентом, полученном совместно с В. И. Ивановым.

Работа выполнена при финансовой поддержке РФФИ (проект 03-01-00647).

О СЛОЖНОСТИ РЕАЛИЗАЦИИ МУЛЬТИПЛЕКСОРНОЙ ФУНКЦИИ СХЕМАМИ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

П. В. Румянцев (Москва)

Изучается сложность реализации так называемой мультиплексорной функции алгебры логики (ФАЛ) $\mu_n(\tilde{x}_n, \tilde{y}_n)$ порядка n, имеющей n «адресных» булевых переменных (БП) $\tilde{x}_n$, 2^n «информационных» БП $\tilde{y}_n$. При этом ФАЛ μ_n на каждом наборе значений БП $\tilde{x}_n$ совпадает с той БП из $\tilde{y}_n$, номер которой в двоичной записи задается значениями «адресных» БП. Функция μ_n часто используется для разложения ФАЛ по переменным и ее оптимальная реализация в различных классах схем имеет как теоретическое, так и прикладное значение.

Рассматриваются стандартные базисы $B_1 = \{x_1 \& x_2, x_1 \vee x_2, \neg x_1\}$, и $B_2 = \{x_1 \& x_2, x_1 \oplus x_2, \neg x_1\}$, где вес каждого функционального элемента равен единице. Сложность реализации ФАЛ f схемами из функциональных элементов в базисе B_i, $i = 1, 2$, понимается обычным образом [1, 3] и обозначается через $L_i(f)$.

ТЕОРЕМА. Для $i = 1, 2$ и четного n выполняются неравенства:

$$2 \cdot 2^n + \frac{1}{3} \cdot 2^{n/2} + O(2^{n/4}) \le L_i(\mu_n) \le 2 \cdot 2^n + 2 \cdot 2^{n/2} + O(2^{n/4}),$$

а в случае нечетного n — неравенства

$$2 \cdot 2^n + 0,32 \cdot 2^{n/2} + O(2^{n/4}) \le L_i(\mu_n) \le 2 \cdot 2^n + \frac{3}{\sqrt{2}} \cdot 2^{n/2} + O(2^{n/4}).$$

Из данной теоремы следует, что сложность ФАЛ μ_n в рассматриваемых базисах равна $2 \cdot 2^n + \Omega(2^{n/2})$, т. е. устанавливаются асимптотические оценки сложности ее реализации с точностью до порядка и знака второго члена асимптотического разложения этой сложности.

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-01000).

Список литературы

1. Алексеев В. Б., Ложкин С. А. Элементы теории графов, схем и автоматов. — М.: Изд-во МГУ, 2000.

2. Коровин В. В. О сложности реализации универсальной функции схемами из функциональных элементов // Дискретная математика. — 1995. —Т. 7, вып. 2. — С. 95–102.

3. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. —М.: Изд-во МГУ, 1984.

О ПРОБЛЕМЕ ЭКВИВАЛЕНТНОСТИ СХЕМ ПРОГРАММ С КОНСТАНТАМИ

Д. М. Русаков (Москва)

В докладе рассматривается модель вычислений, объектами которой являются схемы программ с константами. Проблема включения для этой модели принадлежит к числу фундаментальных в проблематике теории алгебраических моделей программ [1].

Рассматриваемая нами модель аппроксимирует программы, построенные над конечным базисом операторов и булевых выражений и использующих все традиционные средства композиции операторов, кроме аппарата процедур. Спецификой рассматриваемой нами модели является то, что базису принадлежат операторы, которые любое состояние памяти преобразуют в некоторое фиксированное, присущее отдельному оператору; последний именуется константой.

Особое положение рассматриваемой модели в теории моделей программ заключается в том, что полугруппа ее операторов обладает циклами. Исследование проблемы включения в такой модели требует разработки методов, отличных от обычно практикуемых в теории моделей программ, ибо последние относятся к случаям, когда полугруппа операторов, используемых моделью, ациклична.

Основной результат состоит в том, что построен алгоритм, разрешающий проблему включения в рассматриваемой модели. Из него следует разрешимость в нем и проблемы эквивалентности.

Решение проблемы проводится путем ее сведения к разрешимым проблемам для конечных автоматов.

Работа выполнена при финансовой поддержке РФФИ (грант 03-01-00312).

Список литературы

1. Подловченко Р. И. От схем Янова к теории моделей программ // Математические вопросы кибернетики. Вып. 7. — М.: Физматлит, 1998. —- С. 281–302.

О СООТНОШЕНИИ КРОНЕКЕРОВЫХ СПЕКТРОВ БУЛЕВЫХ ФУНКЦИЙ В РАЗНЫХ БАЗИСАХ

Л. В. Рябец (Иркутск)

В работе [1] понятие спектра Рида—Маллера вводится как преобразование, переводящее СДНФ булевой функции f в СПНФ некоторой функции f^T. Такое преобразование является обратимым. С использованием операторного представления булевых функций удалось расширить понятие спектра Рида—Маллера и определить класс кронекеровых спектров [2]. Подробнее с операторными представлениями булевых функций можно познакомиться в [3]. В [2] показано, что кронекеров спектр f_g^K может быть определен одним оператором $\mathbf{a}$ и одной базисной функцией g. Также в [2] представлены способы нахождения спектров для различных операторов $\mathbf{a}$ при фиксированной базисной функции $g = x_1 \cdot \ldots \cdot x_n$. Следующие свойства позволили найти взаимосвязь спектров при различных базисных функциях.

ТЕОРЕМА. 1) $(\psi(f))_h^K = f_g^K$; 2) $\psi(f_g^K) = f_h^K$, где g и h — произвольные базисные функции, ψ — линейное преобразование операторных базисов, переводящее $\{\mathbf{a}^{\tilde{0}} g(\tilde{x}), \ldots, \mathbf{a}^{\tilde{1}} g(\tilde{x})\}$ в $\{\mathbf{a}^{\tilde{0}} h(\tilde{x}), \ldots, \mathbf{a}^{\tilde{1}} h(\tilde{x})\}$, $\mathbf{A} = (\mathbf{a}^{\tilde{0}}, \ldots, \mathbf{a}^{\tilde{1}})$ — двупорожденный пучок, построенный по оператору $\mathbf{d} \ldots \mathbf{d}$.

Работа выполнена при финансовой поддержке РФФИ (проект 04-07-90178в).

Список литературы

1. Stankovic R., Sasao T. A discussion on the history of research in the arithmetic and Reed-Muller expressions // IEEE Transactions on Computer Aided Design of Integrated Circuts and Systems. — 2001. — V. 20, № 9.

2. Винокуров С. Ф., Рябец Л. В. Свойства кронекеровых спектров булевых функций // Дискретные модели в теории управляющих систем: VI Международная конференция. — М, 2004. — С. 21–24.

3. Избранные вопросы теории булевых функций / Под ред. Винокурова С. Ф. и Перязева Н. А.— М.: Физматлит, 2001.— 192 с.

ДИНАМИЧЕСКАЯ СИСТЕМА n-МЕРНЫХ ДВОИЧНЫХ ВЕКТОРОВ

В. Н. Салий (Саратов)

Через $B^n, n > 1$, обозначается множество всех двоичных векторов размерности n. Определяемая динамическая система (B^n, δ) будет функционировать в дискретном времени. Пусть состоянием системы в данный момент времени является вектор $v \in B^n$. Тогда в следующий момент она окажется в состоянии $\delta(v)$, описываемом правилами: 1) если первой компонентой в v является 0, то первой компонентой в $\delta(v)$ будет 1; 2) если в составе v имеются диграммы (две соседние компоненты) 10, то в $\delta(v)$ каждая из них заменяется на 01; 3) если последней компонентой в v является 1, то последней компонентой в $\delta(v)$ будет 0; 4) других отличий между v и $\delta(v)$ нет.

Показано, что состояние (вектор) v недостижимо из других состояний тогда и только тогда, когда в составе v имеется хотя бы один из следующих фрагментов: 1) начальная диграмма 00, 2) тетраграмма 1100, 3) финальная диграмма 11. Получена формула для числа недостижимых состояний.

Система имеет единственный бассейн и аттрактор, представляющий собой двухэлементный цикл. Исследованы симметрии бассейна, вычислена удаленность вектора от аттрактора.

Установлен изоморфизм между системой B^n и динамической системой Γ_n ориентаций n-звенной цепи, где переход в следующее состояние осуществляется одновременным превращением всех стоков в источники (см. [1]). С использованием вышеупомянутых симметрий системы B^n подсчитывается количество неизоморфных ориентаций в Γ_n: оно равно 2^{n-1} при n нечетном и $2^{n-1} + 2^{n/2-1}$ при n четном.

Список литературы

1. Barbosa V. S. An atlas of edge-reversal dynamics. — London: Chapman & Hall CRC, 2001.

О СТРУКТУРЕ МНОЖЕСТВ, СВОБОДНЫХ ОТ СУММ

А. А. Сапоженко (Москва)

Предлагается обобщение теоремы 4 из [1]. Пусть $N = [1, n]$ — множество натуральных чисел, не превосходящих n, а N_r^k — подмножество тех $u \in N$, что имеют остаток r при делении на k. Множество $A \in N$ свободно от сумм, если оно не содержит троек чисел $\{a, b, c\}$, таких, что $a + b = c$. Семейство всех подмножеств множества N, свободных от сумм, обозначим через $S(n)$. Пусть $\mathcal{A}$ и $\mathcal{B}$ — два семейства подмножеств множества N. Скажем, что семейство $\mathcal{B}$ покрывает семейство $\mathcal{A}$, если для всякого $A \in \mathcal{A}$ существует $B \in \mathcal{B}$, такое, что $A \subseteq B$. Множества $B \in \mathcal{B}$ будем называть контейнерами, а семейство $\mathcal{B}$ — системой контейнеров для $\mathcal{A}$. Если $B \subseteq N$, то $B_{i,p} = B \cap [i, i+p-1]$. Положим $\hat{q} = \lfloor n^{3/4} \rfloor$ и $\widetilde{q} = \hat{q} \log_2 n$. Семейство $\mathcal{B}$ подмножеств множества N будем называть правильным, если для любого $1 \le k \le \log_2 n$ и $0 \le r < k$ выполнены следующие условия:

1) Для достаточно больших n и любого $B \in \mathcal{B}$

$$|B| \le n/2 + O(\hat{q}).$$

2) Для достаточно больших n

$$|\mathcal{B}| \le 2^{o(\hat{q})}.$$

3) Для любых $i \in [\widetilde{q}, n - \widetilde{q}]$, $p \in [\widetilde{q}, n - i]$

$$||B_{i,p}| - p/2| \le \hat{q}.$$

4) Для любых $r \in \{0, k-1\}$, $i \in [\widetilde{q}, n - \widetilde{q}]$ и $p \in [\widetilde{q}, n - i]$

$$||B_{i,p} \cap N_r^k| - p/2k| \le \hat{q}.$$

Правильное семейство $\mathcal{B}$ подмножеств множества N будем называть почти правильной системой контейнеров для $\mathcal{A}$, если она покрывает некоторое подсемейство $\mathcal{A}' \subseteq \mathcal{A}$, такое, что $|\mathcal{A} \setminus \mathcal{A}'| = o(2^{n/2})$.

ТЕОРЕМА. Семейство $S(n)$ обладает почти правильной системой контейнеров.

Работа выполнена при финансовой поддержке РФФИ (проект 04–01–00359).

Список литературы

1. Сапоженко А. А. Доказательство гипотезы Камерона—Эрдёша о числе множеств, свободных от сумм // Математические вопросы кибернетики. Вып. 12. — М.: Физматлит, 2003. — С. 5–14.

О КОНТРОЛЕ ПОМЕЧЕННЫХ ГРАФОВ ПРИ НЕИЗВЕСТНОЙ ВЕРХНЕЙ ОЦЕНКЕ ЧИСЛА ВЕРШИН

С. В. Сапунов (Донецк)

Рассматривается задача контроля конечного графа с помеченными вершинами с помощью блуждающего по нему агента (map validation problem) [1, 2]. В [2] рассматривалась проблема контроля таких графов при известной верхней оценке числа вершин. Задача контроля графов с помеченными вершинами при неизвестной верхней оценке числа вершин далека от разрешения. Одному из подходов к решению этой задачи посвящен данный доклад.

Обозначим $\mathcal{K}$ — множество всех конечных, инициально связных, детерминированных [2] графов над алфавитом меток A. Пусть $G \in \mathcal{K}$ и $\mathcal{G} = (G, E, M, \mu, g_0)$, где G — множество вершин, E — множество ребер, $M \subseteq A$ — множество меток, $\mu : G \to M$ — сюръективная функция разметки, g_0 — инициальная вершина. Для такого графа $L_{\mathcal{G}} = L_{g_0}$. Определим частичную операцию $\star : G \star M^+ \to G$ соотношением: для любых $g, g' \in G$, $w \in M^+$, $g \star w = g'$ тогда и только тогда, когда существует путь из вершины g в вершину g' с меткой w. С каждым графом $\mathcal{G} \in \mathcal{K}$ свяжем систему $\{R_{\mathcal{G}}, T_{\mathcal{G}}, Z_{\mathcal{G}}\}$, где $(ux, vx) \in R_{\mathcal{G}}$ точно тогда, когда $ux, vx \in L_{\mathcal{G}}$, $x \in M$ и $g_0 \star ux = g_0 \star vx$, $(ux, vx) \in T_{\mathcal{G}}$ точно тогда, когда $ux, vx \in L_{\mathcal{G}}$, $x \in M$ и $g_0 \star ux \neq g_0 \star vx$, и $wx \in Z_{\mathcal{G}}$ точно тогда, когда $w \in L_{\mathcal{G}}$, $x \in M$ и $wx \notin L_{\mathcal{G}}$

ТЕОРЕМА. $\mathcal{G} \cong \mathcal{H}$ тогда и только тогда, когда $\{R_{\mathcal{G}}, T_{\mathcal{G}}, Z_{\mathcal{G}}\} = \{R_{\mathcal{H}}, T_{\mathcal{H}}, Z_{\mathcal{H}}\}$, $(\mathcal{G}, \mathcal{H} \in \mathcal{K})$.

Предложен алгоритм контроля детерминированных графов с использованием указанных систем и одной дополнительной стираемой метки. Алгоритм аналогичен алгоритму, предложенному в [3] для контроля автоматных лабиринтов (т. е. ориентированных графов с помеченными дугами).

Список литературы

1. Dudek G., Jenkin M., Milios E., Wilkes D. Map validation and robot self-location in a graph-like world // Robotics and Autonomous Systems. — 1997. — V. 22, № 2. — P. 159–178.

2. Сапунов С. В. Контроль детерминированных графов // Труды ИПММ НАНУ. — 2003. — Т. 8. — С. 106–110.

3. Олейник Р. И. О контроле автоматных лабиринтов конечным автоматом // Труды ИПММ НАНУ. — 2000. — Т. 5. — С. 107–114.

РАЗНОСТНАЯ АППРОКСИМАЦИЯ КВАДРАТИЧНОЙ ЗАДАЧИ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ С МНОГОТОЧЕЧНЫМИ УСЛОВИЯМИ

Р. А. Сардарова (Баку)

Рассмотрим следующую задачу оптимального управления: минимизировать функционал

$$J(u) = \int_{t_0}^{T} |x(t,u) - y(t)|^2 \, dt, \tag{1}$$

при ограничениях

$$\dot{x} = A(t)x(t) + B(t)u(t) + f(t) \ , \quad t_0 \le t \le T, \tag{2}$$

$$\sum_{i=0}^{N} n_i x\left(t_{\alpha_i}\right) = A, \tag{3}$$

$$u \in U \left\{u = u(t) \in L_2^r[t_0, T] : u(t) \in V \ \ t \in [t_0, T], \right\}, \tag{4}$$

где $A(t)$, n_i, $\left(i = \overline{0, N}\right)$ — матрицы порядка $n \times n$, $B(t)$ — матрица порядка $n \times r$, $f(t), y(t)$ — n-мерные векторы; моменты времени $t_0 \le t_{\alpha_0} < t_{\alpha_1} < \cdots < t_{\alpha_N} \le T$ фиксированы; точка $B \in E^n$ задана, $\det\left(\sum\limits_{i=0}^{N} n_i\right) \neq 0$.

