

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ
ИНСТИТУТ МАТЕМАТИКИ им. С.Л. СОБОЛЕВА СО РАН

МАТЕРИАЛЫ

XV Международной
школы-семинара
«СИНТЕЗ И СЛОЖНОСТЬ
УПРАВЛЯЮЩИХ СИСТЕМ»
(Новосибирск, 18-23 октября 2004 г.)

Издательство Института математики,
Новосибирск • 2004

УДК 519.7



*Издание осуществлено при поддержке
Российского фонда фундаментальных
исследований по проекту 04 01-10076.*

Материалы XV Международной школы-семинара «Синтез и сложность управляющих систем» (Новосибирск, 18-23 октября 2004 г.) / Под ред. О. Б. Лупанова. Новосибирск: Изд-во Института математики, 2004 г. 118 с.

Сборник содержит материалы XV Международной школы-семинара «Синтез и сложность управляющих систем», проходившей в Новосибирске с: 18 октября по 23 октября 2004 г. при поддержке Российского фонда фундаментальных исследований (проект 04-01-10076). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

Материалы

XV Международной школы семинара

СИНТЕЗ И СЛОЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ

(Новосибирск, 18-23 октября 2004 г.)

под общей редакцией академика РАН О. Б. Лупанова.

Редактор А. Д. Коршунов

Компьютерная верстка Г. В. Шевченко

И/К

Подписано в печать 23.11.04. Формат 60 x 90 1/16. Печать офсетная.

Печ. л. 9,4. Тираж 125 экз. Заказ №90.

Издательство Института математики, пр. Академика Коптюга, 4.

630090 Новосибирск, Россия. Отпечатано в ООО «Омега Принт»,

пр. Лаврентьева, 6, 630090 Новосибирск, Россия.

© коллектив авторов, 2004

СОДЕРЖАНИЕ

М. Алексеев, Д. Барский, А. Воробей, Г. Мерзон, Ю. Прокопчук, Д. Фон-Дер-Флаасс. Об одной задаче последовательного декодирования	5
А. А. Ботев. Об алгебраической иммунности одной рекурсивно заданной последовательности корреляционно-иммунных функций	8
С. Е. Бубнов. О задачах тестирования неповторных булевых функций	12
Ю. Л. Васильев. Комбинаторная двумерность пространства Бэра	16
А. Ю. Васильева. О восстановлении центрированных функций	21
С. Ф. Винокуров. Специальная операторная форма булевых функций и некоторые ее приложения	26
Н. В. Евтушенко, С. В. Жарикова, М. В. Ветрова. Оптимизация декомпозиций конечных автоматов на основе решения автоматных уравнений	29
Г. П. Егорычев, Е. В. Зима. Характеристическая функция в проблеме $3x+1$ I	34
Р. Н. Забалуев. О средней сложности вычислений монотонных булевых функций	40
Р. М. Колпаков. Полиномиальный алгоритм проверки порождаемости конечных распределений рациональных вероятностей	45
Н. К. Косовский. Полнота системы булевых функций на примере отличается от NP-полноты задачи выполнимости их суперпозиций, если $P \neq NP$	50
Ю. В. Мерекин. О сложности полукоммутативных слов	54
Е. А. Михеева. О свособразии конечнозначных логик	55
Е. А. Окольнішнікова. О некоторых комбинаторных задачах, возникающих в теории сложности	57

И. А. Панкратова. Анализ состязаний в переключательных комбинационных схемах	61
Н. Г. Парватов. О функциональной полноте в классе квазимонотонных функций на конечной полурешетке	65
В. Н. Потапов. Об алгоритмическом подходе к понятию сложности символической последовательности	67
А. В. Пролубников, Г. С. Ржаницын. Использование алгоритма проверки изоморфизма графов для осуществления безопасной передачи видеoinформации по общедоступному каналу связи	71
Н. П. Редькин. О сложности реализации булевых функций с малым числом единиц	76
А. М. Романов. О разбиениях q -ичных кодов Хемминга на непересекающиеся компоненты	80
О. Б. Седелев. О сложности реализации булевых функций схемами из функциональных элементов, вложенными в булев куб ...	84
А. А. Семенов. О специфике обращения полиномиально вычислимых перестановок	88
Ф. И. Соловьева. О группах автоморфизмов совершенных двоичных кодов	92
В. А. Стеценко. Сравнение базисов в R_k	96
Н. Е. Тимошевская. Параллельные вычисления в решении систем логических уравнений методом линеаризации	97
Е. Б. Титова. Базис правого модуля несимметричных многоиндексных транспортных задач	102
Т. И. Федоряева. Графы, имеющие продолжение кратчайших цепей ..	105
А. Э. Фрид. Арифметическая сложность бесконечных слов	110
Л. А. Шоломов. Энтропийные свойства частично определенной информации	114

ОБ ОДНОЙ ЗАДАЧЕ ПОСЛЕДОВАТЕЛЬНОГО ДЕКОДИРОВАНИЯ

М. Алексеев (США), **Д. Барский** (Англия),

А. Воробей (Израиль), **Г. Мерзон** (Москва),

Ю. Прокопчук (Минск), **Д. Фон-Дер-Флаасс** (Новосибирск)

На математической олимпиаде «Турнир Городов» в 2004 г. была предложена такая задача.