В данной работе исследована разностная аппроксимация задачи (1)–(4) с помощью методики [1] (см. гл. 3). Известно, что конечномерная аппроксимация задачи (1)–(4) приводит к последовательности конечномерных задач минимизации.

Найдены достаточные условия для сходимости решений последовательности конечномерных задач минимизации к решению исходной задачи (1)–(4) по функционалу и по аргументу (управлению).

Список литературы

1. Васильев Ф. П. Методы решения экстремальных задач. — М.: Наука, 1981.

О РЯДАХ КРАТНОСТЕЙ И КОМБИНАТОРНЫХ ХАРАКТЕРИСТИКАХ МНОГООБРАЗИЙ

И. Ю. Свиридова (Ульяновск)

Полиномиальная производящая функция

$$F_\nu(t_1,t_2,\dots)=\sum_{\lambda_1\geq\dots\geq\lambda_k>0} m_\lambda t_1^{\lambda_1}\dots t_k^{\lambda_k}$$

является эффективным инструментом работы с кохарактерами некоторого многообразия ν ассоциативных алгебр $\chi_n(\nu)=\sum_{\lambda\vdash n} m_\lambda\chi_\lambda$. Следуя [1], будем называть $F_\nu(t_1,t_2,\dots)$ рядом кратностей многообразия ν. Ряд кратностей является носителем важной информации о числовых характеристиках многообразий. Одну из таких числовых характеристик представляет собой показатель полиномиальной степени кратностей $\mathrm{mlt}(\nu)=\limsup\limits_{n\to\infty}\log_n m_n(\nu)$, где $m_n(\nu)=\max_{\lambda\vdash n} m_\lambda$.

Более удобную и компактную форму $H_\nu(s_1,s_2,\dots)$ ряд кратностей принимает в результате замены $t_1=s_1, t_i=s_i/s_{i-1}, i>1$. Все известные автору на настоящий момент ряды кратностей являются рациональными функциями, что говорит о наличии линейных рекуррентных соотношений между кратностями неприводимых модулей. Более того все эти ряды имеют вид $H_\nu=\frac{P(s_1,s_2,\dots)}{Q(s_1,\dots,s_k)}$, где $P(s_1,s_2,\dots)$ — полином, $Q(s_1,\dots,s_k)=\prod_{i=1}^k(1-s_i)^{\alpha_i}$, α_i — натуральные. Заметим, что в этом случае параметр $\mathrm{mlt}(\nu)$ совпадает с порядком полюса $z=1$ функции $\widehat{H}_\nu(z)=H_\nu(s_1,\dots,s_k)|_{s_1=\dots=s_k=z}$.

Работа выполнена при финансовой поддержке РФФИ (проект 04-01-00739-а) и научной программы "Развитие научного потенциала высшей школы".

Список литературы

1. Drensky V., Genov G. K. Multiplicities of Shur functions in invariants of two 3×3 matrices // J. Algebra. — 2003. — T. 264. — С. 496–519.

О ПРИБЛИЖЕНИИ ФУНКЦИЙ МНОГОЗНАЧНЫХ ЛОГИК ПОЛИНОМАМИ ОПРЕДЕЛЕННОГО РАНГА

С. Н. Селезнева (Москва)

Пусть $k\geq 2$, $E_k=\{0,1,\dots,k-1\}$. Функцией k-значной логики называется отображение $f^n: E_k^n\to E_k$, $n=0,1,\dots$. Множество всех функций k-значной логики обозначим через P_k, множество всех функций k-значной логики, зависящих от переменных $x_1,\dots,x_n$, обозначим через P_k^n.

Пусть $0\leq\delta\leq 1$. Для функции $f(x_1,\dots,x_n)$ функция $g(x_{i_1},\dots,x_{i_s})$, $0\leq s\leq n$, называется δ-приближением, если отношение числа наборов значений переменных $x_1,\dots,x_n$, в которых функции f и g различаются, к величине k^n не больше δ.

Произведение по mod k вида $x_{i_1}^{m_1}\cdot\dots\cdot x_{i_r}^{m_r}$, где переменные попарно различны и $1\leq m_1,\dots,m_r\leq k-1$, назовем мономом ранга r, константу 1 — мономом ранга 0. Полиномом назовем сумму по mod k попарно различных мономов с коэффициентами из $E_k\setminus\{0\}$. Рангом полинома назовем наибольший ранг его слагаемых. Константа 0 — полином ранга 0. Если число k простое, то каждую функцию k-значной логики можно однозначно записать полиномом.

Обозначим через $R_k^{n,r}$ множество всех полиномов, зависящих от переменных $x_1,\dots,x_n$, ранга не больше, чем r. Множество $R_k^{n,r}$ называют δ-приближением множества P_k^n, если для любой функции f из P_k^n найдется функция g из $R_k^{n,r}$, которая есть δ-приближение функции f. Заметим, что если множество $R_k^{n,r}$ есть δ-приближение множества P_k^n, то δ-приближением множества P_k^n также является и множество $R_k^{n,q}$ при $q>r$.

Множество $R_k^{n,r}$ назовем точным δ-приближением множества P_k^n, если оно является δ-приближением множества P_k^n, тогда как множество $R_k^{n,r-1}$ уже не является δ-приближением множества P_k^n.

Введем функцию $r_k^\delta(n)$: $r_k^\delta(n)=r$, если множество $R_k^{n,r}$ является точным δ-приближением множества P_k^n.

ТЕОРЕМА. Пусть число k простое. Тогда

1) $r_k^\delta(n)=0$, если $\delta\geq\frac{k-1}{k}$;

2) $r_k^\delta(n)\sim\frac{k-1}{k}\cdot n$ при $n\to\infty$, если $0<\delta<\frac{k-1}{k}$;

3) $r_k^\delta(n)=n$, если $\delta=0$.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, грант 03-01-00783.

КОПРЕДСТАВЛЕНИЕ ЧАСТИЧНЫХ АВТОМАТОВ

А. С. Сенченко (Славянск)

Пусть $A = (A, X, \delta_A, a_0)$ — автомат, у которого A — конечное множество состояний, X — множество входных символов, $\delta_A : A \times X \to A$ — (частичная) функция переходов и a_0 — начальное состояние. Через X^* обозначаем множество всех слов в алфавите X. Обозначим через $Dom\ \delta_A$ множество всех тех слов $p \in X^*$, для которых $\delta_A(a_0, p)$ определена, через $Codom\ \delta_A$ — дополнение $Dom\ \delta_A$ до X^*, а через $Codom_m\ \delta_A$ — множество минимальных по начальным отрезкам слов из $Codom\ \delta_A$. Пусть ρ_A — множество всех таких пар слов (p, q), что $p, q \in Dom\ \delta_A$ и $a_0 p = a_0 q$, а $\bar{\rho}_A = [\rho_A]$ — правоконгруэнтное замыкание ρ_A на X^*. Для автоматов A и B положим $(A, B) \in E$ точно тогда, когда $\bar{\rho}_A = \bar{\rho}_B$. Такие автоматы назовем подобными. Класс всех автоматов, подобных автомату A обозначим через $E(A)$.

Пару $\{\rho, M\}$, где ρ — бинарное отношение на $X^* \times X^*$, а M — подмножество множества X^* назовем системой. Система $\{\rho_A, Codom_m\ \delta_A\}$ однозначно определяет автомат A, так как ρ_A однозначно определяет $E(A)$, а $Codom_m\ \delta_A$ однозначно выделяет A из $E(A)$. Систему $\{\rho, M\}$ назовем копредставлением автомата A, если одновременно выполняются: 1) $[\rho] = \bar{\rho}_A$; 2) $W_\rho \subseteq Dom\ \delta_A$; 3) $[\rho](M) = Codom_m\ \delta_A$, где W_ρ — множество начальных отрезков всех слов из $pr_1\rho \cup pr_2\rho$ и $[\rho](M) = \bigcup\limits_{p \in M} [\rho](p)$ — срез бинарного отношения $[\rho]$ по M.

ТЕОРЕМА. Пусть система $\{\rho, M\}$ удовлетворяет условиям 1–3 для некоторого автомата A. Тогда система $\{\rho, M\}$ однозначно задает автомат A, причем $Dom\ \delta_A = X^* - [\rho](M) \cdot X^*$.

Найдено минимальное (каноническое) копредставление автомата A, построение которого аналогично построению канонической системы определяющих соотношений [1]. Найдены взаимосвязи между ρ и M при которых: 1) Существует автомат, для которого система $\{\rho, M\}$ является копредставлением. 2) Система $\{\rho, M\}$ является копредставлением некоторого конечного автомата. 3) Система $\{\rho, M\}$ является копредставлением фиксированного конечного автомата A.

Список литературы

1. Грунский И. С., Сенченко А. С. Свойства систем определяющих соотношений для автоматов // Дискретная математика. — 2004. — Т. 16, вып. 4. — С. 79–87.

ОБРАЩЕНИЕ ЭЛЕМЕНТА И ДЕЛЕНИЕ В КОНЕЧНОМ ПОЛЕ ХАРАКТЕРИСТИКИ 2 С ЛОГАРИФМИЧЕСКОЙ ГЛУБИНОЙ

И. С. Сергеев (Москва)

В настоящей работе обсуждаются связанные между собой задачи инвертирования и деления в конечных полях характеристики 2 в классе СФЭ (схем из функциональных элементов) в базисе всех двухвходовых булевых функций с глубиной, логарифмической по порядку относительно степени поля. Глубиной называется наибольшее для данной схемы количество элементов в одной цепочке, ведущей от входа к выходу.

В работах [1] и, затем, [2] показано, что обращение элемента может выполняться с глубиной порядка $O(\log n)$. Для сложности метода установлена полиномиальная оценка в форме $O(n^c)$. Ни константа c, ни мультипликативный коэффициент в оценке глубины авторами не оцениваются. По всей видимости, они достаточно велики. По крайней мере, $c \geq 4$. Нами получен следующий результат.

ТЕОРЕМА. Операция обращения элемента (деления) в поле порядка 2^n реализуется в классе схем двухвходовых функциональных элементов с глубиной $6.44 \log n + o(\log n)$ и сложностью $O(n^4)$; или со сложностью $O(m \cdot n^{2+\frac{2}{m}})$ и глубиной $(2m + 6.44) \log n + o(\log n)$, $m > 1$ — натуральный параметр.

Доказательство основывается на идее интерполяции с использованием вспомогательного поля небольшого порядка.

Работа выполнена при финансовой поддержке РФФИ, программы поддержки ведущих научных школ РФ (проект НШ-1807.2003.1), программы «Университеты России» (проект УР 04.02.528) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики» (проект «Оптимальный синтез управляющих систем»).

Список литературы

1. Davida G., Litow B. $O(\log n)$ parallel time finite field inversion // Proc. Aegean Workshop on Computing. — Lecture Notes in Computer Science. — Berlin, 1988. — V. 319. — P. 74–80.

2. von zur Gathen J. Inversion in finite fields using logarithmic depth // J. Symbolic Computation. — 1990. — V. 9. — P. 175–183.

РАСПРЕДЕЛЕНИЕ ЗНАЧЕНИЙ БУЛЕВОЙ ФУНКЦИИ НА ПОДПРОСТРАНСТВАХ

В. М. Сидельников (Москва)

Пусть $f : \mathbb{F}_2^n \to \mathbb{F}_2$ — булева функция и L — подпространство размерности m пространства $\mathbb{F}_2^n$, $0 < m \le n$. Положим

$$\lambda_L(f) = \sum_{\boldsymbol{x}\in L}(-1)^{f(\boldsymbol{x})}, \quad \Lambda_{m,n}(f) = \max_{L\subset\mathcal{L}_{m,n}} |\lambda_L(f)|,$$

где $\mathcal{L}_{m,n}$ — множество всех подпространств размерности m в F_2^n. Величина $\Lambda_{m,n}(f)$ характеризует наибольшее отклонение от 2^{m-1} числа значений, равных 1, которые принимают ограничения функции f на всевозможных подпространствах размерности m пространства F_2^n. Определение $\Omega_{m,n}(f)$ похоже на определение $\Lambda_{m,n}(f)$. Пусть $\boldsymbol{a} \in \mathbb{F}_2^n$ и

$$\lambda_{L+\boldsymbol{a}}(f) = \sum_{\boldsymbol{x}\in L}(-1)^{f(\boldsymbol{x}+\boldsymbol{a})}, \quad \Omega_{m,n}(f) = \max_{L\subset\mathcal{L}_{m,n},\,\boldsymbol{a}\in\mathbb{F}_2^n} |\lambda_{L+\boldsymbol{a}}(f)|.$$

Величина $\Omega_{m,n}(f)$ характеризует наибольшее отклонение от 2^{m-1} числа значений, равных 1, принимаемых ограничениями функции f на всевозможных смежных классах по всевозможным подпространствам размерности m пространства $\mathbb{F}_2^n$. Ее мы называем *аффинной m-устойчивостью функции f*.

Очевидно, что $0 \le \Lambda_{m,n}(f) \le \Omega_{m,n}(f) \le 2^m$. Заметим, что величины $\Lambda_{m,n}(f)$ и $\Omega_{m,n}(f)$ не зависят от выбора базиса пространства $\mathbb{F}_2^n$, в котором мы рассматриваем функцию f.

Функции f с небольшим значением $\Lambda_{m,n}(f)$ или $\Omega_{m,n}(f)$ используются в криптографии.

ЛЕММА. Выполняется равенство

$$\lambda_L(f) = \frac{1}{|L^\perp|}\sum_{\boldsymbol{a}\in L^\perp}\widehat{f}_{\boldsymbol{a}},$$

где $\widehat{f}_{\boldsymbol{a}} = \sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{\langle\boldsymbol{x},\boldsymbol{a}\rangle+f(\boldsymbol{x})}$ — коэффициент Уолша—Фурье функции f.

ТЕОРЕМА 1. Справедливы соотношения

$$\Lambda_{n-1,n} \ge \sqrt{\frac{2^{2n-2}-4}{2^n-1}} \sim 2^{\frac{n-2}{2}},\ n\to\infty.$$

ТЕОРЕМА 2. Пусть $m = n-\omega$, $n\to\infty$, $\omega = o(\sqrt{n}) \ge 1$. Тогда

$$\Lambda_{m,n} \gtrsim 2^{\frac{n}{2}-\omega}\sqrt{(2^\omega-1)}.$$

О ПОДОБИИ МАТРИЦ ВТОРОГО ПОРЯДКА НАД КОЛЬЦОМ ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ

С. В. Сидоров, В. Н. Шевченко (Нижний Новгород)

В линейной алгебре хорошо изучена задача о подобии матриц над полем F (см., например, [1]). Матрицы A и B называются подобными, если существует невырожденная матрица S такая, что $AS = SB$. Ранее авторами была изучена задача о подобии матриц над кольцом Z целых чисел.В данной работе рассматривается аналогичная задача над кольцом $Z[i]$ целых гауссовых чисел. Обозначим через $Z[i]^*$ множество делителей единицы кольца $Z[i]$, т. е. $Z[i]^* = \{\pm1, \pm i\}$.

ОПРЕДЕЛЕНИЕ 1. Будем говорить, что матрица $B\in Z[i]^{n\times n}$ подобна матрице $A\in Z[i]^{n\times n}$ над кольцом $Z[i]$, если существует $S\in Z[i]^{n\times n}$ такая, что $AS = SB$ и $\det S \in Z[i]^*$ и обозначать это $A\sim B$.

Далее мы ограничимся рассмотрением матриц второго порядка. Будем считать, что матрицы A и B имеют одинаковый характеристический многочлен $d(\lambda)$ (нетрудно заметить, что это необходимое условие подобия). Если $d(\lambda)$ приводим над $Z[i]$, то верны следующие теоремы.

ТЕОРЕМА 1. Пусть $d(\lambda)$ приводим над $Z[i]$ и имеет кратный корень α. Тогда множество матриц с таким $d(\lambda)$ распадается на счетное число классов эквивалентности $L_k(\alpha)$ с канонической матрицей $R_k(\alpha) = \begin{pmatrix} \alpha & k \\ 0 & \alpha \end{pmatrix}$, где $k = u + iv \in Z[i]$, причем $u > 0, v > 0$ или $u \ge 0, v = 0$.

ОПРЕДЕЛЕНИЕ 2. Обозначим через $K(u + iv)$ множество целочисленных точек, лежащих внутри квадрата с вершинами $(0,0)$, (u,v), $(-v,u)$, $(u-v,u+v)$ и на двух его смежных сторонах, содержащих вершины $(0,0)$, (u,v), $(u-v,u+v)$.

ТЕОРЕМА 2. Пусть $d(\lambda)$ приводим над $Z[i]$ и имеет различные корни α и β (можно считать, что $\beta - \alpha = m + in$, причем $n \ge 0$, а если $n = 0$, то $m > 0$). Тогда:

1) Множество матриц с таким $d(\lambda)$ распадается на конечное число $(J(\alpha,\beta))$ классов эквивалентности $L_k(\alpha,\beta)$ с канонической матрицей $R_k(\alpha,\beta) = \begin{pmatrix} \alpha & k \\ 0 & \beta \end{pmatrix}$, где $k\in K(\frac{m}{2} + i\frac{n}{2})$.

2) Если $m \equiv 0(\mathrm{mod}\ 2)$, $n \equiv 0(\mathrm{mod}\ 2)$, то $J(\alpha,\beta) = (m^2+n^2)/4+2$.
Если $m + n \equiv 1(\mathrm{mod}\ 2)$, то $J(\alpha,\beta) = (m^2+n^2+3)/4$.
Если $m \equiv 1(\mathrm{mod}\ 2)$, $n \equiv 1(\mathrm{mod}\ 2)$, то $J(\alpha,\beta) = (m^2+n^2+6)/4$.

Список литературы

1. Гантмахер Ф. Р. Теория матриц. — М.: Наука, 1967.

ДВАЖДЫ НЕПРЕРЫВНО-ДИФФЕРЕНЦИРУЕМЫЕ S-СПЛАЙНЫ

Д. А. Силаев (Москва)

Построены дважды непрерывно дифференцируемые S-сплайны, состоящие из полиномов четвертой и пятой степени, доказаны теоремы существования и единственности, установлены условия устойчивости и сходимости таких сплайнов.

Рассмотрим на отрезке $[a,b]$ равномерную сетку $\{x_k\}_{k=0}^{k=K}$, $x_k = a+kh$, h — шаг сетки. Рассмотрим на $[a,b]$ ещё одну равномерную сетку $\{\xi_l\}_{l=0}^{l=L}$, $\xi_l = a+lH$, $H = mh, m \in Z$. Пусть $y = (y_0, y_1, \ldots, y_K) \in \mathbb{R}^{K+1}$, $y_0', y_0'' \in \mathbb{R}$,

$$P_S^n = \left\{ u : u(x) = a_0 + a_1 x + a_2 x^2 + \textstyle\sum_{j=3}^{n} a_j x^j \right\}$$

— множество полиномов степени n с фиксированными коэффициентами a_0, a_1, a_2. Рассмотрим функционал $\Phi^l(u) = \sum_{k=0}^{M} (u(\xi_l + kh) - y_{ml+k})^2$. В P_S^n ищется такой полином $g_l(x)$, который минимизирует Φ^l и удовлетворяет следующим условиям:

$$a_0^0 = y_0,\ a_1^0 = y_0',\ a_2^0 = y_0'',$$

$$a_0^l = g_{l-1}(\xi_l - \xi_{l-1}) = g_{l-1}(H),\quad a_1^l = g_{l-1}'(H), a_2^l = g_{l-1}''(H).$$

Последние условия есть условия гладкой склейки двух последовательных полиномов.

S-сплайном назовем функцию $S_{m,M}^n(x)$, которая совпадает с полиномом $g_l(x)$ на отрезке $\xi_l \le x < \xi_{l+1}$. Здесь $n = 4$ или 5. В случае $n = 5$ доказана следующая

ТЕОРЕМА. Пусть $f(x) \in \mathbf{C}^6[a,b]$ и пусть выполнены предположения:

$$|f(x_k) - y_k| \le Ch^{6+\varepsilon},\quad |f'(0) - y_0'| \le Ch^{5+\varepsilon},\quad |f''(0) - y_0''| \le Ch^{4+\varepsilon},$$

где константа C не зависит от h. Пусть, кроме того, выполнены условия, обеспечивающие устойчивость. Тогда сплайн $S_{m,M}^5(x)$ с узлами на равномерной сетке $\xi_l = a + lH$ имеет дефект три (т. е. $S_{m,M}^5(x) \in \mathbf{C}^2[a,b]$) и для $x \in [a,b]$ справедливы следующие оценки:

$$\left| f^{(p)}(x) - S_{m,M}^{(p)}(x) \right| \le C_p h^{6-p},\quad p = 0,1,2,3,4,5.$$

В работе принимал участие студент ВМК С. В. Прощин.

Список литературы

1. Силаев Д. А., Якушина Г. И. Приближение S-сплайнами гладких функций // Труды семинара имени И. Г. Петровского. Вып. 10. — М.: Изд-во МГУ, 1984. — С. 197–206.

ПРИМЕНЕНИЕ S-СПЛАЙНОВ ДЛЯ РЕШЕНИЯ КРАЕВЫХ ЗАДАЧ

Д. А. Силаев, Д. О. Коротаев (Москва)

S-сплайн — это кусочно-полиномиальная функция, первые коэффициенты которой определяются условиями гладкой склейки, а все остальные — методом наименьших квадратов. Это обеспечивает их свойство сглаживать исходную информацию. Особенностью таких сплайнов является их полулокальность, т. е. каждый полином неявно зависит от тех значений функции, которые участвуют в определении предыдущих полиномов и не зависят от значений функции, определяющих последующие полиномы. S-сплайн на круге определяется как комбинация периодического S-сплайна по φ и непериодического по r, S-сплайн на квадрате определяется как комбинация непериодических S-сплайнов по x и y. В случае гладких функций в [1, 2] были доказаны теоремы существования, получены оценки скорости сходимости S-сплайнов и их производных. S-сплайн может быть представлен как линейная комбинация базисных S-сплайнов (BS-сплайнов). BS-сплайн строится как S-сплайн по таблице, в которой лишь одно значение равно единице, а остальные равны нулю. Представление S-сплайна в виде линейной комбинации BS-сплайнов также позволило применить S-сплайны для получения квадратурных формул 4-го порядка и для решения дифференциальных уравнений. Для этого мы рассматриваем произвольную линейную комбинацию базисных S-сплайнов; далее применяется метод Ритца (или метод Галеркина), результатом которого является система линейных уравнений на коэффициенты в линейной комбинации. Эта система замыкается граничными условиями. Сходимость данного метода обусловлена сходимостью S-сплайнов к приближаемой функции. Таким образом, был получен 4-й порядок сходимости. Особенностью данного метода является то, что он может применяться на областях с негладкой границей.

Список литературы

1. Силаев Д. А., Якушина Г. И. Приближение S-сплайнами гладких функций // Труды семинара имени И. Г. Петровского. Вып. 10. — М.: Изд-во МГУ, 1984. — С. 197–206.

2. Амилющенко А. В., Лукьянов А. И., Силаев Д. А. Применение сплайна для приближения гладких периодических функций // Вестник Московского университета. — 1996. — Сер. 1, № 6. — С. 22–25.

ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ ДВУМЯ FIFO-ОЧЕРЕДЯМИ НА БЕСКОНЕЧНОМ ВРЕМЕНИ

А. В. Соколов, А. В. Тарасюк (Петрозаводск)

Пусть в памяти размера n мы хотим работать с двумя циклическими последовательными FIFO-очередями [1]. Известны вероятности включения и исключения элементов в очереди, время дискретно, в каждый момент времени возможно обращение только к одной из очередей.

В [2] была рассмотрена задача определения оптимальных размеров памяти, выделяемой каждой из очередей, если в качестве критерия оптимальности выбрано среднее время до переполнения одной из очередей. В некоторых случаях организации работы очередей, например, в сетевых маршрутизаторах [3], при переполнении очереди процесс не завершается, а элементы (пакеты), которые должны включаться в переполненную очередь, просто теряются. Таким образом, возникает задача оптимального разбиения памяти между очередями, когда целью оптимизации является минимизация доли потерянных пакетов на бесконечном времени.

Предложен алгоритм нумерации состояний процесса, доказана теорема, которая определяют вид матрицы переходных вероятностей соответствующей регулярной цепи Маркова [4, 5], разработан алгоритм решения задачи, приводятся результаты численных экспериментов.

Список литературы

1. Кнут Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы. — М.: Вильямс, 2001.

2. Соколов А. В., Тарасюк А. В. Об оптимальном управлении циклическими очередями // Труды Института прикладных математических исследований КарНЦ РАН. — 2001. — Вып. 3. — С. 190–195.

3. Inside Cisco IOS Software Arcitecture. Vijay Bollaparagada, Curtis Murphy, Russ White. Indianapolis: Cisco Press, 2000. — IN 46290 USA.

4. Кемени Дж., Снелл Дж. Конечные цепи Маркова. — М.: Мир, 1970.

5. Феллер В. Введение в теорию вероятностей и ее приложения. — М.: Наука, 1984.

ОПИСАНИЕ СЛУЧАЙНЫХ БЛУЖДАНИЙ СО СКАЧКАМИ НА МЕСТЕ

Л. А. Соловьева (Иркутск)

Рассматриваются случайные блуждания частицы по целочисленным точкам правой полуплоскости. Частица выходит из начала координат и способна перемещаться скачками в дискретные моменты времени t, $t{=}\overline{0,\infty}$. Если частица к моменту $t{=}n$ находится в точке с координатами (i,j), то к моменту времени $t{=}n{+}1$ она окажется в точке $(i{+}1, j{+}x)$ с вероятностью $p_i^{(x)}$ $x=\overline{0,m}$; в точке $(i{+}1, j{-}y)$ с вероятностью $p_i^{(-y)}$ $y=\overline{1,s}$ или останется на месте с вероятностью $q_i^{(0)}$, причем

$$\sum_{x=0}^{m} p_i^{(x)} + q_i^{(0)} + \sum_{y=1}^{s} p_i^{(-y)} = 1,$$

где $i=\overline{1,\infty}$, $m=\overline{1,\infty}$, $s=\overline{1,\infty}$, $n=\overline{0,\infty}$.

Обозначим $P_n(i,j)$ — вероятность попадания частицы за n шагов в точку с координатами (i,j), где $i=\overline{0,n}, j=\overline{-ns,nm}$. Нетрудно записать рекуррентное соотношение:

$$P_n(i,j){=}\sum_{x=0}^{m} p_{i-1}^{(x)} P_{n-1}(i{-}1, j{-}x){+}q_i^{(0)} P_{n-1}(i,j){+}\sum_{y=1}^{s} p_{i-1}^{(-y)} P_{n-1}(i{-}1, j{+}y).$$

Очевидно, что $P_i(i,j)$ — вероятность попадания частицы за i шагов в точку с координатами (i,j) для случайного блуждания без скачков на месте.

ТЕОРЕМА. Для вышеописанного случайного блуждания справедливо соотношение:

$$P_n(i,j) = A_i^n \cdot P_i(i,j),$$

где A_i^n — обобщенные числа Стирлинга второго рода (см., напр., [1]), построенные на базе $\left\{q_i^{(0)}\right\}_{i=0}^{n}$, где $i=\overline{1,n}$, $j=\overline{-is,im}$, $n=\overline{0,\infty}$.

Зависимость вероятности $P_n(i,j)$ от $q_\nu^{(0)}$ и $p_\nu^{(x)}$, $\nu=\overline{0,n}$, в полученной формуле разделена: зависимость от $q_\nu^{(0)}$ полностью сосредоточена в коэффициенте A_i^n, а зависимость от $p_\nu^{(x)}$ — в вероятности $P_i(i,j)$.

Список литературы

1. Платонов М. Л. Комбинаторные числа класса отображений и их приложения. — М.: Наука, 1979. — 152 с.

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ СТРУКТУРНОЙ СВЯЗНОСТИ ГИПЕРГРАФОВ

Ю. А. Сушков, Д. Н. Егоров (Санкт-Петербург)

Структурная связность была впервые введена в работе [1] и практически применяется для синтеза многорежимных систем со структурным управлением, в частности для выбора оптимальных схем сочетания трёхзвенных дифференциалов в механических коробках передач.

Задача определения структурной связности гиперграфа "в лоб" обладает экспоненциальной сложностью, что является основной трудностью применения теории гиперграфов, описанной в работе [1], на практике.

В работе предложен новый подход к определению структурной связности, основанный на алгоритме определения максимального паросочетания на матрицах инциденций гиперграфов, представляющих многорежимные системы с двумя степенями свободы. Разработанный алгоритм позволяет с вероятностью, близкой к единице, установить, связен гиперграф или нет за полиномиальное время.

Для сравнения представлен усовершенствованный, в общем случае экспоненциальный, алгоритм, в большинстве реальных случаев решающий задачу определения структурной связности за полиномиальное время [2].

Работа выполнена при финансовой поддержке РФФИ – ГФЕН Китая 2004 (проект 04-01-39002ГФЕН2004а).

Список литературы

1. Сушков Ю. А. Связность в гиперграфах и матроидах // Исследование операций и статистическое моделирование. Вып. 6. — 1994. — С. 111–138.

2. Егоров Д. Н., Митропольский А. В. Гиперграфы и синтез многорежимных систем со структурным управлением // Молодые учёные промышленности Северо-Западного Региона. Материалы семинаров политехнического симпозиума (Санкт-Петербург, май-июнь 2004 г.). — С-Пб.: Изд-во СПбГПУ, 2004. — С. 32.

О СИНТЕЗЕ УНИВЕРСАЛЬНОГО ПЕРЕЧИСЛИТЕЛЯ ДЛЯ КЛАССА АВТОМАТОВ БЕЗ ПОТЕРИ ИНФОРМАЦИИ

А. А. Сытник, Н. С. Вагарина (Саратов)

Обозначим через $\Im_n$ класс автоматов с n состояниями, моделирующих поведение систем без потери информации. Пусть дана автоматная подстановка $\delta_1 = (0, 1, 2, \ldots, n-1)$ и i_1 и i_2 — номера двух различных состояний из этого цикла. Назовем расстоянием $\overline{i_1 i_2}$ между состояниями s_{i_1} и s_{i_2} в подстановке δ_1 наименьшее целое число между 0 и $n-2$, такое, что $i_1 + \overline{i_1 i_2} \equiv i_2 (\mathrm{mod}\ n)$. Наибольший общий делитель целых чисел $a_1, a_2, \ldots, a_k$, $k \geq 2$, обозначим через $D(a_1, a_2, \ldots, a_k)$.

ТЕОРЕМА 1. Пусть дан КДА $M = (S, X, \delta)$ с множеством состояний $S = (0, ..., n-1)$, где n четно, $n \geq 4$, и три его различных состояния $s_{i_1}, s_{i_2}, s_{i_3}$. Необходимым и достаточным условием того, чтобы автомат M с функцией переходов, реализуемой подстановками вида $\delta_1 = (0, 1, 2, \ldots, n-1)$ и $\delta_2 = (s_{i_1}, s_{i_2}, s_{i_3})$, был универсальным для автоматов из класса $\Im_n$, является равенство $D(\overline{i_1 i_2}, \overline{i_2 i_3}, n-1) = 1$.