«Перед экстрасенсом кладут колоду из 36 карт рубашкой вверх. Он называет масть верхней карты, после чего карту открывают, показывают ему и откладывают в сторону. После этого экстрасенс называет масть следующей карты, и т. д. Рубашки карт несимметричны, и экстрасенс видит, в каком из двух положений лежит верхняя карта. Колоду готовит подкупленный служащий — он знает порядок карт в колоде и хотя не может его изменить, но волен выбирать положение рубашек карт. Как надо сговориться экстрасенсу и служащему, чтобы экстрасенс смог гарантированно угадать как можно больше мастей?»

Задача естественно обобщается на случай произвольного числа b мастей, n карт в колоде, a различных пометок, $a < b$, которые служащий может оставить на рубашках карт, и произвольного множества L разрешенных последовательностей мастей. Чему равно $m_{a,b}(n, L)$ — наименьшее число ошибок, которое экстрасенс с гарантией может не превзойти?

Мы дадим верхнюю и нижнюю оценки для $m_{a,b}(n, L)$, которые асимптотически совпадают, если $|L| = b^{n-o(n)}$, $n \rightarrow \infty$.

Определим функцию

$$s_p(n, k) = \sum_{i=0}^k \binom{n}{i} p^i$$

— частичную сумму биномиального ряда.

Теорема 1. (а) Если $s_{b-1}(p, k) \geq (b/a)^p$, то существует такая константа c , зависящая от a, b, p , что для любого натурального t и для любого r , $1 \leq r \leq n$, выполняется неравенство $m_{a,b}(c + pt + r, L) \leq c + kt$ (при любом множестве разрешенных последовательностей длины $c + pt + r$).

(б) Если $|L| = N$ и $s_{b-1}(n, k) < N/a^n$, то $m_{a,b}(n) > k$.

Оценки из теоремы 1 асимптотически совпадают, если $N = |L| = b^{n-o(n)}$ при $n \rightarrow \infty$ (например, в случае, когда все b^n последовательностей разрешены, или в случае, когда каждая масть должна встретиться одно и то же число раз, как в исходной задаче).

Теорема 2. *Если число разрешенных последовательностей длины n равно $b^{n-o(n)}$, то существует предел*

$$\alpha(a, b) = \lim_{n \rightarrow \infty} \frac{m_{a,b}(n, L)}{n}$$

и этот предел является корнем уравнения

$$(b-1)^x = \frac{b}{a} x^x (1-x)^{1-x}.$$

Доказательство теоремы 1. Мы будем измерять количество информации, которой экстрасенс обладает в каждый момент, не в битах, а в более точных единицах — N -итах. Один N -ит обозначает знание, какая из N заранее заданных возможностей выполнена. Например, 2-ит — это один бит; 1-ит — это полное отсутствие информации.

(а) Пусть заданы a, b и p , где $1 < a < b$. Положим $c = \lceil p \cdot \log_a b \rceil$. Пусть $n = c + pm + r$, $1 \leq r \leq p$, и пусть k удовлетворяет требуемому неравенству. Опишем алгоритм, с помощью которого экстрасенс (Э) может угадать масти всех, кроме не более чем $c + pk$ карт, независимо от того, каково множество разрешенных последовательностей. Вначале Э запоминает пометки на первых c картах, называя при этом масти наугад. Это дает не более c ошибок и один a^c -ит информации. Ввиду выбора c мы имеем $a^c \geq b^p$; поэтому полученной информации достаточно, чтобы закодировать любую последовательность из p мастей.