ТЕОРЕМА 2. Пусть дан КДА $M = (S, X, \delta)$ с множеством состояний $S = (0, ..., n-1)$, где n четно, $n \geq 3$. Пусть S_m — некоторое состояние автомата M и i_1, i_2, i_3 — номера состояний автомата M, такие, что, по крайней мере, одно из них меньше или равно m, и одно больше m. Необходимым и достаточным условием того, чтобы автомат M с функцией переходов, реализуемой подстановками вида $\delta_1 = (0, 1, 2, \ldots, s_m)(s_{m+1}, s_{m+2}, \ldots, n-1)$ и $\delta_2 = (s_{i_1}, s_{i_2}, s_{i_3})$, был универсальным перечислителем для автоматов из класса $\Im_n$, является равенство $D(m, n-1-m, d) = 1$, где d — абсолютное значение разности номеров тех состояний из s_{i_1}, s_{i_2} и s_{i_3}, которые содержатся в одном и том же цикле автоматной подстановки δ_1.

УНИВЕРСАЛЬНЫЕ АВТОМАТЫ С ОБОБЩЕННЫМИ ХАРАКТЕРИСТИКАМИ

А. А. Сытник, К. П. Вахлаева (Саратов)

Для семейства автоматов $\{A_i = (S_i, X, \delta_i)\}_{i \in I}$ введем в рассмотрение новый объект, названный пучком автоматов.

ОПРЕДЕЛЕНИЕ. Пусть задано конечное семейство конечных детерминированных автоматов (КДА) $\{A_i\}_{i \in I}$ таких что $\forall\, i \in I \quad A_i = (S_i, X, \delta_i)$. Конечный детерминированный автомат $A_I = (S_I, X, \delta_I)$ типа $< 0, t_2 >, t_2 = |\, I\,| > 1$, с отображением δ_I вида $\delta_I : S_I \times X \to S_I$, где $\delta_I = \bigcup\limits_{k=1}^{t_2} \delta_{i_k}$, $\delta_I(s(t), x(t)) = \delta_{i_k}(s(t), x(t)) = s(t + t_2)$, и системой равенств $S(t, t + t_2 - 1, \overline{s})$, $\overline{s} \in F_{S_I}^{t_2}$, $F_{S_I}^{t_2} = \{\, \overline{s} \,|\ \ |\overline{s}| = t_2 \ \&\ \overline{s} \in \bigcup\limits_{\xi=1}^{t_2!} P_\xi(\overset{t_2}{\underset{i=1}{\times}} S_i)\,\}$, которая определяется следующим образом: $s(t + k - 1) = pr_k \overline{s}$, где $pr_k \overline{s} \in S_{i_k}$, $i_k \in I$, $k = \overline{1, t_2}$, будем называть пучком автоматов для семейства $\{A_i\}_{i \in I}$. $P_\xi(\overset{t_2}{\underset{i=1}{\times}} S_i)$ — некоторая перестановка сомножителей в декартовом произведении $\overset{t_2}{\underset{i=1}{\times}} S_i$ множеств состояний автоматов семейства, $\xi = \overline{1, t_2!}$

ТЕОРЕМА. Пусть задано конечное семейство КДА $\{A_i\}_{i \in I}$, где для каждого $i \in I \quad A_i = (S_i, X, \delta_i)$. Тогда существует универсальный относительно семейства $\{A_i\}_{i \in I}$ конечный детерминированный автомат $A_I = (S_I, X, \delta_I)$ типа $< 0, t_2 >$, который моделирует поведение любого автомата A_{i_k}, $k = \overline{1, t_2}$, $i_k \in I$, в моменты времени $t + k - 1 + l \cdot t_2$, $l = 0, 1, \ldots$.

Теорема решает задачу синтеза универсального автомата A_I для некоторого класса $\{A_i\}_{i \in I}$ и определяет временную организацию моделирования поведения автоматов семейства универсальным автоматом.

Список литературы

1. Сытник А. А. Восстановление поведения сложных систем. — Саратов: Изд-во Сарат. ун-та, 1992. — 192 с.

2. Твердохлебов В. А. Логические эксперименты с автоматами. — Саратов: Изд-во Сарат. ун-та, 1988. — 184 с.

КОНЕЧНЫЕ АВТОМАТЫ И АНАЛИЗ ИХ ГЕОМЕТРИЧЕСКИХ ОБРАЗОВ

В. А. Твердохлебов (Саратов)

Дискретные динамические системы в форме конечных детерминированных автоматов задаются рекурсивно начальным состоянием и правилами, определяющими следующий такт функционирования по результату предшествующего такта функционирования. При этом входные сигналы прикладываемой последовательности распределяются по тактам в абстрактном времени. Рекурсивный характер задания функционирования представлен действиями с таблицами, матрицами, диаграммами Мура, логическими уравнениями и т.п. Имеются формы неявного и неоднозначного задания автоматов автоматными отображениями, допускаемыми множествами входных слов или перечисляемых выходных слов. Для анализа и выявления свойств поведения автомат в целом, на всем множестве входных последовательностей, указанные способы задания автоматов недостаточны. Например, для определения свойств поведения автомата после 1000 тактов функционирования требуется такое же число шагов рекурсивных вычислений. Для исключения полной рекурсии в 1994 году предложено и по настоящее время разрабатывается задание законов функционирования автомата геометрическими фигурами. Разработаны методы построения, анализа и распознавания геометрических образов автоматов (см., например, работу [1] и список литературы к ней). Введены два варианта дискретных словарных геометрий Г0 и Г1 и рассмотрено их изоморфное вложение в целочисленную геометрию Г2. Найдены критерии для выделения во множествах фигур в геометриях Г0, Г1 и Г2 геометрических образов автоматов. Разработаны методы построения автоматов по геометрическим фигурам и определения классов эквивалентных состояний по геометрическому образу (без явного определения автомата). Исследован вопрос рекуррентного представления геометрических образов автоматов функциями k-значной логики. Для дискретных словарных Г0 и Г1, а также числовой Г2 геометрий рассмотрены варианты вложения дискретных структур, с использованием которых можно представлять "непрерывность" (по Р. Арбибу) траекторий состояний, специфические свойства требующихся траекторий и свойства процессов функционирования автоматов. Изучены периодические геометрические образы автоматов.

Список литературы

1. Твердохлебов В. А. Построение и анализ геометрических образов конечных автоматов // Проблемы точной механики и управления. Сб. научных трудов ИПТМУ РАН. — Саратов, 2002. — С. 94–100.

О ЛИНЕАРИЗАЦИОННЫХ МНОЖЕСТВАХ

Н. Е. Тимошевская (Томск)

В связи с исследованием криптографических свойств дискретных функций, обеспечивающих стойкость криптосистем, в которых они применяются, к линеаризационной атаке, возникает ряд важных задач о линеаризационных множествах.

Обозначим $M(X)$ множество всех покрытий конечного множества X.

ОПРЕДЕЛЕНИЕ 1. Подмножество $L \subseteq X$ называется *линеаризационным* множеством покрытия $B \in M(X)$, если $\forall Y \in B$ справедливо неравенство $|Y - L| \leq 1$.

ТЕОРЕМА 1. Задача построения линеаризационного множества с наименьшей мощностью для произвольного покрытия в $M(X)$ является NP-трудной.

ОПРЕДЕЛЕНИЕ 2. *Графическим представлением* покрытия $B \in M(X)$ назовем граф $G(B) = (V, E)$ такой, что $V = X$ и $\{u, v\} \in E$, если и только если существует $Y \in B$ такое, что $u \in Y$ и $v \in Y$.

ТЕОРЕМА 2. Если в графе $G(B)$ есть клика мощности k, то мощность любого линеаризационного множества покрытия B не меньше $k - 1$.

ТЕОРЕМА 3. Если $G(B)$ является полным двудольным графом $K_{t,m}$, то всякое кратчайшее линеаризационное множество для B имеет мощность $\min(t, m)$.

ТЕОРЕМА 4. Если граф $G(B)$ состоит из r компонент связности $G_1, \ldots, G_r$ и для каждого $i = 1, \ldots, r$ в G_i есть клика мощности k_i, то для покрытия B не существует линеаризационного множества мощности меньше $\sum_{i=1}^{r} k_i - r$.

Теоремы 2, 3, 4 позволяют разрабатывать алгоритмы построения покрытий с линеаризационными множествами ограниченной снизу мощности, которые в свою очередь можно использовать для синтеза алгебраических нормальных форм дискретных функций, не имеющих линеаризационных множеств переменных малой мощности. Именно такие функции необходимы для обеспечения высокого уровня стойкости основанных на них криптосистем.

Работа выполнена при финансовой поддержке Минобразования России (проект 34085).

РАСПОЗНАВАНИЕ ДЕТЕРМИНИРОВАННЫХ ГРАФОВ КОНЕЧНЫМИ АВТОМАТАМИ С КРАСКАМИ

М. Ю. Тихончев (Димитровград)

Рассматривается класс $K(M)$ всех конечных простых (т. е. без петель и кратных ребер) связных помеченных инициальных неориентированных графов $G = (S_G, E_G, X_G, \mu, g_0)$, где S_G — конечное множество вершин, E_G — множество ребер, $X_G \subseteq M$ — подмножество фиксированного конечного непустого алфавита отметок M, $\mu : S_G \to X_G$ — сюръективная функция разметки вершин такая, что отметки всех вершин, смежных одной вершине, попарно различны, g_0 — инициальная вершина. По аналогии с [1] будем называть такие графы детерминированными. В работе рассматривается задача распознавания графов из класса $K(M)$ конечным автоматом, взаимодействующим с лабиринтом [2, 3], где в качестве лабиринта выступает граф из указанного класса.

Для любого контрольного эксперимента [1] P для графа G относительно класса $F \subseteq K(M)$ предложен метод синтеза автомата $A(G, P)$ (без красок) с числом состояний $3\vartheta(P) + 1$, распознающего граф G в классе F не более чем за $2\vartheta(P)$ временных тактов, где $\vartheta(P)$ — объем эксперимента P.

Для произвольного графа $G \in K(M)$ разработаны алгоритмы синтеза автоматов с одной и k красками, распознающих граф G в классе $K(M)$, причем k не превосходит n, где n — число вершин графа G. Асимптотическая оценка числа состояний и временной сложности распознавания для автомата с одной краской составляет $O(n^3)$. Автомат с k красками имеет $2n + 1$ состояний и распознает граф G не более чем за $2n - 1$ временных тактов.

Список литературы

1. Сапунов С. В. Эквивалентность помеченных графов // Труды ИПММ НАНУ. — 2002. — Т. 8. — С. 162–167.

2. Килибарда Г., Кудрявцев В. Б., Ушчумлич Щ. Независимые системы автоматов в лабиринтах // Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 3–39.

3. Килибарда Г., Кудрявцев В. Б., Ушчумлич Щ. Коллективы автоматов в лабиринтах // Дискретная математика. — 2003. — т. 15, вып. 3. — С. 3–40.

КОМБИНАТОРНЫЕ ХАРАКТЕРИСТИКИ ОТОБРАЖЕНИЯ ЭНО НАД КОНЕЧНЫМ КОЛЬЦОМ

О. В. Тубольцева (Донецк)

Объект исследования — шифр $E(a,b,c)$, определяемый аналогом системы Эно [1] над конечным кольцом $\mathcal{Z}_{q^k}$ (q — простое число)

$$\begin{cases} x_{t+1} = 1 \ominus a \circ x_t^2 \ominus b \circ x_{t-1} \oplus c \circ u_t \\ V_{t+1} = x_{t+1} \end{cases} (t \in N),$$

где $a,b,c \in \mathcal{Z}_{q^k}$, x_t и u_t — внутренняя и информационная переменные.

ТЕОРЕМА 1. Доля преобразователей $E(a,b,c)$, допустимых в качестве шифра, равна $n_E^{don}(q,k) = (q-1) * q^{3k-1}$.

Одной из наиболее сильных атак является поиск начального состояния $(x_0,x_1) \in (\mathcal{Z}_{q^k})^2$ при известных $a,b,c \in \mathcal{Z}_{q^k}$ и при доступных для обозрения входе и выходе шифра. Сложность этой атаки характеризуется следующим образом.

ТЕОРЕМА 2. Если b — обратимый элемент кольца, то

$$\begin{cases} x_1 = b^{-1} \circ (1 \ominus a \circ V_2^2 \ominus V_3 \oplus c \circ u_2) \\ x_0 = b^{-1} \circ (1 \ominus a \circ x_1^2 \ominus V_2 \oplus c \circ u_1). \end{cases}$$

Пусть b — такой необратимый элемент кольца, что $b \equiv 0 \pmod{q^r}$ и $b \neq 0 \pmod{q^{r+1}}$, тогда множество допустимых начальных состояний состоит из q^{2r} элементов $(x_0,x_1) \in (\mathcal{Z}_{q^k})^2$, являющихся решением системы уравнений

$$\begin{cases} b \circ x_1 = 1 \ominus a \circ V_2^2 \ominus V_3 \oplus c \circ u_2 \\ b \circ x_0 = 1 \ominus a \circ x_1^2 \ominus V_2 \oplus c \circ u_1. \end{cases}$$

Показано, что атаки, состоящие в поиске параметров по известному начальному состоянию являются более слабыми. Таким образом, при надлежащем выборе параметров q,k,r для исследуемого шифра может быть обеспечена вычислительная стойкость сравнимая со стойкостью шифра типа DES, AES.

Литература

1. Кузнецов С. П. Динамический хаос. — М.: Физматлит, 2001. — 296 с.

УТОЧНЕНИЕ ОЦЕНКИ ШИРИНЫ УПОРЯДОЧЕНИЯ ВЕРШИН ОРГРАФОВ

В. А. Турчина, А. Д. Фирсов (Днепропетровск)

В классе оптимальных упорядочений, особое место занимают плотные упорядочения, а эффективные алгоритмы их построения представляют практический интерес.

В общем случае рассматривается следующая задача: дан ориентированный граф $G = (V,U)$, где $|V| = n$, и параметр l, задающий ограничения на длину упорядочения. Требуется распределить вершины графа G по l местам, расположенным в линию так, что на каждом месте стоит h вершин, за исключением, быть может, последнего.

Параллельным упорядочением S вершин графа G, называется такое их размещение по n местам, расположенным в линию, при котором из того, что пара $(i,j) \in U$ следует, что вершина i стоит в упорядочении S левее вершины j. Тогда количество непустых мест в упорядочении называется его длиной и обозначается $l(S)$, а величина $h(S) = \max_{1 \le i \le n} |S[i]|$ называется шириной упорядочения, где $S[i]$ — множество вершин стоящих в упорядочении S на месте i.

Будем считать $l(s)$ и $h(s)$ параметрами упорядочения.

Получение оценок параметров упорядочения, является ключевой задачей для построения оптимального упорядочения. Точное значение параметра l известно только для случая, когда граф является деревом. Для параметра h известны либо грубые оценки, либо требующие больших вычислительных затрат. Хотя, как раз именно значение этого параметра является ограничением, существенно важным при решении практических задач.

Для получения оценки ширины упорядочения по имеющейся формуле для определения длины, нами предлагается использовать итерационный алгоритм полиномиальной сложности, на каждом шаге которого задается текущее значение длины упорядочения, которое используется для уточнения ширины. Критерием остановки итерационного процесса является достижение значения h, при котором l не превосходит заданного значения.

Предлагаемый алгоритм реализован в виде динамической библиотеки, протестирован на десятках тысяч случайным образом сгенерированных графов и используется для построения упорядочений вершин графов.

ПЕРЕЧИСЛЕНИЕ ТЕРНАРНЫХ ДЕРЕВЬЕВ

А. Д. Уадилова (Ульяновск)

Изучаются конечно порожденные алгебры, а также рост коразмерностей многообразий абсолютно свободных алгебр, свободных симметричных неассоциативных алгебр, свободных кососимметричных неассоциативных алгебрх, свободных циклических неассоциативных и свободных двудольных неассоциативных алгебр. Для этих целей используются обычные производящие функции, а также экспоненциальные производящие функции (функции сложности).

В рассматриваемых классах алгебр изучаются такие подклассы как разрешимые, вполне разрешимые, левонильпотентные и вполне левонильпотентные подмногообразия.

Полученные результаты эквивалентны перечислению тернарных деревьев, которые не содержат некоторых запрещенных поддеревьев.

В качестве основного результата доказано, что производящие функции для свободных разрешимых (вполне разрешимых) алгебр ступени q в классе абсолютно свободных алгебр, свободных симметричных неассоциативных алгебр, свободных кососимметричных неассоциативных алгебрх, свободных циклических неассоциативных и свободных двудольных неассоциативных алгебр являются алгебраичными. Данная задача эквивалентна перечислению плоских тернарных деревьев, не содержащих запрещенных поддеревьев: полные тернарные поддереья высоты q в случае свободных разрешимых алгебр и полные тернарные поддереья высоты q после произвольного числа редукций в случае свободных вполне разрешимых алгебр. Также доказано, что функции сложности для свободных левонильпотентных (вполне левонильпотентных) тернарных алгебр в классе абсолютно свободных алгебр являются алгебраичными. Данная задача эквивалентна перечислению плоских тернарных деревьев, не содержащих запрещенных поддеревьев специального вида.

О РАЗНООБРАЗИИ МЕТРИЧЕСКИХ ШАРОВ В ГРАФАХ

Т. И. Федоряева (Новосибирск)

В [1] был предложен подход к изучению строения графов как дискретных метрических пространств через разнообразие и пересекаемость метрических шаров, содержащихся в графе, когда радиусы этих шаров последовательно возрастают от нуля до диаметра всего графа. Пусть $\tau(G) = (\tau_0, \tau_1, \ldots, \tau_d)$, где τ_i — число различных шаров радиуса i в графе G диаметра $d = d(G)$. Тогда $\tau_0 =\mid V(G) \mid$, $\tau_d = 1$ и $\tau_0 \geq \ldots \geq \tau_i \geq \tau_{i+1} \geq \ldots \geq \tau_d$.

ОПРЕДЕЛЕНИЕ. Вектор $\tau(G) = (\tau_0, \ldots, \tau_d)$ назовем вектором разнообразия метрических шаров графа G.

Естественно возникают следующие вопросы. Можно ли по заданному вектору α построить граф G, у которого вектор разнообразия метрических шаров $\tau(G)$ совпадает с α? И в целом возникает задача характеризации векторов, являющихся векторами разнообразия метрических шаров подходящих графов. В настоящей работе эта задача решена в классе деревьев, а именно определяется некоторый класс $\mathcal{A}$ векторов и доказывается следующая

ТЕОРЕМА. Вектор α принадлежит $\mathcal{A}$ тогда и только тогда, когда существует дерево G такое, что $\tau(G) = \alpha$.

Тем самым получено полное описание векторов разнообразия метрических шаров для деревьев.

ОПРЕДЕЛЕНИЕ [1]. Граф G обладает свойством t-разнообразия шаров, если $\tau_i =\mid V(G) \mid$ для любого $i < t$.

Как следствие из теоремы получена характеризация деревьев, обладающих свойством t-разнообразия шаров.

Список литературы

1. Евдокимов А. А. Кодирование структурированной информации и вложения дискретных пространств // Дискретный анализ и исследование операций. Сер. 1. —2000. — Т. 7, № 4. — С. 48–58.

КВАЗИПОРЯДКОВАЯ РАЗМЕРНОСТЬ ЧАСТИЧНО УПОРЯДОЧЕННЫХ МНОЖЕСТВ

В. Ю. Филимонов (Мурманск)

Пусть m,n — натуральные числа, U — конечное множество, $|U|{=}n$, $Ord(U) = (ord(U), \subseteq)$ — решетка частичных порядков (ЧП) на U, $Qord(U) = (qord(U), \subseteq)$ – решетка квазипорядков (КП) на U. Определим $Bul(U) = (2^U, \subseteq)$ — частично упорядоченное множество (ЧУМ) подмножеств множества U. ЧУМ изоморфное $Bul(U)$ назовем булеаном и обозначим $Bul(n)$. ЧУМ, изоморфное n-элементному линейно упорядоченному множеству, обозначим $Chain(n)$. Инъекция $\varphi : P \to Q$ называется вложением ЧУМ (P,T_1) в ЧУМ (Q,T_2), если aT_1b равносильно $\varphi(a)T_2\varphi(b)$ для всех $a,b \in P$, где $T_1, T_2 \in ord(U)$.

Квазипорядковой размерностью КП T называется наименьшее число коатомов решётки $Qord(U)$, пересечение которых равно T, обозначается $\dim_q(T)$ или $\dim_q(U,T)$.

ТЕОРЕМА. Пусть $T \in ord(U)$. Квазипорядковая размерность ЧП T равна наименьшему m, для которого существует вложение частично упорядоченного множества (U,T) в булеан $Bul(m)$.

Теорема является аналогом теоремы для порядковой размерности из [1].

СЛЕДСТВИЕ 1. Пусть $T \in ord(U)$. Тогда $\dim_q(T) \geq \lceil \log_2 n \rceil$.

СЛЕДСТВИЕ 2. Пусть $T \in ord(U)$. Тогда:

1) $\dim_q(T) \leq n$, если (U,T) — ЧУМ без $\widetilde{0}$ и $\widetilde{1}$;

2) $\dim_q(T) \leq n{-}1$, если (U,T) — ЧУМ с $\widetilde{0}$ или $\widetilde{1}$;

3) $\dim_q(T) \leq n{-}1$, если (U,T) — ЧУМ с $\widetilde{0}$ и $\widetilde{1}$.

Пусть $A = \{a_1, \ldots, a_n\}$, $B = \{b_1, \ldots, b_m\}$, $A \cap B = \emptyset$, $U = A \cup B$. Определим на множестве U ЧП $K = \{(a_i, b_j) |\ i = \overline{1,n},\ j = \overline{1,m}\}$.

СЛЕДСТВИЕ 3. Справедливы утверждения:

1) $\dim_q(Bul(n)) = n$;

2) $\dim_q(Chain(n)) = n - 1$;

3) если (U,K) — ЧУМ, то

$$\dim_q(U,K) = \min\left\{\alpha \mid\ n \leq \binom{\alpha}{\lfloor \alpha/2 \rfloor}\right\} + \min\left\{\beta \mid\ m \leq \binom{\beta}{\lfloor \beta/2 \rfloor}\right\}.$$

Список литературы

1. Оре О. Теория графов. — М.: Наука, 1980.

О МИНИМИЗАЦИИ МНОГОЛЕНТОЧНЫХ АВТОМАТОВ

В. Е. Хачатрян (Белгород)

Рассматриваемые многоленточные автоматы определены в [1] и называются диаграммами. Мы устанавливаем, что в общем случае в классе эквивалентных диаграмм может быть несколько минимальных по размеру диаграмм, и описываем алгоритм построения их всех для класса двухленточных автоматов с непересекающимися циклами. Диаграммы строятся над алфавитами P и B, где $P = \{p_1, \ldots, p_n\}$, $n > 1$, $B = \{0,1\}$. Они представляют собой конечные ориентированные графы, в которых выделены две вершины — вход и выход. Каждая вершина диаграммы, кроме выхода, помечена символом из P и имеет две исходящие дуги, помеченные символами 0 и 1 соответственно. Выход не имеет ни метки, ни исходящих из него дуг. Пусть w — путь через диаграмму, и $u_1, u_2, \ldots, u_k$ — последовательность составляющих его дуг. Построим слово $h(w) = (p_{i_1}, \varepsilon_1) \ldots (p_{i_k}, \varepsilon_k)$, предполагая, что p_{i_j} — метка вершины, начинающей дугу u_j, а ε_j — метка самой дуги u_j, $j = 1, \ldots, k$. Пути w сопоставим набор p-проекций слова $h(w)$, где $p \in P$ и p-проекция получается удалением из $h(w)$ всех пар, не содержащих p. Две диаграммы считаются эквивалентными, если, каким бы ни был путь через одну из них, существует путь через другую с тем же набором p-проекций, что и первый. Эквивалентность вершин диаграммы вводится как эквивалентность произрастающих из них поддиаграмм. Диаграмма именуется тупиковой, если ее вершины попарно неэквивалентны.

ЛЕММА 1. Существует класс эквивалентных диаграмм над P, B с бесконечным числом тупиковых диаграмм.

ЛЕММА 2. Существует класс эквивалентных диаграмм над P, B с более, чем более одной диаграммы с минимальным числом вершин.

ТЕОРЕМА. Для множества двухленточных автоматов, представленных диаграммами с непересекающимися циклами, существует алгоритм, который по любому автомату строит все минимальные по числу вершин эквивалентные ему автоматы.

Работа выполнена при поддержке РФФИ (проект 03-01-00312).

Список литературы

1. Bird R. The equivalence problem for deterministic two-tape automata // Journal of computer and system science. — 1973. — V. 7. — P. 218–236.

О РЕШЕНИИ ЗАДАЧИ СИНТЕЗА ИГРОВЫХ ПРОГРАММ В ОБОБЩЁННОЙ ПОСТАНОВКЕ

Р. В. Хелемендик (Москва)

Игровая программа (ИП) представляет собой специальный граф, который описывает выигрышную стратегию при взаимодействии с внешней средой (партнёром). В обычной постановке задача синтеза ИП рассматривается для заданного условия $\mathcal{U}$: конечного числа переменных, принимающих конечное число $k \geq 2$ значений, зафиксированных начальных значений всех переменных, набора функций ("ходов"), типа взаимодействия и цели, записываемой формулой логики ветвящегося времени. Существует ли ИП $\mathcal{P}_\mathcal{U}$, удовлетворяющая условию $\mathcal{U}$? Если существует, то необходимо построить хотя бы одну такую ИП (см. [1]).

Если начальное значение переменной определено, то такая переменная называется фиксированной. Иначе если для неё мы можем выбрать любое значение (её значение может быть определено партнёром произвольным образом), то такая переменная называется внутренней (внешней). Условие задачи синтеза, в котором могут быть внешние и внутренние переменные, называется обобщённым и обозначается $\mathcal{U}^*$. Обобщённая постановка задачи синтеза ИП для условия $\mathcal{U}^*$ — распознавание существования для каждого значения каждой внешней переменной некоторых значений внутренних переменных, при которых для каждого получившегося условия $\mathcal{U}$ существует ИП $\mathcal{P}_\mathcal{U}$, а также построение в случае положительного ответа всех таких ИП $\mathcal{P}_\mathcal{U}$. Решение данной задачи даёт авторский алгоритм, являющийся развитием [1].

Работа выполнена при финансовой поддержке РФФИ (проект 05-01-00581) и программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики" (проект "Оптимальный синтез управляющих систем").

Список литературы

1. Хелемендик Р. В. Об одном алгоритме решения задачи синтеза игровых программ // Дискретные модели в теории управляющих систем: VI Международная конференция. Москва, 7–11 декабря 2004 г. — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова, 2004. — С. 150–153.

СТРУКТУРНЫЙ ПОДХОД К ПОЛУЧЕНИЮ МОЩНОСТНЫХ ОЦЕНОК ДЛЯ НЕКОТОРЫХ КЛАССОВ МОНОТОННЫХ ФУНКЦИЙ

Д. В. Ховратович (Москва)

Будем рассматривать классы функций в $\mathcal{P}_k$, монотонных относительно двух линейных порядков одновременно. Каждый такой класс представляет собой пересечение двух классов M_{O_1} и M_{O_2}. Обозначим его через T_{O_1,O_2}. Введем операцию перестановки на порядке O: $\alpha_1 < \alpha_2 < \ldots < \alpha_k$. Пусть σ — перестановка на $\mathbb{E}_k$. Через σO обозначим порядок $\alpha_{\sigma(1)} < \alpha_{\sigma(2)} < \ldots < \alpha_{\sigma(k)}$. Между функциями класса T_{O_1,O_2} и функциями класса $T_{\sigma' O_1,\sigma' O_2}$ существует взаимно-однозначное соответствие, поэтому будем описывать семейство таких классов, задаваемых одной перестановкой σ такой, что $O_2 = \sigma O_1$, и обозначим его T_σ.

Пусть $\widehat{\sigma} = [1\,k][2\,(k-1)]\ldots[\lfloor\frac{k}{2}\rfloor\lceil\frac{k}{2}\rceil]$. Заметим, что $M_O = M_{\widehat{\sigma}O}$, и $T_\sigma = T_{\sigma^{-1}}$ (то есть эти семейства состоят из одних и тех же классов). Отсюда следует, что $T_\sigma = T_{\sigma^{-1}} = T_{\sigma_*}$, где $\sigma_* = \widehat{\sigma} * \sigma$.

Было проведено исследование семейств классов T_σ для произвольного k и перестановок, имеющих такой вид: $\sigma = [1\,2\ldots m_1][(m_1+1)\ldots m_2]\ldots[(m_{\lambda-1}+1)\ldots m_\lambda]$. Для каждого класса семейства были построены инъективные отображения, переводящие функции от n переменных из этого класса в последовательности функций из других классов: $\mathcal{Q}_n(f) = \langle f_1, f_2, \ldots, f_{l(f)}\rangle$.

В ряде случаев для числа получающихся последовательностей с использованием результатов [1] удается получить оценку на уровне асимптотики логарифма, что дает оценку на число функций из исходного класса. К примеру, на $\mathbb{E}_4$ можно задать 24 перестановки, что с учетом полученного соответствия между семействами классов T_σ, $T_{\sigma^{-1}}$ и T_{σ_*} дает 7 различных семейств типа T. Были получены оценки на уровне асимптотики логарифма для каждого класса из этих 7 семейств.

Работа выполнена при финансовой поддержке РФФИ (проект 03-01-00783).

Список литературы

1. Алексеев В. Б. О числе монотонных k-значных функций // Проблемы кибернетики. Вып. 28. — 1974. — С. 5–24.

ОПТИМАЛЬНОСТЬ РЕШЕНИЯ ПО ДВУМ КРИТЕРИЯМ В ЗАДАЧЕ О РАВНОМЕРНОМ НАЗНАЧЕНИИ

Н. Б. Чаплыгина (Ярославль)

В [1] описана постановка задачи о равномерном назначении. В течение периода из m дней n работников выполняют определенный объем работ. В каждый k-й день они должны произвести s_k работ. Назначение работ согласно заданным возможностям работников и некоторым дополнительным условиям представимо булевой матрицей $X = \{x_{ij}^k\}$, где i — номер рабочего, j — номер работы k-го дня. Необходимо найти назначение, минимизирующее функционал равномерности, введенный в [1].

Задача приобретает двухкритериальный характер при введении критерия стоимости выполнения работ каждым рабочим. Требуется среди всех равномерных найти назначение минимальной стоимости.

Графически условие задачи представляется сетью, в которой отыскивается поток, соответствующий искомому решению. Алгоритм решения поставленной задачи имеется в [2].

Обладает ли построенное решение X этой задачи минимальной стоимостью на всем множестве допустимых решений? В общем случае этого может не быть.

Если S — множество всех назначений минимальной стоимости, а R — множество всех равномерных назначений, то в случае их непустого пересечения указанный алгоритм построит решение именно из пересечения $S \cap R$. Если же в дополняющей сети, в которой уже не будет сохраняющих равномерность отрицательных контуров, все же отрицательные контуры останутся, то оптимизировать решение сразу по двум критериям невозможно. В этом случае пересечение множеств $S \cap R = \varnothing$.

Автор выражает благодарность Рублеву В. С. за помощь и внимание к работе.