Перед началом каждой из следующих m стадий у Э будет достаточно информации, чтобы определить его следующие p ответов. Служащий задает их так, чтобы не более k из них были неверными. Таким образом, в течение этих p шагов Э сделает не более k ошибок. В то же время он собирает один a^p -ит информации из пометок на картах и $s_{b-1}(p, k)$ -ит информации из положений, в которых произошли ошибки, и разностей между ошибочно названной мастью и ее истинным значением. (Масти можно считать занумерованными от 0 до $b-1$; разности вычисляются по модулю b .) Таким образом, к концу каждой стадии Э имеет один $a^p s_{b-1}(p, k)$ -ит информации. Ввиду выбора

k выполняется неравенство $a^p s_{b-1}(p, k) \geq b^p$; таким образом, процесс может быть продолжен. В заключение Э верно угадывает последние r мастей, используя информацию, полученную на последней, m -й стадии. Утверждение (а) доказано.

Для доказательства нижней оценки (б) нам потребуется простая лемма из теории графов.

Лемма 1. Пусть T — корневое дерево, дуги которого (ориентированные в направлении от корня) окрашены в черный и белый цвета так, что выполняются следующие условия:

(i) T имеет высоту n , т.е. расстояние от корня до каждого листа равно n .

(ii) Из каждой вершины выходит не более p черных и не более q белых дуг.

(iii) Каждый простой путь от корня к листу содержит не более k белых дуг.

Тогда число листьев в T не превосходит $p^n \cdot s_{q/p}(n, k)$.

Доказательство. Зафиксируем p и q . Назовем (n, k) -деревом любое дерево, удовлетворяющее условиям леммы. Пусть $m(n, k)$ — наибольшее число листьев в (n, k) -дереве. Выполняются очевидные равенства

$$m(n, 0) = p^n = p^n \cdot s_{q/p}(n, 0) \text{ (белых дуг вообще нет) и}$$

$m(n, n) = (p + q)^n = p^n \cdot s_{q/p}(n, n)$ (ограничений на цвет дуг нет; из каждой внутренней вершины может выходить $p + q$ дуг).

При $0 < k < n$ любое (n, k) -дерево состоит из корня, к которому черными дугами присоединены $(n-1, k)$ -деревья и белыми дугами присоединены $(n-1, k-1)$ -деревья. Таким образом, мы получаем рекуррентную формулу $m(n, k) = pm(n-1, k) + qm(n-1, k-1)$, из которой заключение леммы нетрудно доказать по индукции.

Докажем нижнюю оценку теоремы. Пусть служитель и экстрасенс выбрали стратегию, гарантирующую не более k ошибок. Во-первых, это означает, что для каждой из N возможных последовательностей мастей служитель однозначно определяет последовательность пометок. Каждую такую помеченную последовательность мы рассматриваем как слово длины n над алфавитом размера ab , буквами которого являются пары (s, l) из масти s и пометки l . Определим корневое дерево, вершинами которого являются все начальные сегменты длин от 0 до n всех N слов, а дуги соответствуют добавлению к сегменту сле-

дующего символа.

Для каждого начального сегмента длины менее n и каждого возможного значения метки на следующей карте выбранная стратегия определяет, какую масть назовет экстрасенс. Покрасим черным цветом те дуги, которые соответствуют правильному ответу, и белым цветом — соответствующие ошибке. Легко видеть, что из каждой вершины выходит не более a черных и не более $a(b-1)$ белых дуг. Высота дерева равна n , оно имеет N листьев, а каждый путь от корня к листу содержит не более k белых дуг. Применяя лемму со значениями $p = a$, $q = a(b-1)$, получаем требуемое неравенство. Оценка (b) доказана.

Для первоначальной задачи с 36 картами, авторам известен алгоритм, гарантирующий не более 10 ошибок. В этом случае теорема 1 дает нижнюю оценку в 6 ошибок. Точный ответ остается неизвестным.

Авторы выражают благодарность интернет-проекту LiveJournal (www.livejournal.com), который оказался идеальным средством для организации совместной работы над задачей. Авторы благодарят пользователей *a_konst* и *mi_b* за ценные обсуждения и все сообщество пользователей LiveJournal за постоянный интерес к процессу их работы.

ОБ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ ОДНОЙ РЕКУРСИВНО ЗАДАННОЙ ПОСЛЕДОВАТЕЛЬНОСТИ КОРРЕЛЯЦИОННО-ИММУННЫХ ФУНКЦИЙ

А. А. Ботев (Москва)

В докладе исследуются булевы функции с точки зрения их применимости в качестве так называемых комбинирующих функций в потоковых шифраторах.

Потоковый шифратор — это распространенный криптографический инструмент, применяющийся для шифрования сообщений. Он состоит из линейной части, порождающей последовательность с большим периодом, и нелинейной комбинирующей функции f , которая порождает выходную последовательность по данным линейным входам. Среди атак, которые может предпринять злоумышленник для того, чтоб узнать начальные значения ячеек памяти потокового шифратора и в дальнейшем читать все сообщения, наиболее распространены