Список литературы

1. Рублев В. С., Чаплыгина Н. Б. Расширение задачи о назначениях // Моделирование и анализ информационных систем. — Ярославль, 2002. — Т. 9, № 2. — С. 3–11.

2. Чаплыгина Н. Б. Задача о назначении минимальной стоимости среди равномерных назначени // Вопросы теории групп и гомологической алгебры. — Ярославль: Изд-во ЯрГУ, 2003. — С. 238–245.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ФУНКЦИЙ В ПОЛЯХ ГАЛУА

А. В. Чашкин (Москва)

Рассматривается сложность реализации функций в полях Галуа схемами из функциональных элементов в базисе из умножения, сложения и единицы. Пусть p — простое. Через $L(n, k_0, k_1, \ldots, k_{p-1})$ обозначим сложность самой сложной частичной функции, определенной на произвольном подмножестве D множества $\{0, 1, \ldots, p-1\}^n$ и принимающей значение i ровно на k_i наборах из D при $i = 0, 1, \ldots, p-1$. Положим

$$H(k_0, k_1, \ldots, k_{p-1}) = \frac{(k_0 + k_1 + \cdots + k_{p-1})!}{k_0! k_1! \cdots k_{p-1}!}.$$

Имеет место следующее утверждение.

ТЕОРЕМА. При $n \to \infty$ выполняется соотношение

$$L(n, k_0, k_1, \ldots, k_{p-1}) = \frac{\log H(k_0, k_1, \ldots, k_{p-1})}{\log \log H(k_0, k_1, \ldots, k_{p-1})} (1 + o(1)) + O(n).$$

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1) и программы «Университеты России» (проект УР.04.02.528).

Список литературы

1. Лупанов О. Б. Об одном подходе к синтезу управляющих систем — принципе локального кодирования // Проблемы кибернетики. Вып. 14. — М.: Физматгиз, 1965. — С. 31–110.

2. Шоломов Л. А. О реализации недоопределенных булевых функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 215–226.

3. Чашкин А. В. О сложности реализации булевых функций формулами // Дискретный анализ и исследование операций. — 2005. — Т. 12, вып. 2. — С. 75–91.

4. Miltersen P. Br. On the Shannon function for partially defined Boolean functions. `http://www.brics.dk/~bromille/Papers/index.html`.

СТРОЕНИЕ И ПОКАЗАТЕЛИ СЛОЖНОСТИ ФОРМУЛ

И. Ф. Чебурахин (Москва)

Для булевых формул $f^{(n)}$ строения $\mathbf{r}= (r_1,\dots,r_m)$ приводятся соотношения, связывающие их строение с показателями сложности (сложность — $L_F(f^{(n)},G)$, глубина — $Dep_F(f^{(n)},G)$) представления над различными множествами функциональных символов (ФС) из $G = \{0,1,\neg,\&,\vee,\oplus,\leftrightarrow\}$. Эти соотношения могут быть полезными при разработке интеллектуальных систем синтеза БИС.

В [1] приводятся оценки минимальной глубины суперпозиционной формулы F, получаемой на основе строения $\mathbf{r}$ и параллельной декомпозиции $f^{(n)}$ над G: $\lceil\log_2 n\rceil \le Dep_F(f^{(n)},G) \le \lceil\log_2 n\rceil+1$, где $n = r_1+\ldots+r_m$. Для произвольных (минимальной) ДНФ, полинома Жегалкина и др. эти оценки допускают следующее обобщение:

$$\lceil\log_2 L_{\text{Б}}(f^{(n)})\rceil \le Dep_F(f^{(n)},G) \le \lceil\log_2 L_{\text{Б}}(f^{(n)})\rceil+1,$$

где $L_{\text{Б}}(f^{(n)}) = r_1+\ldots+r_m$. Если $f^{(n)}$ не является минимальной ДНФ, то это неравенство позволит получить верхнюю оценку, может достижимую.

Рассмотрим последовательность $G^{(i)} = \{f_0^{(0)},\ f_1^{(1)},\ f_\neg^{(1)},\ f_\&^{(ni1)},\ f_\vee^{(ni2)}, f_\oplus^{(ni3)}, f_\leftrightarrow^{(ni4)}\dots\}$, $i = 1,\dots,k$, множеств ФС, упорядоченных отношением *предшествования*, причем для их местностей выполняется $n_{i1} \ge n_{i2} \ge n_{i3} \ge n_{i4} \ge 2$. Множество $G^{(i)}$ *предшествует* множеству $G^{(j)}$ (обозначая $G^{(i)} \preceq G^{(j)}$), если для каждого ФС множества $G^{(i)}$ находится инъективно или биективно ФС множества $G^{(j)}$, находящийся с первым в отношении *не проще* и хотя бы для одного ФС в отношении *сложнее* или для инъекции остальные сравнимые между собой ФС множества $G^{(j)}$ *сложнее* последнего ФС множества $G^{(i)}$. Тогда из $G^{(1)} \preceq \ldots \preceq G^{(k)}$ при выполнении условий оптимизации следует $Dep_{F1}(f^{(n)},G^{(1)}) \ge \ldots \ge Dep_{Fk}(f^{(n)},G^{(k)})$ и $L_{F1}(f^{(n)},G^{(1)}) \ge \ldots \ge L_{Fk}(f^{(n)},G^{(k)})$. Требования к элементам последовательности $\{G^{(i)}\}$ можно существенно снизить и элементы последовательности дополнять по правилам новыми ФС. Выбирая определенные последвательности можно улучшать оценки различных показателей сложности представления булевых функций в различных базисах.

Список литературы

1. Чебурахин И. Ф. Методы декомпозиции булевых функций: алгоритмы, показатели качества // Изв. РАН. ТиСУ. — № 5. — 2003. — С. 56–61.

ОБЩАЯ СХЕМА ПОСТРОЕНИЯ ИНВАРИАНТОВ ГРУПП ИНЕРЦИИ ДЛЯ ОБОБЩЕННЫХ АФФИННЫХ ГРУПП

А. В. Черемушкин (Москва)

В докладе описывается схема построения инвариантов группы инерции двоичной функции в обобщенной аффинной (линейной) группе, основанная на инвариантах этой группы на множестве функций. Пусть $n \ge 3$, $\mathcal{F}_n$ — множество двоичных функций от n переменных, $V = \mathrm{GF}(2)^n$ и V^* — сопряженное пространство, $\mathrm{AGL}(n,2)$ — полная аффинная группа, $\mathcal{U}_s = \{f : \deg f \le s\} \subset \mathcal{F}_n$, $0 \le s < n$.

Пусть $G \le \mathrm{AGL}(n,2)\mathcal{U}_s$, W — одно из пространств V или V^*, $R^W = \{W \to R\}$, R — некоторое множество. Рассмотрим оператор $D : \mathcal{F}_n \to R^W$, где $D : f \mapsto D_f$, удовлетворяющий свойству: существуют гомоморфизмы $\varphi : G \to \mathrm{AGL}(W)$ (если $G \subseteq \mathrm{GL}(n,2)\mathcal{U}_s$, то надо взять группу $\mathrm{GL}(W)$) и $\psi : G \to \mathrm{S}(R)$, при которых диаграмма

$$\begin{array}{ccc} f & \mapsto & D_f \\ \downarrow\alpha & & \downarrow(\varphi(\alpha),\psi(\alpha)) \\ f^\alpha & \mapsto & D_{f^\alpha} \end{array}$$

коммутативна, то есть $D_{f^\alpha}(a) = D_f(a^{\varphi(\alpha)^{-1}})^{\psi(\alpha)}$, $a \in W$.

ТЕОРЕМА. Пусть $f \in \mathcal{F}_n$, $G \subseteq \mathrm{AGL}(n,2)\mathcal{U}_s$, D — введенный выше оператор. Тогда

1) если J — инвариант группы $(R,\psi(G))$, то функция $I(a) = J(D_f(a))$, $a \in W$, будет инвариантом группы $(W,\varphi(G_f))$;

2) если $X_1, X_2, \ldots, X_m$ — разбиение пространства W на подмножества, состоящие из векторов a, для которых инвариант I принимает одинаковые значения, то выполняется включение

$$\varphi(G_f) \subseteq \bigcap_{i=1}^{m} \mathrm{AGL}(W)_{\{X_i\}}.$$

Данная схема охватывает практически все известные способы построения инвариантов групп инерции, включая способы, основанные на использовании преобразования Уолша, функции автокорреляции, операторов нахождения производных по направлению, ограничений на гиперплоскости и единичных окрестностей исходной функции.

Работа выполнена при поддержке гранта Президента РФ НШ-2358.2003.9.

ОБОБЩЕНИЕ ПОНЯТИЯ ДЕТЕРМИНИРОВАННОЙ ФУНКЦИИ

А. Н. Черепов (Смоленск)

Рассмотрим множество всех бесконечных двоичных последовательностей E. Множество всех функций вида $f : E^n \longmapsto E$ обозначим P. Рассмотрим $\tilde{a} = (a_1, a_2, \ldots, a_n) \in E^n$. Пусть $a_1 \mid k, a_2 \mid k, \ldots, a_n \mid k$— первые k членов последовательностей $a_1, a_2, \ldots, a_n$ соответственно, тогда $\tilde{a} \mid k = (a_1 \mid k, a_2 \mid k, \ldots, a_n \mid k)$. Обычным образом введем понятие детерминированной функции. Класс детерминированных функций обозначим P_∂. Обобщим понятие детерминированной функции.

Говорим, что f является функцией с задержкой τ, если для любого $i = 1, 2 \ldots$ и любых $\tilde{a}, \tilde{b}$ выполнено: $\tilde{a} \mid i + \tau = \tilde{b} \mid i + \tau \Rightarrow f(\tilde{a}) \mid i = f(\tilde{b}) \mid i$. Обозначим $P(\tau)$ множество всех функций с задержкой τ и пусть $PZ = \bigcup_\tau P(\tau)$.

Заметим, что при $\tau = 0 \quad P(\tau) = P_\partial$, и класс PZ является замкнутым. Название "функции с задержкой" связано с трактовкой таких функций как функций, реализуемых устройствами, у которых в течение первых τ тактов работы нет сигнала на выходе, $f(\tilde{a}) \mid 1$ появляется в момент времени $\tau + 1$ и считается первым значением функции, а далее устройство функционирует обычным образом.

Пусть $\tilde{r} = (r_1, r_2, \ldots)$ — произвольная неубывающая последовательность натуральных чисел, такая, что $r_i \geq i$. В множество $P(\tilde{r})$ включим все функции, удовлетворяющие свойству: для любого i и любых $\tilde{a}, \tilde{b}$ выполнено: $\tilde{a} \mid r_i = \tilde{b} \mid r_i \Rightarrow f(\tilde{a}) \mid i = f(\tilde{b}) \mid i$.

В устройствах, реализующих такие функции, i-е значение выхода появляется после получения r_i значений на входе. Очевидно, что $P(\tau) = P(\tilde{r})$ при $\tilde{r} = (\tau + 1, \tau + 2, \ldots)$. Положим $POD = \bigcup_{\tilde{r}} P(\tilde{r})$, где объединение берется по всем $\tilde{r}$. Класс POD назовем классом обобщенно-детерминированных функций. Все остальные функции из P будем называть абсолютно недетерминированными.

Получены некоторые результаты о структуре замкнутых подклассов классов POD и PZ.

О МАКСИМАЛЬНОМ ЧИСЛЕ ЛИСТЬЕВ ДВОИЧНЫХ ДЕРЕВЬЕВ С ЗАДАННЫМИ ЗНАЧЕНИЯМИ ЧИСЛА ЯРУСОВ И ВЫСОТЫ ИХ ВЛОЖЕНИЯ В ПЛОСКИЕ ПРЯМОУГОЛЬНЫЕ РЕШЕТКИ

П. Н. Чернецов (Москва)

Рассматриваются гомеоморфные вложения двоичных корневых деревьев в плоские прямоугольные решетки (ППР) высоты h и длины $\lambda, \lambda \leq h$, с расположением листьев дерева на границе ППР [1]. Решается задача о максимизации числа листьев вкладываемого дерева при заданных значениях для числа его ярусов и высоты его вложения в ППР. В [2] были построены деревья $D_2(k, h)$ с k ярусами, которые допускают указанное вложение в ППР высоты h с расположением листьев на любых сторонах ППР, кроме верхней, и имеют максимальное число листьев среди всех таких деревьев. При этом дерево $D_2(k, h)$ в случае $k \leq 2h-1$ совпадает с полным k-ярусным двоичным деревом, а при $k > 2h-1$ получается из дерева $D_2(k-1, h)$ подразбиением его прикорневых ребер и «привешиванием» к средним вершинам соответствующих цепочек двух деревьев $D_2(k-2, h-1)$ через дополнительные ребра. В данной работе установлено, что деревья $D_2(k, h)$ имеют наибольшее число листьев и в том случае, когда листья вкладываемого дерева могут располагаться на произвольных заданных границах ППР.

Работа выполнена при поддержке гранта РФФИ 05-01-01000.

Список литературы

1. Ложкин С. А., Ли Да Мин. О некоторых оптимальных вложениях двоичных и троичных деревьев в плоские прямоугольные решётки // Вестник Московского университета. Сер. 15. Вычисл. матем. и киберн. — 1995. — № 4. — С. 49–55.

2. Ли Да Мин. Некоторые оптимальные вложения древовидных графов в плоские прямоугольные решетки // Диссертация на соискание ученой степени кандидата физ.-мат. наук. — М., 1994.

О СХЕМАХ ГЛУБИНЫ 2 В БАЗИСЕ P_2

Д. Ю. Черухин (Москва)

Рассматривается класс схем из функциональных элементов глубины 2 в базисе P_2, состоящем из всех булевых функций. Сложностью схемы будем считать число рёбер. Сложность оператора F в данном классе обозначим через $L_2(F)$.

Пусть $F = (f_1, \ldots, f_m)$ и каждая из функций f_j, $1 \leqslant j \leqslant m$, зависит от двух наборов переменных: $\tilde{x} = (x_1, \ldots, x_n)$ и $\tilde{y} = (y_1, \ldots, y_k)$. Разложим f_j в полином Жегалкина по переменным $\tilde{x}$:

$$f_j = f_j^0 \oplus f_j^1 x_1 \oplus \ldots \oplus f_j^n x_n \oplus f_j',$$

где функция f_j^i, $0 \leqslant i \leqslant n$, зависит от $\tilde{y}$, f_j' — нелинейная по $\tilde{x}$ часть.

Рассмотрим матрицу $M = (f_j^i)$, $i = 1, \ldots, n$, $j = 1, \ldots, m$. Пусть i-му столбцу (j-й строке) матрицы M приписано множество функций M^i (M_j) от переменных $\tilde{y}$ таким образом, что каждая функция f_j^i вычислима через функции из множества $M^i \cup M_j$, т. е. представима в виде $h(g_1, \ldots, g_s)$, где $g_1, \ldots, g_s$ — функции из $M^i \cup M_j$, $h \in P_2$. Тогда набор $(M;\ M^1, \ldots, M^n;\ M_1, \ldots, M_m)$ назовём *M-функциональной таблицей*. Обозначим

$$\mathcal{L}(M) = \min\Big(\sum_i |M^i| + \sum_j |M_j|\Big),$$

где минимум берётся по всем M-функциональным таблицам.

ТЕОРЕМА. $L_2(F) \geqslant \mathcal{L}(M)$.

С помощью теоремы можно получить нижние оценки сложности вида $\Omega(N^{3/2})$ (где $N = n + k + m$) для операторов циклической свёртки, произведения многочленов, произведения матриц. Наибольшие известные нижние оценки в данном классе схем имеют вид $\Omega(N \log^2 N / \log\log N)$ и основаны на теоретико-графовой технике [1].

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.1) и программы "Университеты России" (проект УР 04.02.528).

Список литературы

1. Radhakrishnan J., Ta-Shma A. Bounds for dispersers, extractors, and depth-two superconcentrators // SIAM J. of Discrete Mathematics. — 2000. — V. 13 (1). — P. 2–24.

О РЕАЛИЗАЦИИ «ПОЧТИ СИММЕТРИЧЕСКИХ» ФУНКЦИЙ

С. Е. Черухина (Москва)

В работе продолжено изучение класса монотонных булевых функций, рассмотренного в [1]. Класс $\mathcal{F}_n$ определяется следующим образом: $f(x_1, \ldots, x_n) \in \mathcal{F}_n$, если $S_n^2 \geqslant f \geqslant S_n^3$ (S_n^i — монотонная симметрическая функция с порогом i). Обозначим через $M(f)$ количество наборов, содержащих ровно 2 единицы, на которых функция f обращается в 0. (Назовем их "нулями" функции.) Очевидно, $0 \leqslant M(f) \leqslant C_n^2$.

Пусть $L(f)$ — сложность функции f в классе формул вида $\&\vee\&$ над базисом $\{\&, \vee\}$. Ранее было показано, что для любой $f \in \mathcal{F}_n$ справедливо $\sqrt{2}n^{3/2} \lesssim L(f) \lesssim 2n^2$.

Далее была сделана попытка найти связь между сложностью функции и количеством ее "нулей".

У функций с количеством "нулей", близким к границам возможных значений, сложность близка, соответственно, к сложности S_n^2 и S_n^3, точнее,

ТЕОРЕМА 1. Если $M(f) = o(n)$, то $L(f) \sim 2n^{3/2}$. Если $M(f) \sim n^2/2$, то $L(f) \sim n^2$.

Выражение для сложности при малых значениях $M(f)$ следует (отчасти) из следующей оценки для $L(f)$ и $M(f)$.

ТЕОРЕМА 2. $L(f) \leqslant 4M(f)\sqrt{n} + 2n^{3/2}$ для любой $f \in \mathcal{F}_n$.

Нижняя оценка для $L(f)$ была получена ранее: $L(f) \geqslant 2M(f) - 7n$.

Достигается ли верхняя оценка ($2n^2$) для какой-либо функции из $\mathcal{F}_n$, не доказано, но, по всей видимости, этой функцией является функция, построенная на основе матрицы Нечипорука, для которой верна

ТЕОРЕМА 3. Существует некоторая функция $f \in \mathcal{F}_n$ с $M(f) = \mathcal{O}(n^{3/2})$ такая, что $L(f) = \Omega(n^{7/4})$.

Список литературы

1. Черухина С. Е. О сложности реализации одного класса «почти симметрических» функций $\&\vee\&$-формулами // Материалы VIII Международного семинара «Дискретная математика и ее приложения» (Москва, 2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 109–111.

ПРИНЦИПЫ ПОСТРОЕНИЯ РАСПОЗНАЮЩИХ СИСТЕМ ДЛЯ ПРОГНОЗНО-МЕТАЛЛОГЕНИЧЕСКОГО АНАЛИЗА ПЕРСПЕКТИВНЫХ ПЛОЩАДЕЙ

И. А. Чижова (Москва)

Распознающие системы строятся на основе принципа общности свойств или принципа перечисления объектов. В первом случае необходимо выделить системы информативных признаков, описывающих группу объектов в целом (отождествляющие признаки) и каждый тип в отдельности (делящие признаки), и на их основе построить решающее правило отнесения вновь предъявляемого объекта к одному из выделенных типов объектов. Во втором случае используется некоторая мера сходства для оценки экспертируемого объекта при определении степени его близости к одному из эталонов из базы данных. При этом возможен выбор аналога по любому набору признаков, что дает возможность пользователю проверить различные гипотезы и сравнить работоспособность различных критериев. Для построения распознающих систем первого типа предложена технология построения интеллектуальных систем АСТРА, база знаний которых формируется на основе логико-информационного и статистического анализов имеющейся базы данных изучаемых объектов. С использованием данной технологии создано несколько специализированных экспертных систем. Среди них «Автоматизированный прогнозно-поисковый комплекс на объекты золото-кварцевой и золото-редкометально-кварцевой формации Северо-Востока» (Чижова И. А., Курбанаев Г. М. и др.), «Автоматизированная экспертная система прогноза золоторудных месторождений на примере Охотско-Чукотского вулканогенного пояса» (Чижова И. А., Стружков С. Ф., Константинов М. М.). Для построения распознающих систем второго типа предложена технология построения интеллектуальных систем, база данных которых содержит набор правил для попарного сравнения объектов исходя из природы анализируемой информации (возраст, минеральный состав и т. д.) с учетом возможных типов представления исходных данных (количественный, качественный, логический). Технология апробирована при создании информационно-аналитической системы АНАЛОГ для поиска ближайшего аналога золоторудных месторождений (Константинов М.М., Чижова И.А. и др.)

О $(n-1)$-МЕРНОМ ПРИБЛИЖЕННОМ РЕШЕНИИ n-МЕРНОЙ ЗАДАЧИ О РЮКЗАКЕ

А. Ю. Чирков (Нижний Новгород)

Множество вещественных чисел обозначим через R, а множество целых чисел — через Z. Для числового множества M обозначим через M_+ — множество неотрицательных чисел из M, через M^n — множество n-элементных наборов с компонентами из M. Элементы множества M^n называются векторами или точками. Под ax будем понимать обычное скалярное произведение векторов a и x, то есть $ax = a_1x_1 + ... + a_nx_n$. Для $a \in R^n_+$ и $b \in R_+$ определим $G(a,b) = \{x \mid x \in Z^n_+,\ ax \geqslant b\}$. В работе рассматривается задача о рюкзаке $\min_{x \in G(a,b)} cx$. Точка $p \in G(a,b)$, на которой достигается минимум целевой функции, называется оптимальным решением, а величина $\gamma(a,b,c) = cp$ — оптимальным значением. Обозначим через $G_0(a,b)$ множество точек из $G(a,b)$, имеющих хотя бы одну нулевую компоненту. Точку $p' \in G_0(a,b)$, на которой достигается минимум значения целевой функции cx, назовём $(n-1)$-мерным приближённым решением n-мерной задачи о рюкзаке или просто приближенным решением, а величину $\gamma_0(a,b,c) = cp'$ — приближённым значением. Близость приближённого и оптимальных значений задается отношением $\beta(a,b,c) = \gamma(a,b,c)/\gamma_0(a,b,c)$ (если $\gamma_0(a,b,c) = 0$, то будем считать, что $\beta(a,b,c) = 1$). По определению $0 < \beta(a,b,c) \leqslant 1$. Положим $\beta_n = \inf\{\beta(a,b,c) \mid a,c \in R^n_+, b \in R_+\}$. Величину β_n назовем гарантированной точностью $(n-1)$-мерного приближенного значения n-мерной задачи о рюкзаке или просто гарантированной точностью. Цель работы заключается в исследовании зависимости гарантированной точности от размерности задачи. Для вектора $a \in R^n_+$ положим $a_0 = a_1 + ... + a_n$.

ЛЕММА. Для любых $a,c \in R^n_+$, $b \in R_+$ найдутся $a', c' \in R^n_+$ такие, что $\beta(a,b,c) \geqslant \beta(a', a'_0, c')$.

Положим $c = (2^{n-1}, \mu, 2\mu, ..., 2^{n-2}\mu)$ и $a = (1, \nu, 3\nu, ..., 3^{n-2}\nu)$, где $\mu, \nu \in Z_+$ и $\nu > \mu > 2^n$. Тогда $\beta(a, a_0, c) = 1/\mu + 1 - 2^{1-n}$.

ТЕОРЕМА. Точность $(n-1)$-мерного приближенного решения n-мерной задачи о рюкзаке строго больше, чем $1 - 2^{1-n}$, и для любого $\varepsilon > 0$ найдётся задача, в которой эта точность не превосходит $\varepsilon + 1 - 2^{1-n}$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 05-01-00522-а).

ДИСКРЕТНАЯ МОДЕЛЬ КВАНТОВОЙ СИСТЕМЫ, ИМЕЮЩЕЙ N БАЗИСНЫХ СОСТОЯНИЙ

С. В. Шалагин (Казань)

Исследуется задача сравнительной оценки сложности моделей вычислений, реализуемых на базе квантово-механических систем (КМС), и классических моделей вычислений [1, 2]. КМС, имеющая N базисных состояний, задана вектором $|\Psi\rangle = \left(r_0 e^{i\varphi_0} \dots r_{N-1} e^{i\varphi_{N-1}}\right)^T$, где $\sum_{j=0}^{N-1} r_j^2 = 1$. Изменение состояния КМС, описывается квантовым вентилем — матрицей G размерности $N \times N$. Теоретически мощность множества состояний КМС, $S \to \infty$. В случае предполагаемой реализации $|S| < \infty$, то есть будет ограничено точностью задания, поддержания и считывания информации, что позволяет ставить и решать задачу дискретного моделирования КМС на основе вычислений в полях Галуа вида $GF(2^n)$ [3]. Сформулированы

ТЕОРЕМА 1. Квантово-механическая система, имеющая N базисных состояний, представима в виде вектора, включающего $2(N-1)$ параметров $(\theta_{00}, \dots, \theta_{ql}, \dots, t_{00}, \dots, t_{ql}, \dots)$, причем $(\theta_{00}, \dots, \theta_{ql}, \dots)$ определяют амплитудные, а $(t_{00}, \dots, t_{ql}, \dots)$ — фазовые составляющие $|\Psi\rangle$.

ТЕОРЕМА 2. Операция по варьированию состояния квантово-механической системы, имеющей N базисных состояний представлена вектором, включающим $2(N-1)$ параметр $(\Delta\theta_{00}, \dots, \Delta\theta_{ql}, \dots, \Delta t_{00}, \dots, \Delta t_{ql}, \dots)$, при этом $(\theta_{00}, \dots, \theta_{ql}, \dots)$ определяют варьирование амплитудных, а $(t_{00}, \dots, t_{ql}, \dots)$ — варьирование фазовых составляющих $|\Psi\rangle$.

Работа выполнена при финансовой поддержке РФФИ, проект № 03-01-00769.

Список литературы

1. Ablayev F. Comparative power of quantum and classical computation models // Int. Symp. "Quantum informatics – 2004". Oct. 2004, Moscow. — Inst. of Physics and Technology (FTIAN), 2004. — p. 2.

2. Шалагин С. В. К задаче дискретного моделирования квантового регистра // Материалы межд. науч. конф. "Актуальные проблемы математики и механики". — Т. 25. — Казань: Изд-во Казанского матем. общ-ва, 2004. — С. 281–282.

3. Захаров В. М., Нурутдинов Ш. Р., Шалагин С. В. Построение модели умножителя в полях Галуа // Материалы VII межд. сем-ра "Дискр. математика и ее приложения". Ч. I. — М.: Изд-во центра прикл. исследований при мех-мат ф-те МГУ, 2001. — С. 62–65.

ЗАДАЧА ОПТИМАЛЬНОГО УПРАВЛЕНИЯ ДЛЯ ГИПЕРБОЛИЧЕСКИХ СИСТЕМ С ИНТЕГРАЛЬНЫМИ УСЛОВИЯМИ

Я. А. Шарифов (Баку)

Пусть управляемый процесс описывается системой уравнений

$$y_{ts} = f\left(t, s, y, y_z, y_s, u\right), (t,s) \in Q = \{(t,s) : 0 \le t \le T, 0 \le s \le l\}, \quad (1)$$

с интегральными условиями

$$\int_0^\alpha n(t) y(t,s) dt = a(s), s \in [0,l]; \int_0^\beta m(s) y(t,s) ds = b(t),\ t \in [0,T]$$
$$\left(\int_0^\alpha n(t) b(t) dt = \int_0^\beta m(s) a(s) ds\right) \quad (2)$$

Здесь $u(t,x)$ — r-мерная управляющая функция, $y(t,x)$, $y \in R^n$, характеризует состояние процесса в области Q; $n(t)$ и $m(s)$ — матричные функции, и $n(t) \in L_\infty^{n\times n}[0,\alpha]$, $m(s) \in L_\infty^{n\times n}[0,\beta]$, $n(t)m(s) = m(s)n(t)$, $\det \int_0^\alpha n(t)dt \ne 0$, $\det \int_0^\beta m(s)ds \ne 0$; $a(s) \in L_\infty^n[0,l]$, $b(t) \in L_\infty^n[0,T]$.

Предполагается, что функция $f(t,x,y,p,q,u)$ непрерывна по совокупности (t,x,y,p,q,u) своих аргументов с частными производными по y, p, q, u.

Управления $u = u(t,s)$ выбираются из множества

$$u \in U = \{u : u \in L_\infty^r(Q),\ u(t,s) \in V \subset R^r,\ \text{п.в. } (t,s) \in Q\}, \quad (3)$$

где V — заданное ограниченное непустое множество.

Качество управляемого процесса оценивается функционалом

$$J(u) = \Phi\left(y(0,0), y(\tau,l)\right) + \iint_Q F\left(t,s,y,y_t,y_s,u\right) dtds, \quad (4)$$

где Φ, F — заданные скалярные функции.

В работе доказывается существование, единственность и устойчивость решения краевой задачи (1)–(2) и получено необходимое условие оптимальности в виде линеаризованного принципа максимума в оптимальной задаче (1)–(4).

СУПЕР-РЕБЕРНО-МАГИЧНОСТЬ ГРАФОВ

Ю. А. Шатских (Кировоград)

Обыкновенный (p,q)-граф $G=(V,E)$ называют супер-реберно магическим (super edge magic [1], $G\in SEM$), если существует такая нумерация $f: V\cup E\to\{1,2,\ldots,p+q\}$ множества $V\cup E$ его элементов, что $f(V)=\{1,\ldots,p\}$ и сумма $f(u)+f(v)+f(uv)=k=const$ для каждого $uv\in E$. Верно ли, что $G\in SEM$ для заданного графа G?

ТЕОРЕМА 1. Если $G\in SEM$, то $q\leq 2p-3$.

В самом деле, при супер-реберно магической нумерации графа каждому из q ребер соответствует сумма $f(u)+f(v)$, значения сумм не повторяются и берутся из множества $\{3,4,\ldots,2p-1\}$ мощности $2p-3$.

ТЕОРЕМА 2. Если G — r-регулярный граф и $G\in SEM$, то $r\in\{1,2,3\}$.

Для p-вершинного r-регулярного графа $q=pr/2$. Ввиду теоремы 1 имеем $pr/2\leq 2p-3$, откуда следует $r\leq 4-6/p\leq 3$.

ТЕОРЕМА 3. $C_n\in SEM$ тогда и только тогда, когда n нечетно.

ТЕОРЕМА 4. $P_n\in SEM$ (P_n — цепь длиной n звеньев).

ТЕОРЕМА 5. Треугольная призма — супер-реберно магический граф.

Вот две SEM-нумерации треугольной призмы:

1(15)2 1(14)3 1(12)5 2(13)3 2(10)6 3(11)4 4(9)5 4(8)6 5(7)6;

1(15)2 1(14)3 1(11)6 2(13)3 2(12)4 3(10)5 4(9)5 4(8)6 5(7)6.

Двойной звездой $DS(m,n)$ называют дерево порядка $m+n+2$, имеющее центральное ребро, из одного конца которого выходят m концевых ребер, а из другого — n концевых ребер.

ТЕОРЕМА 6. $DS(m,n)\in SEM$.

Супер-реберно магическая нумерация вершин для двойной звезды $DS(m,n)$ осуществляется следующим образом: концевым вершинам, смежным с вершиной x, имеющей в $DS(m,n)$ степень m, присваиваются номера $1,2,\ldots,m$, сама вершина x получает номер $m+2$, противоположный конец центрального ребра получает номер $m+1$, а оставшиеся вершины нумеруются от $m+3$ до $m+n+2$.

Список литературы

1. Figeroa-Centeno R. M., Ichishima R., Muntaner-Batle F. A. On super edge magic graphs // Ars Combinatoria. — 2002. — V. 64. — P. 81–95.

О СЛОЖНОСТИ КОНТРОЛЯ И ДИАГНОСТИКИ "И"("ИЛИ") ЗАМЫКАНИЙ В ФОРМУЛАХ МОНОТОННЫХ БУЛЕВЫХ ФУНКЦИЙ

В. И. Шевченко (Нижний Новгород)

Пусть B — некоторое конечное множество монотонных булевых функций (базис), A_n — формула в базисе B от n переменных. Обозначим через $U(A_n)$ следующее множество формул: а) $A_n\in U(A_n)$; б) пусть $U\in U(A_n)$ и $U^0,U^1,\ldots,U^r$ — некоторая последовательность ее подформул, при этом U^0 не предшествует $U^1,\ldots,U^r$. Тогда формула, которая получается из U подстановкой вместо U^0 формулы $U^0\wedge U^1\wedge\ldots\wedge U^r$, принадлежит $U(A_n)$. Никаких других формул $U(A_n)$ не содержит. Заметим, что $U(A_n)\backslash\{A_n\}$ представляет собой множество возможных "И" замыканий в A_n (для "ИЛИ" замыканий получаем двойственным образом). Пусть $\{f_0,f_1,\ldots,f_m\}$ — множество различных булевых функций, реализуемых формулами из $U(A_n)$. Для $i=0,\ldots,m$ через $\Delta_i(A_n)$ обозначим множество двоичных наборов минимальной мощности, в котором для любого $0\leqslant j\leqslant m$ и $j\neq i$ найдется набор $\tilde\delta\in\Delta_i(A_n)$ такой, что $f_i(\tilde\delta)\neq f_j(\tilde\delta)$. Через $T(A_n)$ обозначим множество двоичных наборов минимальной мощности, в котором для любой пары $0\leqslant i<j\leqslant m$ найдется набор $\tilde\delta\in T(A_n)$ такой, что $f_i(\tilde\delta)\neq f_j(\tilde\delta)$. Через $C(l,k)$ обозначим число возможных сочетаний из l по k.

ТЕОРЕМА 1. Если базис B содержит только конъюнкции и, возможно, константы, или только дизъюнкции и, возможно, константы, то для любой формулы A_n в этом базисе справедливы неравенства $0\leqslant|\Delta_0(A_n)|\leqslant n-1$. В противном случае для $n\geqslant 4$ в базисе B найдется формула A_n такая, что $C(n-2,\lfloor(n-2)/2\rfloor)+C(n-2,\lfloor(n-2)/2\rfloor+1)\leqslant|\Delta_0(A_n)|\leqslant C(n,\lfloor n/2\rfloor)+C(n,\lfloor n/2\rfloor+1)$.

ТЕОРЕМА 2. Если базис B содержит только конъюнкции и, возможно, константы, то для любой формулы A_n в этом базисе справедливы неравенства $0\leqslant|\Delta_0(A_n)|\leqslant|T(A_n)|\leqslant n-1$. В противном случае для $n\geqslant 3$ в базисе B найдется формула A_n и $0\leqslant i_0\leqslant m$ такие, что $C(n-1,\lfloor(n-1)/2\rfloor)+C(n-1,\lfloor(n-1)/2\rfloor+1)\leqslant|\Delta_{i_0}(A_n)|\leqslant|T(A_n)|\leqslant C(n,\lfloor n/2\rfloor)+C(n,\lfloor n/2\rfloor+1)$.

Работа выполнена при финансовой поддержке Программы "Университеты России" (проект УР.04.01.181).

ДООПРЕДЕЛЕНИЕ НЕЧЕТКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С СОХРАНЕНИЕМ ИНФОРМАЦИОННЫХ СВОЙСТВ

Л. А. Шоломов (Москва)

Рассматривается задача максимально возможного доопределения нечетких данных, сохраняющего их информационные свойства.

Пусть $M = \{0,1,\ldots,m-1\}$ и каждому $T \subseteq M$, $T \neq \emptyset$, сопоставлен символ a_T. Алфавит A символов a_T назовем нечетким, его подалфавит $A_0 = \{a_0, a_1, \ldots, a_{m-1}\}$ — четким. Символ $a_{T'}$ четче a_T, если $T' \subseteq T$. Результат замены символа a_T более четким назовем его частичным доопределением. Пусть задан источник S, порождающий символы $a_T \in A$ независимо с вероятностями p_T. Энтропией источника $S = (A, P)$, $P = (p_T, T \subseteq M)$, назовем величину

$$H(S) = \min_{(q_0,\ldots,q_{m-1})} \left(- \sum_{T \subseteq M} p_T \log_2 \sum_{i \in T} q_i \right),$$

где минимум по всем наборам вероятностей $(q_0, \ldots, q_{m-1})$. Она характеризует сжимаемость последовательностей источника S [1].

Скажем, что источник S_2 четче S_1, если он может быть получен из S_1 операцией уточнения [1], состоящей в частичном доопределении некоторых символов. Если S_2 четче S_1, то будем говорить, что источник S_2 (информационно) адекватен S_1 , если для любого источника S выполнено $H(S_2 S) = H(S_1 S)$. Источник назовем приведенным, если не существует адекватного ему более четкого источника. Скажем, что символ $a_i \in A_0$ мажорирует в источнике $S = (A, P)$ символ $a_j \in A_0$, если для любого T из $p_T > 0$ и $j \in T$ следует $i \in T$.

ТЕОРЕМА. Существует единственный с точностью до переобозначения некоторых четких символов приведенный источник, адекватный заданному источнику S. Он может быть получен последовательным исключением из S в любом порядке мажорируемых символов (операция исключения символов описана в [1]).

Работа выполнена при финансовой поддержке ОИТВС РАН по программе фундаментальных исследований.

Список литературы

1. Шоломов Л. А. Кодирование частично определенных дискретных источников без памяти // Доклады Академии наук. — 2004. — Т. 397, № 2. — С. 178–180.

О КОНЕЧНЫХ ПРОСТЫХ n-АРНЫХ МЕДИАЛЬНЫХ КВАЗИГРУППАХ

В. А. Щербаков (Кишинев)

Напомним, что n-арной квазигруппой называется непустое множество Q с n-арной операцией f такой, что в равенстве $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ любые n элементов из множества $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$ однозначно определяют $(n+1)$-й элемент [1].

n-арная квазигруппа (Q, f) с тождеством (тождеством медиальности)

$$\begin{array}{l} f(f(x_{11}, x_{12}, \ldots, x_{1n}), f(x_{21}, x_{22}, \ldots, x_{2n}), \ldots, f(x_{n1}, x_{n2}, \ldots, x_{nn})) = \\ f(f(x_{11}, x_{21}, \ldots, x_{n1}), f(x_{12}, x_{22}, \ldots, x_{n2}), \ldots, f(x_{1n}, x_{2n}, \ldots, x_{nn})) \end{array}$$

называется n-арной медиальной квазигруппой [1].

Элемент d n-арной квазигруппы (Q, f) такой, что $f(d, \ldots, d) = d$, называется идемпотентным элементом этой квазигруппы. Как обычно, $f(x_1^n)$ обозначает $f(x_1, x_2, \ldots, x_n)$.

Эквивалентность θ называется нормальной конгруэнцией n-арной квазигруппы (Q, f), если верны следующие импликации:

$$(a_1 \theta b_1, a_2 \theta b_2, \ldots, a_n \theta b_n) \Longrightarrow f(a_1^n) \theta f(b_1^n),$$

$$f(c_1^{i-1}, a, c_{i+1}^n) \theta f(c_1^{i-1}, b, c_{i+1}^n) \Longrightarrow a \theta b.$$

n-арная квазигруппа (Q, f) называется простой, если ее единственными нормальными конгруэнциями являются диагональная конгруэнция $\hat{Q} = \{(q, q) \,|\, q \in Q\}$ и $Q \times Q$.

Изучаются конечные простые n-арные медиальные квазигруппы. В частности, доказана

ТЕОРЕМА. Конечная простая медиальная n-арная квазигруппа (Q, f) имеет порядок p^n, где p — простое число, и любая такая квазигруппа в случае $|Q| > 1$ принадлежит одному из трех попарно непересекающихся классов квазигрупп: 1) идемпотентные квазигруппы; 2) квазигруппы без идемпотентных элементов; 3) квазигруппы с единственным идемпотентом.

Работа выполнена при финансовой поддержке MRDA и CRDF (проект MM1-3040-CH-02).

Список литературы

1. Белоусов В. Д. n-арные квазигруппы. — Кишинев: Штиинца, 1972.

ИСПОЛЬЗОВАНИЕ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ ДЛЯ БЫСТРОГО ВЫЧИСЛЕНИЯ НЕЛИНЕЙНЫХ СВЕРТОК

М. А. Щербаков (Пенза)

При реализации алгоритмов вычисления нелинейных сверток следует учитывать, что данные могут быть представлены лишь с некоторой ограниченной точностью, определяемой разрядностью n вычислительного устройства. Поэтому без потери общности можно считать, что сигналы принимают значения в некотором конечном поле $GF(p)$ (поле Галуа), состоящем из $p < 2n$ элементов, и определены на конечном множестве $T_N = \{0, 1, ..., N-1\}$ временных отсчетов, являющимся носителем циклической группы H_N. При подходящем выборе значения p, исключающего переполнение разрядной сетки при получении окончательного результата, все вычисления могут выполняться по законам $GF(p)$-арифметики. Для конечных полей целых чисел могут быть определены теоретико-числовые преобразования (ТЧП) [1], обладающие по сравнению с традиционным дискретным преобразованием Фурье (ДПФ) обладают рядом достоинств.

В работе рассматриваются возможности использования ТЧП для вычисления многомерных нелинейных сверток. Для расширения динамического диапазона обрабатываемых последовательностей предлагается схема вычислений, основанная на китайской теореме об остатках [2] и дающая возможность расчленить вычисление нелинейной свертки в поле $\mathbb{Z}_p$ на n аналогичных задач меньшей размерности, решаемых в полях $GF(p_i),\ i = 1, ..., n$. Следует заметить, что отдельные задачи над полями $GF(p_i),\ i = 1, ..., n$, независимы и могут решаться параллельно. В зависимости от выбора значений p_i модулей могут быть построены различные алгоритмы вычисления нелинейных сверток, использующие ТЧП по различным основаниям ε_i. Предложенная схема вычислений позволяет построить эффективные алгоритмы вычисления нелинейных сверток, наиболее пригодные для практической реализации.

Список литературы

1. Макклеллан Дж. Г., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. — М.: Радио и связь, 1983.

2. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток. — М.: Радио и связь, 1985.

О ПРЕДЕЛЬНОЙ ЗАДАЧЕ ДЛЯ ДИСКРЕТНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ СО СЛОЖНЫМ ОТКЛОНЕНИЕМ

Т. К. Юлдашев (Ош)

Рассматривается функционально-разностная система первого порядка со сложным отклонением в нелинейной части

$$\Delta x(n) = A(n)x(n) + \sum_{i=1}^{l} A_i(n)x\left[a_i(n)\right] + F\left(n, x\left[b_j\left(n, x(n)\right)\right]\right),\ n \geq n_0, \tag{1}$$

с предельным условием

$$\lim\left\{x(n) | n \to \infty\right\} = x^{\infty}, \tag{2}$$

где $\Delta x(n) = x(n+1) - x(n)$; $x(n)$ — искомая $(r \times 1)$-мерная векторная функция; $A(n)$, $A_i(n)$ $(i = 0, ..., l)$ — $(r \times r)$-мерные матричные функции, определенные на множестве $I = \{n_0, n_0 + 1, ...\}$; a_i, b_j, $(i = 1, ..., l;\ j = 1, ..., m)$ — целочисленные функции на I, причем $a_i(n) \geq n + 1$, $b_j\left(n, x(n)\right) \geq n + 1$ при $n \in I$;

$$\left\|F(n, x_j^{(1)}) - F(n, x_j^{(2)})\right\| \leq \sum_{j=1}^{m} g_j(n) \left\|x_j^{(1)} - x_j^{(2)}\right\|,$$

где $g_j(n) \geqslant 0$ $(j = 1, ..., m)$; x^{∞} — заданный постоянный $(r \times 1)$-мерный вектор.

ТЕОРЕМА. Пусть выполняются следующие условия:

$$\left\|\sum_{n=n_0}^{\infty} A(n)\right\| < \infty,\ \det\left[E + A(n)\right] \neq 0,\ B(n) = \sum_{s=n}^{\infty} A(s),\ n \geq n_0;$$

$$\left\|b_j(n, x^{(1)}(n)) - b_j(n, x^{(2)}(n))\right\| \leq f(n) \left\|x^{(1)}(n) - x^{(2)}(n)\right\|,\ 0 \leq f_j;$$

$$\sum_{n=n_0}^{\infty} \left\|B(n+1)A(n)\right\| < \infty,\ \left\|\sum_{n=n_0}^{\infty} \left[E + B(n+1)\right] F(n, 0)\right\| < \infty;$$

$$\sum_{n=n_0}^{\infty} \left[\sum_{i=1}^{l} \left\|A_i(n)\right\| + \sum_{j=1}^{m} g_j(n) f_j(n)\right] < \infty.$$

Тогда предельная задача (1)–(2) имеет единственное решение $x(n)$, $n \geq n_0$. Любое решение системы (1) устойчиво относительно предельного данного (2).

ИНТЕРПОЛЯЦИЯ LINSPACE-КОНСТРУКТИВНЫХ ФУНКЦИЙ

С. В. Яхонтов (Санкт-Петербург)

Рассматривается вычислительная сложность линейной интерполяции (см. [1]) LINSPACE-конструктивных вещественных функций, заданных на $[a,b] \subseteq \mathrm{LINSPACE}_{CF}$ (см. [2]).

ОПРЕДЕЛЕНИЕ. Последовательность интерполяционных многочленов $L_n(x) = \sum_{j=1}^{n} a_j P_j(x)$ называется LINSPACE-вычислимой на интервале $[a,b]$, если существует машина Тьюринга M с оракулом такая, что для любого натурального q, любого $x \in [a,b]$ и любой функции $\phi \in CF_x$, машина M^ϕ вычисляет такие натуральное n и значение $L_n(x) \in D_n$, что $|f(x) - L_n(x)| \le 2^{-q}$, используя при этом Cq ячеек промежуточной памяти.

Данное определение аналогично определению полиномиально вычислимой последовательности вещественных функций (см. [3]). Интерполяционный многочлен функции $f \in C[a,b]$ с узлами в нулях многочленов Чебышева записывается в виде (см. [1]):

$$L_n(x) = \sum_{j=0}^{n-1} a_j \tilde{T}_j(x), \quad a_j = \frac{2}{n} \sum_{k=1}^{n} f(p_j)\tilde{T}_j(p_k). \qquad (1)$$

Обозначим $\|f\| = \max_{[a,b]} |f(x)|$. Основным результатом является

ТЕОРЕМА. Если $\|f\| \le C_1$, $\log \|f^n\| \le C_2 n$ для всех $n > 0$, то последовательность интерполяционных многочленов $\{L_n\}$, построенных по схеме (1), является LINSPACE-вычислимой на $[a,b]$.

Список литературы

1. Бахвалов Н. С., Жидков Н. П., Кобельков Г. М. Численные методы. — БИНОМ. Лаборатория знаний, 2004.

2. Яхонтов С. В. LINSPACE-конструктивность алгебраических чисел // Труды V Международной конференции "Дискретные модели в теории управляющих систем" (Ратмино, 26–29 мая 2003 г.). — М.: Издательский отдел факультета ВМиК МГУ имени М. В. Ломоносова, 2003.

3. Ко К. Complexity theory of real functions. — Birkhauser, 1991.

С О Д Е Р Ж А Н И Е